eCH-0014 SAGA.ch

Nom	SAGA.ch
eCH- nombre	eCH-0014
Catégorie	Norme
Stade	implémenté
Version	8.0
Statut	Approuvé
Date de décision	2017-09-06
Date de publication	2017-10-23
Remplacé version	V7.0 Major Change
Condition préalable	-
Annexes	-
Langues	Allemand (original), Français (traduction)
Auteurs	Groupe spécialisé Technologie Josef Schmid, direction du GS, Sopra Steria AG Sue Paredi, Microsoft Schweiz GmbH Daniel Muster Hans-Rudolf Thomann Elmar Hayoz Erich Vogt Daniel Gabi, Chancellerie fédérale de la Suisse Leo Lehmann, OFCOM Eric Dubuis, Haute école spécialisée bernoise Benjamin Barras, EPFL, Stefan Wyss eHealth Suisse Thomas Teske, Oracle Software (Suisse) GmbH Norbert Bollow, Swiss Open Systems User Group /ch/open Alexandre De Spindler, Zürcher Fachhochschule André Amport, DFJP, Marcel Matter VBS FuB Gregoire Hernan, Conférence suisse sur l'informatique (CSI)
Éditeur / Distribution	Verein eCH, Mainaustrasse 30, Postfach, 8034 Zürich T 044 388 74 64, F 044 388 71 80 www.ech.ch / info@ech.ch

Condensé

Le présent document SAGA.ch (Standards und Architekturen für eGovernment-Anwendungen Schweiz, Normes et architectures pour les applications de cyberadministration en Suisse) présente sous forme condensée les directives techniques à respecter pour la réalisation d'applications de cyberadministration en Suisse. Il décrit des normes souvent utilisées pour le développement de systèmes de cyberadministration. De telles normes favorisent la réalisation de solutions à un coût avantageux. En effet, les systèmes de cyberadministration ne doivent pas être développés à partir de zéro, puisque l'on peut ainsi faire appel, lors de leur conception, à des composantes de base qui ont déjà fait leurs preuves dans l'industrie des TIC (technologies de l'information et de la communication). On évite ainsi les doublons et les solutions isolées au sein de l'administration. En outre, la normalisation devrait permettre de maintenir les frais d'ingénierie au niveau le plus bas possible.

SAGA.ch doit être compris comme une base de normalisation réalisée selon une approche globale, expliquant les principaux aspects requis pour atteindre les objectifs mentionnés ci-dessus. Ce document s'adresse en priorité aux décideurs de l'administration œuvrant dans les domaines de l'organisation et des techniques d'information (équipes de cyberadministration).

SAGA.ch a été conçu en référence aux documents SAGA.de, versions 1.1 à 5.0, réalisé en Allemagne par l'administration (voir ci-dessous). On consultera également les normes françaises[1], britanniques[2] et mondiales pertinentes (dont SAGA Inde, e-Gif Nouvelle-Zélande, EIF).

Remarque

Référence à la série de documents du KBSt; avec l'autorisation spéciale du KBSt allemand

Ce projet de norme a été réalisé par le groupe spécialisé «Technologie» de eCH, en référence à SAGA.de (réalisé en Allemagne par le KBSt, un office du Ministère fédéral de l'intérieur, en collaboration avec le Bundesamt pour Sécurité in der Informationstechnik, BSI).

Rédaction: groupe spécialisé Technologie de **eCH**

Interlocuteur: Administration ***eCH***

E-mail: info@ech.ch

Site internet et téléchargement de la version informatique: www.eCH.ch

[1] Le cadre commun d´interopérabilité des systèmes d'information publics

[2] eGIF eGovernment Interoperability Framework

Sommaire

1 Introduction

1.1 Statut

Approuvé: le document a été approuvé par le Comité des experts et a force normative pour le domaine d'application défini dans la sphère de validité stipulée.

1.2 Remarque préliminaire

Ce document présente, sous forme condensée, des normes techniques déjà largement appliquées pour le développement de systèmes de cyberadministration[3], mais non pas les déroulements, processus, méthodes et produits s'y rapportant.

Nous savons par expérience que les experts de ce domaine utilisent de nombreuses abréviations et acronymes anglais. Certaines de ces appellations sont protégées par le droit d'auteur, ou déposées comme marques ou noms de produit par différents fabricants ou organes de normalisation, sur les plans national et international. Dans un souci de simplification, nous avons renoncé de manière générale à faire référence aux droits d'auteur et aux sources. Les «appellations» ou abréviations mentionnées dans ce document ne sont donc pas nécessairement exemptes de droits d'auteur ni utilisables librement.

En outre, l'éditeur, les auteurs et les experts consultés déclinent toute responsabilité en ce qui concerne le bon fonctionnement technique, la compatibilité ou l'exhaustivité des normes présentées. Le lecteur adressera de préférence ses commentaires et ses propositions de compléments ou de corrections à l'interlocuteur officiel mentionné à la page 2.

Les numéros de version sont indiqués lorsqu'ils sont importants dans le contexte. Ils sont aussi indiqués implicitement par le numéro de la norme concernée; l'absence d'indication explicite n'est toutefois pas une garantie de conformité. Lorsqu'une norme est mentionnée sans numéro de version, nous nous appuyons sur la version la plus stable du point de vue commercial, laquelle n'est pas toujours la plus récente. A partir de la version 2.1 de SAGA.ch, les versions des différentes normes ont été prises en compte et indiquées pour toutes les technologies mentionnées.

Dans la mesure du possible, nous utilisons une terminologie neutre en termes de genre. Pour simplifier la formulation, nous nous limitons parfois à la forme masculine, mais les deux genres sont toujours concernés.

1.3 Contexte

En publiant sa stratégie de cyberadministration de la Confédération, le 13 février 2002, le Conseil fédéral a défini des axes stratégiques d'après lesquels peut s'orienter en premier lieu l'administration fédérale, mais aussi les cantons et les communes. Dans ce document, il en-

[3] Aide aux relations, aux processus et à la participation politique à tous les échelons de l'Etat ainsi qu'envers tous les groupes d'utilisateurs par la mise à disposition de fonctions interactives sur médias électroniques.

gage l'administration fédérale à fournir aussi vite que possible sur l'internet ses prestations susceptibles de l'être.

1.4 Utilisation des normes

La mise à disposition de prestations électroniques par l'administration ne suffit pas à elle seule. Les systèmes des autorités fédérales, cantonales et communales doivent aussi assurer leur interopérabilité non seulement entre eux, mais aussi avec les systèmes correspondants dans les entreprises. Cela ne peut être réalisé qu'à l'aide de normes techniques, entre autres pour les raisons suivantes.

- La normalisation favorise la réalisation de solutions à des coûts plus avantageux. En effet, les systèmes ne doivent pas être développés à partir de zéro, car leurs concepteurs peuvent faire appel à des composantes de base ayant fait leurs preuves dans l'industrie TIC. On évite ainsi les développements à double, et aussi les solutions isolées, au sein de l'administration. De plus, les frais d'ingénierie devraient pouvoir être maintenus au niveau le plus bas possible.
- Seule l'adoption de normes crée la condition préalable pour une interopérabilité au niveau national et pour les avantages que l'on cherche à obtenir par l'introduction de la communication électronique.
- Les solutions incompatibles génèrent non seulement des coûts d'investissement, mais encore des charges d'exploitation (inutiles) dues à une acquisition supplémentaire et à de nouveaux travaux de réalisation technique. Les normes permettent de réaliser des économies en conséquence.
- L'optimisation structurelle (modularité), optimisée au niveau des coûts, des solutions existantes n'est possible que si l'on convient d'utiliser des normes.
- L'utilisation de normes permet de changer plus facilement de prestataire et fait ainsi obstacle à la création de monopoles.

Conclusion: les normes favorisent l'extensibilité, la flexibilité et l'interopérabilité des solutions nouvelles et anciennes.

1.5 Public visé

SAGA.ch s'adresse en priorité aux décideurs de l'administration œuvrant dans les domaines de l'organisation et des techniques de l'information (équipes de cyberadministration). Le présent document les aide à s'orienter quand ils conçoivent des architectures et des applications techniques dans le domaine de la cyberadministration.

SAGA.ch s'adresse toutefois aussi aux gestionnaires de produits et aux développeurs de systèmes de cyberadministration dans l'industrie des technologies de l'information et de la communication (TIC). Cette dernière est invitée à participer à la discussion et à la définition des normes ***eCH***, et à proposer des solutions ou des alternatives si les normes présentées ne suffisent pas pour la mise en œuvre technique.

1.6 Objectif et structure du document

1.6.1 Principes de base

La cyberadministration moderne requiert des systèmes d'information, de communication et de transaction interopérables, c'est-à-dire pouvant (dans le cas idéal) fonctionner entre eux sans aucun problème. Des normes et des spécifications simples et claires permettent

d'optimiser, voire de réaliser l'interopérabilité de ces systèmes. SAGA.ch identifie les normes, formats et spécifications nécessaires, définit les règles de conformité s'y rapportant et les adapte au fil de l'évolution technologique.

1.6.2 Objectifs

SAGA.ch poursuit les objectifs suivants:

- Il définit les formats et protocoles sur lesquels se base la technologie concernée et qui permettent de réaliser électroniquement l'échange d'informations et le déroulement de transactions au sein de l'administration ainsi qu'entre les autorités et les citoyens, les entreprises et les organisations.
- Les normes prescrites, qui sont essentiellement d'ordre technique, définissent une architecture de base stable et fiable, sur laquelle doivent s'appuyer les solutions de cyberadministration développées en Suisse.
- SAGA.ch se fonde autant que possible sur des normes internationales, disponibles sur le marché et ayant déjà fait leurs preuves.
- Les développeurs de composantes locales doivent rester aussi libres que possible dans le choix de la technologie de leurs solutions.
- SAGA.ch peut être utilisé comme partie de la spécification des exigences dans les appels d'offres des pouvoirs publics pour les projets de cyberadministration.

Le présent document mentionne essentiellement les normes relatives à la technologie de l'information, mais non pas celles concernant l'organisation ou le déroulement de projets (informatiques). Toute référence à l'organisation et au processus n'y est faite que pour placer les explications techniques dans un contexte qui en facilite la compréhension.

1.6.3 Etendue

SAGA.ch doit être considéré comme une base de normalisation réalisée selon une approche globale, qui explique les aspects les plus importants à respecter pour atteindre les objectifs fixés. Les normes ou architectures non mentionnées ne le sont pas pour l'une ou l'autre des raisons suivantes

- elles ne sont ni pertinentes ni utiles pour les applications de cyberadministration,
- elles sont comprises ou référencées dans des normes citées,
- elles sont trop nouvelles ou trop contestées, de sorte que leur acceptation générale par le marché ne peut pas être espérée dans un délai proche.

En outre, SAGA.ch ne prend pas en considération tous les éléments d'une architecture technique, mais seulement les domaines ayant une influence importante sur les objectifs visés. Ce document contient des descriptions de normes essentiellement dans les deux parties suivantes:

- Le chapitre 4 décrit dans les grandes lignes un modèle d'interface et d'architecte
- Les chapitres 5 à 7 décrivent les normes relatives à ce modèle d'interface

Si certaines technologies sont décrites plus en détail que d'autres dans ce document, cela ne signifie pas qu'elles sont plus importantes.

1.7 Services à représenter

Les services offerts par l'administration peuvent s'adresser aux quatre groupes cibles ci-après:

- **Particuliers** (G2C Government to Citizen)
- **Entreprises** (G2B Government to Business)
- **Organisations** (G2O Government to Organisations), ex. organisations non gouvernementales (NGO)
- **Autorités** (G2G Government to Government)

De nombreuses prestations offertes par l'administration fédérale, cantonale ou communale sont connues. A cet égard, on distingue d'ordinaire entre les types de services suivants:

- **Services d'information.** Informations des autorités aux utilisateurs, le flux étant unilatéral
- **Services de communication.** Echange entre les autorités et les utilisateurs ainsi qu'entre les utilisateurs eux-mêmes, le flux d'information étant bilatéral
- **Services de transaction.** Déroulement de processus d'affaires entre les autorités et les utilisateurs.

2 L'évolution de SAGA.ch

2.1 Tâche

SAGA.ch est une base de normalisation globale établie par le groupe spécialisé Technologie de ***eCH*** pour recommander les normes de la technologie de l'information et communication (TIC) (aussi les architectures, mais seulement dans les grandes lignes) à utiliser dans les projets de cyberadministration.

2.2 Origine

Le contenu de SAGA.ch se fonde sur les expériences d'autres pays, notamment l'Allemagne, la France, l'Angleterre, l'Inde et la Nouvelle-Zélande, ainsi que sur les expériences et connaissances personnelles des membres experts du groupe spécialisé. A intervalles réguliers, SAGA.ch est complété, actualisé, adapté aux évolutions les plus récentes et publié à l'adresse www.eCH.ch.

2.3 Prises de position et commentaires

Qu'elles travaillent dans l'administration, la recherche ou l'industrie, toutes les personnes intéressées sont priées de commenter le contenu du présent document. Elles peuvent transmettre directement à l'interlocuteur officiel (voir page 2) leurs commentaires et remarques, qui seront ensuite évalués dans le groupe spécialisé puis, s'ils sont jugés judicieux, pris en compte dans la mesure des possibilités.

3 Application de SAGA

3.1 Classifications des normes

eCH subdivise les normes en quatre classes en leur attribuant les statuts:

- Vivement recommandé
- Recommandé
- En observation
- Non recommandé

Vivement recommandé

Sont déclarées «vivement recommandées» les normes qui ont fait leurs preuves du point de vue de ***eCH*** et qui représentent la solution préférée. Elles doivent être prises en compte et appliquées en priorité. Des normes concurrentes peuvent être recommandées parallèlement lorsqu'elles se distinguent sensiblement quant à leurs fonctionnalités ou leurs priorités d'application. On utilisera alors la norme la mieux appropriée pour l'application concernée.

Lorsqu'elles existent parallèlement à des normes vivement recommandées, les normes recommandées ou en observation ne doivent être appliquées que dans des cas exceptionnels justifiés.

Recommandé

Sont déclarées «recommandées» les normes qui ont fait leurs preuves, mais qui soit ne sont pas impérativement nécessaires, soit qu'elles ne représentent pas la solution préférée, soit qu'elles doivent encore être affinées pour être déclarées «vivement recommandées». Si aucune norme concurrente «vivement recommandée» n'existe parallèlement, on ne s'écartera des normes «recommandées» que dans des cas exceptionnels justifiés.

Des normes concurrentes peuvent être recommandées parallèlement lorsqu'elles se distinguent sensiblement quant à leurs fonctionnalités ou leurs priorités d'application. On appliquera alors la norme la mieux appropriée pour l'application concernée.

Lorsqu'elles existent parallèlement à des normes recommandées, les normes en observation ne seront utilisées que dans des cas exceptionnels justifiés.

En observation

Sont déclarées «en observation» les normes qui vont dans le sens de développement désiré, mais qui ne sont pas encore arrivées à maturité ou qui n'ont pas encore suffisamment fait leurs preuves sur le marché.

En l'absence de normes concurrentes vivement recommandées ou recommandées, les normes «en observation» peuvent servir de base d'orientation.

Non recommandé

Sont explicitement déclarées «non recommandée» des normes obsolètes qui avaient été recommandées dans des versions antérieures de SAGA ou dont l'utilisation peut entraîner, pour d'autres raisons, des problèmes d'interopérabilité.

Le choix des recommandations à utiliser pour les différentes technologies se fonde essentiellement sur les critères suivants:

- acceptation générale, ce qui rend l'implémentation plus économique,
- technologie souvent utilisée,
- définition d'après SAGA.de et d'autres recommandations du domaine de la cyberadministration.
- sécurité

Les raisons pour lesquelles certaines recommandations ont été préférées à d'autres pour des normes déterminées ne sont en règle générale pas exposées dans le présent document.

3.2 Directives

Concernant les directives, les recommandations de SAGA doivent être interprétées comme suit:

- vivement recommandé signifie «MUST»
- Recommandé signifie «SHOULD»
- en observation signifie «en observation»
- Non recommandé signifie «MUST NOT»

Ceci sur le modèle des normes IETF pour les technologies Internet et les protocoles.

3.3 Application de SAGA dans les appels d'offres

Les recommandations de SAGA peuvent être mises en œuvre selon quatre niveaux différents en termes de qualité:

3.3.1 Déclaration d'application SAGA (dans l'appel d'offres)

Le donneur d'ordre intègre aux documents relatifs à l'appel d'offres (WTO) d'un système informatique le renvoi vers SAGA.ch. Il choisit dans quelle ampleur il veut évaluer la mise en œuvre des recommandations de SAGA.ch: s'il décide qu'il s'agit d'un critère impératif resp. critère d'aptitude, un mandataire, s'il veut parvenir à la phase de sélection, doit confirmer qu'il est disposé et apte à mettre en place le système à créer conformément aux recommandations SAGA. Le donneur d'ordre a également la possibilité de récompenser par des points supplémentaires dans l'évaluation, l'intention du mandataire de mettre en œuvre les recommandations SAGA. L'ampleur dans laquelle le logiciel terminé est au final conforme à SAGA – c.à.d. interopérabilité, etc – reste encore à définir.

Vivement recommandé

3.3.2 Clause de conformité SAGA (pour la réception)

Après l'exécution des travaux, le mandataire établit une déclaration de conformité SAGA, parce qu'il a fait de la garantie du respect des exigences de SAGA une partie intégrante de son offre. Cette déclaration fait l'objet d'un contrôle avec l'offre initiale du donneur d'ordre. Un contrôle réussi est une condition préalable à la réception technique du système informatique TIC. Afin que le résultat puisse être mesuré, il faut toutefois que des indications pré-

cises soit faites à certains endroits dans le cahier des charges, comme dans SAGA. Par exemple concernant les versions exigées des normes, le degré de compatibilité des sites Internet pour les personnes handicapées ainsi que leur compatibilité avec les navigateurs ou la qualité du code de programme (v. entre autres OWASP-Top-10 https://www.owasp.org/index.php/Top_10_2010-Main)

[semblable: «Concept pour SAGA 5.0», décidé par le Conseil des responsables IT le 05.06.2009; version 1.1, chap. 3.7]

	Vivement recommandé

3.4 Procédure en cas d'incompatibilités SAGA

Les fournisseurs d'une application de cyberadministration devraient disposer d'une gestion professionnelle des services IT selon la norme ISO/IEC 20000. Les exigences minimales requises pour les processus, qu'une organisation doit établir pour pouvoir fournir et gérer les services IT dans la qualité définie, sont spécifiées et représentées à cette fin. La norme ISO/IEC 20000 est axée sur les descriptions de processus, telles décrites par l'IT Infrastructure Library (ITIL) de l'Office of Government Commerce (OGC), et les complètent. La bibliothèque ITIL répartit les exigences pour les processus et la gestion entre la stratégie, le design, la mise en œuvre, l'exploitation et l'amélioration.

Un incident («Incident», ex. un résultat de test ou d'audit imprévu, inattendu, l'expiration d'un délai, une décision concernant une fonctionnalité ou son budget etc.), qui affecte les règles et directives stipulées dans le contrat de prestation de service ou le règlement interne, concernant la fonctionnalité, le taux d'utilité et la disponibilité, l'interopérabilité, la confidentialité et la sécurité d'une application ou d'une interface, doit être constaté et transmis selon l'organisation interne ou contractuelle et les procédures prévues. En règle générale, la suite du déroulement du traitement et la prise des mesures dépendent de l'ampleur des répercussions d'un tel «incident». Les procédures décrites dans les normes sont valides pour tous les incidents, pas seulement pour les incompatibilités SAGA.

ISO/IEC 20000	Vivement recommandé

Normes: www.snv.ch, www.ISO.org, www.IEC.org

ITIL V.3/4	Vivement recommandé

Normes: www.itil.org

4 Limites du système et interfaces

4.1 Composants

Du point de vue de l'utilisateur, il est judicieux de subdiviser les applications de cyberadministration d'après les groupes cibles (particuliers, entreprises, organisations, autorités). D'un point de vue technique, une subdivision d'après les composantes suivantes est plus adéquate:

- terminal
- système
- centre de clearing

Un **terminal** permet à une personne d'accéder à un système. Exemples de terminaux: ordinateur personnel (PC), ordinateur de poche (PDA) et un téléphone portable (mobile) et appareils portables à venir. .

Un **système** est une application de cyberadministration.

Un **centre de clearing** est un service d'intermédiaire (de courtage) qui relie deux ou plusieurs systèmes afin de transmettre et relayer des messages électroniques (par exemple des documents XML), de surveiller et coordonner des modifications de données et de protéger la cohérence des informations. Le centre de clearing travaille sans interaction d'un utilisateur et est souvent exploité dans une zone DMZ (demilitarised zone; voir Appendice C – Glossaire).

Nous distinguons entre centre de clearing actif et centre de clearing passif.

- Le centre de clearing actif reçoit les messages provenant de systèmes, en extrait la destination et les relaye vers le système correspondant.
- Le centre de clearing passif reçoit les messages provenant de systèmes et les met en attente jusqu'à ce qu'ils soient pris en charge par les systèmes auxquels ils sont destinés. Le centre de clearing passif est fréquemment exploité dans des domaines de haute sécurité.

D'une manière générale, un centre de clearing a l'avantage de permettre une participation relativement rapide des nouveaux systèmes utilisateurs, parce que les interfaces ne doivent être développées que par rapport au point de jonction normalisé du centre de clearing.

Remarque: Au lieu de «centre de clearing», les termes anglais «transaction manager» ou «coordinator» sont utilisés dans l'architecture Web Services. Les instances suivantes sont ou pourraient être des exemples de centre de clearing ou de transaction manager:

- Sega Intersettle pour le déroulement du négoce des actions ou de leur aliénation
- SIX (successeur de Telekurs SA) pour le trafic des paiements entre les banques en Suisse
- La Poste

4.2 Interfaces

Si nous partons du principe qu'un centre de clearing n'interagit directement ni avec un terminal ni avec un autre centre de clearing, nous avons trois interfaces différentes entre les trois composantes concernées (voir la figure ci-dessous):

- **S1:** terminal-système
- **S2:** système-système
- **S3:** système-centre de clearing

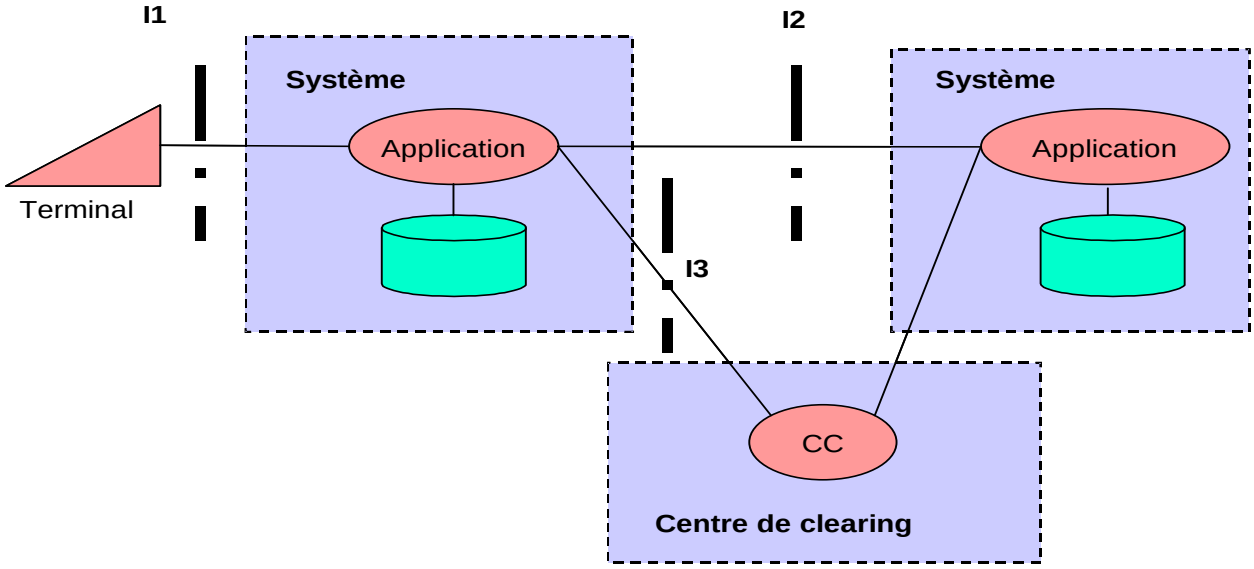


Figure 5-1 Interfaces

La communication et l'échange de données entre les centres de clearing doivent en outre être possibles, comme pour l'interface S3.

Important: Les recommandations présentées ci-après pour la réalisation d'applications de cyberadministration se limitent que, dans un premier temps (c'est-à-dire dans cette version de SAGA.ch), essentiellement aux technologies visant à permettre la communication et l'échange de données aux interfaces mentionnées ici, à savoir S1, S2 et S3. C'est pourquoi nous nous contentons de recommander les formats de données, les protocoles de communication et les mécanismes de sécurité qui peuvent ou doivent être utilisées à ces interfaces. Par conséquent, cette version de SAGA.ch ne donne, elle non plus, aucune indication sur la manière de développer, de configurer et de sécuriser les systèmes de bases de données. De même, elle ne donne pas de recommandations sur les protocoles de base de données tels que SQL et Xquery.

L'interface entre les centres de clearing se présente très rarement dans la pratique; non ne la traiterons donc pas plus en détail dans ce document.

4.3 Délimitation

Pour délimiter les recommandations faites dans le présent document et mieux comprendre l'objectif de ce dernier, nous présentons dans ce chapitre un modèle d'information pour expliquer quelles sont les composantes à normaliser dans cet ouvrage.

4.3.1 Modèle d'information

En informatique, le traitement de l'information peut être classé de manière schématique et sommaire dans les 4 catégories (couches ou layers) suivantes, cf.[GuA], page 16.

- Client. Définit les canaux d'accès et les plates-formes clientes.
- Présentation. Définit les formats de présentation et les protocoles pour le client.
- Intergiciel (middleware) et logique d'application. Définit la fonctionnalité nécessaire pour la fourniture des contenus et des formats dont a besoin la présentation.
- Données, gestion des ressources, conservation des données ou couche de persistance. Définit les sources et les éléments de conservation de données dont a besoin la logique d'application.

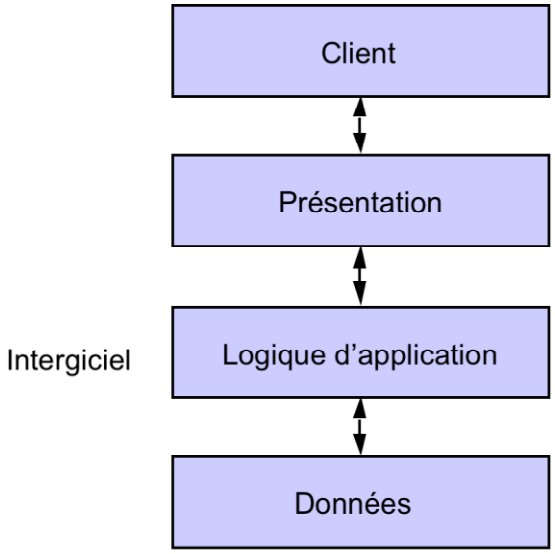


Figure 5-2 Couches de traitement de l'information

Ce document émet des recommandations concernant les protocoles de communication ainsi que les formats et contenus de données devant être utilisés entre le client et la présentation de même qu'entre la présentation et la logique d'application. Nous n'y donnons volontairement aucune recommandation sur le déroulement de la communication entre la couche de données et la logique d'application et sur les formats de données à échanger, parce que cela dépend, entre autres, du système d'exploitation sous-jacent et des systèmes utilisés pour la gestion des bases de données et de l'information.

Exprimé en termes plus simples: «par exemple, l'Internet fonctionne également seul en ce que les protocoles de communication et les contenus des données en sont définis. Nous nous abstenons donc de toute affirmation concernant les systèmes d'exploitation ou les bases de données à utiliser.»

La figure ci-dessous représente les différentes possibilités de communication, les voies de communication représentées par des traits interrompus («-----») ne faisant pas l'objet de la présente norme.

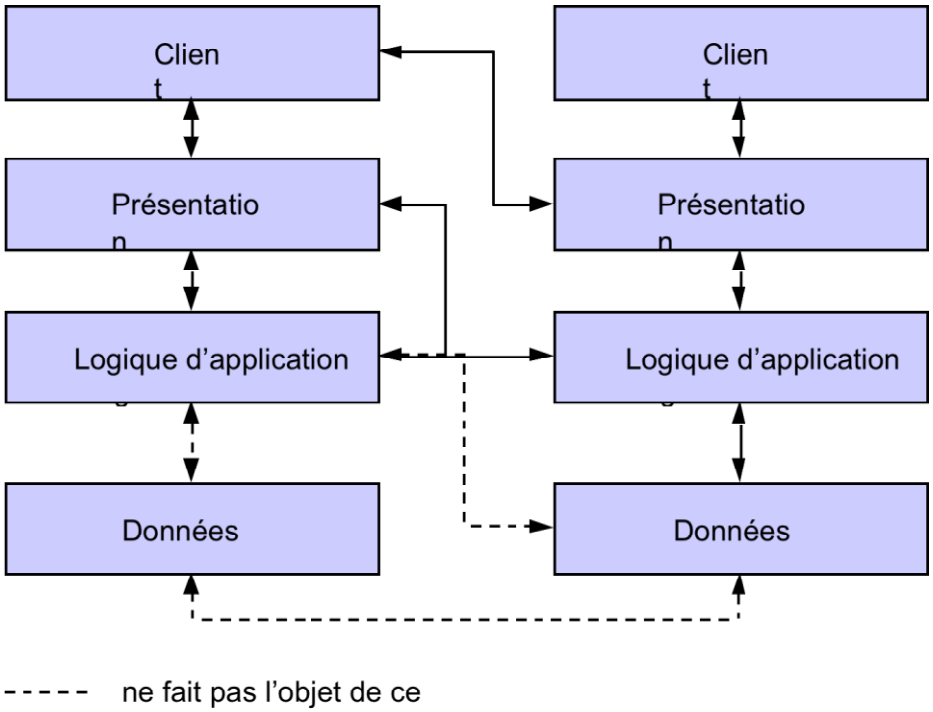


Figure 5-3 Voies de communication possibles

Exception: le chapitre 5.7.4 «Protocoles de serveur d'annuaire selon X.500 X.500» émet des recommandations sur la communication entre les couches de données, mais le fait uniquement pour normaliser la vérification des données personnelles et des certificats s'y rapportant.

4.3.2 Exemple architecture à 3 niveaux

Le modèle ci-dessus de traitement de l'information se présente de la manière suivante dans une architecture à trois niveaux:

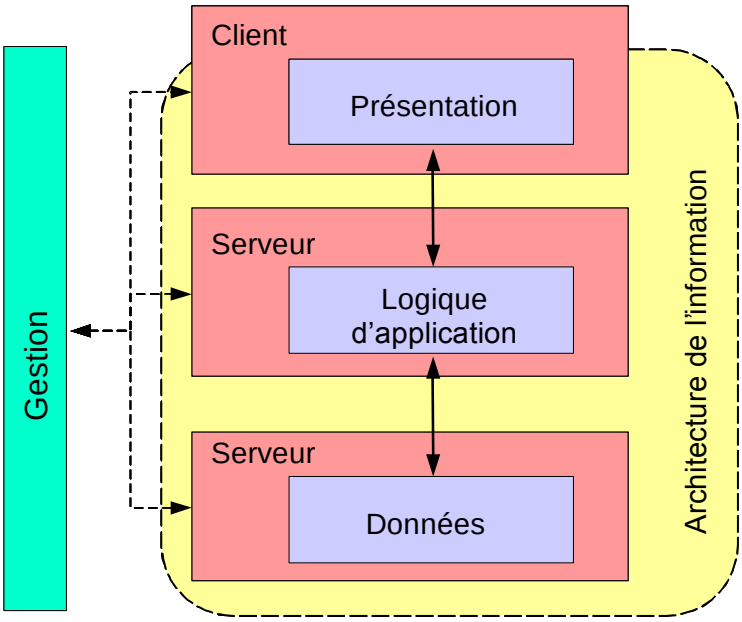


Figure 5-4 Architecture à 3 niveaux

Remarque: l'architecture à 3 niveaux intervient dans de nombreuses applications client-serveur. La couche de présentation y réside sur la plate-forme côté client.

La figure ci-dessus représente également l'interface de gestion avec les différentes plates-formes et couches. La gestion des différentes composantes ne peut pas être normalisée d'une manière uniforme, parce que leur administration et leur configuration sont effectuées par diverses autorités, institutions ou personnes morales et physiques et dépendent en outre du système d'exploitation sous-jacent et des exigences correspondantes en matière de sécurité. C'est pourquoi nous n'émettons ici presque aucune recommandation concernant cette interface ou les protocoles de gestion.

La communication des informations de gestion peut, devrait ou doit être sécurisée. Comme la gestion et, par conséquent, la sécurité des composantes sont le fait de différentes institutions, comme nous l'avons déjà mentionné, nous n'émettons, dans ce domaine, aucune recommandation concernant les mécanismes et protocoles de sécurité, tels que SSH (Secure Shell).

4.3.3 Exemple architecture à n niveaux avec interface Web

La figure ci-dessous représente une architecture à n niveaux. L'accès à la plate-forme cliente y est réalisé par le protocole HTTP et d'autres (figure tirée du document [GuA] et légèrement modifiée). Cette architecture, ou cette répartition du traitement de l'information, est utilisée, entre autres, pour la consultation de bases de données à travers l'internet.

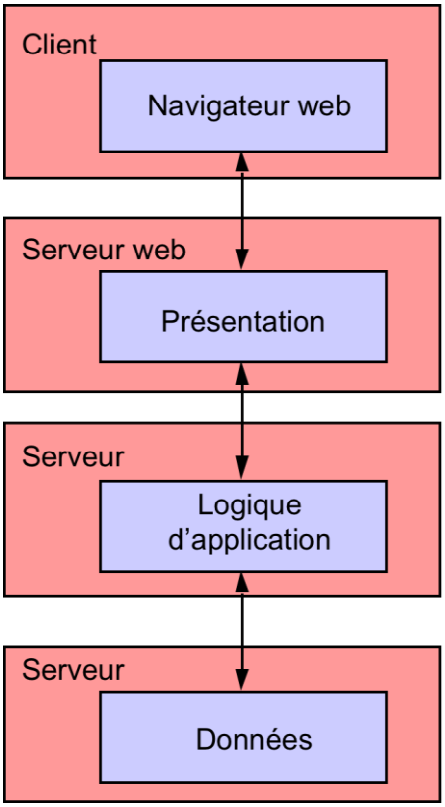


Figure 5-5 Architecture à n niveaux

4.3.4 Remarque concernant Service-Oriented Architecture (SOA)

L'architecture orientée service (Service-Oriented Architecture), SOA en abrégé, est ou exprime un concept d'architecture logicielle définissant l'utilisation de services. Ces services doivent remplir les exigences des utilisateurs du logiciel concerné.

Dans l'environnement SOA, les nœuds d'un réseau fournissent à d'autres parties impliquées des ressources d'une manière standardisée (définie). La plupart des définitions ou des concepts SOA se rapportent à l'utilisation de services Web (par exemple SOAP). Toutefois, d'autres technologies se basant sur le service peuvent être utilisées pour la réalisation de l'architecture SOA.

Les technologies mentionnées dans SAGA, notamment dans le contexte des Web Services, permettent une architecture orientée service.

5 Protocoles de communication

Dans ce chapitre, une distinction est établie entre les protocoles suivants:

- Protocoles de réseau et de transport, voir chapitre 5.4.1 «Protocoles de réseau et de transport»
- Protocoles d'application, voir chapitre 5.5 «Protocoles d'application»
- Protocoles pour la communication mobile, voir chapitre Communication mobile
- Protocoles pour l'accès aux services d'annuaire
- Protocoles ou échange de données dans la domaine de l'intergiciel, voir chapitre 5.9 «Web Services (WS)»

En outre, nous indiquerons à quelles interfaces S1, S2, S3 (voir chapitre Interfaces «Interfaces»),il y a lieu d'utiliser les protocoles de communication et de respecter les normes s'y rapportant. Si une interface n'est pas mentionnée, le protocole ne doit y être ni supporté ni utilisé. Exemple:

L'indication suivante est faite pour le protocole XY:

S2 S3

Selon les recommandations faites, le protocole XY est utilisé aux interfaces S2 (système-système) et S3 (système-centre de clearing), mais non pas à l'interface S1 (terminal-système).

Les définitions mentionnées ici se basent sur les recommandations de l'IETF (www.ietf.org), du W3C (www.w3C.org) et autres. Certains profils spécifiques pour les protocoles ou applications concernés doivent éventuellement encore être élaborés et approuvés.

5.1 Remarque concernant la sécurité

Un grand nombre des protocoles mentionnés dans ce chapitre ne sont équipés d'aucune mesure de sécurité. Si l'on veut transmettre des données confidentielles à l'aide de ces protocoles, on devrait utiliser en outre les mesures et technologies de sécurité adéquates, telles qu'elles sont mentionnées au chapitre 7.

5.2 Adressage et identificateurs

En cyberadministration, les identifications au moyen d'identificateurs sont pertinentes, elles sont utilisées dans différentes variantes (voir notamment ETSI UID EN) pour les identités numériques (voir aussi IAM).

5.2.1 OID

Les Object Identifiers (OID) sont des marqueurs sans ambigüité au niveau mondial, qui sont utilisés afin de désigner un objet d'information (cf. URN). Un OID représente un nœud dans un espace de nom classé de façon hiérarchique, qui est défini par la norme ASN.1. Chaque nœud se distingue clairement par une séquence de numéros, qui indique sa position en commençant par la racine de l'arborescence. Il est possible de demander de nouveaux nœuds pour une utilisation spécifique, auprès des autorités compétentes du nœud placé au-dessus dans la hiérarchie. L'administration de l'arborescence des OID et la garantie de

l'absence d'ambigüité des OID reposent sur le transfert de compétence pour les nœuds subordonnées au détenteur d'un OID (source Wikipedia).

OID V.2.1	En observation

Normes: ISO/IEC 9834, ITU-T X.recommendations, DIN 66334.

5.3 Protocoles Link Layer

Les normes de l'industrie (ISO/OSI Layer1 et 2) sont recommandés par principe à ce stade.

S1	S2	S3	
ISO/IEC 8802 (toutes les parties)			Recommandé

Normes: voir ISO/IEC 8802-11 (la partie 11 est WLAN), 8802-3 (la partie 3 est Ethernet); voir notamment aussi les normes IEEE802 ex. IEEE802.3 (Ethernet / MEF) et autres normes pertinentes.

5.4 Protocoles de réseau et de transport

Le lecteur peut se renseigner sur les protocoles de réseau et de transport et sur certains protocoles d'application dans [Hem].

5.4.1 Internet Protocol Stack

L'Internet Protocol Stack (pile de protocole Internet) comprend les protocoles IP, TCP et UDP ainsi que les protocoles d'application basés sur TCP ou UDP.

S1	S2	S3	
Internet Protocol Stack selon les normes IETF			Vivement recommandé

Tutorial: IETF RFC 1180 TCP/IP et autres pertinents.

5.4.2 IPv6

Les nouveaux réseaux, les migrations de réseau et les extensions de réseaux doivent être réalisés sur la base du protocole IPv6.

IPv6			Vivement recommandé
S1	S2	S3	

Normes: RFC 2460, 2640, 3315, 3633, 3972, 4862, 4884, 5942, 5952, 6052, 6275, Informational 6434, 6437, 6494, 6495, Best Current Practice 6540, 6969, 7048, 7346, 7371, 7373, 7374, 7381 et autres pertinents (OSPF, BGP, Dual stack architectures, DNS sec).

5.4.3 IPv4

A l'heure actuelle, c'est le protocole IPv4 qui est utilisé, associé aux protocoles TCP (Transmission Control Protocol) et UDP (User Datagram Protocol).

S1	S2	S3	
IPv4			Recommandé

Normes: IPv4 (RFC 791,951,2131,3232 et correspondants), TCP RFC 793, UDP RFC 768.

5.5 Protocoles d'application

Les protocoles d'application sont les protocoles échangés au niveau 4 et supérieurs du modèle internet (IETF).

5.5.1 File Transfer Protocol, FTP

Pour le transfert des fichiers, on utilisait par le passé un FTP (Port 21) non sûr. Par principe aucun passeport ne doit être transmis non crypté. Afin de pouvoir utiliser le cryptage et l'authentification, on peut utiliser le Transport Layer Security (FTP via SSL, FTPS en abrégé; voir pour SSL ou TLS selon chapitre 0 Selon les recommandations faites, la technologie de sécurité YZ doit être appliquée aux interfaces I1 (terminal-système) et I2 (système-système), mais non pas à l'interface I3 (système-centre de clearing).

SSL/TLS), ou le FTP peut être transmis en tunnels par SSH (Secure File Transfer Protocol) (selon sFTP pour SSH).

S1	S2	S3	
File Transfer Protocol (sFTP Port 22)			Recommandé

Normes: RFC 2228, RFC 2428, RFC 2640, RFC 3659, RFC 5797, RFC 7151.

Remarque: à titre d'alternative, on peut utiliser également le chapitre 5.5.2 HTTP ou le chapitre 5.5.8 WebDAV.

5.5.2 Hyper Text Transfer Protocol, HTTP

HTTP doit être appliqué pour la communication Web (avec port 80 resp. HTTPS avec port 443). En cas d'utilisation de la gestion de session et de cookies HTTP, le mécanisme HTTP normalisé pour la gestion des états doit être respecté..

S1	S2	S3	
Hyper Text Transfer Protocol (HTTP V.1.1)			Vivement recommandé

Normes: HTTP IETF RFC 1945 resp. RFC 2965, RFC 5785, RFC 7230-40.

Remarque: la sécurisation du protocole HTTP sur SSL ou TLS est aussi appelée HTTPS. Concernant SSL ou TLS, voir le chapitre 7.9.1 La sécurisation du protocole HTTP sur S-HTTP (RFC 2660) n'est toutefois pas recommandée, cf. chapitre 7.9.8 Secure HTTP et autres pertinents.

La norme HTTP/2 a été adoptée en mai 2015 par l'IETF. La HTTP/2 doit permettre d'accélérer et d'optimiser le transfert. A cet égard, la nouvelle norme doit cependant être entièrement rétrocompatible avec HTTP/1.1.

S1	S2	S3	
HTTP V2			Recommandé

Norme: IETF RFC 7540.

5.5.3 Simple Mail Transfer Protocol & Format, SMTP

Le transport de courriels nécessite l'utilisation de protocoles de messagerie électronique suivant les spécifications SMTP et MIME pour l'échange de messages. En 1995, le protocole fut étendu à ESMTP. Les pièces jointes doivent correspondre aux formats de fichier prescrits par SAGA.ch.

S1	S2	S3	
Simple Mail Transfer Protocol / Format (SMTP avec Port 25 et MIME)			Vivement recommandé

Normes: RFC 2822, RFC 2046, RFC 2049, RFC 2231, RFC 4288, RFC 4289, RFC 5321, RFC 5322, RFC 6152, RFC 6854, RFC 7672 et autres pertinents.

5.5.4 Protocoles d'accès à la messagerie électronique

Il peut arriver que des boîtes aux lettres électroniques soient proposées. On utilisera pour cela les normes POP3, IMAP4 ou HTTP d'une manière standard pour l'accès aux courriels. L'authentification pour le serveur de messagerie électronique doit être effectuée via un canal sécurisé.

S1	
POP3, IMAP4, HTTP pour E-Mail	Vivement recommandé

Normes: POP3 RFC 1939 mises à jour par RFC1957, RFC2449, IMAP4 RFC 2060, 2061, HTTP für E-Mail RFC 1945 v.1.0 , RFC 3501, RFC 6186, RFC 6237, RFC 7162, RFC 723x, RFC 7377 et autres pertinents.

5.5.5 Telnet

Telnet doit être remplacé par une interface utilisateur plus conviviale, interactive et basée sur l'internet.

Telnet	Non recommandé

5.5.6 Remote Procedure Call (RPC)

RPC sert entre autres à l'activation de commandes sur un ordinateur distant.

S2	S3	
Remote Procedure Call (RPC) avec ports dynamiques		Non recommandé

S2	S3	
Remote Procedure Call (RPC) authentifié avec ports fixes		Recommandé

Normes: RFC 1050, RFC 5531, 5665 , 5666, 5717, 7861.

5.5.7 Protocoles Terminal Service et Thin Client

L'utilisation de Terminal Service et de protocoles Thin Client n'est éventuellement possible qu'à l'interface S1. Terminal Service et les protocoles Thin Client nécessitent toutefois que les deux systèmes soient configurés, gérés et sécurisés par la même institution aux interfaces S1. Leur utilisation n'est donc pas recommandée.

S1	S2	S3	
Protocoles Terminal Service et Thin Client			Non recommandé

Il arrive que les protocoles Thin Client et Terminal Service soit utilisés au sein d'une organisation. La fonctionnalité client du côté gauche de l'interface S1 est toutefois assurée par le Terminal Server.

5.5.8 WebDAV

Le protocole WebDAV (Distributed Authoring and Versioning) est défini dans le document RFC 2518 initial et constitue une extension du protocoles HTTP/1.1 selon RFC 723x. Il permet en outre d'utiliser des méthodes et des possibilités pour publier, manipuler et verrouiller des contenus ou des documents sur le serveur (WebDAV) ou d'y faire des recherches selon des attributs élargis.

S1	S2	S3	
WebDAV			Recommandé

Norme: IETF RFC 3648, 3744, 4331, 5323, 5397, 5689, 6764, 7809, 7953 et autres pertinents notamment d'ISO/IEC/W3C.

5.5.9 XMPP

Le protocole Extensible Messaging and Presence (XMPP, protocole de présence et de message extensible en anglais (anciennement Jabber)) est une norme de l'IETF pour le XML-Routing. XMPP suit la norme XML et est utilisé principalement pour l'Instant Messaging. Les extensions de XMPP représentent les XMPP Extension Protocols publiés par XSF (source notamment Wikipedia).

S1	S2	S3	
XMPP			Recommandé

Normes: IETF RFC 3922, 3923, 6121,7247,7248,7572,7573,7590,7622,7700,7702 et autres pertinents, ISO/IEC/IEEE/W3C/OASIS dans les travaux et reviews.

5.5.10 CMIS

La norme CMIS (Content Management Interoperability Services Standard) d'OASIS est utilisée pour l'échange de documents entre ECM, GEVER (systèmes de gestion administrative), les systèmes ERP. La norme CMIS un modèle de domaines et des services Web. Elle intègre notamment des objets WSDL, JSON, SOAP et REST. Les serveurs CMIS enregistrent les contenus, qui sont à leur tour proposés au moyen de protocoles CMIS pour les applications les plus variées (source notamment Wikipedia).

S2	
CMIS V1.1/2	En observation

Normes: https://www.oasis-open.org/news/announcements/content-management-interoperability-services-cmis-version-1-1-approved-and-publis.

5.5.11 AMQP

L'Advanced Message Queuing Protocol (AMQP V.1) sert à échanger les données de manière efficace et hautement qualitative. Ce mode d'échange est utilisé pour les systèmes de messages avec des applications hétérogènes, des infrastructures mobiles et des systèmes Cloud. Il définit un protocole ouvert pour les systèmes de messages d'affaires, qui permet un «mécanisme binary wire-level» pour l'échange de données entre deux parties.

S1	S2	S3	
AMQP V.1			Recommandé

Normes: ISO/IEC 19464-2014, voir OASIS.

5.5.12 MQTT

Message Queue Telemetry Transport (MQTT) est un protocole de message ouvert pour la communication M2M, qui permet le transfert de données sous la formes de messages entre appareils en dépit de pertes de qualité (des restrictions de performance notamment comme de faibles débits, temps de latence élevé, ressources réseau limitées par exemple). La spécification MQTT établit une distinction entre les réseau basés sur IP et non TCP/IP.

S1	S2	
MQTT		En observation

Normes: ISO/IEC 20922-2016, voir notamment http://mqtt.org/MQTT.org

OASIS http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/csprd02/mqtt-v3.1.1-csprd02.html

5.5.13 STOMP

Le Simple Text-Oriented Messaging Protocol (STOMP) est un protocole optimisé pour les messages interopérationnels simples par rapport aux autres Messaging Stacks. STOMP est employé dans les architectures IoT (comme le MQTT), son utilisation est très répandue et il intervient en appui des services Web. (voir également Wikipedia).

S1	S2	
STOMP V.1.2		En observation

Spécification: STOMP 1.2 (Rel.10/22/2012; il existent des ver. antérieures 1.1/1.0), RFC 7692, 7936.

Mailinglist: stomp-spec google group; http://groups.google.com/group/stomp-spec .

5.6 Communication mobile

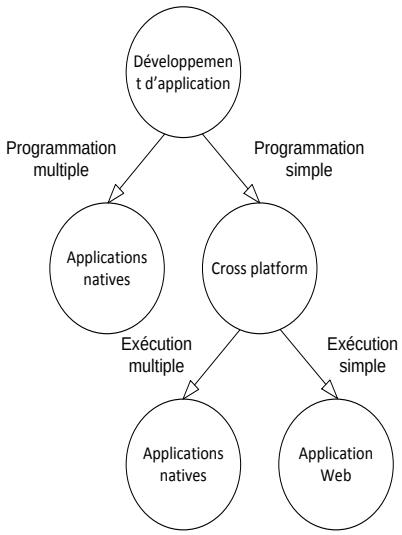
Concernant l'implémentation d'applications mobiles, il existe fondamentalement deux variantes de mise en œuvre distincte. Un service, qui est proposé comme application (App) native, doit être implémentée individuellement pour chaque plateforme (ex. Apple iOS, Google Android, Microsoft Windows Phone, Blackberry, etc.) et par conséquent à plusieurs reprises. Il en résulterait dans les faits plusieurs applications, qui ne devraient non seulement être im-

plémentées individuellement, mais aussi distribuées (ex. appstore), entretenues et perfectionnées individuellement.

Face à un tel constat, on a assiste au déploiement d'efforts visant à trouver d'autres «cross platform application frameworks» – plateformes d'applications, permettant d'implémenter une application une seule fois et de pouvoir l'utiliser ensuite sur toutes les plateformes propriétaires sans charge supplémentaire. De telles plateformes sont toutefois sujettes à des restrictions, qui, dans des cas particuliers, rendent inévitable un développement multiple. Dans toutes les éventualités, il est recommandé de décider au cas par cas laquelle parmi ces variantes doit être utilisée.

Dans l'autre variante, l'application souhaitée est implémentée en tant qu'application Web (avec des technologies Web courantes côté client et serveur) et sur les smartphones, celle-ci est utilisée avec un navigateur Web. Si la distribution via un appstore est souhaitée, il est alors possible d'avoir recours à des applications natives, qui ne sont en fait rien d'autres que des navigateurs cachés.

L'arborescence de décision suivante offre une vue d'ensemble des possibilités décrites.



Recommandations:

Il existe également deux façons pour ces «cross platform application frameworks» d'éviter le développement multiple. Dans l'une des variantes, l'application est programmée une seule fois et les applications propriétaires sont générées à partir de ce code de programme. Ceci signifie qu'à la fin du développement, il existe une application native pour chaque plateforme d'application propriétaire. Si aucune fonctionnalité spécifique (capteurs etc.) n'est nécessaire, une application Web de cyberadministration pour appareils mobiles devrait être développée de manière optimisée. S'en est alors fini de la dépendance envers le canal de distribution (appstore notamment). Par ailleurs, les considérations de sécurité à prendre en compte sont les même que pour les applications Web conventionnelles.

S1	S2	S3	
HTML (voir aussi chap. 6.2.7)			Vivement recommandé

S1	S2	S3	
Cross platform applications			Recommandé

En outre**:** lorsque cela est inévitable, l'on a recours à des Native Apps (applications natives).

5.7 Services d'annuaire

5.7.1 LDAP

LDAP (Lightweight Directory Access Protocol) est un protocole internet optimisé pour les informations classées hiérarchiquement et utilisé pour l'accès à des services X.500 ou à des services d'annuaire du même genre. Les versions plus anciennes ne sont pas recommandées.

	S1	S2	S3	
LDAP V.3				Vivement recommandé

Normes: RFC 4511 à 4515 et pertinentes correspondantes selon RFC 4510 (Roadmap), notamment RFC 4523, 4524 ainsi que ISO/IEC pertinentes.

5.7.2 LDAP Replication

Cette norme propose une méthode pour la réplication des données par les annuaires LDAP entre eux.

	S2	S3	
LDAP (Version 3) Replication Requirements			En observation

Norme: RFC 3384 et pertinentes.

5.7.3 DSML

DSML (Directory Services Markup Language) est une norme d'OASIS (www.oasis-open.org) pour l'échange d'informations par le biais d'un service d'annuaire (directory) en format XML. La version 2 de cette norme définit comment réaliser les demandes adressées à un service d'annuaire et les modifications devant y être effectuées, les commandes se basant sur XML.

	S1	S2	S3	
Directory Services Markup Language (DSML V.2.0)				Recommandé

Norme: Directory Services Markup Language (DSML) v.2.0, January 2002, par OASIS SPML, SAML, XACML font figure d'alternatives.

5.7.4 Protocoles de serveur d'annuaire selon X.500 X.500

Les protocoles d'annuaire suivants existent selon la norme X.519 pour la réplication, la consultation et l'actualisation de données:

- DSP Directory System Protocol
- DISP Directory Information Shadowing Protocol
- DOP Directory Operation Binding Management Protocol

	S2	S3	
Protocoles de serveur d'annuaire selon X.500 X.500			Recommandé

Normes: X.519, X520 Selected Attribute Types, X521 Selected Object Classes et autres affiliés par l'ITU www.itu.org; voir également IETF RFC 2605 concernant le Monitoring.

5.7.5 OCSP

Le Online Certificate Status Protocol (OCSP) permet de déterminer le statut actuel d'un certificat, sans devoir avoir recours à un CRL. OCSP s'appuie sur le HTTP.

S1	S2	S3	
Online Certificate Status Protocol (OCSP)			Recommandé

Norme: RFC 6960

Remarque: La décision de déclarer OCSP vivement recommandé ou seulement recommandé devrait aussi être étudiée dans le cadre du rattachement à une infrastructure de clé publique (voir architecture technologie PKI).

5.8 Protocoles pour l'échange d'informations en temps réel

5.8.1 SIP

Le Session Initiation Protocol (SIP) pour la voix sur IP a été normalisé par l'IETF et comprend plusieurs normes et Best Practices RFC.

S1	S2	S3	
Session Initiation Protocol (SIP)			Recommandé

Norme: La norme de base RFC 3261 (voir aussi RFC 3265, 3853, 4168 SCTP, 4320, 4916, 5367, 5393, 5621, 5622 Profile Experimental, 5626, 5630, 5922, 5994 MPLS TP Informational, 6026, 6141, 6323, 6446, 6665, 6878, 7118, 7462, 7463, 7621, 7957 et pertinentes) a élargie et actualisée dans les Best Practices et normes mentionnés entre parenthèses.

5.8.2 Famille de protocoles H.323

La famille de protocoles H.323 a été mise au point par l'ITU pour la voix sur IP.

S1	S2	S3	
Famille de protocoles H.323			Recommandé

Norme: H.323 est une norme de l'UIT pour la voix sur IP. Des aspects techniques supplémentaires ont été actualisé dans diverses autres normes, telles que les séries H.224, 225, 235, 245, 246, 281, 283, 325, 328, 341ou H.450/460/500 (voir notamment le groupe d'étude 13 d'ITU).

5.8.3 Skype

Skype est un protocole de voix sur IP (téléphonie Internet) propriétaire, qui n'a pas encore été normalisé par ITU/ISO/IEC.

S1	S2	S3	
Skype			En observation

Norme: pas de norme, protocole propriétaire.

5.8.4 RTP

Le Real-time Protocole (RTP) définit un protocole, qui est utilisé pour le trafic audio, vidéo et vocal sur réseaux IP. Le RTP est utilisé en combinaison avec le Contrôle Protocole (RTCP) pour les signalisations et les Call Controls pour les services multimédias. Le RTCP est également pertinent pour la surveillance de transmissions, Quality of Services et synchronisations en cas de canaux multiples (multiple streams).

	S1	S2	S3	
RTP				Recommandé

Normes: IETF RFC 3550, 3551, 5506, 5761, 6051, 6222, 7007, 7022, 7160, 7164, 8035 et autres pertinents.

Informations: voir aussi Secure RTP RFC 3711, 5506, 6904.

5.9 Web Services (WS)

5.9.1 Définition

Les organisations de normalisation dans cette domaine (par ex. OASIS, WS-I, W3C) et leurs membres utilises plusieurs définitions de l'expression «Web Services», voir aussi le document [GuA]. Nous utiliserons la définition suivante, selon le W3C[4]:

> Web Services est un système se composant de plusieurs services séparés au réseau. Couplés de manière souple, ces derniers sont évolutifs et leur interopérabilité est garantie. Leurs interfaces et fonctionnalités sont définies dans un format lisible par machine (Web Services Définition Language). Les machines communiquent entre eux par messages habituellement en formats XML.

[4] Pas la traduction littérale du glossaire des services Web: http://www.w3.org/TR/ws-gloss/.

5.9.2 Dépendances

La figure suivante[5] résume les dépendances entre SOAP, WSDL et UDDI:

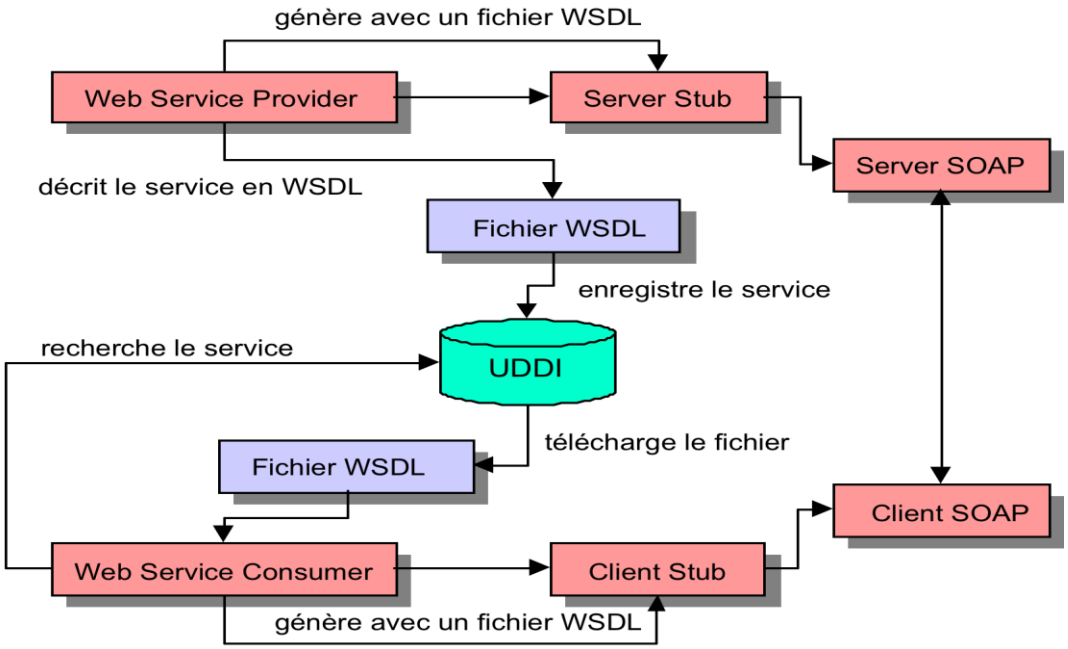


Figure 6-1 Dépendances des services en lignes

5.9.3 Architecture des Web Services

L'architecture des Web Services peut être représentée par le schéma suivant:

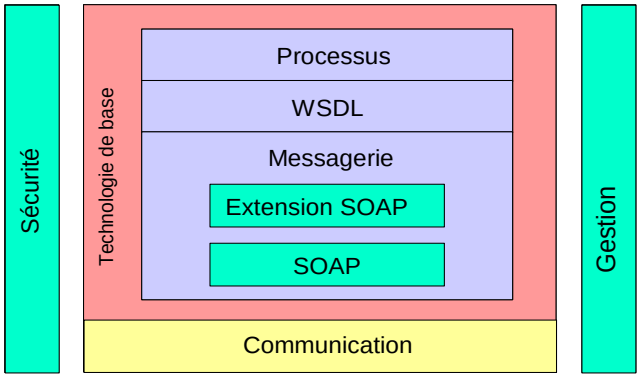


Figure 6-2 Modèle d'architecture des Web Services

La sécurité (security) est une partie intégrante de tous les domaines mentionnés ici. Aspects comme la communication protégée, messagerie sécurisée, documents WSDL authentifiés, processus ou transactions fiables sont mentionnées dans les recommandations suivantes et au chapitre 7 «Sécurité».

[5] Les informations et les dessins suivants proviennent notamment de [GuA]. Les lecteurs qui s'intéressent aux services Web, mais qui n'y sont pas rompus devraient consulter ce livre, [ZoT] également pour les lecteurs techniquement chevronnés disposant de connaissances de base en XML.

5.9.4 SOAP

SOAP est un protocole ainsi qu'un format de messages. Ce format est lui-même une application XML et possède les trois composantes suivantes: L'enveloppe (*enveloppe*) constitué de l'en-tête (*header;* comprenant des informations supplémentaires facultatives sur le déroulement du processus et le contrôle du protocole, telles que des indications sur l'authentification ou la qualité de service) et le corps (*body*) du message – le contenu.

SOAP se fonde sur un protocole d'application TCP (par ex. HTTP, SMTP, etc.):

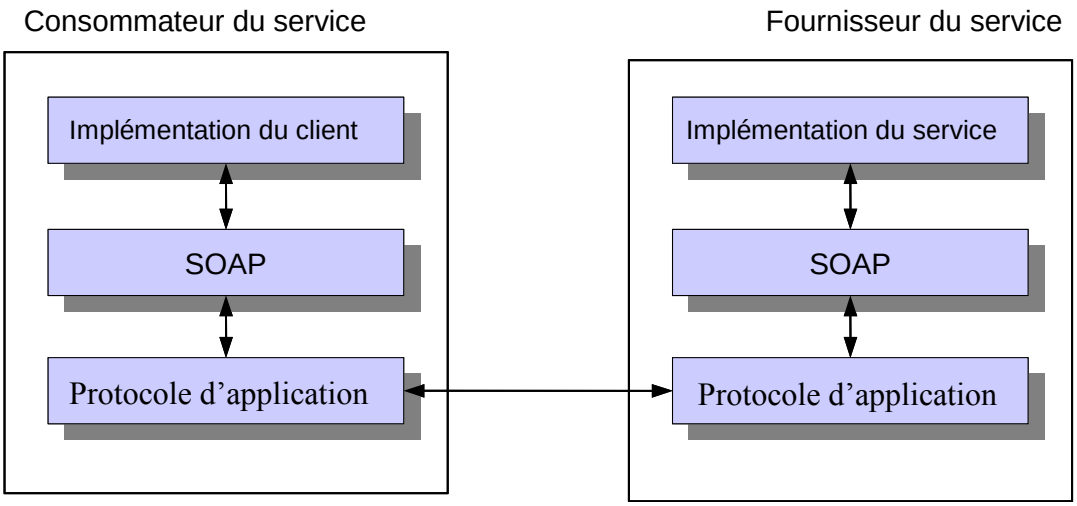


Figure 6-3 Pile de protocoles des messages SOAP

S1 S2 S3

SOAP V.1.2	Vivement recommandé

Norme: SOAP v.1.2, June 2003, de W3C www.w3C.org, RFC 4227, RFC 7878

SOAP V.1.1	Recommandé

5.9.5 Message Transmission Optimization Mechanism (MTOM)

MTOM est une norme mise à disposition par W3C pour transporter les données binaires pour un message SOAP. Les données binaires ne sont pas encodées comme texte et intégrées dans le message SOAP, mais sont comprimées conformément à la norme « *XML-binary Optimized Packaging (XOP)* », avec le message SOAP. Le message SOAP comprimée est pourvu de liens qui renvoient vers les parties avec les données binaires comprimées.

S1 S2 S3

Message Transmission Optimization Mechanism (MTOM) V.1.2	Recommandé

Norme: MTOM, W3C Recommendation, 25 January 2005, de W3C www.w3c.org, XOP, W3C Recommendation, 25 January 2005, de W3C www.w3c.org; notamment aussi pour JAX WS.

5.9.6 Web Service Description Language (WSDL)

Les services Web sont décrits au moyen du langage WSDL (Web Service Description Language). Celui-ci se fonde sur XML et définit, entre autres, les points d'extrémité (ports) de la

communication ainsi que les messages à échanger (par SOAP). Aucun protocole d'application particulier n'est prescrit pour l'échange des messages. Toutefois, dans la version actuelle, seuls le protocole HTTP ou le Container MIME peuvent être utilisés pour SOAP v.1.1.

S1	S2	S3	
Web Service Description Language (WSDL V.1.1)			Vivement recommandé

Norme: WSDL Web Services Description Language v.1.1, 15.3.2001 W3C www.w3C.org

Web Service Description Language (WSDL V.2.0)	Recommandé

Norme: WSDL Web Services Description Language Version 2.0 Part 1: Core Language, W3C Rec. 26.6.2007 W3C et autres, www.w3C.org; Les V.3 Experimentals sont connus.

5.9.7 WS-Addressing

Le WS-Addressing permet d'échanger des services Web, des informations concernant les adresses et facilite l'utilisation d'interrogations de services Web asynchrones, chaque message SOAP contenant en entête des métainformations supplémentaires concernant l'expéditeur et le destinataire de la réponse ainsi que le destinataire de messages d'erreur.

S1	S2	S3	
Web Services Addressing (V.1.0)			Vivement recommandé

Norme: Web Services Addressing (Core, SOAP Binding, Metadata) v.1.0, May 2006 / Sept. 2007 de W3C www.w3C.org ; notamment aussi pour JAX WS.

5.9.8 Universal Description, Discovery and Integration (UDDI)

Universal Description, Discovery and Integration (UDDI) standardise la publication des services dans le domaine des Web Services.

S1	S2	S3	
Universal Description, Discovery and Integration (UDDI V.2/3)			Recommandé

Norme: Universal Description, Discovery and Integration (UDDI) v.2.0, February 2003 d'OASIS (www.oasis-open.org), RFC 4403 Informational.

5.9.9 Protocoles de transaction

SOAP n'est pas suffisant pour traiter les processus d'affaires complexes au moyen des différentes technologies disponibles. C'est la raison pour laquelle les protocoles suivants de transaction ont déjà été conçus et spécifiés:

- Web Services Reliable Messaging
- Web Services Coordination
- Web Services Atomic Transactions
- Business Activity
- OSCI Transport

5.9.9.1 WS Reliable Messaging

WS Reliable Messaging a été conçu pour échanger des messages de manière fiable.

S1	S2	S3	
WS-Reliable Messaging V.1.1/2			Recommandé

Norme: OASIS, Web Services Reliable Messaging (WS-ReliableMessaging) Version 1.1/2 Version 1.2, 2. février 2009.

5.9.9.2 WS Coordination

WS Coordination a été conçu par OASIS (www.oasis-open.org) et définit un espace de travail (framework) commun pour la coordination d'activités distribuées. Les normes WS-AtomicTransaction et WS-BusinessActivity s'appuient sur ce framework.

S1	S2	S3	
WS-Coordination V1.1/2 + errata			Recommandé

Norme: OASIS, Web Services Coordination (WS-Coordination) Version 1.1/2.

5.9.9.3 WS Atomic Transaction

WS-Atomic Transaction repose sur le protocole WS Coordination et a été conçu et spécifié en collaboration par IBM, Microsoft et Bea Systems (www.bea.com) surtout pour les transactions de courte durée. Trois possibilités y sont spécifiées pour le déroulement d'une transaction cohérente de brève durée de vie. WS Atomic Transaction a été adoptée par OASIS (www.oasis-open.org).

S1	S2	S3	
WS-Transaction V.1.1/2 + errata			Recommandé

Norme: OASIS, Web Services Transaction (WS-Transaction) Version 1.1/2.

5.9.9.4 WS Business Activity

Le protocole Web Services Business Activity (WS Business Activity) a été conçu par OASIS (www.oasis-open.org) et repose sur le protocole WS Coordination. Les développeurs peuvent l'utiliser pour réaliser des applications Web Services contenant des conventions cohérentes et devant se dérouler pendant une longue période sur des systèmes distribués.

S1	S2	S3	
WS-BusinessActivity V.1.1/2 + errata			Recommandé

Norme: OASIS, Web Services Business Activity (WS-BusinessActivity) Version 1.1/2.

5.9.9.5 OSCI-Transport

OSCI (Online Service Computer Interface) comprend toute une série de protocoles couvrant les exigences de la cyberadministration et élaborés par le centre de gestion OSCI. Ces protocoles ont pour objectif de soutenir les transactions sous forme de services Web ainsi que l'ensemble de leur déroulement. Sedex utilise OSCI.

S1	S2	S3	
OSCI-Transport V.1.2/2			Recommandé

Norme: Norme: OSCI a été conçu en Allemagne dans le cadre du concours MEDIA@Komm. OSCI Version 2 est améliorée en continu et repose sur la pile WS.

5.9.9.6 Sedex

Dans le cadre de l'harmonisation des registres des personnes de la Confédération et des registres cantonaux resp. communaux des habitants, la Confédération met à disposition, depuis le début de l'année 2008, une plateforme d'échange de données en toute sécurité entre les participants: elle a été baptisée Sedex (pour: Secure Data Exchange). En 2016, plus de 13,7 millions d'annonces sedex ont été transmises.

La communication est asynchrone, mais permet l'échange de messages très grands et de nombreux messages simultanés, contrairement aux systèmes de messagerie conventionnels. Toutes les transmissions de données sont chiffrées et ne peuvent être déchiffrées que par le destinataire concerné.

Sedex peut être utilisée dans d'autres domaines, la priorité étant donnée aux applications de cyberadministration. La connexion à Sedex requiert l'intégration d'un adaptateur dans l'application participante et les exigences en matière de sécurité doivent être remplies (authentification du participant, le cas échéant, certification de l'application).

La version 2 comme la 3 et la 4 ne sont désormais plus en service.

Le client Sedex propose, par défaut, un proxy de service Web, qui se charge de l'authentification d'un participant sedex sur la base du certificat d'organisation par rapport aux services Web, l'administration des utilisateurs disparaissant ainsi pour les services Web. L'exploitation des certificats est garantie par sedex.

S1	S2	S3	
Sedex (Secure Data Exchange)			Recommandé

Normes: Sedex , V.2.x , 2007–2010: spécifications voir www.sedex.ch .

5.9.10 **Web Services Resource Framework (WSRF)**

WSRF est une famille de normes de services Web à des fins d'extension du modèle de communication fondamentalement sans état des services Web en un modèle de communication à états. Lors d'une session, un état de conversation sous forme de ressources est attribué aux partenaires de communication. Les ressources et leurs propriétés (cycle de vie, traitement des erreurs, appartenance à un groupe) sont mises à disposition et administrées par un service Web spécial. Un client de service Web envoie un message au fournisseur du service Web et référence, ce faisant, une ressource au moyen d'un URI.

S1	S2	S3	
WS-Resource Framework V.1.2			Recommandé

Norme: Web Services Resource 1.2 (WS-Resource), OASIS www.oasis-open.org, 1.April 2006; Web Services Resource Properties 1.2 (WS-ResourceProperties) OASIS 1.April 2006; Web Services Resource Lifetime 1.2 (WS-ResourceLifetime) OASIS 1.April 2006; Web Services Service Group 1.2 (WS-ServiceGroup) OASIS 1.April 2006; Web Services Base Faults 1.2 (WS-BaseFaults) OASIS 1.April 2006. Le cadre est utilisé globalement pour les applications, champs de système et domaines d'information les plus divers.

5.10 REST ou RESTful HTTP

REST est l'acronyme de l'expression anglaise «Representational State Transfer» et désigne un style d'architecture pour les systèmes répartis, qui repose directement sur http et permet d'éviter d'avoir recours à l'utilisation d'un Webservice Protocole Stack complexe. Les informations importantes concernant le statut sont imprimées dans les URI dynamiques.

S1	S2	S3	
Representational State Transfer (REST ou RESTful HTTP)			Recommandé

Normes: IETF RFC 6690, RFC 723x (HTTP) : notamment aussi avec OData, JAX-RS, Spring.

5.11 Service Provisioning Markup Language (SPML)

«Provisioning» correspond à l'automatisation de toutes les étapes nécessaires à l'administration (création, modification et révocation) de données et d'autorisations d'accès des utilisateurs ou d'autres systèmes en rapport avec les services publiés de façon électronique («Services»). L'administration et l'échange des données d'autorisation se font via SAML (voir chapitre 7.8.11.3).

S1	S2	S3	
Service Provisioning Markup Language V.2.0			Recommandé

Norme: Service Provisioning Markup Language (SPML), v.2.0, , 2005 von OASIS. https://docs.oasis-open.org/provision/spml-2.0-cd-01/pstc-spml2-cd-01.html.

5.12 ebXML

ebXML (Electronic Business XML) comprend toute une série de normes élaborées en collaboration par OASIS (www.oasis-open.org) et par UN/CEFACT, dont aussi un protocole de transaction CPPA (Collaborative Partner Profile Agreement). Toutes ces normes ont pour objectif la définition d'une infrastructure devant permettre l'utilisation mondiale du commerce électronique et assurer son interopérabilité.

Dans ce cadre, plusieurs normes ont été spécifiées et normalisées plus en détail.

S1	S2	S3	
electronic business using XML (ebXML V.2.1/V.3 pour RIM/RS/V.4)			Recommandé

Normes: ISO15000 partie1-5 2014: le développement d'ebXML se poursuit notamment par l'OASIS TC.

Différentes normes ebXML Security ont été élaborées.

ebXML Security	En observation

Normes: les normes concernant ebXML sont également disponibles auprès d'OASIS www.oasis-open.org.

5.13 UBL

Universal Business Language (UBL) est une spécification d'OASIS pour les documents d'E-Business standardisés (ex. facture ou commande). UBL utilise XML et repose sur les ebXML Core Components (notamment XML DSig, XAdES et autres pertinents).

S1	S2	S3
UBL V.2.1		Recommandé

Normes: ISO/IEC 19845 2015, ISO 14662 2010, ISO 15000 parties 1-5 2014, CWA 16667.

Informations: : la facturation conforme à l'OeIDI impose une signature électronique. Se pose alors le problème pour les documents composés de plusieurs fichiers et objets externes. La signature électronique est pertinente à cet égard.

5.14 swissdec/PUCS4.0

L'industrie et l'économie utilisent la norme relative suisse aux salaires PUCS (Procédure unifiée de communication des salaires, version 4.0). Elle est également employée dans la Confédération (décision UPIC, EPA, BIT). Avec PUCS, il n'est plus nécessaire de remplir ou de transférer manuellement les formulaires de communication des salaires au moyen d'une annonce électronique de salaire. Dans le cadre de l'introduction susmentionnée, une solution technique de transmission des données PUCS aux partenaires sociaux est recherchée pour la transmission des résultats du décompte de l'impôt à la source (extraits de SAP dans la Confédération par exemple).

Cette norme met à disposition une connexion sûre et établie directe à «swissdec», qui permet d'éviter de grever les clients avec les évolutions en cours – sur la base de questions d'ordre technique, légal et stratégique.

S1	S2	S3
swissdec/PUCS4.0		Recommandé

Norme: voir https://www.swissdec.ch/de/releases-und-updates/richtlinien/

5.15 Langages de description de processus d'affaires

Un processus d'affaires peut se composer de différents services, et les transactions intervenant dans ce contexte peuvent être complexes. C'est pourquoi des modèles sont nécessaires pour la représentation des services de manière à les rendre compréhensibles d'une manière générale. Il existe différentes formes de réalisation du déroulement du processus, dont les deux modèles ci-après[6]:

- le modèle de composition (composition model), qui définit les caractéristiques des différents éléments constituant le processus d'affaires et la transaction.
- le modèle d'orchestration (orchestration model), qui définit l'abstraction et le langage nécessaire pour décrire le déroulement des services impliqués dans le processus d'affaires.

[6] D'autres modèles sont mentionnés dans [GuA].

5.15.1 BPEL

BPEL (Business Process Execution Language) est un langage basé sur XML et servant à la description, à la modélisation et à la «composition» de processus d'affaires sur la base de Webservices.

BPEL est établi en concertation avec WSDL.

S1 S2 S3

Business Process Execution Language (BPEL) V.1.1/2.0	Recommandé

Norme: Business Process Execution Language for Web Service (BPEL 4WS) v.1.1, décembre 2003 d'OASIS www.oasis-open.org, version 2 April 2007.

5.15.2 BPMN

BPMN (Business Process Model and Notation) est une norme ouverte de description qui convient tant pour la représentation graphique (notation) de processus internes que pour l'organisation de processus généraux. BPMN contient un set très étendu de symboles graphiques..

S1 S2 S3

Business Process Modeling Notation (BPMN)	Vivement recommandé

Normes: ISO/IEC 19510 2013 notamment Part5 2015, BPMN Version 2.0 selon eCH0140/158, voir aussi Object Management Group (www.omg.org; www.bpmn.org), divers développement sont actuellement en cours pour BPMN Version 3.

5.15.3 UML

UML (Unified Modeling Language) est un langage ou un mode de représentation servant à décrire le processus selon le modèle d'orchestration. Il prévoit des diagrammes d'états (state charts) pour décrire le déroulement du processus avec ses différents états et indiquer quels sont les passages possibles entre ces états et comment ils peuvent se réaliser.

S1 S2 S3

Unified Modeling Language (UML) V.1.5	Recommandé

Norme: Unified Modeling Language, développé par l'Object Management Group (OMG) et normalisé par ce dernier et par l'ISO (ISO/IEC 19505 pour la version 2.x).

Unified Modeling Language (UML) V.2.0/2.4.x	Recommandé

Norme: ISO/IEC 24156-1 daté de 2014, ISO/IEC 19505 UML V.2.4.1 – version actuelle 2.5 de juin 2015 ; Unified Modeling Language de Object Management Group www.omg.org. En cas de doute, utiliser la v.2.0.

5.15.4 XMI

XMI est une spécification permettant la description et l'échange de modèles de données et de processus dans XML. L'OMG a défini XMI. La version 2.1.1 est datée de décembre 2007, et la version 2.0.1 a été normalisée par l'ISO comme ISO/IEC 19503:2005 puis élargie à la version 2.5.1 juin 2015 et la nouvelle ISO/IEC 19509 en cours d'élaboration.

XMI devrait être utilisé pour l'échange pour tous les modèles de processus, qui reposent sur la spécification Meta-Object Facility (MOF) de l'OMG, c'est à dire en particulier pour les modèles UML dans la version 2.x. XML Medata Interchange (XMI) dans la version 2.x est un format d'échange correspondant pour les modèles de processus sur base UML-2.x.[7]

S1	S2	S3	
XMI V.2.x (XML Metadata Interchange)			Recommandé

Normes: ISO/IEC 19503-V.2.0.1-2005, 19509-V.2.4.2-2014; http://www.omg.org/spec/XMI/

5.15.5 XPDL

Process Définition Language (XPDL) est une application XML pour la définition de processus et de flux de travail. La norme relative au XPDL a été définie par la Workflow Management Coalition, WFMC (www.wfmc.org) et est notamment employé pour le BPMN.

S1	S2	S3	
XML Process Définition Language (XPDL) V.2.X			Recommandé

Norme: XML Process Définition Language (XPDL) de WFMC www.wfmc.org .

5.16 CORBA

CORBA est l'abréviation de Common Object Request Broker Architecture et est, comme Web Services, une plate-forme intergicielle (middleware).

CORBA	Non recommandé

CORBA et les protocoles (IIOP) s'y rapportant se sont vu attribuer le statut «non recommandé» parce que:

- le protocole IIOP (Internet Inter-ORB Protocol) qu'il utilise présente une sécurité insuffisante, notamment parce que le serveur établit une connexion de rappel (call back) avec le client (voir à cet effet [ZeCs]) et que le numéro de port du protocole TCP est attribué de manière dynamique dans certaines applications.
- Web Services utilise des formats et contenus de données normalisés et convient particulièrement bien pour la communication intergicielle entre différentes organisations.
- nous pensons que Web Services sera davantage utilisé à l'avenir, et sera supporté et proposé par un plus grand nombre de grands fabricants de logiciels.
- il est trop coûteux d'assurer la réalisation, la maintenance et la coordination de deux architectures intergicielles.

[7] UML 2.x devrait être utilisé pour la préparation et la documentation de grands projets pour la modélisation axée sur les objets. A titre d'exemple, les Use Cases et les diagrammes d'activité ont fait leurs preuves dans la pratique et permettent d'élaborer et d'ajuster des spécifications transparentes. Les diagrammes de flux sont une notation graphique pour le déroulement d'un programme. Les diagrammes de flux ont été introduits à l'origine en lien avec le paradigme des programmes impératifs, mais peuvent aussi être mis à contribution avec des paradigmes de systèmes plus récents.

6 Formats de descriptions de fichiers et de données

Ce chapitre «Formats de descriptions de fichiers et de données» définit les formats de descriptions de fichiers et de données qui doivent être utilisés pour l'échange de données. Un tableau indique à quelles interfaces S1, S2, S3 les formats correspondants doivent être appliqués. (Pour la définition de S1, S2, S3 cf. chapitre 4.2«Interfaces», page 19.) Exemple:

- Pour le format de fichier XZ, l'indication suivante est donnée.
- S1 S3
- Selon les recommandations faites, le format de fichier XZ doit être utilisé aux interface S1 (terminal-système) et S3 (système-centre de clearing), mais non pas à l'interface S2 (système-système).

Dans ce chapitre, nous distinguons entre les formats suivants de description de fichier et de données:

- Documents et descriptions correspondantes, voir chapitre 6.1
- Images et graphiques (dans les documents), chapitre 6.3
- Multimédias, voir chapitre 6.4
- Divers, voir chapitre 6.4.7 et suivants
- Concernant les recommandations en matière d'accessibilité, se reporter à ISO/IEC 40500-2012, ETSI EN301549 V.1.0, WCAG 2.0 et eCH 0059/0060.

6.1 Remarques

6.1.1 Concernant la sécurité

Un grand nombre des formats de fichier mentionnés dans ce chapitre ne sont équipés d'aucune mesure de sécurité. Si l'on veut transmettre des données confidentielles sous ces formats, on devrait utiliser en outre les mesures et technologies de sécurité adéquates, telles qu'elles sont mentionnées au chapitre 7.

6.2 Documents et descriptions correspondantes

6.2.1 Jeux de caractères et encodage

Encodage des caractères: afin d'accroître la compatibilité et l'interopérabilité des applications et des documents, les informations concernant les jeux de caractère utilisés doivent être mentionnées aux endroits appropriés pour qu'elles puissent être correctement lues par tout logiciel.

De manière générale, nous recommandons d'utiliser le format Unicode UTF-8 et de constituer des caractères spéciaux à partir de ce format. Si cela pose problèmes ou qu'il n'y a pas de compatibilité, il faut utiliser à la place le jeu de caractère ISO-8859-**15** (so in: Art. 80 de l'Ordonnance sur l'état civil), car celui-ci, contrairement à l'ISO-8859-**1**, couvre correctement le caractère € et les caractères spéciaux du français.

S1	S2	S3	
UTF 8 (8-bit UCS Transformation Format)			Vivement recommandé

Normes: IETF RFC 3629, ISO/IEC 10646-2014/Amd1-2015/Amd2-2016.

ISO/IEC 8859 Teil 1 bis 16	Recommandé

Norme: ISO/IEC 8859, le développement de cette famille de normes a été interrompu et elle est appelée à être remplacée par la famille UTF / ISO 10646-Familie.

6.2.2 CSS (Cascading Stylesheet)

Inventeur URL Håkon Wium Lie, Bert Bos Version 1, W3C Version 2 , www.w3C.org

La version 2 de Cascading Stylesheet (CSS) a été définie par le W3C sur la base de la version 1 et est utilisée, comme celle-ci, pour la définition de la présentation de contenus. CSS peut servir à la représentation des contenus XML, HTML et XHTML.

Utilisation

Définition de la représentation d'informations aux formats XML, HTML et XHTML

S1	
CSS (Cascading Stylesheet) Level 2 (CSS 2 et CSS 2.1)	Vivement recommandé

Normes: Cascading Style Sheets Level 2 (CSS 2) Specification, mai 1998 de W3C Cascading Style Sheets Level 2 Revision 1 (CSS 2.1) Specification, sept. 2011, CSS 2.2 2016 en cours d'élaboration (www.w3C.org) et en observation (notamment RFC 7993 Dec2016 Informational).

S1	S2	S3	
CSS (Cascading Stylesheet) Level 3			Recommandé

Remarque: les navigateurs actuels sont globalement compatibles avec la norme CSS 2.1 dans le domaine d'application clé (notamment HTML V.5 avec CSS Level 3).

6.2.3 CSV (Comma Separated Value List)

Inventeur URL Borland, www.borland.com

Les fichiers CSV sont des fichiers ASCII souvent utilisés pour coder et structurer un contenu extrait d'une base de données (p. ex. dBASE, ACCESS, banque de données SQL) afin de le reprendre dans une autre. Un enregistrement (ou bloc de données) correspond alors souvent à une ligne. Les cellules sont séparées par un caractère spécial, voir également à ce sujet RFC 4180.

Utilisation

Echange de données de produits et de plates-formes différentes

S1	S2	S3	
Comma Separated Value List (CSV)			Vivement recommandé

6.2.4 SIARD

SIARD (Software-Independent Archival of Relational Databases) est un format mis au point par les Archives fédérales suisses, qui est utilisé par plusieurs offices fédéraux suisses. . Il s'agit d'un format de fichier pour la conservation sur le long terme d'informations provenant de bases de données sur les relations. Le format SIARD repose sur les normes ISO/IEC 14721 Unicode, XML et les normes industrielles SQL 1999 et ZIP.

	S2	S3
SIARD V.2.0 (eCH 0165)		Vivement recommandé

Normes: ISO/IEC 14721 Open Arch.Information System (OASIS), ISO/IEC 10646 Unicode; voir aussi:

https://www.bar.admin.ch/bar/de/home/archivage/ablieferung/digitale-unterlagen.html

URL: http://www.ech.ch/vechweb/page?p=dossier&documentNumber=eCH-0165 .

6.2.5 EPS (Encapsulated Post Script)

Inventeur URL Adobe Systems, www.adobe.com

EPS est l'acronyme pour «Encapsulated PostScript». Le fichier EPS est élaboré avec un programme compatible PostScript et peut être repris dans un autre programme. Le terme «Encapsulated» (en français inclus, enveloppé) provient du fait que la partie PostScript du fichier est placée entre un préfixe et un suffixe contenant d'importantes informations sur le fichier.

Utilisation

Surtout dans l'industrie graphique, pour l'échange de données vectorielles, textes compris.

	S1	S2	S3
Encapsulated Post Script (EPS)			Non recommandé

La norme EPS a été remplacée par PDF dans la pratique et a donc perdu de son importance.

6.2.6 GML

Geographic markup language (GML) est un langage de description pour les objets spatiaux, qui sont utilisés pour l'échange de tout type de données géographiques.

	S1	S2	S3
GML V.3.2.x			Recommandé

Normes: ISO/IEC 19136-2007 et Part2-2015, ISO 19107-2003; eCH-0056/0118 s'applique pour l'utilisation (eCH0117). Voir également http://www.opengeospatial.org/standards/gml .

6.2.7 HTML (Hypertext Markup Language)

Inventeur URL Tim Berners-Lee, www.w3c.org

Hypertext Markup Language (HTML) est un langage normalisé pour la description des pages WWW dans internet ou intranet et contient également une structure de base.

Utilisation

Pour définir la présentation et le contenu de la page ainsi que les liens (liens hypertextes, renvois) vers les pages d'un autre ou du même site.

S1	S2	S3	
Hypertext Markup Language (HTML) V.4.01 (strict)			Vivement recommandé

Norme: ISO/IEC 15445-2000, HyperText Markup Language (HTML); Recommendation 24 December 1999, de W3C www.w3C.org.

Hypertext Markup Language (HTML) V.4.01 (transitional)			Vivement recommandé

HTML V.5.x			Vivement recommandé

Normes: ISO/IEC 15445; W3C (www.w3C.org). Remarque: pour des raisons d'interopérabilité, l'encodage doit être indiqué dans chaque document HTML.

6.2.8 Interlis

Développeur URL „Equipe centrale Interlis", www.interlis.ch

Interlis est un langage de description de données axées sur les objets de géoinformation et un mécanisme de transfert. Il est possible de déduire du modèle de données conceptuel des descriptions de format pour les différents formats de transfert (pour Interlis1 avec ITF, Interlis2 avec XTF, avec GML). Ce langage favorise la sélection ciblée des types de géo-données géométriques.

En Suisse, on distingue deux versions différentes d'Interlis utilisées. Version 1 (SN 612030) et version 2 (eCH-0031).

Utilisation

Pour les modélisations au moyen d'un langage de description de données et l'échange de données spatiales (informations géographiques), notamment pour les secteurs des mensurations cadastrales, de l'aménagement du territoire, de l'environnement ou de la circulation et autres domaines géographiques.

S1	S2	S3	
Interlis V.1			Recommandé

La version 1 d'Interlis (voir également www.snv.ch) devrait être remplacée par la version 2. Voir www.interlis.ch .

S1	S2	S3	
Interlis V.2.x			Vivement recommandé

Les normes eCH-0031/0117/0118 s'appliquent pour l'utilisation.

6.2.9 WFS

Les Web Feature Services (WFS) décrivent les données vectorielles des géo-données et des objets spatiaux, qui sont restitués à GML.

Utilisation

Pour l'échange de tout type de données géographiques

S1	S3	
WFS au moins V.1.0.0 / dans la mesure du possible V.1.1.0		Recommandé

Norme: ISO 19142 2010; Voir eCH-0056 ; http://www.opengeospatial.org/standards/wfs.

6.2.10 **WMS**

Les Web Map Services (WMS) sont utilisés par les systèmes de géo-informations.

Un Web Map Service (WMS) est une interface servant à consulter des extraits de cartes géographiques sur le World Wide Web. Un WMS est un cas particulier de Web Services.

S1	S3	
WMS au moins V.1.1.1 / dans la mesure du possible V.1.3.0		Recommandé

Normes: ISO 19128 2005 ; Voir www.W3C.org . eCH-0056 s'applique pour l'utilisation.

Voir également http://www.opengeospatial.org/standards/WMS

6.2.11 **LDIF**

Le **format** des données publiées avec LDAP est souvent LDAP Data Interchange Format (LDIF).

S1	S2	S3	
LDIF			Recommandé

Norme: RFC 2849.

6.2.12 **MIME (Multipurpose Internet Mail Extension)**

Inventeur URL IETF (N. Borenstein, T. Rose), www.ietf.org

Multipurpose Internet Mail Extension (MIME) est une norme IETF (www.ietf.org) pour les formats de fichiers et pour l'indication des types de fichiers transférés. L'importance de ces informations augmentera de plus en plus avec l'utilisation des éléments multimédias sur les pages www. Les types MIME sont utilisés lors de la communication entre serveurs et navigateurs www. Tant le serveur www que le navigateur gèrent une liste des types de fichiers qu'ils connaissent. Dans de nombreux navigateurs, cette liste se trouve dans les «applications auxiliaires» (helper applications). Lors du transfert de fichiers du serveur au navigateur, le type MIME est fourni via le protocole HTTP. Sur la base de sa liste des types MIME, le navigateur sait comment il doit traiter le fichier reçu selon les IETF RFC pertinents.

Utilisation

Développé à l'origine pour le courrier électronique, ce format d'échange de données - appelé aussi Multi-Part Mail - est maintenant également utilisé pour d'autres applications internet. Ainsi, des éléments Javascript et CSS peuvent être insérés dans un fichier HTML 4.0 et plus ou dans un fichier XHTML, avec une option type=«text/javascript» ou type=«text/css». Cette option signale l'inclusion d'un fichier d'un autre format. Cette méthode est également appliquée pour l'intégration de fichiers multimédias.

S1	S2	S3	
Multipurpose Internet Mail (MIME)			Vivement recommandé

Normes: RFC 2231, 3676, 3798, 4288, 5147, 6532, 6533, 6657 et autres pertinents.

6.2.13 **Format XML de Microsoft Office**

Inventeur URL Microsoft, www.microsoft.com

Microsoft a publié le format de fichiers XML pour Word (.docx), Excel, Visio et InfoPath. Les spécifications à ce sujet sont accessibles **moyennant licence, mais sans frais** à toute personne et lui permette d'utiliser ces formats dans ses propres applications sur n'importe quelle plate-forme. Cette autorisation englobe également les modifications futures de ces formats. Malgré la large diffusion de Microsoft Office, nous ne recommandons pas ce format de données parce que Microsoft préfère elle-même en utiliser un autre.

Utilisation

Plus pertinent; remplacé par les Office Open XML File Formats.

S1	S2	S3	
Format XML 2003 de Microsoft Office			Non recommandé

6.2.14 **ODF**

Inventeur URL OASIS, www.oasis-open.org et www.openoffice.org

ODF (Open Document Format) est un format de fichier basé sur XML destiné aux applications de bureautique pour l'échange de documents pouvant contenir du texte, des tableaux, des diagrammes et des éléments graphiques. Ce format de document peut être transformé simplement dans des formats alternatifs, car il intègre la plupart des normes existantes.

Utilisation

Echange, indépendant de l'application, de documents tels que textes, tableaux, formulaires, diagrammes ou graphismes

S1	S2	S3	
ODF V.1.0			Non recommandé

Normes: ISO/IEC 26300 ou par OASIS.

ODF V.1.1/1.2			Recommandé

6.2.15 Office Open XML File Formats

Inventeur URL ecma, www.ecma-international.org

Office Open XML File Formats se base sur XML et est un format, proposé par Microsoft et perfectionné par l'ECMA, qui peut être implémenté librement dans différentes applications et plates-formes.

Utilisation

Echange, indépendant de l'application, de documents tels que textes, tableaux, formulaires, diagrammes ou graphismes. Ce format a été conçu d'emblée de manière à ce que son codage soit compatible avec MS Office.

S1	S2	S3	
Office Open XML File Formats			Recommandé

Normes: ISO/IEC 29500:2008 (Part1-4). Il n'existe aucune implémentation ISO connue, mais des implémentations ECMA 376 1ère édition version (avec docx) sont disponibles.

6.2.16 PDF (Portable Document Format)

Inventeur URL Adobe Systems, www.adobe.com

Le Portable Document Format (PDF) est un format de fichier pour la représentation de documents sources quelconques; il conserve de manière (quasiment) complète les textes, les formatages, les couleurs et les graphismes, indépendamment du système d'exploitation et du programme avec lequel le document initial a été créé. PDF est un format orienté page pour la représentation de documents, contrairement à HTML qui ne définit pas de présentation fixe des pages transmises.

S1	S2	S3	
Portable Document Format (PDF) V.1.7 (selon ISO)			Vivement recommandé

Normes: ISO 32000-1:2008. PDF V.1.7 peut être lu à l'aide du programme Acrobat Reader, version 8.0 ou plus. Seuls les fonctions spécifiées dans la norme ISO mentionnée doivent être utilisées.

Portable Document Format (PDF) V.1.4, 1.5, 1.6	Recommandé

Normes: ISO 32000 Part1-3 avec corrigenda.

PDF V.1.4/ 1.5/ 1.6 peut être lu à l'aide du programme Acrobat Reader, version 5.0/6.0/7.0 ou plus.

6.2.17 PDF/A-1/2/3

PDF/A est une version normalisée par l'ISO du Portable Document Format. PDF/A n'offre qu'une partie des possibilités du format PDF, mais est spécialement adapté aux exigences de l'archivage à long terme et de l'absence de barrières pour les personnes handicapées ainsi que pour la restitution sur les terminaux mobiles tels que les PDA.

La norme est un sous-ensembe de PDF V 1.4, qui est spécifié dans ISO 19005-1:2005 (PDF/A-1) et définit deux niveaux de concordance:

- PDF/A-1a - Level A
- PDF/A-1b - Level B (exigences restreintes / exigences minimales)

La norme PDF/A-2 est un sous-ensemble de PDF V 1.7, qui est spécifié dans ISO 19005-2:2011 et définit trois niveaux de concordance:

- PDF/A-2a - Level A
- PDF/A-2b - Level B (exigences restreintes / exigences minimales)
- PDF/A-2u - comme 2b, mais l'ensemble du texte est représenté en Unicode

PDF/A-1 reste en vigueur. Les fichiers conformes avec PDF/A-1 satisfont également aux exigences du niveau de conformité correspondant PDF/A-2. Lorsque les fonctions de PDF/A-1 suffisent, il n'y a aucune raison de passer impérativement à PDF/A-2. En outre, PDF/A-2 propose notamment des possibilités d'utiliser des niveaux (transparents), d'intégrer des polices OpenType et d'utiliser des signatures numériques concordant avec les PAdES (PDF Advanced Electronic Signatures, ETSI TS 102 778). Par ailleurs, les fonctions de Container ont été spécifiées dans la 3ème version PDF/A.

Utilisation

Portable Document Format (PDF)/A-1	Vivement recommandé

Norme: ISO 19005-1:2005, Part 1 mit corrigenda: Use of PDF V.1.4 (PDF/A-1).

Portable Document Format (PDF)/A-2	Vivement recommandé

Norme: ISO 19005-2:2011, Part 2: Use of ISO 32000-1 (PDF/A-2); voir chap.Archivage

Portable Document Format (PDF)/A-3	Recommandé

Standard : ISO 19005-3 :2012, Part 3 : Use of ISO 32000-1 (PDF/A-3)

Remarque concernant PDF/A-3 – uniquement pour une durée d'archivage limitée ex. archives d'une entreprise respectivement par pour un archivage permanent: http://kost-ceco.ch/cms/index.php?pdf-a-2_3_study_de.

6.2.18 **PDF/UA/VT/E/H**

Les normes PDF Universal Access (UA), PDF pour la gestion des outputs (VT), PDF Engineering und PDF Health Care sont des formats pour des utilisations spécifiques.

	S1	S2	S3
Portable Document Format (PDF) UA/VT/E/H			Recommandé

Normes: ISO 14289 2014 pour PDF/UA (=Universal Access), ISO 16612-2 2010 pour PDF/VT (= Variable and Transactional Printing, Outputmanagment), pour PDF/H (= Health care; encore aucun ISO disponible), ISO 24517 2008 pour PDF/E (=Engineering, CAD/CAM).

6.2.19 PDF/X

PDF/X est une version normalisée du Portable Document Format, qui a été adaptée aux exigences de l'industrie de l'imprimerie envers les modèles d'impression. PDF/X n'offre donc elle-même qu'un sous-ensemble des caractéristiques techniques du format PDF. Cette norme interdit les contenus PDF qui peuvent nuire à la prévisibilité du résultat de l'impression (fonctions de transfert, transparences) ou qui ne peuvent pas être imprimés de manière utile (vidéo, audio), et formule des prescriptions à respecter pour la communication précise avec le prestataire de service d'impression (coupe, désignation des couleurs, etc.).

Utilisation

Echange de données d'affichage dans l'industrie des journaux et des revues ou pour la transmission de modèles dans le cadre d'ordres d'impression.

Portable Document Format (PDF) X1/3/4	Recommandé

Norme: ISO 15930 Serie (Part 1, 3, 4, 6 à 8 avec corrigenda).

Remarque: PDF/X-3 2002 est utilisé principalement en Europe

Portable Document Format (PDF) X/8	En observation

Normes: ISO 15930-6/7/8:2010 (corrigenda 1-2011).

Remarque concernant les versions: là encore, on a recours à la directive PDF-X/A-1. La version à utiliser dans un ordre doit être convenue entre le créateur des modèles d'impression et le prestataire des services d'impression.

6.2.20 PS (Post Script)

Inventeur URL Adobe Systems, www.adobe.com

Lancé sur le marché en 1984 par Adobe System Inc., Post Script (PS) est un langage de description de pages, pour l'impression et l'enregistrement page par page de graphismes et de textes. Le logiciel travaille indépendamment du système, de la taille des caractères et de la résolution. La qualité de l'impression se base uniquement sur les possibilités techniques du périphérique de sortie.

Utilisation

Langage de description de pages pour imprimantes ou développeur de film.

	S1	S2	S3	
Post Script V.3				En observation

Voir également: http://www.adobe.com/products/postscript/ .

6.2.21 ePUB

ePUB est une norme publique pour les livres numériques, qui repose sur un certain nombre de normes libres de droits, dont les principales sont XML, XHTML, CSS, NCX (de DTBook), Dublin Core et ZIP. Comme pour PDF, les données sont fournies indépendamment de l'appareil. Les documents ePUB permettent d'adapter de manière dynamique le format du texte aux dimensions de l'écran de l'appareil d'affichage et conviennent ainsi tout particulièrement aux appareils mobiles et autres lecteurs de livres numériques. On préférera ePUB

aux formats spécifiques aux constructeurs; dans bien des situations, des HTML ou PDF conventionnels devraient toutefois être mis à la disposition du lecteur.

S1

ePUB V.3.0.x	Recommandé

Norme: http://idpf.org/epub du International Digital Publishing Forum (IDPF), DRM.

6.2.22 RDF (Resource Description Framework)

Inventeur URL W3C, www.w3C.org

RDF signifie «Resource Description Framework», c'est-à-dire cadre de description des ressources, et représente une application XML servant à décrire des ressources, telles que textes, images, logiciels, etc. Les informations présentées dans RDF sont des métadonnées, qui constituent en fait des informations sur une informations, telles que source, auteur, copyright ou adresses.

Utilisation

Sert de complément à la désignation d'un fichier, en indiquant la source, l'auteur, le numéro ISBN, etc.

S1 S2 S3

RDF (Resource Description Framework) V.1.0/1.1	Recommandé

Norme: Resource Description Framework Model et Syntax Specification Recommendation, RDF V.1.1 2014, norme de W3C.

6.2.23 Newsfeeds (ATOM, RSS)

Les portails, qui mettent rapidement en ligne les nouveautés et veulent proposer ce service dans le cadre d'un abonnement (publish and suscribe), utilisent l'un des formats pour les Newsfeeds. Ainsi, la réception de l'information se fait non pas en raison de l'action du lecteur (Pull) comme cela est habituellement le cas sur Internet, mais de manière automatique après la mise en ligne par l'auteur (Push). Ces formats reposent sur XML et proposent une étendue variable de tags. A l'heure actuelle, ces trois formats sont en règle générale supportés par les logiciels correspondants:

S1

RSS V.2.0	Vivement recommandé

Spécification: RSS V.2.0, RSS Advisory Board, http://www.rssboard.org/rss-specification .

RSS V.1.0 et autres versions	Recommandé

Spécification: W3C, http://web.resource.org/rss/1.0/spec .

Atom Publishing Protocol, AtomPub V.1.0	Recommandé

Normes: RFC 4287, 5023, 5988 2010. Spécification: Atom V.1.0 voir AtomEnabled.org .

http://atomenabled.org/developers/syndication/ .

6.2.24 RTF (Rich Text Format)

Inventeur URL Microsoft, www.microsoft.com

RTF (Rich Text Format) était développé pour transférer des textes formatés, avec graphismes, entre différents programmes de traitement de texte. Inconvénient du format RTF: il ne prend pas en compte toutes les possibilités de formatage des traitements de texte complexes.

Utilisation

Format pour l'échange de textes formatés.

S1	S2	S3	
Rich Text Format (RTF) V.1.9			Recommandé

La spécification peut être obtenue auprès de Microsoft.

6.2.25 WML (Wireless Markup Language)

Inventeur URL OMA, www.openmobilealliance.org

Wireless Markup Language, WML en abrégé, basé sur XML.

Utilisation

Pour la transmission efficace de textes et d'images à destination et en provenance d'appareils mobiles.

S1	S2	S3	
WML (Wireless Markup Language) V.2.0			En observation

Contrairement à la version 1, la version 2 de WML contient XHTML pour systèmes mobiles en tant que sous-ensemble et intègre CSS.

6.2.26 XHTML (eXtensible Hypertext Markup Language)

Inventeur URL W3C, www.w3C.org

XHTML (eXtensible Hypertext Markup Language) est un langage de description de données et de structures pour le WWW, basé sur XML. Il s'agit de l'adaptation de HTML 4.0 dans XML 1.0, de manière à pouvoir coder des pages Web en format XML en tant que fichiers structurés. XHTML est censé remplacé HTML comme format de présentation ou de document pour les pages Web.

Utilisation

Présentation de contenus sur le World Wide Web.

S1	S2	S3	
eXtensible Hypertext Markup Language (XHTML) V.1.0 strict			Vivement recommandé
eXtensible Hypertext Markup Language (XHTML) V.1.0 transitional/frameset			Recommandé

eXtensible Hypertext Markup Language (XHTML) V.1.1/V.2.0	En observation

Normes: XHTML V.1.0/1.1/2.0 2010 de W3C.

6.2.27 XML (eXtensible Markup Language)

Développeur URLW3C, www.w3C.org

Le XML (eXtensible Markup Language) est un langage générique indépendant des plates-formes, qui utilise un format de donnés particulier. Ce langage est normalisé par le W3C depuis février 1998.

Le document XML possède un contenu structuré, mais sans formatage défini (présentation). Les éléments du contenu sont définis par le langage de déclaration DTD (Document Type Definition) ou par le langage de déclaration XSDL (XML Schema Definition Language), plus récent et plus complet. XML repose sur ces normes de base non décrits plus avant dans SAGA.ch: les jeux de caractère Unicode, URI pour les espaces nominatifs XML et pour l'adressage ainsi que les normes ISO notamment pour nommer les pays et les langues.

Utilisation

XML définit des structures de données et de documents.

	S1	S2	S3	
eXtensible Markup Language (XML) V.1.0				Vivement recommandé

eXtensible Markup Language (XML) V.1.1/2.0	Recommandé

Norme: Extensible Markup Language (XML) Recommendation de W3C www.w3C.org. Voir également eCH-0018/0033/0035/0036/0050; IETF RFC 3470.

6.2.28 XML-Schema

Développeur URLW3C, www.w3C.org

XML Schema est un langage de description de format basé sur XML pour les formats de transfert XML, notamment pour les descriptions de modèles de contenus et la déclaration des éléments (structures et types de données).

Utilisation

XML Schema sert à déclarer des contenus et les types de données XML.

	S1	S2	S3	
XML-Schema Part 0,1,2,3				Vivement recommandé

Concernant les normes et les versions, voir eCH-0036/0062.

6.2.29 Document Schema Definition Languages (DSDL)

Dans certaines applications XML, quelques-unes des 11 parties de ce cadre (en particulier RELAX NG, Schematron et DTD capable des espaces nominatifs XML) sont utilisées pour le modelage des données et la validation. Toutefois, on utilise la plupart du temps le schéma XML pour cette tâche.

S1	S2	S3	
Document Schema Definition Languages (DSDL)			Recommandé

Normes: ISO/IEC 19757 (toutes les parties avec corrigenda 2016).

6.2.30 XBRL (eXtensible Business Reporting Language)

Inventeur URL XBRL International, https://www.xbrl.org/

XBRL est un langage basé sur XML destiné à l'impression d'informations d'affaires et financières. Afin de couvrir les besoins propres à la branche, différents domaines d'application ou divers standards de comptabilité, on utilise des « taxonomies » distinctes. Les « juridictions nationales » sont compétentes pour la définition complémentaire de taxonomies supplémentaires conformément aux besoins locaux ou nationaux, en Suisse il s'agit de l'association XBRL CH; http://xbrl-ch.ch/

S1	S2	S3	
eXtensible Business Reporting Language (XBRL) V.2.1/2.2/3			Recommandé

6.2.31 XSL (eXtensible Stylesheet Language)

Inventeur URL W3C, www.w3C.org

XSL (eXtensible Stylesheet Language) définit la représentation ou l'aspect visuel d'une classe de documents XML. La normalisation de la représentation des documents XML comprend essentiellement:

- XSLT (XSL Transformations), un langage de conversion de documents XML dans d'autres formats XML ou en simple texte;
- XPath (XML Path Language), un langage permettant de référencer des éléments de documents XML (nœuds ou ensembles de nœuds) ou d'atteindre des parties de ceux-ci;
- XSL-FO (XSL Formatting Objects), un langage décrivant sous quel aspect les pages XML sont présentées au lecteur.

Les trois langages ci-dessus sont regroupés dans la norme XSL.

Utilisation

XSL sert à la conversion de documents XML dans d'autres formats, tels que des formats XML ou des documents HTML, ainsi que pour la sortie formatée (avec XSL-FO) p. ex. dans des documents PDF ou RTF.

S1	S2	S3	
eXtensible Stylesheet Language (XSL) V.1.0 (XSL-FO)			Non recommandé

Normes: Extensible Stylesheet Language (XSL), W3C V.1.0, 15 Oct.2001.

eXtensible Stylesheet Language (XSL) V.1.1 (XSL-FO)			Vivement recommandé

Normes: Extensible Stylesheet Language (XSL) V.1.1, W3C 5.Dec.2006.

XSL Transformations (XSLT) V.1.0 (mit XPath V.1.0)			Vivement recommandé

Normes: XSL Transformations (XSLT) V.1.0, W3C Rec. 16 Nov.1999.
XML Path Language (XPath) V.1.0, W3C Rec. 16 Nov.1999.

XSL Transformations (XSLT) 2.0 (mit XPath 2.0)	Recommandé

Normes: W3C XSL Transformations (XSLT) V.2.0, W3C Rec. 23.Jan. 2007, XML Path Language (XPath) 2.0; XSLT 3 Working Draft 2015 (www.w3C.org).

Remarque: eCH dispose de toute une série de documents (normes et meilleures pratiques) concernant XML. Les documents les plus récents peuvent être téléchargés sur le site www.ech.ch. Les XML XSL XSLT sont en cours de développement.

6.2.32 **XForms**

Inventeur URL W3C, www.w3C.org

XForms est une norme W3C pour les formulaires électroniques et les éléments interactifs d'une interface utilisateur. XForms est structurée selon le principe Model-View-Controller (MVC)et sépare par conséquent les champs de données (p. ex. XML Schema), la représentation (p. ex. HTML) et l'exécution (p. ex. ECMA Script). XForms peut envoyer des données XML au serveur. Les XForms peuvent être générées et traitées au moyen d'outils XML. En cas d'utilisation recommandée de XForms côté serveur, les formulaires sont convertis en HTML et envoyés ainsi au navigateur. L'utilisation directe, qui exige de l'utilisateur l'installation d'une extension de navigateur, n'est pas recommandée.

Utilisation

Enregistrement, édition, stockage et affichage d'unités d'information dans les champs de formulaire.

S1 **S2** **S3**

XForms V1.1/2.0. (utilisation server-side)	Recommandé

Norme:XForms V.1.1, W3C Rec. 20 Oct. 2009, V.2.0 2013 de W3C.

6.2.33 **JSON**

JSON est une structure de description des données (en lieu et place de XML) et est fréquemment employé pour Javascript, AJAX ou Rest API.

S1 **S2** **S3**

JSON	Recommandé

Norme: ISO/IEC 20802-2 2016, IETF RFC 7159, voir aussi spécifications Javascript/AJAX/Rest API et autres normes pertinentes.

6.2.34 **ADMS**

L'Asset Description Metadata Schema (ADMS) définit un modèle normalisé de métadonnées (spécifié par l'administration publique européenne ISA pour l'interopérabilité). ADMS permet de décrire des Semantic Assets de façon semblable dans les domaines d'activités (notamment les organismes de normalisation, les établissements académiques), afin de permettre une planification «seamlessly cross-queried and discovered». SAGA n'émet aucune recommandation quant aux métadonnées, mais renvoie à un bon exemple d'«attributs de géodonnées de géo-normes» par delà les limites de l'application.

ADMS V.2.0	En observation

Norme: W3C working group : http://www.w3.org/TR/vocab-adms ; voir EU : https://joinup.ec.europa.eu/asset/adms/description . Voir notamment aussi CAMS /DCAT .

6.2.35 **OAI-PMH**

Le protocole OAI basé sur XML et REST et destiné au Metadata Harvesting a été conçu afin de rendre de grands volumes de données de publications électroniques plus faciles à trouver sur Internet et plus utiles. Les jeux de données de titre sont mis à disposition par les fournisseurs (ex. bibliothèques nationales). Compte tenu du grand nombre de formats de métadonnées, le plus petit dénominateur commun prescrit est le modèle de données Dublin Core; l'extension à des formats supplémentaires, comme MARC par exemple, au moyen de MARCXML est toutefois recommandée et est également mise en pratique.

S1	S2	S3	
OAI-PMH V.2			Recommandé

Normes: ISO 15489-1 2016, eCH 169/175.

Open Archives Initiative Protocol for Metadata Harvesting Version 2.0 du 2002-06-14, document version 2015-01-08: http://www.openarchives.org/OAI/openarchivesprotocol.html

http://www.openarchives.org/OAI/2.0/guidelines-rights.htm

6.2.36 **Dublin Core (DC)**

Les éléments de Dublin Core sont un jeu d'éléments servant à la description des documents (œuvres ou autres objets). Outre les données techniques (ID, format, type de données/fichier, langue, date), les descriptions de contenu (titre, mots clé, description etc.), les indications de source (auteur, détenteur des droits etc.) et les connexions (relations avec les autres objets, comme les copies sous d'autres formats, les versions antérieures etc.), d'autres renseignements détaillés peuvent être enregistrés avec ce que l'on appelle les Refinements (licenses, derniers renseignements modifiés, remplace renseignements, etc.).

Les éléments Dublin Core sont souvent utilisés dans les documents (MS Word, OpenDocumentFormat, PDF) et devraient être utilisés sous la forme de Meta-Tags pour la description des pages HTML.

S1	S2	S3	
Dublin Core			Vivement recommandé

Normes: Dublin Core Metadata Initiative (DCMI), Dublin Core Metadata Element Set, Version 1.1 (ISO 15836:2009 plus corrigenda1 2009, ANSI/NISO norme Z39.85-2012, IETF RFC 5013 Aug.2007) les extensions : http://dublincore.org/documents/dcmi-terms/

6.2.37 **MoReq**

MoReq (Modular Requirements for Records Systems) sera un jour la norme européenne pour le Records Management électronique. Elle a été à l'origine mise au point afin d'harmoniser l'échange de documents entre la Commission européenne et les gouvernements des Etats-membres. Bien que la norme n'ait pas été élaborée par un organe de normalisation officiel (ISO par exemple), elle s'est depuis établie par delà les frontières de l'Europe en tant que norme de facto pour la gestion électronique des documents, archives et

écrits. Lors de l'élaboration de MoReq2, des compléments tirés des documents sources pertinents comme l'ISO 15489, l'ISO 23081 et l'ISO 14721 par exemple, ainsi que la norme allemande DOMEA et la spécification UK TNA 2002 ont été pris en compte, MoReq2010 est structurée de façon modulaire et en tant que services.

S1	S2	S3	
MoReq1			Non recommandé
MoReq2 (V.1.1)			Vivement recommandé
MoReq2010			En observation

Normes: ISO 15489-1 2016, MoReq2, MoReq2010 avec spécifications UE pertinentes.

6.3 Images et graphiques

6.3.1 GIF (Graphics Interchange Format)

Inventeur URL Compuserve, www.compuserve.com

GIF est l'abréviation de «Graphics Interchange Format», en français format d'échange d'images. GIF est le format le plus important, avec JPEG, pour l'enregistrement d'images de manière adaptée à la représentation sur les navigateurs. Les images GIF peuvent contenir au maximum 256 couleurs et sont adaptées surtout pour les graphismes, les logos ou les signatures. (JPEG prend par contre en charge le mode "True Color" et convient mieux pour les photos!). GIF permet en outre une compression sans perte et la possibilité de définir une couleur transparente.

S1	S2	S3	
Graphics Interchange Format (GIF) 89a			Vivement recommandé
Graphics Interchange Format (GIF) 87a			Non recommandé

6.3.2 JPEG (Joint Photographic Expert Group)

Inventeur URL JPEG (Joint Photographic Expert Group), www.jpeg.org

Joint Photografic Expert Group (JPEG) est une commission qui définit des modes de compression et d'enregistrement de données images et vidéo. JPEG permet en outre une compression sans perte et la représentation de plus de 16 millions de couleurs.

S1	S2	S3	
Joint Photographic Expert Group (JPEG / JPG)			Vivement recommandé

Normes: ISO/IEC 10918-1. JPEG XR à l'avenir sur le modèle d'ISO/IEC 29199-2.

6.3.3 JPEG 2000

JPEG 2000 est un format graphique pour les graphiques en matrice avec compression d'image, un perfectionnement du format JPEG et PNG. Faute de compatibilité permanente avec les navigateurs, le format peut parfois être déconseillé pour les administrations publiques. Remarque: JPEG2000 est utilisé dans les applications internes comme les archives.

S1	S2	S3	
JPEG 2000 (pour applications internes)			Recommandé

Norme: ISO 15444-1 2016. Voir également IETF RFC 5371, 5372.

6.3.4 PNG (Portable Network Graphics)

Inventeur URL W3C, www.w3C.org

PNG (Portable Network Graphics) est un format de fichier développé et normalisé par le World Wide Web Consortium (W3C).

S1	S2	S3	
Portable Network Graphics (PNG)			Vivement recommandé

Norme: ISO/IEC 15948, IETF RFC 2083; PNG Rec.10 Nov.2003, de W3C.

6.3.5 SVG (Scalable Vector Graphics)

Inventeur URL W3C, www.w3C.org

Scalable Vector Graphics (SVG) est une application XML, recommandée par le World Wide Web Consortium (W3C), permettant de décrire des images et des animations vectorielles bidimensionnelles, qui peuvent être intégrées dans des pages internet. SVG prend en compte trois sortes d'images:

- images géométriques vectorielles (p. ex. lignes et courbes),
- images à base de pixels et
- texte

S1	S2	S3	
Scalable Vector Graphics (SVG) V.1.1/1.2			Recommandé

Norme: Scalable Vector Graphics (SVG) V.1.1 2003 second Edition 2011, V.1.2. de W3C www.w3C.org . La version 2 est encore en cours de finalisation et d'examen en 2016.

6.3.6 TIFF (Tagged Image File Format)

Inventeur URL aldus/adobe, www.adobe.com

TIFF (Tagged Image File Format) est un format de fichier et une norme pour les images à base de pixels. Cette norme a été développée par Aldus, Hewlett Packard et Microsoft comme format de sortie pour les scanners. La plupart des programmes graphiques qui traitent des images à base de pixels prennent ce format en charge. TIFF est utilisé principalement dans l'archivage numérique, parfois aussi pour l'échange sans perte de données d'image (bitmap).

	S1	S2	S3	
Tagged Image File Format (TIFF) V.5.0				Non recommandé

Tagged Image File Format (TIFF) V.6.0	Vivement recommandé

Normes: ISO 12234-2 2001, 12639 2004 plus Amd.2007, IETF RFC 3302, 3950 et autres pertinents.

6.4 Multimédias

6.4.1 MPEG (Motion Pictures Expert Group)

Inventeur URL MPEG (Motion Pictures Expert Group), www.mpeg.org

MPEG (Motion Picture Expert Group) a défini et définit encore des formats de fichiers et des techniques permettant de comprimer et d'enregistrer des données vidéo ou multimédias (vidéo, image et son) à un haut niveau de qualité. Il existe plusieurs normes MPEG.

6.4.1.1 MPEG-1

MPEG-1 permet des taux de compression atteignant 1,5 mégabits par seconde (Mbps) environ et est utilisé surtout pour le codage des CD vidéo. MPEG-1 Audio Layer III est le nom complet du format audio MP3. **Celui-ci nécessite une licence, non gratuite**, tant pour le codage et le décodage que pour la simple transmission de contenus (streaming, transmission de fichiers).

MPEG-1	Recommandé

Norme: ISO/IEC 11172 Part 1-5 (avec différents corrigenda), ISO/IEC 14496.

6.4.1.2 MPEG-2

MPEG-2 est la norme prévue pour la télévision numérique, les «set-top boxes» et les DVD. **MPEG-2 nécessite une licence, non gratuite**, pour le codage et le décodage ainsi que pour la transmission de contenus!

MPEG-2	Recommandé

Norme:ISO/IEC 13818, 14496.

6.4.1.3 MPEG-4

Pour simplifier, on peut considérer MPEG-4 comme une extension technique (pour les débits à partir de 64 kbit/s) de MPEG 1 et 2 et permet l'utilisation de nouvelles méthodes optimisées pour la compression de contenus vidéo et audio. **MPEG-4 nécessite une licence, non gratuite**, pour le codage et le décodage ainsi que pour la transmission de contenus. Ce format existe en plusieurs versions, compatibles vers le bas, c'est-à-dire que la version 2 (de 1999) comprend la version 1 (1998), etc. Nous en sommes actuellement à la version 3. Toutefois, comme pour tous les autres formats audiovisuels, c'est le profil utilisé qui importe surtout, car il définit l'algorithme de compression.

Utilisation

Echange de films et d'animations.

S1	S2	S3	
MPEG-4			Vivement recommandé

Norme: ISO/IEC 14496 (all Parts); Voir développements ultérieurs MPEG7 et pertinentes.

6.4.2 MP3/MP4

Voir chapitre 6.4.1.1/6.4.1.3 pour MP4 (voir normes ISO/IEC 14496 Parts 12/14).

6.4.3 OGG

Inventeur URL Xiph.org Foundation, www.xiph.org

Ogg est une famille de formats de données (formats bitstream) développés par la fondation Xiph.org. Le plus connu est Ogg Vorbis, un format ouvert, du domaine public, et développé pour faire concurrence à MP3. Citons aussi Ogg Theora, un format vidéo ouvert, du domaine public, et développé pour faire concurrence aux formats payants MPEG-4, RealVideo et Windows Media Video.

Utilisation

Echange de données audio et vidéo.

S1	S2	S3	
OGG Theora			En observation

OGG Vorbis/FLAC			Recommandé

Norme: RFC 5354 (Ogg Bitstream Format).

6.4.4 QT (QuickTime)

Inventeur URL Apple Macintosh

QuickTime (QT) est un format de données multimédia développé par Apple et pouvant enregistrer des données de différents types (vidéo, audio, etc.). **En règle générale,** QuickTime **nécessite une licence, qui est toutefois gratuite**, pour le codage et le décodage ainsi que pour la transmission de contenus. Il est disponible pour les systèmes d'exploitation Macintosh OS, Windows, ainsi que Linux avec certaines restrictions.

Utilisation

Pour l'enregistrement et l'échange de données audio et vidéo.

S1	S2	S3	
QT (QuickTime) V.6.5			Non recommandé

6.4.5 WAVE (WAVEform audio format)

Inventeur URL Microsoft

WAV (WAVEform audio format) est une variante du format bitstream RIFF pour l'enregistrement de données audio à l'aide de différents algorithmes. Parmi ceux-ci, le plus utilisé est la modulation PCM, sans compression et sans perte, qui peut être considérée

comme norme de fait pour les données audio et est supporté sur pratiquement toutes les plates-formes. WAV n'est pas soumis à licence et peut être utilisé gratuitement.

Utilisation

Pour l'enregistrement de données audio.

S1	S2	S3	
WAV (WAVEform audio format)			Vivement recommandé

Norme: http://www.tactilemedia.com/info/MCI_Control_Info.html

6.4.6 WMV/A (Windows Media Video/Audio)

Inventeur URL Microsoft

WMV/A (Windows Media Video/Audio) est l'appellation donnée à toute une série de technologies vidéo et audio développées par Microsoft et faisant partie du «Windows Media Framework». WMV/A a été choisi comme nouveau standard industriel pour les DVD haute définition (HD). Il nécessite une **licence, qui est toutefois gratuite** en règle générale, pour le codage et le décodage ainsi que pour la transmission de contenus. Il est disponible sur les systèmes d'exploitation Macintosh OS, Windows, Solaris et Linux.

Utilisation

Pour la transmission et l'enregistrement de données audiovisuelles.

S1	S2	S3	
WMV/A (Windows Media Video/Audio) V.9.x			Recommandé

Norme: http://msdn.microsoft.com/en-us/library/bb331849(VS.85).aspx .

6.4.7 SWF file format (Adobe Flash Player)

SWF est un format de données permettant de transmettre des graphiques vectoriels, du texte, de la vidéo, de l'audio via l'Internet pour être lus avec le plugin de navigateur de la société Adobe, un langage de script étant également supporté, ce qui permet des applications interactives.

Des problèmes de sécurité récurrents ont été constatés avec ce plugin de navigateur. Des problèmes qui peuvent être évités en n'installant pas le plugin.

Le format est documenté publiquement, mais n'est pas une norme publique: en dehors du plugin de navigateur de la société Adobe, il n'existe aucune autre implémentation intégrale dans un plugin de navigateur. L'amélioration du format est décidée par une seule société.

S1	
SWF file format	Non recommandé

6.4.8 SMIL

SMIL est une norme ouverte mise au point par W3C d'un langage de description basé sur XML pour le positionnement synchronisé dans le temps et l'espace d'un ou de plusieurs objets médias dans les produits multimédias.

SMIL V.3	En observation

Norme: W3C http://www.w3.org/TR/2008/REC-SMIL3-20081201/

Informations: TTML1 (Time Text Markup Language) a été identifié comme une nécessité dans le cadre de SMIL. TTML sert à la commande lorsque des textes de sites Web ou des films (ex. MPEG-4) sont visibles. Ceci est particulièrement pertinent pour l'échange entre systèmes d'auteurs.

6.5 Divers

6.5.1 Compression

6.5.1.1 GZIP (Gnu ZIP)

Inventeur Abraham Lempel, Jacob Ziv, Terry Welch

GZIP sert à la compression de données sans perte d'information et est une version open source, qui était à l'origine contenue dans les systèmes d'exploitation UNIX, mais aujourd'hui disponible dans les systèmes d'exploitation courants. GZIP se base sur le même algorithme que ZIP et a été normalisé dans l'IETF RFC 1952.

Utilisation

Compression de données sans perte d'information.

S1 **S2** **S3**

GZIP (Gnu ZIP) V.4.x	Recommandé

6.5.1.2 ZIP

Inventeur A. Lempel, J. Ziv

ZIP est une méthode de compression sans perte d'information qui permet de conserver intégralement les données originales, ce qui est indispensable pour les programmes, les textes ou les tableaux (ex. les logiciels tels que Winzip travaillent selon cette méthode).

Utilisation

Echange de données sous forme comprimée.

S1 **S2** **S3**

ZIP V.6.x	Vivement recommandé

Référence à la norme: www.pkware.com; IETF RFC 1950, 1951 (Status Informational).

6.5.1.3 TAR

La combinaison GZIP/TAR devrait toujours être préférée au format ZIP (version2), lorsque de nombreux fichiers de même type doivent être comprimés en une même archive, car GZIP compresse les informations redondantes par delà les limites des fichiers, ce qui permet d'atteindre un taux de compression plus élevé.

S2 **S3**

TAR V.2 (Archive notamment avec GZIP)	Recommandé

Norme: ISO/IEC 9945 2009 (avec corrigenda1 2013).

Informations: voir aussi IETF RFC 1951/1952 et autres pertinents notamment d'IEEE.

6.5.2 SMS (Short Message Service)

Inventeur URL ETSI / SMS Forum, www.ETSI.org / www.smsforum.net

SMS signifie Short Message Service et a été spécifié par l'ETSI et le SMS Forum pour l'échange de données entre téléphones portables. En principe, SMS n'offre aucune sécurité. Par conséquent, l'échange de messages SMS ne devrait avoir lieu que si la communication, la modification ou la perte de leur contenu n'entraîne aucune conséquence regrettable.

Utilisation

Surtout pour la transmission de données en provenance et à destination de téléphones mobiles.

	S1	S2	S3	
SMS (Short Message Service)				Recommandé

Référence à la norme: www.3gpp.org .

6.6 Composantes exécutables dans des fichiers

Certains fichiers (HTML, etc.) peuvent aussi intégrer des programmes tels que JavaScript qui seront exécutés seulement chez le destinataire (client) des données. Ces programmes sont appelés composantes exécutables. L'utilisation non contrôlée de données comprenant des composantes exécutables peut entraîner de graves problèmes de sécurité, voir aussi [Nem]. C'est pourquoi les composantes exécutables ne devraient être acceptées que si elles sont signées, le certificat de vérification de la signature devant avoir été établi par un service de certification digne de confiance.

Composantes exécutables non signées, telles qu'ActiveX, Applets, non recommandé

Il est possible de déroger au principe des Applets signés en prenant le concept de sécurité pour justification. L'Application Owner est responsable de la sécurité (dans l'AF selon un concept ISDS; la conformité WIsB s'applique également).

6.6.1 Java Script

Inventeur URL Brendan Eich, Netscape Communication

Utilisation

JavaScript est un langage de programmation indépendant de toute plate-forme. Les programmes JavaScript sont intégrés essentiellement dans HTML ou XML pour lancer des processus ou mettre en forme des données chez le client.

	S1	
JavaScript		Recommandé

L'utilisation de JavaScript est autorisée, mais elle n'est pas sans risque. Le meilleur moyen d'éviter ces risques est de l'utiliser de manière restreinte et appropriée. Les sites Web devraient être utilisables même quand Javascript n'est pas activé dans le navigateur.

Norme: voir notamment aussi ISO/IEC 16262-2011.

6.6.2 ActiveX

Inventeur URL Microsoft

Utilisation

Pour l'intégration de données et de programmes multimédias dans des applications ou des fichiers Web. ActiveX est utilisé pour la communication d'applications croisées (Cross Applications).

S1

ActiveX signé	En observation

Norme: http://msdn.microsoft.com/en-us/library/aa751972(VS.85).aspx

6.6.3 Java Applets

Inventeur URL Sun Microsystems

Utilisation

Java est un langage de programmation indépendant de toute plate-forme. Les programmes Java peuvent aussi être intégrés dans des sites Web ou d'autres applications.

S1

Java Applets V.1.6 signées	Recommandé

Normes: JCP (Jave community process) et recommandations de sécurité[8].

Recommandation: Si l'exécution de composantes actives est autorisée chez le destinataire, un contrôle actualisé de sécurité du contenu devrait y être activé afin d'analyser les données reçues pour bloquer les contenus dangereux (composantes).

6.6.4 . Net Assembly

Inventeur URL Microsoft

Utilisation

Dans Microsoft .NET Framework (ou Mono), un Assembly est une bibliothèque de programmes partiellement compilés. Dans les implémentation Microsoft Windows de .NET, un Assembly est un fichier transférable (*portable*) et exécutable.

S1

.Net Assembly signé	En observation

6.6.5 AJAX

Inventeur Jesse James Garrett

Utilisation

[8] Compléments:JAVASecurityOverview - http://docs.oracle.com/javase/7/docs/technotes/guides/security/overview/jsoverview.html

-Overview-AppletSecurityBasics - http://docs.oracle.com/javase/6/docs/technotes/guides/plugin/developer_guide/security.html

-WhatAppletsCanandCannotDo - http://docs.oracle.com/javase/tutorial/deployment/applet/security.html

AJAX, abréviation anglaise signifiant Asynchronous JavaScript and XML, est une technique de développement d'applications Web interactives. AJAX vise à concevoir les pages Web de manière qu'il ne soit pas nécessaire de les recharger si elles sont modifiées. Ainsi, la vitesse de transfert perçue et le nombre d'interactions possibles sont augmentés.

S1

AJAX Files	Recommandé

AJAX doit être préféré à d'autres alternatives, en particulier les alternatives spécifiques aux fabricants. Javascript est une condition préalable impérative, voir à ce sujet (risques de sécurité).

7 Sécurité

La sécurité des données est importante pour assurer la réalisation et le bon fonctionnement des services (p. ex. services web) dans le cadre des applications de cyberadministration. Elle constitue à la fois la base et le catalyseur de la communication sécurisée entre les citoyens se faisant mutuellement confiance, entre les autorités[9] et les citoyens ainsi qu'entre les autorités et l'économie. La confiance des utilisateurs est ébranlée, entre autres, lorsque des pannes se produisent, que la validité juridique de la transaction peut être mise en doute ou que les processus se déroulent d'une manière peu fiable et non transparente[10] pour les parties impliquées.

La sécurité des données est à considérer comme une thématique permanente, qui peut ou doit être assurée, en fonction des besoins et des exigences, par des méthodes adéquates sur tous les segments de la communication. L'utilisation des moyens techniques et organisationnels doit être aménagée de manière que:

- les instances se faisant mutuellement confiance puissent établir entre elles une communication sécurisée.
- la protection minimale soit possible.
- les besoins de protection classiques soient satisfaits.
- les conditions juridiques de base soient remplies.

L'importance des mesures de sécurité ayant extrêmement augmenté au cours de ces dernières années en raison de l'utilisation croissante d'internet et de la communication globale, on observe une recrudescence des efforts de normalisation dans ce domaine. Il existe donc aujourd'hui un grand nombre de normes, de directives et de recommandations en matière de sécurité.

Le présent chapitre présente, sous une forme succincte, les normes et les recommandations de sécurité pour les services de cyberadministration. Comme les précédents, ce chapitre recommande essentiellement des technologies et des normes, qui portent maintenant sur la sécurisation des interfaces S1, S2 et S3. Il ne traite pas de la manière de sécuriser les systèmes et d'attribuer les droits d'accès.

Les recommandations sont accompagnées d'explications supplémentaires dans le but de:

- placer les technologies présentées ici dans un contexte permettant d'en faciliter la compréhension.
- montrer quelles recommandations supplémentaires sont encore à formuler par *eCH* et SAGA.ch en plus de celles concernant la stratégie de sécurité informatique[11].

7.1 Modèle structurel pour la sécurité des données

Le modèle structurel ci-après (voir figure suivante) a été élaboré pour faciliter la présentation et la compréhension des normes de sécurité. Il ne s'agit pas d'un modèle en couches, mais

[9] http://intranet.isb.admin.ch/themen/sicherheit/00530/01276/index.html?lang=fr voir aussi principes de sécurité UPIC.

[10] Concernant la transparence et la validité juridique de processus, voir SNR CWA 14842-1

[11] Plus tard, les chapitres concernés pourront être raccourcis en conséquence et se limiter éventuellement à des références bibliographiques.

d'une représentation des différents domaines de spécification sous forme de blocs. Ce modèle sert à mieux catégoriser la sécurité informatique malgré sa complexité et en facilite ainsi la compréhension.

Une norme de sécurité des données englobe en général plusieurs blocs du modèle structurel présenté ici. C'est pourquoi on renonce à établir une correspondance entre les normes et les blocs.

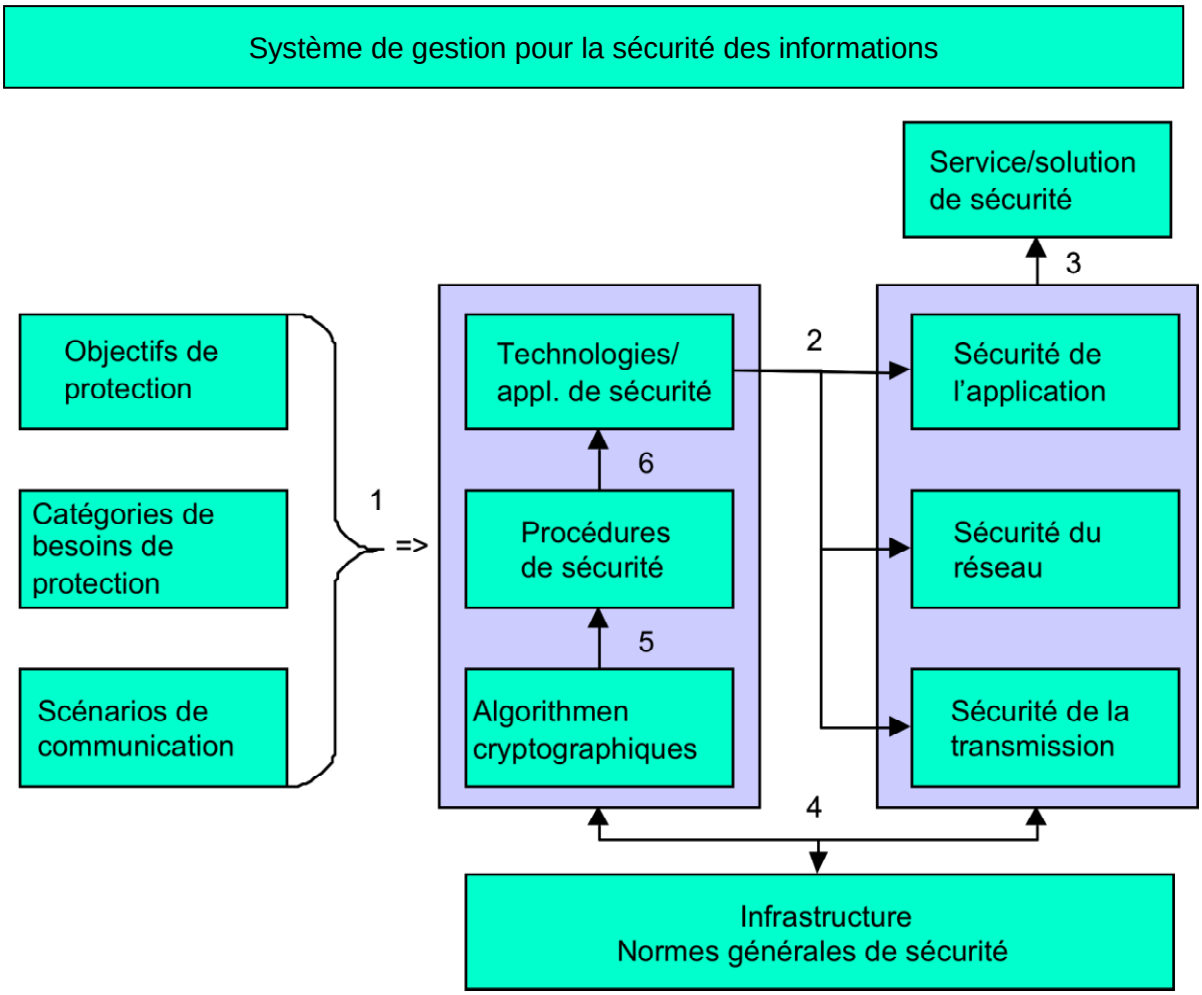


Figure 8-1 Modèle structurel pour les normes de sécurité

1. Les objectifs de protection, les catégories de besoins de protection et les scénarios de communication influencent les algorithmes cryptographiques, les procédures de sécurité à appliquer et les technologies de sécurité à utiliser.

2. Les tronçons ou parties de la communication qui sont effectivement sécurisés dépendent de la technologie de sécurité que l'on a choisie. Par exemple, S/MIME (sécurité au niveau des données de l'application) permet de sécuriser les données sur tout le trajet, c'est-à-dire de l'expéditeur au destinataire, alors qu'IPSEC assure une sécurisation au niveau du réseau, mais rarement sur tout le trajet.

3. Les tronçons de communication protégés font partie intégrante de la solution de sécurité.

4. Définit l'interface avec l'infrastructure et les ressources utilisées en commun telles que cartes intelligentes, service d'annuaire ou annuaire UDDI.

5 Les algorithmes cryptographiques déterminent les procédures de sécurité à utiliser.

6. Les procédures de sécurité déterminent le type et l'usage des technologies et applications de sécurité.

Système de gestion pour la sécurité des informations (ISMS): voir chap.7.4. Selon ISO2700x, un système de Management System est pertinent sur tous les blocs structures ci-dessus.

Objectifs de protection: voir chap..7.3. On définit dans ce bloc le besoin de protection exigé pour le cas d'application (use case) ou le service offert.

Catégories de besoins de protection: voir chap..7.3. On définit dans ce bloc les besoins et les risques en particulier par rapport aux catégories suivantes:

- authenticité
- confidentialité
- intégrité
- disponibilité
- Incontestabilité

Scénarios de communication. Dans ce bloc est défini le processus de communication pour les différents scénarios possibles.

Algorithmes cryptographiques: voir chap. 7.6. Dans ce bloc sont définis les algorithmes cryptographiques à soutenir.

Procédures de sécurité: voir chap..7.6 . Les différents algorithmes cryptographiques peuvent être combinés entre eux de manière à assurer une ou plusieurs catégories de protection. Par exemple, la signature numérique garantit l'authenticité et l'intégrité.

Technologie/application de sécurité: voir chap..7.8. Une technologie de sécurité est une norme pouvant être mise en œuvre dans un produit ou pouvant en constituer une composante indépendante (produit semi-fini)[12]. Une technologie ou application de sécurité est composée d'un grand nombre de procédures de sécurité (p. ex. SSL/TLS), de manière à protéger des protocoles et des parties de réseau déterminés. On définit dans ce bloc les technologies et les applications de sécurité à utiliser. Le classement protégé de documents et la protection de banques de données sont également attribués au domaine technologie/applications de sécurité.

Sécurité de la transmission: Dans ce bloc sont sécurisées les données et les informations sur les différents tronçons de la transmission. Il s'agit p. ex. de la sécurisation des données transmises en mode synchrone, telles que le contenu d'une communication téléphonique. Le chiffrement de la couche «liaison de données» fait également partie de ce bloc.

Sécurité du réseau: Dans ce bloc, les informations sont sécurisées et protégées au niveau du réseau. A ce niveau, sont sécurisés les paquets IP porteurs d'informations utiles ainsi que ceux contenant des informations de routage (RIP, OSPF ou BGP), les premiers étant éventuellement protégés différemment (à un autre niveau) que les seconds.

Sécurité de l'application: Ce bloc sécurise les informations se trouvant juste au-dessous du niveau 4 de l'Internet Modèle d'architectures (IETF; voir aussi ISO/IEC/ITU Frame-works)

[12] Concernant la délimitation par rapport aux procédures de sécurité, voir le chapitre 8.7.

dans une couche intermédiaire (SSL/TLS) ou directement sur la couche d'application par l'application elle-même (S/MIME).

Infrastructure et normes générales de sécurité: voir chap. 7.10. L'utilisation de systèmes à clés publiques nécessite, lorsque les partenaires de communication sont nombreux, des certificats ainsi qu'une infrastructure pour gérer ces derniers et, le cas échéant, les clés elles-mêmes. En ce qui concerne les normes générales de sécurité, ce bloc comprend aussi le raccordement de smart cards et les interfaces pour le service d'annuaire.

Solution de sécurité: Une solution de sécurité sécurise un cas d'application (use case) et peut comprendre une ou plusieurs composantes des blocs «sécurité de la transmission», «sécurité du réseau» ou «sécurité de l'application». Généralement cependant, d'autres composantes s'y ajoutent, telles que

- la sécurisation d'un système (renforcement de la sécurité d'un serveur)
- l'intégration d'un pare-feu et de Secure-Gateways
- des mesures pour la sauvegarde de la disponibilité
- la sauvegarde de l'annuaire UDDI
- la sécurisation de l'enregistrement et du transport de fichiers WSDL
- l'authentification de fichiers WSDL
- etc[13]. Voir notamment Protection de l'information au sein de la Confédération

Remarque: Le modèle structurel et les normes de sécurité des données que nous présentons ici ne dispensent pas l'organe qui les utilise

- de faire procéder, par les spécialistes concernés, à une analyse approfondie de la conformité légale de l'application en question,
- de respecter les lois,
- d'examiner et de respecter, dans toutes les instances et processus de la chaîne de communication, le niveau de sécurité qui a été défini.

Il est indispensable d'analyser les risques spécifiques à l'application, de déterminer les besoins de protection et d'élaborer un concept de sécurité. Les objectifs des mesures à prendre en matière de sécurité sont déterminés par les objectifs de protection, les besoins de protection et les cas d'application.

Certaines combinaisons de Use Case ou compositions de systèmes se révèlent souvent peu avantageuses et plombées par des points faibles. Il nous est malheureusement impossible de les représenter dans ces pages, il convient donc de les contrôler en temps voulu. Il n'est pas possible de normaliser des solutions de sécurité en tant que telles, mais seulement de publier des guides, des conseils ou des exemples à suivre («meilleures pratiques»). Par conséquent, aucune norme ne sera recommandée ou vivement recommandée dans ce contexte.

13 http://intranet.isb.admin.ch/themen/sicherheit/00530/01276/index.html?lang=de voir également les principes de sécurité de l'UPIC.

Pour l'élaboration et la conception de solutions de sécurité ainsi que pour les mesures à prendre en la matière, nous conseillons la lecture, entre autres, du manuel de protection de base (Grundschutzhandbuch, GSHB) de l'Office fédéral allemand de la sécurité. Concernant la conduite et le déroulement de projets informatiques, nous conseillons la lecture du manuel Hermes voir www.hermes.admin.ch de l'UPIC. Le document SNR CWA 14842-3 de l'Association suisse de normalisation donne un bref aperçu des consignes de sécurité à respecter au niveau des sites internet.

7.2 Objectifs de protection

Les objectifs de protection définissent les intérêts ou les besoins de sécurité des partenaires de communication concernés et sont décrits sous forme générale par rapport aux différentes menaces ci-après:

- **Confidentialité**: protection contre la prise de connaissance par des personnes non autorisées
  Menace: les données sont mises à la disposition ou exposées à la connaissance d'individus, d'entités ou de processus non autorisés.
  Définition 1 de la confidentialité: une information est considérée comme **confidentielle** lorsque ses destinataires peuvent supposer que personne d'autre ne peut la lire ou la consulter.
  Définition 2 de la confidentialité: garantie que l'information n'est accessible qu'à un cercle déterminé de personnes autorisées [SNR CWA 14842-3].
- **Intégrité** – protection contre des manipulations non désirées
  Menace: des données peuvent être modifiées ou détruites de manière involontaire, ou non autorisée par leur propriétaire ou par leur responsable.
  Définition 1 de l'intégrité: des données sont considérées comme **intègres** lorsque l'on peut supposer pouvoir en percevoir, avec la plus grande sécurité possible, toute modification non autorisée ou non souhaitée par leur propriétaire ou lorsque l'on peut supposer pouvoir les protéger, , avec la plus grande sécurité possible, contre toute modification illicite ou involontaire.
  Définition 2 de l'intégrité: protection de l'exactitude de l'intégrité de l'information ainsi que des méthodes de processus.
- **Identification** – Contrôler si une personne est bien celle qu'elle prétend être ou établir l'identité d'une personne. L'on dispose pour cela d'instruments techniques tels que la procédure biométrique ou les renseignements comme la photo d'identité. Menaces: échange de données biométrique comme la photo d'identité ou les empreintes digitales, modifications des renseignements personnels tels le nom, la date de naissance, la ville d'origine ou de domiciliation.
- **Authenticité** – Protection contre la falsification de l'origine (affectation des informations à une personne ou une entité).
  Menace: une entité ou une ressource (p. ex. personne, processus, système) usurpe une identité pour tenter d'accéder à des données confidentielles ou pour faire croire que l'information fournie, ou à vérifier, provient de quelqu'un d'autre.
  Définition 1 de l'authenticité: des données ou des informations sont considérées comme **authentiques** lorsque l'on peut supposer, avec la plus grande sécurité, possible de quelle entité elles proviennent.

Définition 2 de l'authentiticité: l'authenticité est l'assurance que les données proviennent bien de l'entité qui dit ou prétend en être l'émetteur (voir ISO 7498-2).

- **Disponibilité**: protection contre la défaillance des systèmes informatiques ou des voies de communication
  Menace: des informations urgentes ne sont plus accessibles ou ne peuvent être consultées ou traitées qu'avec peine ou avec un certain retard.
  Définition de la disponibilité: l'entité ou la ressource A est **disponible** lorsqu'une entité autorisée peut y accéder et la consulter dans la forme souhaitée et dans un laps de temps prédéfini.

Nous n'avons pas mentionné ci-dessus tous les objectifs de sécurité (Security Services) (voir ISO 7498-2), mais ceux qui sont en principe les plus importants. Il en existe d'autres, indiquées ci-après, qui résultent de la combinaison ou sont une conséquence de ceux que nous avons mentionnés plus haut.

- **Incontestabilité:** protection évitant que la réception ou l'envoi d'un message puisse être contesté.
  Menace: Si l'envoi ou la réception des informations peut être contesté, aucune transaction engageant l'une ou l'autre partie ne peut avoir lieu.
  Définition pour l'expéditeur: Le destinataire reçoit la preuve que les données proviennent bien de l'expéditeur présumé. Celui-ci ne peut donc plus en contester l'envoi.
  Définition pour le destinataire: L'expéditeur reçoit la preuve que les données sont bien arrivées au destinataire. Celui-ci ne peut donc plus en contester la réception.
- **Autorisation:** protection contre l'attribution de droits trop nombreux ou trop restreints.
  Menace: Si trop de droits (privilèges) sont attribués, l'entité concernée peut accéder de manière non justifiée à certaines données. Si trop peu de droits sont attribués, les fonctions désirées ne peuvent pas être utilisées, ou ne pas l'être entièrement, bien que l'entité concernée doive y être autorisée.
  Définition de l'autorisation: attribution correcte à une entité, après authentification de celle-ci, des droits (privilèges) définis au préalable.

Le cryptage des informations constitue, entre autres, une aide importante pour protéger la confidentialité, mais les impératifs légaux concernant la conservation des documents et les questions de responsabilité exigent souvent que l'authenticité, l'intégrité et la disponibilité soient aussi assurées à un haut niveau par d'autres moyens techniques. Une disponibilité élevée peut, par exemple, être atteinte par la multiplicité, la protection de l'accès, l'enregistrement distribué et/ou la redondance.

7.3 Besoin de protection

Le besoin de protection doit être déterminé pour chaque application ou service informatique (cas d'utilisation). Il se base sur les dommages qui peuvent résulter de la dégradation de l'application informatique concernée ainsi que sur leur probabilité de survenance.

Pour la partie civile de l'administration fédérale, le besoin de protection est couvert conformément à l'ordonnance sur l'informatique dans l'administration fédérale (OIAF, RS 172.010.58) et aux directives qui en résultent du CI sur la sécurité informatique de l'administration fédérale (WIsB) avec leurs annexes. Si un besoin accru de protection est démontré, un concept de sûreté de l'information et de protection des données (concept

SIPD[14]) doit être établi en collaboration entre le bénéficiaire et le fournisseur de prestation. Les risques seront évalués en fonction du produit à partir de la probabilité de survenance, de l'étendue des dommages possibles et d'une pondération. On distingue les catégories suivantes:

Niveau	Remarque	Description
1	Invraisemblable	Possible mais plutôt invraisemblable
2	Rare	Survenance rare, mais avec laquelle il faut compter
3	Occasionnel	Survenance occasionnelle
4	Probable	Survient assez souvent
5	Fréquent	Survient fréquemment

Tableau 8-1 Probabilité de survenance

Déterminer la probabilité de survenance dans le système informatique n'est pas facile ou n'est pas rentable ni adéquat étant donné que la situation en termes de menace se modifie presque quotidiennement. C'est pourquoi on a renoncé à donner des indications quantitatives.

Remarque: Dans le tableau ci-après, on a volontairement renoncé à donner des chiffres absolus concernant l'étendue du dommage, parce que des montants très différents sont considérés comme critiques ou catastrophiques par les particuliers ou par l'administration au niveau cantonal ou communal..

Niveau	Conséquence	Critères d'évaluation
1	Négligeable	Le respect des obligations légales et contractuelles n'est pas en danger. L'accomplissement des tâches est gêné d'une manière tout au plus modérée. Les droits de la personnalité ne sont pas en danger. Les dommages à l'environnement sont minimes. Accidents ou maladies sans absence du travail.

[14] S'adresser à l'UPIC pour de plus amples renseignements. Concept SIPD:

http://www.isb.admin.ch/themen/sicherheit/00151/00842/index.html?lang=de

Analyse des besoins de protection:

http://www.isb.admin.ch/themen/sicherheit/00151/00174/index.html?lang=de

		Pas de dommage pour l'image de l'administration fédérale.
2	Marginal	Le respect des obligations légales et contractuelles est en danger ou l'accomplissement de tâches importantes est gêné. Des droits de la personnalité sont en danger. L'environnement subit des dommages qui peuvent être réparés. Des accidents ou des maladies avec plusieurs jours de travail perdus, mais sans séquelles, sont possibles. Le dommage causé à l'image de l'administration fédérale est faible et de courte durée (pas de télévision et, tout au plus, bref article dans la presse).
3	Critique	Le respect d'obligations légales et contractuelles est fortement restreint ou l'accomplissement de tâches importantes est empêché. Des droits de la personnalité sont en danger dans une mesure importante. L'environnement subit des dommages qui peuvent être réparés. Accidents ou maladies avec hospitalisation et séquelles (invalidité partielle). Dommage assez important à l'image de l'administration fédérale (article dans la presse, mais pas en page 1, pas de télévision).
4	Catastrophique	Le respect d'obligations légales et contractuelles ou l'accomplissement de tâches importantes est empêché. Violation des droits de la personnalité. Danger de mort. L'environnement subit des dégâts durables. Dommage important pour l'image de l'administration fédérale (article en page 1 dans la presse et passage à la télévision).

Tableau 8-2 Etendue des dommages

Pour évaluer les cas d'application (use cases) du point de vue de la sécurité, on attribuera à chaque objectif de protection (authenticité, intégrité, disponibilité et confidentialité selon art. 3 al 5 OIAF) une catégorie de besoin de protection selon le tableau (cette méthode est également appelée classification). De la même manière que dans le manuel allemand de protection de base (IT-Grundschutzhandbuch du BSI; http://www.bsi.bund.de/gshb/), la catégorie de protection a été élargie ici aux critères de l'authenticité et de la reproductibilité, compte tenu du fait que l'intégrité et l'authenticité sont des notions différentes et qu'il existe des services de sécurité nécessitant un besoin accru d'intégrité, mais pas d'authenticité.

Il est en outre recommandé d'attribuer à chaque catégorie le facteur temps relatif au besoin de protection. La confidentialité de certaines données doit p. ex. être protégée pour une courte période seulement, alors que celle d'autres informations, telles que les clés privées ou les éléments secrets, doit l'être durant des années.

Remarque: Une bonne protection de la confidentialité présuppose une bonne protection de l'authenticité, car il est nécessaire de savoir à qui on envoie un message confidentiel ou de qui on en reçoit un. Le fait que la confidentialité présuppose, d'une manière générale, l'authenticité ressort de la définition de [SNR CWA 14842-3]. La protection contre l'accès non autorisé présuppose une autorisation qui ne peut être accordée que si l'entité «autorisante» a été authentifiée.

7.3.1 Normes de sécurité pour la détermination du besoin de protection

Le besoin de protection ne doit pas seulement être mesuré aux dommages matériels possibles, mais doit aussi prendre en compte les éventuels dommages immatériels, en particulier lors du traitement de données se rapportant à des personnes. Le cadre légal, notamment le droit de la protection des données et les obligations de garder le secret prévues dans le droit pénal, doivent donc être respectées. SAGA.ch renonce à expliquer les différentes mesures de protection des données. Les règles correspondantes doivent être fixées par les préposés à la protection des données de la Confédération et des cantons. En Allemagne, une proposition de chapitre sur la protection des données figure dans SAGA.de, avec une liste des dangers et des mesures conseillées.

Pour chaque cas d'application (use case), le besoin de protection doit être défini pour les différents processus et pour les différents tronçons et scénarios de communication. Pour déterminer le besoin de protection, on considérera notamment les points suivants:

- dommages matériels (directs et indirects)
- dommages immatériels (directs et indirects) concernant p. ex. la réputation ou l'image
- dispositions légales
- réflexions d'ordre économique sur les coûts, la «praticabilité» et l'acceptation

Une aide concrète à la détermination du besoin de protection doit encore être élaborée et publiée par eCH sous forme de norme ou de recommandation.

7.3.2 Mesures

Après avoir défini le besoin de protection par objectif de sécurité, on déterminera par quels moyens cryptographiques et techniques on veut atteindre les différents objectifs de protection (authenticité, confidentialité, etc.). Les mesures de sécurité concrètes s'orientent aux normes internationales actuelles concernées, telles que ISO/IEC 17799/27001, ou aux catalogues de protection de base informatique du BSI (Bundesamt für Sicherheit in der Informationstechnik).

Exemple: La première colonne du tableau ci-dessous énumère les catégories de besoin de protection pour l'authenticité. La deuxième colonne indique les mesures à prendre pour assurer la protection correspondante.

Conséquence (risque) Authenticité	Mesures
Négligeable	Aucune mesure n'est nécessaire
Marginale	Nom d'utilisateur et mot de passe, mot de passe à utilisation unique
Critique	MAC, HMAC, signatures numériques, transfert de clé avec clés courtes
Catastrophique	MAC, HMAC, signatures numériques, transfert de clé avec clés d'une longueur minimale déterminée, dont la production doit satisfaire à des critères précis

Tableau 8-3 Catégories de besoins de protection et mesures

Il s'agit ici d'un exemple et non pas d'une recommandation. Les mesures à prendre pour chaque catégorie de protection doivent encore être déterminées et publiées sous la forme d'une norme ou d'une recommandation.

7.4 Gestion de système comme impératif à la sécurité du système

La norme internationale ISO/IEC 27001 spécifie les exigences pour la fabrication, l'introduction, l'exploitation, la surveillance, l'entretien et l'amélioration d'un système documenté de gestion de la sécurité des informations.

La norme internationale ISO/IEC 27002 contient un guide pour la gestion de la sécurité des informations..

ISO/IEC 27001, 27002 (avec corrigenda)	Recommandé

Normes: www.snv.ch, www.iso.org .

La norme internationale ISO/IEC 19770-1 définit un cadre de procédure pour l'administration du logiciel comme en particulier les logiciels exécutables (comme le système d'exploitation, les programmes d'application et les programmes d'assistance), mais aussi les logiciels non-exécutables (comme les polices, les graphiques, les enregistrements audio et vidéo, les documents et les données). Il ne s'agit ici pas uniquement de questions de droits de licence: des informations fiables concernant les programmes et leur lieu d'installation sont une condition préalable importante pour la gestion de la sécurité du système.

ISO/IEC 19770-1 2012	Recommandé

Normes: www.snv.ch, www.iso.org .

7.5 Algorithmes cryptographiques

Ce sous-chapitre recommande les algorithmes cryptographiques, les mécanismes de sécurité et les protocoles de sécurité (voir ISO cités) qui peuvent être appliqués dans le cadre d'***eCH***. Les algorithmes qui ne sont pas mentionnés sont réputés non recommandés. Les différents algorithmes sont répartis dans les catégories suivantes:

- Cryptographie à clé publique (basée sur des algorithmes asymétriques)
- Cryptographie symétrique

- Stéganographie
- Fonctions hash
- Générateurs de chiffres aléatoires

Concernant les procédés cryptographiques, il existe des paramètres de sécurité à définir, dont la longueur de clé, la taille des groupes et autres, voir ECRYT II (www.ecrypt.eu.org ; Report on Algorithms and Keysizes 2016) *et aussi www.NIST.org, www.BSI.de, www.rsa.com, NESSI (*Networked European Software and Services Initiative).

La norme ISO/IEC JTC1/Sc27 contient des descriptions de mécanismes de sécurité (versus les algorithmes de sécurité). Les implémentations des protocoles de sécurité concernés jouent un rôle critique en matière de sécurité. Il faut par conséquent que ceux-ci ne soient pas «cousus main», mais implémentés avec la plus grande prudence selon les normes ISO IEC mentionnées ci-après.

7.5.1 Cryptographie à clé publique

RSA	Vivement recommandé

Selon l'Use Case «Traitement en ligne pour les Session Keys» et le besoin de protection, le procédé RSA a seulement le statut «en observation».

Normes: ISO/IEC 14888 (Teil 1-2), ISO/IEC 18033-2.

A titre informatif: IETF RFC 8017, PKCS#1 v.2.2, IEEE P1363. [Sch] et [Stw] décrivent comment fonctionne le procédé.

Diffie-Hellman	Vivement recommandé

Selon le cas d'application (use case) et le besoin de protection, l'algorithme Diffie Hellman a seulement le statut «en observation» [Sch] et [Stw] décrivent comment fonctionne le procédé.

A titre informatif: IEEE P1363

Courbes elliptiques	Vivement recommandé

Selon le cas d'application (use case) et le besoin de protection, l'algorithme des courbes elliptiques a seulement le statut «en observation». Voir également notamment IETF RFC 7748.

Normes: ISO/IEC 15946 (all parts 2016), 14888-3, 18033-2

A titre informatif: IETF RFC 5639: IEEE P1363. Le lecteur trouvera une introduction aux courbes elliptiques dans [Sad] et [Mud].

Les prescriptions techniques et administratives de l'OFCOM [TAV] font référence à la norme ETSI TS 101 176 par le biais de la norme TS 102 456. Ces descriptions ainsi que le document [Bek] de RegTP (Allemagne) définissent les paramètres et les longueurs de clé pour les algorithmes à clés publiques (pour l'utilisation de signatures électroniques). Pour RSA, le document ETSI TS 102 176 et al. indique selon quelle méthode les nombres premiers doivent être générés.

7.5.2 Cryptographie symétrique

IDEA	Recommandé

Normes: Sans être lui-même une norme, l'algorithme IDEA n'est pas mentionné dans ISO18033 et est mentionné dans de nombreuses normes, telles que SSL et TLS. Son fonctionnement est décrit dans [Sch] et [Stw]. L'utilisation d'IDEA nécessite une licence payante. Les brevets correspondants arrivent à échéance en 2010 (aux Etats-Unis) et en 2011 (en Europe).

DES avec clé de 56 bits	Non recommandé

3DES avec clé de 112 bits	Recommandé

Normes: ISO/IEC 18033-3

3DES avec clé de 168 bits	Recommandé

Normes: ISO/IEC 18033-3; Le fonctionnement de 3DES est décrit dans [Sch] et [Stw].

AES	Vivement recommandé

Normes: ISO/IEC 18033-3; «MISTY, CAST, HIGHT, Camellia, SEED» sont décrits dans ISO/IEC 18033-3.

Compression	Recommandé

La compression en tant que telle n'est pas une technique de cryptage, mais une compression avant le chiffrage augmente la protection de la confidentialité, cf. [Mau].

Concernant la génération des nombres aléatoires pour les clés, nous renvoyons à la norme ETSI TS 102 176 (voir aussi le chapitre 7.5.7 «Générateurs de nombres aléatoires»).

7.5.3 Modes de fonctionnement pour le chiffrement par blocs

Divers modes de fonctionnement ont été lancés dans un souci d'éviter qu'un même texte n'aboutisse au même texte chiffré et donc de permettre la déduction du texte clair à partir du texte chiffré. EX. Counter Mode et mode CBC. La littérature sur ce dernier est abondante, notamment en lien avec l'implémentation pour SSL/TLS. [Vau] suggère une implémentation en toute sécurité. Cependant, les implémentations antérieures de SSL/TLS (voir chap.0) permettaient à un tiers non autorisé de demander si le dernier Record présentait un Padding correct. Ceci permettait ensuite, par des requêtes, de déchiffrer le dernier Record. Ce n'est donc pas la sécurité de CBC qui est en cause mais celle de son implémentation.

Lors de Beast Attacks concernant CBC, on suppose fortement que du code malveillant est téléchargé chez le client. EX. avec Javascript. Ce code peut ensuite isoler certains textes dans la connexion SSL. A ce sujet:

- Au lieu de remettre en cause l'utilisation de Javascript dans un environnement, on a remis en question le mode CBC.

Le téléchargement et la mise en service de code malveillant donne lieu à d'autres attaques graves et plus efficaces, que l'isolement de texte dans une connexion sûre.

Le Padding doit être maintenu à un minimum (v. [Vau])	Recommandé

Normes: ISO/IEC 10116, CCM Mode selon ISO/IEC, ISO/IEC 18033-4 (application sur chiffrement par bloc). Modes of operation CBC (Cipher Block Chaining), Counter-modes selon ISO18033. CCM Mode selon (ISO/IEC: Mechanism3), GCM (Mechanism6), Key Wrap (Mechanism1), EAX, Encrypt then-MAC, ou une sélection de ce type de procédés, ou autres mécanismes redéveloppés.

7.5.4 Stéganographie

La stéganographie en tant que moyen de transmission incognito d'informations confidentielles ne s'appliquera guère dans la cyberadministration, car la transmission dans cet environnement doit être normalisée et utiliser des procédés accessibles à tous. Si tout le monde sait qu'elle est utilisée, la stéganographie perd son caractère intrinsèque (cf. [Sad] pour plus de détails sur cette technique).

Elle pourrait cependant jouer un rôle à l'avenir pour insérer des informations de protection des droits d'auteur, mais les techniques ne sont pas encore d'une sûreté et d'une robustesse suffisantes. La partie de la sténographie qui concerne l'insertion d'informations de droits d'auteur est connue sous l'appellation «digital watermarking».

Stéganographie pour la protection des droits d'auteur	En observation

7.5.5 Digital Watermarking

Le Digital Watermarking ou tatouage numérique est un procédé à l'aide duquel on peut intégrer n'importe quelle information dans des médias numériques. Des modifications ciblées – en règle générale imperceptibles – apportées aux données multimédias permettent par exemple d'attester de l'authenticité d'un fichier et de garantir sa traçabilité. Contrairement au filigranage conventionnel, le tatouage numérique n'est pas directement perceptible par les personnes, mais est conçu pour être repéré uniquement par un procédé prescrit, lui aussi numérique. La *robustesse* de la signature décide si le tatouage numérique peut encore être lu suite à une conversion de format par exemple

Utilisation

Gestion des droits numériques — droits d'auteur du point de vue du citoyen

H265 Video Watermarking (pour MPEG2/4)	Recommandé

Audio Watermarking (pour MP3/WAV)	Recommandé

Filigranage numérique	En observation

Normes: ISO 26429-3/4/6/7/9/10:2008/9; Digital cinema packaging: Part3: Spound and picture track file; Part4: MXF JPEG 2000 application; Part6: MXF track file essence encryption; Part7: Composition playlist; Part9: Asset mapping and file segmentation; Part10: Stereoscopic picture track file.

7.5.6 Fonction Hash

SHA-1	Recommandé - pour applications à court terme uniquement

Non recommandé, lorsque les **données doivent être protégées sur une «période prolongée»**, comme par exemple pour la signature d'un certificat ou pour un contrat (à utiliser par conséquent seulement pour l'intégrité de la session par exemple).

Normes: Fonction Hashen voir ISO/IEC 10018, FIPS 180-1, IETF RFC 6234

MD5	Par principe non recommandé

Non recommandé pour une **protection des données sur une longue durée.** Comme pour la signature d'un certificat ou d'un contrat (à utiliser par conséquent seulement pour l'intégrité de la session par exemple).

A titre informatif: IETF RFC 1321

SHA-2 224/256/384/512	Vivement recommandé

Normes: FIPS 180-3/4.

SHA-2 224/256/384/512 a obtenu ce statut pour les raisons suivantes: dans les algorithmes de cryptage à courbes elliptiques et Diffie-Hellmann, la structure de sous-groupe q pour la signature a été fixée à 160 bits dans différentes normes. Toutefois, pour éviter toute collision et toute diminution de sécurité de la fonction hash, q doit comprendre un nombre de bits plus grand que la longueur de la valeur hash. Un besoin d'harmonisation existe donc. Si l'on utilise SHA 224/256/384/512 en laissant la structure de sous-groupe q à 160 bits, on n'obtient pas une sécurité plus élevée qu'avec SHA-1.

SHA-3[15]	Recommandé

RIPEMD-160	Recommandé

7.5.7 Générateurs de nombres aléatoires

Les générateurs de nombres aléatoires doivent être installés de façon modulaire afin qu'ils puissent être remplacés. Les générateurs de nombres aléatoires sont spécifiés dans ISO/IEC 18031.

La norme ETSI TS 102 176 définit comment les générateurs de nombres aléatoires doivent être générés ou renvoie à cet effet à la littérature spécialisée ainsi qu'à d'autres normes. Le lecteur trouvera dans [MOV] un aperçu de ces générateurs et des références bibliographiques à ce sujet.

[15] http://de.wikipedia.org/wiki/SHA-3

7.6 Procédures de sécurité

7.6.1 Authentification en ligne

7.6.1.1 Nom d'utilisateur et mot de passe, mot de passe à utilisation unique

L'utilisation d'un nom d'utilisateur et d'un mot de passe sur une ligne non sécurisée au niveau de la confidentialité n'offre guère de protection. Les mots de passe à utilisation unique n'offrent pas non plus une sécurité suffisante parce que la communication, une fois l'authentification effectuée, peut-être reprise par un tiers non autorisé ou, comme pour l'authentification par mot de passe ordinaire, les informations envoyées peuvent être modifiées, effacées ou interceptées.

Nom et mot de passe sur ligne non sécurisée pour l'accès à des données confidentielles.	Non recommandé

L'utilisation d'un nom d'utilisateur et d'un mot de passe ordinaire ou à utilisation unique sur une ligne non sécurisée au niveau de la confidentialité et de l'intégrité (p. ex. par SSL/TLS) offre une assez bonne protection en ce qui concerne l'authenticité.

Nom et mot de passe, mot de passe à utilisation unique sur une ligne sécurisée (p. ex. SSL/TLS ou connexion IPSEC)	Recommandé

7.6.1.2 Challenge Response

Challenge Response est une procédure d'authentification d'un utilisateur ou d'une instance. La personne ou l'instance procédant à l'authentification doit convaincre (Challenge) la partie adverse qu'elle connaît un élément secret sans le lui communiquer.

Pour les Challenge Response Methods (CRAM), qui ne conviennent d'aucune Session Key afin de protéger la connexion, les recommandations du chapitre 7.6.1.1. s'appliquent de la même manière.

Procédures de Challenge Response, sans négociation d'une clé de session pour la protection de la communication, sur connexion non sécurisée.	Non recommandé

Procédures de Challenge Response, sans accord sur une clé de session pour la protection de la communication, sur connexion sécurisée.	Recommandé

Pour obtenir des recommandations concernant les procédures de Challenge Response avec négociation d'une Session Key sur connexion sécurisée, se reporter aux chapitres 7.8.1 à 7.8.3.

7.6.1.3 Signature numérique

L'authenticité, l'intégrité et, à titre facultatif, l'incontestabilité peuvent être produites au moyen d'une signature numérique. Cette signature numérique requiert une procédure Hash et une procédure de Public Key Signature. On peut utiliser comme fonction hash les procédures définies au chapitre 7.5 «Algorithmes cryptographiques». Pour la procédure Public Key Signature, il est possible d'utiliser RSA, DSA ou ECDSA (DSA avec courbes elliptiques).

RSA	Vivement recommandé

Normes: PKCS#7 1.5, RFC 5652 (mise à jour RFC 4853, 5083), IEEE P1363.

Courbes elliptiques (ECDSA) und Diffie-Hellman (DSA)	Recommandé

Normes: IEEE P1363, FIPS 186-2.

Remarque: L'algorithme de génération de signatures numériques à l'aide du système de cryptage à clé publique Diffie-Hellman est appelé Digital Signature Algorithm, DSA en abrégé (basé sur El Gamal); l'algorithme utilisant le système de cryptage à courbe elliptique est appelé Elliptic Curve DSA (ECDSA en abrégé). Voir également la signature à long terme au chap.7.6.2 .

7.6.1.4 Transfert de clé

Pour le transfert de clés de session, on utilisera l'algorithme RSA.

RSA	Vivement recommandé

Normes: Cette procédure est implémentée dans SSL/TLS, WTLS pour l'authentification du serveur et dans IPSEC pour celle du participant à la communication.

.

Diffie-Hellmann et l'algorithme à courbes elliptiques ne sont pas utilisés en pratique pour ce domaine.	en observation

7.6.1.5 MAC/HMAC

L'intégrité et l'authenticité peuvent être sécurisées au moyen d'une clé (mot ou phrase de passe, suite binaire) et d'une fonction hash, comme dans l'algorithme MAC (Message Authentication Code). Lorsque l'application MAC est modifiée d'une manière déterminée et définie, on parle également d'algorithme HMAC.

HMAC/MAC	Vivement recommandé

Normes: IETF RFC 2104 (mise à jour RFC 6151). L'algorithme MAC lui-même n'est pas normalisé IETF, mais utilisé en pratique pour la sécurisation des protocoles de routage.

7.6.1.6 Procédure biométrique

Les procédures biométriques peuvent (notamment dans le contexte des TIC) être utilisées à des fins de vérification et/ou d'identification d'une personne. Cela signifie que l'on compare les caractéristiques biométriques précédemment saisies et enregistrées avec les caractéristiques biométriques à nouveau soumises par la personne en sa présence.

Les caractéristiques biométriques pouvant être copiées comme «modèle mécanique» ou jeu de données, il faut également s'assurer, selon le cas de figure et la caractéristique, que le système de reconnaissance biométrique est aussi en mesure de distinguer les contrefaçons des originaux (ex. détection du caractère vivant) et, le cas échéant, de rejeter les contrefaçons repérées. Il faut en outre s'assurer que les données soient conservées de manière sûre. Cela est d'autant plus important que les caractéristiques biométriques ne peuvent en règle générale être remplacées comme un passeport.

Dans le domaine de la cyberadministration, à savoir des échanges (en ligne) sur Internet, l'identification ne présente pas un grand intérêt, dans le sens où les conditions décrites précédemment concernant la saisie, l'enregistrement et la sécurité contre la contrefaçon ne peuvent être remplies. C'est pour cette raison que la procédure biom. n'est pas recommandée en cyberadministration.

Procédure biométrique pour l'authentification	Non recommandé

Normes: voir ISO/IEC19794, recommandations BSI.

A titre informatif: NIST, ANSI, IETF RFC 3739, XML Common Biometric Format (XCBF) v1.x d'OASIS. Les réserves relatives au respect de la vie privée (Privacy) sont majeures.

7.6.2 Signature électronique valable à long terme

Une signature électronique à long terme, p. ex. pour la conclusion d'un contrat ou l'établissement de certificats, doit être générée à l'aide d'une fonction hash produisant une somme de contrôle d'au moins 160 bits). La clé doit être générée avec une entropie suffisamment importante (RSA: 4096-Bit, DSA: 4096-Bit, ECDSA: 512-Bit, eCH-0048).

Signature électronique valable à long terme	Recommandé

Norme: IETF RFC 5126. est techniquement équivalent à la norme ETSI TS 101 733 V.1.7.4. C'est pourquoi il est mentionné ici, bien qu'il n'ait que le statut «informational». Concernant les problèmes de conservation à long terme des signatures numériques, v. également [Mud].

7.6.3 Négociation en ligne d'une clé de session

Dans la plupart des procédures d'authentification, les parties ne se bornent pas à s'authentifier, mais négocient également une clé de session. Si la connexion doit être protégée de manière durable au niveau de la confidentialité, un algorithme de Diffie-Hellmann ou à courbes elliptiques devrait également être utilisé pour négocier cette clé.

Une connexion (session) doit être protégée de manière durable (au niveau de la confidentialité) si elle sert par exemple à transférer des clés. Cette protection est assurée si la clé de session négociée ne peut pas être déterminée même en connaissance de la clé privée du participant à la communication.

Dans certains modes de configuration SSL/TLS (technologie utilisée, entre autres, pour la sécurisation de l'internet banking), toutes les connexions avec le serveur peuvent être décryptées rétroactivement si l'on connaît la clé privée de celui-ci et que l'on dispose des données transmises. Contrairement à SSL/TLS, IPSEC ne comporte pas cette faiblesse[16], car il permet l'utilisation de l'algorithme de Diffie-Hellmann ou à courbes elliptiques, au choix, pour négocier la clé de session.

[16] Concernant le Perfect Forward Secrecy (PFS), on connaît également des technologies AKE. Eu égard aux faiblesses Heartbleed dans OpenSSL, nous attirons l'attention sur ce thème hautement actuel. RSA Key Transport n'est par principe pas compatible PFS. DH et ECDH le sont.

Algorithme de Diffie-Hellmann ou à courbes elliptiques si la confidentialité doit être protégée de manière durable	Recommandé

Nous déconseillons toutefois l'utilisation des modes Ephemeral-Static et Static-Static (voir IETF RFC 2631)[17]. (TLS, par exemple, permet de négocier les clés en ligne en utilisant la méthode mentionnée.)

Normes: IEEE P1363, PKCS#3, IETF RFC 2631. La négociation des clés sur la base des algorithmes de Diffie-Hellman et à courbes elliptiques est définie, entre autres, dans les normes IPSEC (IETF RFC 2412, RFC 4306 – mise à jour RFC 4109).

RSA	En observation

7.6.4 Procédures hybrides

En raison de son efficacité moindre par rapport à la cryptographie symétrique, la cryptographie asymétrique ne convient que pour les quantités de données limitées. Dans le cas de grandes quantités de données, le chiffrement est souvent effectué de manière symétrique avant que la clé symétrique soit elle-même transmise au partenaire de communication chiffrée de façon asymétrique (procédure hybride).

7.7 Données et connexions authentifiées et confidentielles

Concernant les données et les connexions authentifiées, on observera, entre autres, les aspects suivants:

- Pour les connexions, l'authentification s'effectue en ligne. Dans un environnement PKI, toute authentification (voir également Certification Path Validation IETF RFC 5280 chap.6) se basant sur le certificat de l'utilisateur devrait être invalidée si ce certificat n'est plus valable ou a déjà été révoqué.
- L'authentification de la connexion doit être protégée aussi longtemps que celle-ci est établie.
- La protection de l'authenticité des données doit être durable. Il est possible (p. ex. en cas d'obligation légale) que les données doivent conserver leur authenticité au-delà de la durée de validité du certificat (voir ISO/IEC19794).
- Dans l'environnement PKI, l'authenticité peut aussi être réalisée, pour des connexions authentifiées, par le transfert de clé (Secure Channels) suivi d'une procédure MAC ou HMAC, alors que, dans le même environnement, l'authenticité des données est réalisée au moyen de la signature numérique.
- Pour les connexions confidentielles, les informations ne sont protégées que sur la liaison et peuvent ensuite se trouver en texte clair sur les PC clients ou le serveur.
- Suivant les exigences, les données peuvent être enregistrées sur leur support de manière cryptée. Le changement des clés correspondantes doit être réalisé de manière que les données cryptées avec l'ancienne clé restent lisibles. Le Rekeying (changement de chiffrement des informations archivées chiffrées) doit être possible! Cela pose une exigence accrue au système de gestion des clés.

[17] En fonction de l'application, il peut être malgré tout judicieux d'avoir recours à un Static-Ephemeral DH Key Exchange. Par exemple lorsqu'une Chip doit toujours être authentifiée comme identique d'un côté.

7.8 Technologie de sécurité

Une technologie de sécurité est une norme qui peut être implémentée dans un produit ou en former une composante indépendante (produit semi-fini)[18]. Une technologie ou application de sécurité, telle que SSL/TLS, se compose d'une multitude d'algorithmes de sécurité, de manière à protéger des protocoles et des segments de réseau déterminés. SSL, par exemple, supporte différents algorithmes et procédures pour l'authentification, la négociation des clés, le chiffrage et le contrôle de l'intégrité des paquets.

Voici deux exemples des possibilités de déroulement d'un protocole dans SSL:

- négociation des clés à l'aide de Diffie-Hellman, authentification avec une signature selon Diffie-Hellman, cryptage 3 DES, MAC avec fonction hash SHA-1,
- transfert de clé avec RSA, authentification avec la signature RSA, cryptage IDEA en mode CBC, MAC avec fonction hash SHA-1.

Les technologies de sécurité suivantes sont proposées ici pour la normalisation:

- SSL/TLS
- WTLS
- Kerberos
- SSH
- IPSEC
- S/MIME
- XML Security
- PGP
- Web Services Security
- Protocole pour services d'horodatage
- Sécurité de la transaction

Les différentes technologies de sécurité peuvent utiliser différents algorithmes cryptographiques, au choix. Elles doivent cependant pouvoir aussi être configurées de sorte que seules les procédures mentionnées au chapitre 7.3 puissent être utilisées.

Remarque: en plus de la mention permettant de savoir si la technologie de sécurité en question est fortement recommandée, recommandée, non recommandée ou en observation, nous indiquons à quelle interface I1, I2 et I3 elle devrait être appliquée (pour la définition de ces interfaces, cf. chapitre S1, S2, S3 cf. chapitre 4.2 «Interfaces», page 18.) Exemple:

> Pour la technologie de sécurité YZ, nous donnons l'indication suivante.
>
> **S1** **S2**
>
> Selon les recommandations faites, la technologie de sécurité YZ doit être appliquée aux interfaces I1 (terminal-système) et I2 (système-système), mais non pas à l'interface I3 (système-centre de clearing).

[18] Concernant la délimitation par rapport aux procédures de sécurité, voir aussi le chapitre **Fehler! Verweisquelle konnte nicht gefunden werden.**

7.8.1 SSL/TLS

Secure Socket Layer (SSL) et Transport Layer Security (TLS) sont des technologies de sécurité qui sont intégrées au-dessous de la couche d'application du modèle internet et au-dessus du protocole de transport TCP et peuvent théoriquement protéger par TCP tous les protocoles d'application.

S1 S2 S3

Secure Socket Layer (SSL) V.2.0	Non recommandé
Secure Socket Layer (SSL) V.3.0 (voir NIST)	Non recommandé

Normes: concernant SSL V.3.0, il n'existe qu'une ébauche de RFC IETF.

Transport Layer Security (TLS) V.1.0 (avec SSL V.3.0; voir NIST)	Non recommandé

Normes: TLS V.1.0 0 est défini par l'IETF dans le RFC 2246.

Transport Layer Security (TLS) Extensions	Recommandé

Normes: RFC 3546, Tcpcrypt.

Transport Layer Security (TLS) V.1.1 (TLS Extensions incl.)	Non recommandé

Normes: TLS V.1.1 est défini par l'IETF dans le RFC 4346. Voir également BSI

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf?__blob=publicationFile

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf

S1=Recommandé / S2/3 Vivement recommandé

Transport Layer Security (TLS) 1.2	Vivement recommandé

Normes: TLS v.1.2 est défini par l'IETF (www.ietf.org) dans le RFC 5246. Elimine les attaques Beast et Vaudenay connues; Voir également les études BSI. C'est la raison pour laquelle la version à privilégier doit être TLS v.1.2. Concernant la rétrocompatibilité, voir la norme correspondante IETF RFC 5246 et pertinentes.

Les Cyphersuites courantes sont également répertoriées dans le RFC 5246. Le serveur devrait être configuré de manière à ce que seules les procédures recommandées ici soient utilisées. Dans le cas contraire, la connexion devrait être refusée.

7.8.2 WTLS

Wireless Transport Layer Security (WTLS) sert à sécuriser la communication mobile (téléphones portables). Bien que très semblables en ce qui concerne l'échange et le contenu des messages, WTLS, SSL et TLS sont incompatibles entre eux.

S1

Wireless Transport Layer Security (WTLS)	Recommandé[19]

Norme: WTLS a été spécifié par le WAP Forum (www.wapforum.org) afin que les applications WAP puissent être sécurisées. Une norme existe à ce sujet.

7.8.3 DTLS

TLS peut être utilisé uniquement afin de sécuriser les données d'application de TCP. Le Standard Datagramm Transport Layer Security (DTLS) a été défini afin de sécuriser également les messages UDP.

S1 (S2/S3 notamment pour requêtes DNS)

Datagramm Transport Layer Security (DTLS) V.1.0	Recommandé

Norme: RFC 4347 (rendu obsolète par RFC 6347; mise à jour RFC 5746 (mises à jour 5 RFC), 7507).

Datagramm Transport Layer Security (DTLS) V.1.2	Recommandé

Norme: IETF RFC 6347 (mise à jour RFC 7507, 7905).

7.8.4 TSP

L'horodatage a vocation à prouver la disponibilité de certains documents à un moment particulier et contient notamment une indication temporelle et une signature. Les services d'horodatage sont fournis par un tiers digne de confiance (engl. Trusted Third Party). Le protocole de sollicitation des services d'horodatage et de fourniture d'horodatage est désigné par le terme anglais Time Stamp Protocol (TSP) et est standardisé dans l'IETF RFC 3161. Les services d'horodatage sont notamment employés afin de protéger la validité sur le long terme des signatures numériques.

Time Stamp Protocol (TSP)	Recommandé

Norme: IETF RFC 3161 (mise à jour RFC 5816).

7.8.5 Secure Shell (SSH)

Secure Shell (SSH) est utilisé essentiellement pour la sécurisation de la communication dans les tâches de gestion informatique, telles que la configuration d'un serveur.

S1 S2 S3

Secure Shell (SSH)	Recommandé

Normes: Secure Shell a été adopté par l'IETF depuis janvier 2006 comme norme et est défini dans les RFC 4250 à 4256, 4332, 4344, 4419, 4462, 6242, 6668 et autres normes pertinentes.

---

[19] L'éventuelle utilisation de WTLS dépendra, entre autres, du fait que la cyberadministration offre ou non des services sur téléphones mobiles (par WAP). Si WAP est utilisé pour la transmission de données confidentielles, nous recommandons de sécuriser la transmission par WTLS.

7.8.6 IPSEC

IPSEC sert à sécuriser les paquets IP (p. ex. pour les applications UDP/TCP pour les réseaux privés virtuels VPN). Les normes à son sujet ont été spécifiées par l'IETF dans les RFC correspondants. IPSEC doit être supporté et peut être appliqué en même temps que d'autres technologies de sécurité.

S1 S2 S3

IP Security (IPSEC) V.1.X	Vivement recommandé

Normes: IPSEC a été normalisé par l'IETF dans les RFC 2402, 2412, 4303, 7296 (mise à jour RFC 5998, 6989, 7427, 7670) correspondants et dans les autres RFC pertinents s'y rapportant.

Encapsulating Security Payload (ESP mit IP ProtNr50; voir notamment aussi RFC 7321) fait partie de l'Ipsec Protocole Suite. ESP permet des origin authenticity, integrity et confidentiality protections (non sans points faibles).

IP Security (IPSEC) V.2.0	Recommandé

IP Security version 2.0 comporte quelques faiblesses lors de l'établissement de la clé de session pour la confidentialité ainsi que pour l'authentification et l'intégrité. Le type de génération de clé décrit dans le RFC 7296 (mise à jour 5998, 6989, 7427, 7670) IKE v.2 2 peut notamment accélérer fortement les attaques de type «Brute Force» ainsi que le contrôle de plausibilité d'un candidat pour une clé. Le NIST recommande malgré tout IKEv2 et considère que le KDF ne pose pas de problème[20].

Normes: IKEv2 IETF RFC 8031, 7296 (mise à jour RFC 5998, 6989, 7427, 7670), 5998, MIKEY RFC 4738, NAT and IKE RFC 3947. Autres selon l'IKE Roadmap.

7.8.7 S/MIME

S/MIME signifie Secure MIME et sert à sécuriser le courrier électronique et le transport de données en mode store et forward. Les mécanismes de sécurité interviennent directement dans l'application (à la couche 4 du modèle internet).

S1 S2 S3

Secure MIME (S/MIME) V.2.0	Vivement recommandé

Norme: RFC 2311 S/MIME Version 2 Message Specification et correspondants.

Secure MIME (S/MIME) V.3.2	Recommandé

Normes: les normes correspondantes sont spécifiées par l'IETF (www.ietf.org) dans le RFC 5751 (RFC 3851 obsolète; V.3.1) et les recommandations s'y rapportant «voir également les autres MIME pertinents dont RFC 5035 pour les implémentations».

[20] „The IKEv2 KDFs, which are compliant with SP 800-56C, are approved, when used with an approved HMAC function using an approved hash function".

7.8.8 Secure HTTP (S-HTTP)

Protocole servant à la sécurisation de contenus http (à ne pas confondre avec HTTPs, qui est la dénomination du protocole HTTP protégé sur SSL ou TLS).

Secure HTTP (RFC 2660)	Non recommandé

Norme: The Secure Hypertext Transfer Protocol (RFC 2660) et voir également les autres pertinentes Voir aussi chap. 5.5.2.

7.8.9 XML Security

Par XML Security, on entend la sécurisation des documents en format XML. En font partie les éléments suivants:

- XML Signature
- XML Encryption

Tout comme pour S/MIME, il s'agit ici d'une protection pour une communication de type store and forward.

7.8.9.1 XML Signature

XML Signature est une norme commune reconnue de manière générale par les organismes de normalisation W3C (www.w3C.org), OASIS (www.oasis-open.org) et IETF (www.ietf.org) (voir RFC 3275); voir notamment aussi ISO 14533-Part1 2014 ainsi que Part2 2012.

Cette norme décrit l'intégrité des données, l'authentification des données au moyen de signatures numériques et de procédures HMAC pour des données quelconques (mais en règle générale de type XML), en mettant à disposition un schéma XML et un ensemble de règles pour la génération et la vérification de la signature. Cette dernière peut se composer d'un ou de plusieurs documents (ou données) de différentes sortes (image, texte, etc.).

Les trois possibilités suivantes sont prévues pour le placement de la signature XML:

- intégration (enveloped): la signature peut être intégrée dans le document pour lequel elle a été générée, c'est-à-dire que le fragment XML qui représente la signature est inséré dans le document signé.
- enveloppe (enveloping): la signature peut tenir lieu d'enveloppe, c'est-à-dire qu'elle s'applique à un document auquel elle fait elle-même référence.
- indépendance (detached): la signature peut être indépendante (detached) du document auquel elle s'applique, c'est-à-dire qu'elle est conservée séparément de la source, soit dans le même soit dans un autre document XML.

Une caractéristique centrale de XML Signature est la possibilité de signer non pas tout le document XML, mais seulement des parties de celui-ci. Des algorithmes HMAC ou des signatures numériques peuvent être utilisés pour l'authentification.

L'attribution de préférences cryptographiques à des scénarios de communication déterminés n'a pas encore été effectuée; Méthodes de canonisation voir également Recommandations W3C.

	S1	S2	S3	
XML Signature				Vivement recommandé

Normes: ISO 14533 Part1 2014 und Part2 2012, IETF RFC 3275, XML Signature and Syntax Processing Recommendation, February 2002, de W3C.

7.8.9.2 XML Encryption

XML Encryption définit le cryptage de documents XML et est une norme du W3C (www.w3C.org) reconnue par OASIS (www.oasis-open.org), mais pas encore par l'IETF (www.ietf.org), contrairement à XML Signature.

	S1	S2	S3
XML Encryption			Vivement recommandé

Norme: XML Encryption and Syntax Processing Rec.V.1.1 April 2013, de W3C.

7.8.10 **OpenPGP**

Pretty Good Privacy (PGP) est un produit pour la sécurisation du courrier électronique qui a été développé par Phil Zimmermann. En raison de sa grande diffusion et de sa large utilisation, PGP s'est imposé comme une norme de fait. PGP est normalisé dans l'IETF RFC 2440 (rendu caduc par RFC 4880 et mise à jour 5581-Informational) sous l'appellation OpenPGP.

PGP utilisent d'autres formats de données que S/MIME.

	S1	S2	S3
Open Pretty Good Privacy (OpenPGP), si les certificats X.509v.3 sont supportés.			Recommandé,

Normes: IETF RFC 4880 (mise à jour RFC 5581-Informational) pour PGP. RFC spécifie l'interopérabilité avec S/MIME. Nous attirons l'attention sur les réserves de sécurité émanant de différentes sources concernant PGP dans la cyberadministration.

7.8.11 **Web Services Security**

L'importance croissante de XML en tant que format d'échange de données et de spécification ainsi que l'introduction de Web Services en tant qu'intergiciel (middleware) activent fortement l'élaboration des normes de sécurité XML par les deux organismes W3C (www.w3C.org) et OASIS (www.oasis-open.org).

La notion de «Web Services Security» englobe différents aspects de la sécurité de l'information, p. ex

- XML Security (voir chapitre 7.8.9)
- WS-Security (SOAP Message Security)
- WS-SecureConversation
- WS-ReliableMessaging (voir chapitre 5.8.9.1)
- Security Assertion Markup Language (SAML)
- Web Services Policy Framework, Web Services Policy Attachment et WS-SecurityPolicy
- eXtensible Access Control Markup Language (XACML)
- eXtensible rights Markup Language (XRML)

- WS-Trust
- XML Key Management Standard (XKMS)
- Sécurité de la transaction (engl. Transaction Security)
- WS Security Profiles.

7.8.11.1 WS-Security (SOAP Message Security)

SOAP Security est une norme définie pour l'échange sécurisé d'informations SOAP sur des connexions non sécurisées. Elle protège la confidentialité, l'intégrité et l'authenticité des messages SOAP sur la base de XML Security. Elle spécifie aussi l'intégration de jetons de sécurité, tels que Kerberos Tickets et les certificats X.509 V.3.

S1	S2	S3	
SOAP Message Security V.1.1			Recommandé

Norme: SOAP Message Security (http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SOAPMessageSecurity.pdf) daté du 1er février 2006.

7.8.11.2 WS-SecureConversation

WS-SecureConversation est une norme; elle élargit la norme WS-Security pour l'échange en toute sécurité de messages SOAP dans le cas de répétitions par la définition et l'échange de contextes de sécurité et la déduction de Session Keys.

S1	S2	S3	
WS-SecureConversation V.1.3			Recommandé

Norme: WS-SecureConversation (http://docs.oasis-open.org/ws-sx/ws-secureconversation/200512/ws-secureconversation-1.3-os.html).

7.8.11.3 Security Assertion Markup Language (SAML)

Security Assertion Markup Language (SAML) est un format XML pour représenter et échanger des informations relatives à l'authentification et à l'autorisation.

S1	S2	S3	
Security Assertion Markup Language (SAML) V.1.1			Recommandé

Security Assertion Markup Language (SAML V.1.1) (http://www.oasis-open.org/committees/download.php/3406/oasis-sstc-saml-core-1.1.pdf).

Security Assertion Markup Language (SAML) V.2	Vivement recommandé

Norme: Security Assertion Markup Language (SAML V.2.0) (http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf) daté de 13.März 2005.

SAML V.3 ou également OpenSAML V3 sont en cours de développement ou d'implémentation. Shibboleth propose aux utilisateurs de navigateur une autorisation inter-domaine basée sur Single sign-on et Attribute. Avec la boîte à outils OpenSAML, Shibboleth implémente les SAML 1.x browser profiles pour les Identity & Service Providers (source: OpenSAML V3 Workgroup).

7.8.11.4 Web Services Policy Framework

Web Services Policy Framework définit un modèle général de syntaxe et de sémantique pour la formulation de règles de sécurité. Le cadre général définit les principes de la syntaxe et de la sémantique des règles de sécurité (policies).

S1	S2	S3	
Web Services Policy V.1.5 - Framework			Recommandé

Norme: Web Service Policy V.1.5 – voir Framework (http://www.w3.org/TR/ws-policy/).

7.8.11.5 Web Services Policy Attachment

Web Services Policy Attachment est une norme pour l'attribution des directives (policies) aux points finaux, messages, ressources et opérations.

S1	S2	S3	
Web Services Policy V.1.5 - Attachment			Recommandé

Norme: Web Service Policy V.1.5 – Attachment (http://www.w3.org/TR/ws-policy-attach/).

7.8.11.6 WS-SecurityPolicy

WS-SecurityPolicy est une norme pour la stipulation de spécifications de sécurité pour SOAP Message Security, WS-Trust et WS-SecureConversation.

S1	S2	S3	
WS-SecurityPolicy V.1.2			Recommandé

Norme: WS-SecurityPolicy (http://docs.oasis-open.org/ws-sx/ws-securitypolicy/v1.2/ws-securitypolicy.html).

7.8.11.7 eXtensible Access Control Markup Language (XACML)

eXtensible Access Control Markup Language (XACML) est un format XML pour la représentation et l'échange des règles concernant le contrôle d'accès (en anglais Access Control par exemple Attribute Based Access Control (ABAC) notamment Very Different ABAC pour Next Generation Access Control - NGAC).

S1	S2	S3	
eXtensible Access Control Markup Language (XACML) V.2.0			Recommandé

Norme: eXtensible Access Control Markup Language (XACML) V.2.0, février 2005 (http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf), voir NIST SP800_178 Draft (spécialement Fig.4 : XACML Reference Architecture) et autres pertinents.

7.8.11.8 XRML (eXtensible Rights Markup Language)

XRML est une langue XML et contient une méthode générale pour la spécification de droits et de conditions pouvant être associés à différents types de sources et de contenus numériques. En outre, un environnement de confiance peut être défini à partir de plusieurs domaines pour qu'y soit protégée de manière générale l'intégrité des droits et des conditions.

Utilisation

Pour la définition de droits et de conditions.

S1	S2	S3	
XRML (eXtensible Rights Markup Language) V.2.0			Recommandé

Norme: XRML (eXtensible Rights Markup Language) V.2.0 d'OASIS.

7.8.11.9 WS-Trust

Définit un mécanisme pour l'établissement, le renouvellement, la validation et l'annulation de balises de sécurité sur le principe du «brokered trust».

S2	S3	
WS-Trust V.1.3/1.4		Recommandé

Norme: OASIS, http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/ws-trust.html , voir errata 01 du 25 avril 2012.

7.8.11.10 XKMS

XML Key Management Specification (XKMS) a été développé par le consortium W3C (www.w3C.org) et définit l'intégration de XML Security dans une infrastructure à clés publiques.

XKMS V.2.0	Recommandé

Norme: W3C XML Key Management Specification (XKMS), Rec. V.2.0 dat. 28. June 2005.

Restriction: XKMS est adapté pour des tâches de gestion de clés notamment au sein d'une unité administrative ou d'une entreprise. Dans le domaine de la communication contraignante (signature) de la cyberadministration, il existe des prescriptions restreignant considérablement les possibilités du protocole XKMS et qui remettent donc en question son utilisation sans profil correspondant.

7.8.11.11 Web Services Coordination (WS-Coordination)

Définit un cadre extensible pour la coordination d'activités distribuées.

S1	S2	S3	
WS-Coordination V.1.2			Recommandé

Norme: WS-Coordination voir OASIS Standard daté de 2 fév. 2009.

7.8.11.12 Web Services Atomic Transaction (WS-AtomicTransaction)

Définit la coordination d'activités distribuées sur la base de transactions atomiques.

S1	S2	S3	
WS-Transaction V.1.2			Recommandé

Norme: WS-Transaction voir OASIS Standards); resp. aussi V.1.1+errata possible.

7.8.12 **Kerberos**

Kerberos est un protocole de sécurité qui est utilisé notamment à l'intérieur du réseau d'une administration ou d'une entreprise pour sécuriser la communication client-serveur et pour l'authentification.

Kerberos	Recommandé pour utilisation interne au sein des organisations

On privilégiera notamment SAML pour la délégation des authentifications.

7.8.13 OAuth

OAuth (Open Authorisation Protocol) est utilisée comme norme d'autorisation. Oauth V2 s'est établi pour l'autorisation des services REST pour les clients mobiles (ex. comme Web-Service Security OAuth).

Concernant OAuth 2.0, différentes extensions de norme sont en cours de discussion, telles Open ID Connect, Assertion Profile et SAML Bearer Assertion Profile. Ces extensions définissent de nouveaux workflows et en particuliers des formats Token, permettant l'utilisation d'OAuth 2.0 dans un contexte fédéral également. OAuth 2.0 peut ainsi être aussi employé comme alternative au SAML V.2.0.

OAuth V.2.0/3.x	En observation

Normes: http://oauth.net/documentation http://openid.net/connect/ , IETF RFC 6749
Information: le recours à Oauth V.1 donne lieu à des réserves de sécurité importantes.

7.8.14 OpenID connect

OpenID Connect est une couche d'authentification reposant sur le protocole OAuth. Cela permet aux clients, de vérifier notamment les identités des utilisateurs. L'information pour l'authentification passe par un Autorisation Server System spécial. Ce dernier vérifie les informations du profil de l'utilisateur et les paramètres d'interopérabilité. OpenID Connect utilise pour ce faire RESTful HTTP APIs (et emploie JSON comme format de données). OpenID Connect permet aux clients les plus divers (Web based, mobile and JavaScript Clients) de procéder à un identification avec/et des fédérations (pour LOA, Trustlevels, Accesstokens etc.) au moyen d'informations concernant les «authenticated sessions and end-users».

OpenID connect V.1.0/2.x	En observation

Utilisé par: Google, Microsoft, Ping Identity, Deutsche Telekom, salesforce.com, Nomura Research Institute of Japan – voir notamment aussi : http://openid.net/developers/specs/

http://openid.net/2014/02/26/the-openid-foundation-launches-the-openid-connect-standard/

7.9 Normes générales en matière de sécurité des données

Par normes générales en matière de sécurité, on entend les normes qui ne concernent pas spécifiquement certaines applications, voire certains scénarios de communication mais qui peuvent être mises en œuvre dans plusieurs technologies de sécurité, telles par exemple

- la connexion de cartes intelligentes (smart cards)
- l'interface avec l'annuaire (directory)
- les contenus, les formats et la gestion des certificats
- la consultation du statut d'un certificat
- l'interface avec l'application

7.9.1 Utilisation de cartes intelligentes (Smart Card)

Dans le présent document, on entend par carte intelligente une «smart crypto card», soit une carte à puce munie d'un microprocesseur qui effectue les opérations cryptographiques avec les clés privées. Ces dernières ne doivent pas quitter la puce (c'est-à-dire le microprocesseur de la carte).

Il existe une multitude de normes pour les smart cards. Cependant, nous nous limitons à recommander les interfaces que la technologie de sécurité doit supporter afin de transmettre les données à la smart card puis d'être en mesure de réceptionner le résultat fourni ainsi par le traitement de ces données.

D'autres supports pour la conservation de clés, tels que les jetons USB ou Hardware Security Modul (HSM) dédié, **présentant des propriétés équivalentes au niveau de la sécurité**, ont le même statut de recommandation que les «smart crypto cards».

ISO/IEC 7816 toutes les parties	Vivement recommandé

ISO/IEC 14443 1-4	Recommandé

ISO/IEC 15693 1-3	Recommandé

ISO/IEC 18092 (NFCIP-1)	Recommandé

Norme: ISO/IEC 21481 (NFCIP-2), ISO/IEC 13157 (NF-SEC), ISO 24727.

Références EU concernant les documents Privacy Data Protection Impact et Opinion WP180:

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_en.pdf
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_annex_en.pdf

Concernant le transport de données critiques, des mécanismes de sécurité complémentaires End to End doivent être prévus.

Pour la réalisation de la signature qualifiée, il est exigé que la carte à puce ait été certifiée suivant certains critères de sécurité, cf. [TAV].

Les exigences de la Confédération (UPIC) concernant les smart cards elles-mêmes ainsi que leur intégration et leur connexion sont définies dans [**a006d**] (cf. [RwEw] pour les informations concernant les cartes à puce).

PC/SC	Vivement recommandé

URL: www.pcscworkgroup.com

PKCS#11 (dans la mesure de la pertinence Smart Card et HSM)	Vivement recommandé

Quelques-unes des normes ISO/IEC concernant les Smart Card sont certifiées FIPS.

7.9.2 RFID

RFID (systèmes d'identification par radiofréquences) désigne une série de technologies sophistiquées et très répandues pour les plages de fréquence (de 50-135 kHz, 13.56 MHz, 433 MHz, 860-960 MHz et 2GHz, voir plans de fréquence UIT). Les protocoles de communication, les formats de données et la sécurité sont normalisés au niveau international. Il existe des réserves relatives au respect de la vie privée.

ISO/IEC18000	Recommandé

7.9.3 Interface avec l'annuaire

On y définit le protocole permettant d'interroger des données personnelles, des certificats ou des listes CRL et qui doit être supporté par la technologie de sécurité.

LDAP V.3	Vivement recommandé

Normes: voir chapitre Services d'annuaire et leurs utilisations (Use cases).

7.9.4 Certificats et CRL

7.9.4.1 Généralités

Les formats de certificat sont définis dans les normes X.509 V.3 et dans le RFC 3280, la préférence devant être accordée à ce dernier en cas de doute. Les profils de certificats qualifiés sont normalisés, en partie, dans le RFC 3739 et dans le document [TAV] de l'OFCOM, la primauté devant être accordée à ce dernier en cas de doute.

Des certificats sont émis non seulement pour la génération de signatures, mais aussi, par exemple, pour le cryptage des courriels. Les contenus des certificats, ceux des CRL et la gestion des certificats sont toutefois décrit dans des documents séparés (des RFCS IETF ET ITU.

7.9.4.2 Gestion des certificats

On doit pouvoir définir au niveau de la configuration quels certificats CA sont considérés comme dignes de confiance et lesquels ne le sont pas; en particulier, on doit pouvoir aussi enlever les certificats CA considérés comme dignes de confiance par défaut.

7.9.4.3 Identification et contenus des certificats

Il y a lieu de contrôler la bonne appartenance non seulement des attributs de l'identité contenue dans le «nom distingué», mais de toutes les identifications enregistrées dans le certificat, telles que l'adresse e-mail ou URL, pour éviter qu'il soit possible de contourner l'authentification basée sur des certificats, voir [Mus].

Avec le remaniement de l'OeDI, un règlement technique [TAV-MWST] a été introduit pour définir les attributs numériques des identités à utiliser dans les certificats dans le contexte de la facturation électronique conforme avec la TVA.

7.9.4.4 Complément concernant le certificat

Une distinction devrait être établie entre l'authentification et la signature numériques. Une authentification numérique comprend uniquement l'affectation de l'information à l'entité de l'expéditeur. Il est recommandé de bien protéger l'authentification des systèmes dans

l'environnement de cyberadministration, afin que l'on puisse se fier à l'information qui en provient. L'authentification par clé publique permet d'atteindre un bon niveau de sécurité, mais elle nécessite l'utilisation de certificats.

Certificats pour serveur (certificats machine)	Vivement recommandé

Une signature numérique comprend toujours une authentification et une protection de l'intégrité. Depuis l'entrée en vigueur de l'article correspondant du CO (art. 14 al. 2bis) et de loi fédérale sur les services de certification dans le domaine de la signature électronique (SCSE), il est possible (dans les affaires privées) d'utiliser des signatures électroniques avec la même valeur juridique que les signatures manuscrites. Cette disposition ne s'applique toutefois qu'aux signatures électroniques de personnes physiques.

Si l'on veut utiliser, p. ex. les Web Services (en cyberadministration) de manière juridiquement contraignante et sûre avec les technologies de sécurité correspondantes, on respectera impérativement, entre autres, les règles suivantes (correspondant à la situation à atteindre):

- Des certificats pour serveur, générés et émis par des fournisseurs de services de certification (CA) reconnus selon la SCSE, peuvent être utilisés (voir également les certificats avancés; eCH0048).
- Les signatures numériques d'un serveur qui ont été générées à l'aide des clés privées correspondant à ces certificats ont une valeur juridique similaire à celle des signatures numériques de personnes physiques, qui sont conformes à l'art. 14, al. 2bis CO, dans la mesure ou des règles de sécurité adéquates, encore à définir, soient respectées lors de l'utilisation de certificats pour serveur et des clés privées correspondantes.

Les champs d'application suivants sont possibles, entre autres:

- justificatifs ou quittances numériques pour la gestion électronique des affaires ou pour la remise de documents juridique au Tribunal fédéral
- justificatifs numériques pour la gestion électronique des affaires entre particuliers et offices fédéraux
- services d'horodatage (art. 12 SCSE), entre autres pour l'archivage

Avec le remaniement de l'OeDI ont été introduits et définis au niveau fédéral non seulement les services d'horodatage et la signature de certificats, mais d'autres applications de certificats de serveur (certificats de fonction). De plus, un règlement technique [TAV-MWST] a été introduit pour définir les identités numériques (mieux : attributs numériques) à utiliser dans les certificats dans le contexte de la facturation électronique conforme avec la TVA.

7.9.5 Signature – numérisation des processus de cyberadministration

La SCSE, l'ordonnance OSCSE correspondante ainsi que ses prescriptions d'exécution [TAV] sont en vigueur (1.1.2017).

Depuis la révision correspondante du Code des obligations (CO), les signatures électroniques (dans la correspondance commerciale privée entre particuliers, mais pas entre particuliers et autorités ou entre autorités entre elles) sont réglementées, voir entre autres [DigSig]. La PA (procédure administrative au niveau fédéral) a été révisée suite aux nouvelles lois concernant le Tribunal fédéral. Dans le cadre de la procédure administrative avec les autorités, les documents peuvent être envoyés par voie électronique avec l'accord de deux

parties. L'envoi doit toutefois être doté d'une signature électronique reconnue, c'est-à-dire d'une signature qualifiée, qui peut être établie au moyen d'un certificat de l'un des prestataires reconnus selon la SCSE.

En conséquence, nous recommandons que lorsque des processus réels de cyberadministration sont numérisés et qu'une signature manuscrite est exigée pour eux, cette signature manuscrite soit remplacée par une signature électronique qualifiée, qui peut être vérifiée au moyen d'un certificat d'un prestataire reconnu.

Depuis le 1er janvier 2007 sont en vigueur la loi sur le Tribunal fédéral et la loi sur la procédure administrative qui permet l'envoi électronique de documents juridiques aux deux cours fédérales. Des signatures qualifiées reconnues sont également exigées dans ces cas.

7.9.6 Téléchargement de documents contenant des composantes actives (Java, JavaScript, ActiveX)

Si une opération doit, obligatoirement ou non, être effectuée avec la clé privée (de l'utilisateur), que ce soit pour l'authentification uniquement, pour la fourniture d'une signature électronique contraignante ou pour le décryptage d'un e-mail, on respectera les points suivants:

- Toute la procédure, de son début jusqu'à sa fin, doit être conçue de manière qu'aucun programme caché, tel que Java, JavaScript ou ActiveX, ne doive ou ne puisse être téléchargé.
- L'application sur le terminal utilisé pour la prestation de cyberadministration doit être configurée de manière que le téléchargement des programmes susmentionnés ne soit pas autorisé ou qu'il soit affiché à l'écran.
- Le processus de cyberadministration doit pouvoir se dérouler malgré le paramétrage mentionné ci-dessus.

7.9.7 Consultation du statut d'un certificat

Le statut d'un certificat peut être consulté à l'aide de la liste CRL ou du protocole OCSP. Les protocoles suivants pour la consultation des listes CRL devraient être supportés par les technologies de sécurité.

HTTP, LDAP	Vivement recommandé

Normes: voir chapitre 5.5 Protocoles d'application et Services d'annuaire chap. 5.7.

OCSP	Recommandé

Normes: voir chapitre Services d'annuaire.

7.9.8 Interface avec l'application

Après qu'une entité (p. ex. utilisateur, serveur, client) ait été authentifiée à partir de certificats, la technologie de sécurité devrait mettre une interface à disposition de l'application . Le contenu du certificat devrait être transmis à l'entité venant d'être authentifiée, via cette interface dont l'objectif est de procéder à l'autorisation sur la base d'une authentification reposant elle-même sur une clé publique. L'importance de ce processus est notamment décrite dans les ouvrages [Mud] et [Nem].

Interface avec l'application	En observation

Malheureusement, il n'existe aucune norme à ce sujet.

7.10 Vérification des signatures numériques

Nous posons dans ce chapitre les conditions minimales pour le contrôle des signatures numériques. La liste des critères mentionnés se fonde sur le IETF RFC 3850. Si un seul des critères ci-après est rempli, l'application de sécurité doit émettre un message d'erreur et, si les règles définies le prévoient, interrompre la communication.

- Le contrôle de la signature à l'aide de la clé publique dans le certificat correspondant n'aboutit pas.
- L'adresse de l'expéditeur indiquée dans l'application ou accessible à partir de celle-ci ne correspond pas à l'adresse figurant dans le certificat ou ne s'y trouve pas (d'où l'importance des recommandations des chapitres 7.9.4.2 et 7.9.8). Concernant l'importance de l'émission d'un message d'erreur, voir [Mus].
- La chaîne de certificats ne conduit pas à une autorité de certification (CA) à laquelle on fait confiance.
- La CRL et les informations de révocation (par ex. selon OCSP) ne peuvent pas être vérifiées.
- La CRL reçue n'est pas valable ou sa validité est échue.
- Le certificat est déjà échu ou a été révoqué.
- Le certificat ne dispose pas des Key Usage et Extended Key Usage correspondants

D'autres recommandations pour la production et le contrôle de signatures numériques figurent dans les recommandations techniques CWA 14170 et CWA 14171 du CEN.

7.11 Key Management

La gestion des clés implique des aspects complexes de la sécurité des TIC et revêt une importance fondamentale pour la sécurité des applications. Les principes de la gestion des clés sont décrits dans l'ISO/IEC 11770 partie 1 (des parties existantes 1 à 6 avec corrigenda).

7.11.1 Clés pour la signature et le chiffrement

Différentes clés doivent être utilisées pour la signature des données pour les E-mails ainsi que pour le chiffrement des données. Concernant la signature, l'expéditeur conserve toujours la clé, qui, dans certaines circonstances, est même générée sur la Smartcard qu'elle ne quitte jamais. Par la suite, les données signées une fois peuvent être vérifiées à tout moment au moyen de la clé publique, même si la clé privée n'est plus disponible.

Concernant le chiffrement, la clé privée du destinataire doit être encore disponible pour chaque opération de décryptage, faute de quoi les données ne pourront plus être déchiffrées et donc lues. Cette question est essentielle dans le domaine du «Long Term Storage», car les données qui y sont stockées une fois doivent pouvoir être lues correctement à une date ultérieure. C'est la raison pour laquelle la clé privée servant au décryptage doit être conservée de manière sûre et redondante (Key Escrow), afin qu'il soit toujours possible d'accéder aux données même lorsque la clé du destinataire est perdue. C'est la raison pour laquelle la clé privée doit être encore disponible dans au moins une copie (ex. sous forme de sauvegardes).

Key Escrow (Key Backup/Recovery)	Recommandé

Normes: ISO/IEC 11770.

7.11.2 Génération des clés

La norme *ETSI TS 102 176* définit comment doivent être générées les clés pour les différents algorithmes à clé publique. Elle définit également les tests que doivent passer les générateurs de chiffres aléatoires. Les générateurs de nombres aléatoires sont également utilisés pour générer des clés symétriques.

7.11.3 Conservation des clés

Voir chapitre 7.9.1 «Utilisation de cartes intelligentes (Smart Card)» et Standard PKCS#11 avec HSM (Hardware Security Module).

7.11.4 Interface pour les opérations avec des clés (privées)

Voir chapitre 7.9.1 «Utilisation de cartes intelligentes (Smart Card)» et Standard PKCS#11.

La norme PKCS#12 prévoit l'utilisation d'un fichier qui est intégré dans l'application de sécurité. Contrairement au cas de l'utilisation d'une smart crypto card, les clés privées peuvent alors être lues par l'application de sécurité.

PKCS#12 devrait être principalement appliqué dans un environnement de serveur, bien que nous préconisions ici aussi l'utilisation d'une carte HSM (Hardware Security Module avec redondance).

7.11.5 Changement de la clé lorsqu'elle doit être renouvelée

Le changement de la clé ne pose que peu de problèmes pour les communications confidentielles et authentifiées (voir aussi chapitre 7.7 «Données et connexions authentifiées et confidentielles»). Toutefois, des mesures de sécurité particulières doivent être prises pour protéger l'authenticité et la confidentialité des données.

- Confidentialité: assistant pour changement de clé (publique), rétablissement de clé (Key Recovery), dossiers cryptés dans lesquels plusieurs entités peuvent accéder aux données de différentes manières.
- Authenticité: (voir également ISO/IEC 19794 (JTC1/Sc37)).

7.11.6 Négociation d'une clé de session

Les applications et technologies de sécurité, telles que SSL ou IPSEC, définissent les procédures de négociation d'une clé de session. Ces procédures se basent le plus souvent sur le transfert de clé et la négociation en ligne (voir chapitre 7.6.1.4, 7.6.3).

7.11.7 Transport de clé

Un transfert de clé désigne le processus de transfert d'une clé, d'une entité à une autre, avec une protection raisonnable (voir ISO/IEC 11770-1 définition 2.33).

ISO/IEC11770 (partie 1-4)	Recommandé

Norme: Les parties 2 et 3 ne mentionnent aucun entête de message (n°.), messages d'erreur (etc.) au sens des protocoles de transport. La norme est encore très générale.

7.12 Coordination

Une coordination est nécessaire en matière d'attribution des noms (p. ex. WS Addressing), des contenus des certificats, de l'autorisation et de l'authentification ainsi que des interactions entre les différentes technologies de sécurité (p. ex. SSL/TLS avec SAML). De la sorte, la sécurité reste constante et ne subit aucune interruption. Des interruptions peuvent apparaître p. ex. lorsqu'un utilisateur de services web doit se faire authentifier plusieurs fois et de manière différente lors d'un processus de cyberadministration. *Cette coordination devrait être examinée et normalisée.*

8 Thèmes transversaux

8.1 Cloud Computing

Le Cloud Computing a donné naissance, dans les TIC et la cyberadministration, à de nouveaux modèles d'affaires, caractérisés par de nouvelles technologies de virtualisation, d'automatisation, des améliorations des performances des ordinateurs et des systèmes de stockage, ainsi que de nouveaux produits logiciels, sans oublier une plus vaste disponibilité et des débits plus élevés. A titre de synthèse de ces nouveaux environnements basés sur l'informatique et les télécommunications, les services apparus avec le Cloud Computing Service sont pour l'essentiel répartis entre les trois niveaux suivants:

- IaaS (Infrastructure as a Service),
- PaaS (Platform as a Service) et
- SaaS (Software as a Service).

Le terme Cloud Computing marque également une étape dans l'évolution des TIC dans le cadre de la quatrième révolution industrielle. Celle-ci peut être décrite comme l'époque au cours de laquelle les «produits et processus de décision autonomes, des réseaux de création de valeur sont pilotés quasiment en temps réel». Voir également le programme de cyberadministration de la Suisse http://www.egovernment.ch/index.html?lang=de

Normes de Cloud Computing	En observation

Normes: ISO/IEC 13187, 17203, 17788:2014, 17789:2014 (Reference architecture), 27018:2014, ITU SG13/17 Y.3501/3510/3520 X.1600, eCH 199 et autres pertinents.

Toujours à ce sujet, il existe d'autres thèmes ou questions juridiques distincts, qui doivent être clarifiés avec le partenaire contractuel (notamment la protection des données, l'obligation de confidentialité, les exigences AAA, la Legal Compliance, le lieu de conservation des données, la publication des données, le droit applicable et le for juridique).

A titre informatif: il est nécessaire d'observer les projets Confédération RZ2020 (consolidation du centre informatique) et Vision 2025 (consolidations des plateformes TIC dans le sens du Cloud).

NIST SP 500-291	En observation

Normes: pages 43-45, NIST SP800-144/146/147 .

CDMI (Cloud Management Interface) ISO 17826	En observation

Normes: voir Open Stack Foundation (notamment Open Source Standards); OASIS/CAMP, DMTF, SAGA.de, recommandations de sécurité BSI pour les opérateurs de Cloud Computing, CSA, ETSI, ENISA, y compris Compliance et Governance pertinente notamment (ISO 27001/27002, ISAE 3402).

8.2 Gestion de l'accès aux identités

Les recommandations suivantes sont pertinentes pour la gestion de l'accès aux identités (systèmes IAM/eID).

S1	S2	
ISO/IEC 29115:2013		En observation

Normes: voir aussi eCH 107 (principes de conception IAM) 167,168,169,170,171,172,174, PKCS#11, ISO/IEC 15408, ISO/IEC 24760 et autres pertinents.

Informations: voir Fédération suisse d'identités (B2.06), Eurocloud, EU STORK www.eid-stork.eu, FIDO Allianz, NIST.

8.3 IHE (eHealth)

IHE (abréviation d'*Integrating the Healthcare Enterprise*) est une initiative d'utilisateurs et de fabricants visant à standardiser et à harmoniser l'échange de données entre les systèmes informatiques dans le domaine de la santé. L'accent est mis à cet égard sur la mise en œuvre des procédures médicales entre les systèmes et la création de l'interopérabilité. IHE formule à ce sujet les exigences tirées de la pratique dans ce que l'on appelle les Use Cases, identifie les normes pertinentes et développe les lignes directrices techniques, appelées profils, qui permettent à un fabricant de réaliser et de tester son produit. A l'occasion d'un «Connectathon» international, les fabricants testent leurs systèmes entre eux et les préparent à la mise en pratique.

Jusqu'à l'entrée en vigueur de la législation suisse relative au dossier électronique des patients (LDEP, entrée en vigueur prévue en 2017, voir LDEP LAF), nous vous renvoyons à la décision 2015/1302 de la Commission européenne du 28 juillet 2015 concernant la détermination des profils «Integrating the Healthcare Enterprise», auxquels il convient de se référer lors de l'attribution de commandes publiques. Une partie des profils recommandés par l'UE sera utilisée en Suisse pour l'application de la LDEP. La référence à ces profils IHE est également judicieuse lors de l'acquistion de systèmes primaires pour la documentation clinique par des prestataires médicaux.

S1	S2	S3	
IHE Profile			Recommandé

Remarques: voir aussi IHE Suisse http://www.ihe-suisse.ch/ , ITU H81x/86x Continua, ISO, EU MSP, HL7 V.3, ETSI EG202952, CEN Ref. Model 13606 et pertinentes.

http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32015D1302&from=DE

8.4 Archivage

Certains des formats de fichier répertoriés au chapitre 6 sont titulaires du statut d'un format d'archive selon l'archive fédérale (AFS). Voir à ce sujet «formats de fichiers compatibles avec les archives»:

https://www.bar.admin.ch/bar/de/home/archivage/ablieferung/digitale-unterlagen.html

Catalogue des formats de fichier d'archive avec recommandations:
http://kost-ceco.ch/wiki/whelp/KaD/index.php

eCH-0160: Interface de versements d'archives

S1	S2	S3

Utilisation de formations de fichiers compatibles avec les archives	Vivement recommandé

Précision: il n'existe actuellement aucune règle obligatoire ni suffisante concernant les documents signés électroniquement.

8.5 Big Data

Le terme Big Data désigne des quantités de données, qui sont trop volumineuses ou trop complexes ou changent trop rapidement, pour être évaluées en s'appuyant sur les méthodes pratiques et classiques de traitement des données. Le terme «Big Data» lui-même ne cesse d'évoluer; ainsi il sert aussi bien souvent à décrire le complexe de technologies, qui sont utilisés pour collecter et évaluer de telles quantités de données. Les données collectées peuvent provenir de quasiment toutes les sources: à commencer par la communication électronique de quelque nature que ce soit, aux enregistrements des systèmes de surveillance les plus divers en passant par les données collectées par des autorités ou des entreprises.

Le souhait de l'industrie et de certaines autorités de bénéficier, dans la mesure du possible, d'un vaste accès à ces données, de pouvoir mieux les analyser et d'exploiter les enseignements tirés, entre toutefois en conflit avec les droits individuels (source: Wikipedia).

Le Big Data est un «effet» et une exigence politique (par exemple, les accès rapides à de nombreuses données différentes avec autant d'occurrences que possibles etc. sont particulièrement sollicités), voir Cloud Computing, Internet of Things et autres aspects pertinents (voir à ce sujet également ISO/IEC JTC1, ITU SG13). Le sujet est actuellement en phase d'observation et des recommandations SAGA Big Data à venir sont en cours d'étude et de révision, des discussions (notamment avec l'EPFL/ETHZ) et d'autres comparaisons avec les politiques de la Confédération sont nécessaires.

Voir PFPDT: http://www.edoeb.admin.ch/datenschutz/00683/01169/index.html?lang=de

9 Exclusion de responsabilité - droits de tiers

Les normes élaborées par l'Association eCH et mises gratuitement à la disposition des utilisateurs, ainsi que les normes de tiers adoptées, ont seulement valeur de recommandations. L'Association eCH ne peut en aucun cas être tenue pour responsable des décisions ou mesures prises par un utilisateur sur la base des documents qu'elle met à disposition. L'utilisateur est tenu d'étudier attentivement les documents avant de les mettre en application et au besoin de procéder aux consultations appropriées. Les normes eCH ne remplacent en aucun cas les consultations techniques, organisationnelles ou juridiques appropriées dans un cas concret.

Les documents, méthodes, normes, procédés ou produits référencés dans les normes eCH peuvent le cas échéant être protégés par des dispositions légales sur les marques, les droits d'auteur ou les brevets. L'obtention des autorisations nécessaires auprès des personnes ou organisations détentrices des droits relève de la seule responsabilité de l'utilisateur.

Bien que l'Association eCH mette tout en œuvre pour assurer la qualité des normes qu'elle publie, elle ne peut fournir aucune assurance ou garantie quant à l'absence d'erreur, l'actualité, l'exhaustivité et l'exactitude des documents et informations mis à disposition. La teneur des normes eCH peut être modifiée à tout moment sans préavis.

Toute responsabilité relative à des dommages que l'utilisateur pourrait subir par suite de l'utilisation des normes eCH est exclue dans les limites des réglementations applicables.

10 Droits d'auteur

Tout auteur de normes eCH en conserve la propriété intellectuelle. Il s’engage toutefois à mettre gratuitement, et pour autant que ce soit possible, la propriété intellectuelle en question ou ses droits à une propriété intellectuelle de tiers à la disposition des groupes de spécialistes respectifs ainsi qu’à l’association eCH, pour une utilisation et un développement sans restriction dans le cadre des buts de l’association.

Les normes élaborées par les groupes de spécialistes peuvent, moyennant mention des auteurs eCH respectifs, être utilisées, développées et déployées gratuitement et sans restriction.

Les normes eCH sont complètement documentées et libres de toutes restrictions relevant du droit des brevets ou de droits de licence. La documentation correspondante peut être obtenue gratuitement.

Les présentes dispositions s’appliquent exclusivement aux normes élaborées par eCH, non aux normes ou produits de tiers auxquels il est fait référence dans les normes eCH. Les normes incluront les références appropriées aux droits de tiers.

Annexe A – Références & bibliographie

Littérature spécialisée

[a006d] a006d Smart Card Version 1.3, Conseil informatique de la Confédération, Pascal Horner, Stefan Zbinden

[AcLs] Adams Carlisle, Lloyd Steve, Understanding Public-Key Infrastructure, MTP Publishing 1999, ISBN 1 57870 166 x

[Bek] Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung vom 2. Januar 2004, RegTP

[FiR] Roy T. Fielding, Architectural Styles and the Design of Network-based Software Architectures, Dissertation an University of California Irvine, www.ics.uci.edu/~fielding/pubs/dissertation/rest_arch_style.htm

[GSHB] Grundschutzhandbuch, Hrsg. Deutsches Bundesamt für Sicherheit, ISBN 3 88784 915 9, http://www.bsi.de/gshb/deutsch/menue.htm

[GuA] Gustavo Alonso, et al., Web Services, Springer Verlag, 2003, ISBN 3 540 44008 9

[Hem] Hein Mathias, TCP/IP, Thomson Publishing, 1998, 4ème édition, ISBN 3 8266 4035 7

[Hermes] Hermes, Conduite et déroulement de projets dans le domaine des technologies de l'information et de la communication, édité par l'unité de pilotage informatique de la Confédération, art. n°. 609.201 (vente comme publication de la Confédération; voir www.hermes.admin.ch)

[Mau] Maurer Ueli, Provable Security in Cryptography, Diss. ETH (Nr. 9260) 1990, referee J. Massey, co-referee W. Diffie

[MOV] Alfred Menezes, Paul van Orschot, Vanstone Scott, Handbook of Applied Cryptography, CRC Press 1996, ISBN 0 8493 8523 7 http://cacr.math.uwaterloo.ca/hac/

[Mud] Muster Daniel, Digitale Unterschriften und PKI, 3ème édition 2006, ISBN 3 9522387 3 3

[Nem] Mark O'Neal, et al, Web Services Security, Mc Graw Hill/ Osborne, 2003, ISBN 0 07 222471 1

[NaMa] Nussbacher Alfred, Mistlbacher August, XML Entpackt, MITP Press, 2002, ISBN 3 8266 0884 4

[RwEw] Rankl Wolfgang, Effing Wolfgang, Handbuch der Chipkarten, 3ème édition, Carl Hanser Verlag 1999, ISBN 3 446 21115 2

[Sad] Salomon David, Data Privacy and Security, Springer Verlag 2003, ISBN 0 387 00311 8

[Sch] Schneier Bruce, Angewandte Kryptographie, Addison Wesley, 1ère édition 1996, ISBN 3 89319 854 7

[Stw] Stallings William, Network and Internetwork Security, Prentice Hall 1995, ISBN 0 13 180050 7

[Vau]	Vaudenay Serge, Security Flaws induced by CBC Padding Applications to SSL, IPSEC, WTLS, Advances in Cryptology EUROCRYPT 02, Amsterdam, Netherlands, Lecture Notes in Computer Science No. 2332, pp. 534-545, Springer-Verlag, 2002 ou sur: http://lasecwww.epfl.ch/php_code/publications/search.php?ref=Vau02a
[WSA]	Web Services Architecture, W3C Working Group Note 11 February 2004 www.w3.org/TR/2004/NOTE-ws-arch-20040211/
[ZeCs]	Zwicky Elisabeth, Copper Simon, Einrichten von Internet Firewalls, O'Reilly 2001, ISBN 3 89721 346 X
[ZoT]	Zimmermann Olaf, Mark Tomlinson, Stefan Peuser, Perspectives on Web Services, Springer Verlag 2003, ISBN 3 540 00914 0
eGIF	eGovernment Interoperability Framework, EIF European Interoperability Framework
HERMES	Siehe www.hermes.admin.ch
Norme de cyberadministration France	Le cadre commun d'interopérabilité des systèmes d'information publics
SAGA.de	Standards und Architekturen für E-Government-Anwendungen in Deutschland, V.4.0, Bundesministerium des Innern
eGIF Nouvelle-Zélande	Interoperability eGIF

Textes législatifs (www.admin.ch Recueil systématique du droit fédéral)

[TAV]	Prescriptions techniques et administratives de l'OFCOM du 6 décembre 2004 concernant les services de certification dans le domaine de la signature électronique (RS 943.032.1)
[TAV-MWST]	Ordonnance de l'AFC du 12 octobre 2007 sur les services de certification dans le domaine de l'OelDI: Prescriptions techniques et administratives du DFF sur les services de certification dans le cadre de l'OelDI en rapport avec l'émission de certificats se fondant sur des signatures avancées1 (RS 641.201.11)
LTF	Loi fédérale du 17 juin 2005 sur le tribunal fédéral (RS 173.110)
OIAF	Ordonnance du 26 septembre 2003 sur l'informatique et la télécommunication dans l'administration fédérale (Ordonnance sur l'informatique dans l'administration fédérale (RS 172.010.58)
OelDI	Ordonnance du DFF du 30 janvier 2002 concernant les données et informations électroniques (RS 641.201.1)
CO	Loi fédérale du 30 mars 1911 complétant le code civil suisse (Livre cinquième: Droit des obligations; RS 220)
LTAF	Loi fédérale du 17 juin 2005 sur le tribunal administratif fédéral (RS 173.32)
PA	Loi fédérale du 20 décembre 1968 sur la procédure administrative (RS 172.021)
OSCSE	Ordonnance du 23 novembre 2016 sur les services de certification dans le domaine de la signature électronique (RS 943.032) et autres applications des certificats numériques
WIsB	Directives du CI concernant la sécurité informatique dans l'administration fédérale
SCSE	Loi fédérale du 18 mars 2016 sur les services de certification dans le domaine de la signature électronique (RS 943.03) et autres applications des certificats numériques

Normes du CEN (www.cen.eu) (www.cencenelec.eu)

CWA 14170: CEN (European Committee for Standardization), Security Requirements for Signature Creation Applications, May 2004

CWA 14171 CEN (European Committee for Standardization), General Guidelines for electronic signature verification, May 2004

CWA 16667 CEN (European Committee for Standardization), Reference Architecture, 2013

CEN eHealth Reference Model EN 13606 (Health informatics - Electronic Health Record Communication)

eCH (www.ech.ch)

eCH-0018	XML Best Practices
eCH-0036	Documentation pour l'échange de données orienté XML
eCH-xxxx	Autres normes eCH de cyberadministration voir www.ech.ch

ECMA (www.ecma-international.org)

Normes Open Office XML Format

ECMA xx	Autres documents ECMA voir ECMA International

ESTI (www.etsi.org)

ETSI TS 102 176 v.1.2.1	Electronic Signatures and Infrastructures (ESI) - Algorithms and Parameters for Secure Electronic Signatures
ETSI EN/ES	Autres normes/standards ETSI (ETSI Guidelines-EG) voir www.etsi.org

Normes IEEE (www.ieee.org)

IEEE P1363	Standard for RSA, Diffie-Hellman and related Public-Key Cryptography
IEEE xx.x	Autres normes IEEE voir www.ieee.org

Normes IETF (www.ietf.org)

RFC 768	User Datagram Protocol
RFC 791	Internet Protocol
RFC 793	Transmission Control Protocol
RFC 959	File Transfer Protocol
RFC 1050	Remote Procedure Call Protocol Specification
RFC 1123	Requirements for Internet Hosts - Application and Support
RFC 1180	TCP/IP Tutorial
RFC 1321	The MD5 Message Digest Algorithm
RFC 1349	Type of Service in the Internet Protocol Suite
RFC 1730	Internet Message Access Protocol Version 4
RFC 1750	Randomness Recommendations for Security
RFC 1831	Remote Procedure Call Protocol Specification. Version 2
RFC 1866	Hypertext Markup Language - 2.0.
RFC 1939	Post Office Protocol - Version 3
RFC 1945	Hypertext Transfer Protocol 1.0
RFC 1950	ZLIB Compressed Data Format Specification version 3.3
RFC 1951	DEFLATE Compressed Data Format Specification version 1.3
RFC 1952	GZIP File Format Specification Version 4.3
RFC 2015	MIME Security with Pretty Good Privacy (PGP)
RFC 2047	MIME (Multipurpose Internet Mail Extensions) Part Three: Message Header Extensions for Non-ASCII Text
RFC 2048	Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures
RFC 2049	Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples
RFC 2060	Internet Message Access Protocol - Version 4rev1
RFC 2083	PNG (Portable Network Graphics) Specification Version 1.0-Informational
RFC 2104	HMAC Keyed-Hashing for Message Authentication

RFC 2228	FTP Security Extensions
RFC 2231	MIME Parameter Value and Encoded Word Extensions: Character Sets, Languages, and Continuations
RFC 2242	Security Architecture for the Internet Protocol
RFC 2246	Transport Layer Security (TLS)
RFC 2251	LDAPv.3 Lightweight Directory Access Protocol
RFC 2311	S/MIME Version 2 Message Specification et apparentés
RFC 2315	PKCS #7: Cryptographic Message Syntax Version
RFC 2402	IP Authentication Header
RFC 2407	DOI The Internet IP Security Domain of Interpretation for ISAKMP
RFC 2408	ISAKMP Internet Security Association and Key Management Protocol
RFC 2412	The Oakley Key Determination Protocol
RFC 2439	POP3 Extension Mechanism
RFC 2440	PGP Message Exchange Formats
RFC 2460	Internet Protocol, Version 6 (IPv6)
RFC 2518	HTTP Extensions for Distributed Authoring – WEBDAV
RFC 2605	X.500 Directory Monitoring MIB
RFC 2616	Hypertext Transfer Protocol 1.1 (obsolète, voir nouveau: RFC 7230)
RFC 2631	Diffie-Hellman Key Agreement Method
RFC 2634	Enhanced Security Services for S/MIME
RFC 2640	Internationalization of the File Transfer Protocol
RFC 2817	Upgrading to TLS Within HTTP/1.1 (mises à jour par RFC 7230)
RFC 2821	Simple Mail Transfer Protocol
RFC 2822	Internet Message Format
RFC 2849	The LDAP Data Interchange Format
RFC 2854	The 'text/html' Media Type.
RFC 2965	HTTP State Management Mechanism
RFC 3126	*Electronic* Signature Formats for long term electronic Signatures
RFC 3156	MIME Security with Pretty Good Privacy (PGP)
RFC 3161	Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)
RFC 3174	US Secure Hash Algorithm 1 (SHA-1)
RFC 3232	Assigned Numbers
RFC 3265	Session Initiation Protocol (SIP)-Specific Event Notification
RFC 3275	XML Signature Syntax and Processing
RFC 3279	Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL)
RFC 3280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

RFC 3302	Tag Image File Format (TIFF) - image/tiff MIME Sub-type Registration
RFC 3315	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
RFC 3384	LDAP (version 3) Replication Requirements
RFC 3470	Guidelines for the Use of Extensible Markup Language (XML) within IETF Protocols
RFC 3501	Internet Message Access Protocol - version 4rev1
RFC 3546	Transport Layer Security (TLS) Extensions
RFC 3550	RTP: A Transport Protocol for Real-Time Applications
RFC 3551	RTP Profile for Audio and Video Conferences with Minimal Control
RFC 3629	UTF-8, a transformation format of ISO 10646
RFC 3633	IPv6 Prefix Options for DHCPv6
RFC 3648	WebDAV Ordered Collections Protocol
RFC 3676	The Text/Plain Format and DelSp Parameters
RFC 3711	The Secure Real-time Transport Protocol (SRTP)
RFC 3739	Qualified Certificates Profile
RFC 3744	WebDAV Access Control Protocol
RFC 3798	Message Disposition Notification
RFC 3850	S/MIME v.3.1 Certificate Handling
RFC 3851	Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1
RFC 3853	S/MIME Advanced Encryption Standard (AES) Requirement for the Session Initiation Protocol (SIP)
RFC 3922	Mapping XMPP to CMIP
RFC 3923	End to End Signing and Object Encryption to XMPP
RFC 3947	Negotiation of NAT-Traversal in the IKE
RFC 3950	Tag Image File Format Fax eXtended (TIFF-FX) - image/tiff-fx MIME Sub-type Registration
RFC 3972	Cryptographically Generated Adresses
RFC 4109	Algorithms for Internet Key Exchange version 1 (IKEv1)
RFC 4168	The Stream Control Transmission Protocol (SCTP) as a Transport for the Session Initiation Protocol (SIP)
RFC 4180	Common Format and MIME Type for Comma-Separated Values (CSV) Files
RFC 4227	Using the Simple Object Access Protocol (SOAP) in Blocks Extensible Exchange Protocol (BEEP)
RFC 4250	The Secure Shell (SSH) Protocol Assigned Numbers
RFC 4251	The Secure Shell (SSH) Protocol Architecture
RFC 4252	The Secure Shell (SSH) Authentication Protocol
RFC 4253	The Secure Shell (SSH) Transport Layer Protocol
RFC 4254	The Secure Shell (SSH) Connection Protocol

RFC 4255	Using DNS to Securely Publish Secure Shell (SSH) Key Fingerprints
RFC 4256	Generic Message Exchange Authentication for the Secure Shell Protocol (SSH)
RFC 4288	Media Type Specifications and Registration Procedures BCP
RFC 4287	The Atom Syndication Format
RFC 4289	Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures BCP
RFC 4294	IPv6 Node Requirements
RFC 4303	IP Encapsulating Security Payload (ESP)
RFC 4306	The Internet Key Exchange (IKE v.2) Protocol
RFC 4320	Actions Addressing Identified Issues with the Session Initiation Protocol's (SIP) Non-INVITE Transaction
RFC 4331	Quota and Size Properties for Distributed Authoring and Versioning (DAV) Collections
RFC 4332	Cisco's Mobile IPv4 Host Configuration Extensions (Informational)
RFC 4344	The Secure Shell (SSH) Transport Layer Encryption Modes
RFC 4346	The Transport Layer Security (TLS) Protocol Version 1.1
RFC 4403	Lightweight Directory Access Protocol (LDAP) Schema for Universal Description, Discovery, and Integration version 3 (UDDIv3) (Informational)
RFC 4419	Diffie-Hellman Group Exchange for the Secure Shell (SSH) Transport Layer Protocol
RFC 4462	Generic Security Service Application Program Interface (GSS-API) Authentication and Key Exchange for the Secure Shell (SSH) Protocol
RFC 4510	Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map
RFC 4511	Lightweight Directory Access Protocol (LDAP): The Protocol
RFC 4512	Lightweight Directory Access Protocol (LDAP): Directory Information Models
RFC 4513	Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms
RFC 4514	Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names
RFC 4515	Lightweight Directory Access Protocol (LDAP): String Representation of Search Filters
RFC 4523	Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates
RFC 4524	COSINE LDAP/X.500 Schema
RFC 4738	MIKEY-RSA-R: An Additional Mode of Key Distribution in Multimédias Internet KEYing (MIKEY)
RFC 4853	Cryptographic Message Syntax (CMS) Multiple Signer Clarification
RFC 4862	IPv6 Stateless Adress Autoconfiguration
RFC 4880	OpenPGP Message Format

RFC 4884	Extended ICMP to Support Multi-Part Adresses
RFC 4916	Connected Identity in the Session Initiation Protocol (SIP)
RFC 5013	The Dublin Core Metadata Element Set
RFC 5035	Enhanced Security Services (ESS) Update: Adding CertID Algorithm Agility
RFC 5083	Cryptographic Message Syntax (CMS) Authenticated-Enveloped-Data Content Type
RFC 5095	Deprecation of Type 0 Routing Headers in IPv6
RFC 5096	Mobile IPv6 Experimental Messages
RFC 5126	CMS Advanced Electronic Signatures (CAdES)
RFC 5147	URI Fragment Identifiers for the text/plain Media Type
RFC 5246	The Transport Layer Security (TLS) Protocol Version 1.2
RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
RFC 5323	WebDAV Search
RFC 5354	OGG Media Types
RFC 5367	Subscriptions to Request-Contained Resource Lists in the Session Initiation Protocol (SIP)
RFC 5371	RTP Payload Format for JPEG 2000 Video Streams
RFC 5372	Payload Format for JPEG 2000 Video: Extensions for Scalability and Main Header Recovery
RFC 5393	Addressing an Amplification Vulnerability in Session Initiation Protocol (SIP) Forking Proxies
RFC 5397	WebDAV Current Principal Extensions
RFC 5393	Addressing an Amplification Vulnerability in Session Initiation Protocol (SIP) Forking Proxies
RFC 5506	Support for Reduced-Size Real-Time Transport Control Protocol (RTCP): Opportunities and Consequences
RFC 5531	RPC Specification V2
RFC 5581	The Camellia Cipher in OpenPGP (Informational)
RFC 5621	Message Body Handling in the Session Initiation Protocol (SIP)
RFC 5622	Profile for Datagram Congestion Control Protocol (DCCP) Congestion ID 4: TCP-Friendly Rate Control for Small Packets (TFRC-SP)
RFC 5626	Managing Client-Initiated Connections in the Session Initiation Protocol (SIP)
RFC 5630	The Use of the SIPS URI Scheme in the Session Initiation Protocol (SIP)
RFC 5639	Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation (Informational)
RFC 5652	Cryptographic Message Syntax (CMS)
RFC 5665	RPC Network Identifiers und Universal Adress Formats
RFC 5666	Remote Direct Memory Access Transport for RPC

RFC 5689	Extended MKCOL for WebDAV
RFC 5717	Partial Lock for RPC for NETCONF
RFC 5746	Transport Layer Security (TLS) Renegotiation Indication Extension
RFC 5751	Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification
RFC 5761	Multiplexing RTP Data and Control Packets on a Single Port
RFC 5785	Defining Well-Known Uniform Resource Identifiers (URI's)
RFC 5797	FTP Command and Extension Registry
RFC 5816	ESSCertIDv2 mis à jour par RFC 3161
RFC 5922	Domain Certificates in the Session Initiation Protocol (SIP)
RFC 5942	IPv6 Subnet Model
RFC 5988	Web Linking
RFC 5994	Application of Ethernet Pseudowires to MPLS Transport Networks
RFC 5998	An Extension for EAP-Only Authentication in IKEv2
RFC 6026	Correct Transaction Handling for 2xx Responses to Session Initiation Protocol (SIP) INVITE Requests
RFC 6051	Rapid Synchronisation of RTP Flows
RFC 6052	IPv6 Adressing of IPv4/IPv6 Translators
RFC 6141	Re-INVITE and Target-Refresh Request Handling in the Session Initiation Protocol (SIP)
RFC 6151	Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms
RFC 6152	SMTP Services Extension for 8 bit MIME Transport
RFC 6186	Use of SRV Records for Locating Email Submission/Access Services
RFC 6222	Guidelines for Choosing RTP Control Protocol (RTCP) Canonical Names (CNAMEs)
RFC 6234	US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)
RFC 6237	IMAP4 Multimailbox SEARCH Extension
RFC 6239	Suite B Cryptographic Suites for Secure Shell (SSH) (Informational)
RFC 6242	Using the NETCONF Protocol over Secure Shell (SSH)
RFC 6275	Mobility Support in IPv6
RFC 6323	Sender RTT Estimate Option for the Datagram Congestion Control Protocol (DCCP)
RFC 6347	Datagram Transport Layer Security Version 1.2
RFC 6437	IPv6 Flow Label Specification
RFC 6446	Session Initiation Protocol (SIP) Event Notification Extension for Notification Rate Control
RFC 6532	Internationalized Email Headers
RFC 6533	Internationalized Delivery Status and Disposition Notifications

RFC 6540	IPv6 Support Required for all IPv6-Capable Nodes
RFC 6657	Updated to MIME regarding "charset" Parameter Handling in Textual Media Types
RFC 6665	SIP-Specific Event Notification
RFC 6690	Constrained RESTful Environments (CoRE) Link Format
RFC 6749	The OAuth 2.0 Authorization Framework
RFC 6764	Locating Services for Calendaring Extensions and vCard Extensions to WebDAV
RFC 6878	IANA Registry for the Session Initiation Protocol (SIP) "Priority" Header Field
RFC 6904	Encryption of Header Extensions in the Secure Real-time Transport Protocol (SRTP)
RFC 6960	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
RFC 6969	OSPFv3 Instance Id Registry mis à jour
RFC 6989	Additional Diffie-Hellman Tests for the Internet Key Exchange Protocol Version 2 (IKEv2)
RFC 7007	Update to Remove DVI4 from the Recommended Codecs for the RTP Profile for Audio and Video Conferences with Minimal Control (RTP/AVP)
RFC 7022	Guidelines for Choosing RTP Control Protocol (RTCP) Canonical Names (CNAMEs)
RFC 7048	Neighbor Unreachability Detection is Too Impatient
RFC 7111	URI Fragment Identifiers for the text/csv Media Type
RFC 7118	The WebSocket Protocol as a Transport for the Session Initiation Protocol (SIP)
RFC 7151	File Transport Protocol Host Command for Virtual Hosts
RFC 7159	The application/json Media Type for JavaScript Object Notation (JSON)
RFC 7162	IMAP Extensions: Quick Flag Changes Resynchronization (CONDSTORE) and Quick Mailbox Resynchronization (QRESYNC)
RFC 7164	RTP and Leap Seconds
RFC 7230-40	Hypertext Transfer Protocol
RFC 7247	Interworking SIP and XMPP Architecture, Adresses and Error Handling
RFC 7248	Interworking SIP and XMPP, Presence
RFC 7296	Internet Exchange Protocol V.2 (IKE)
RFC 7321	Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)
RFC 7346	IPv6 Multicast Adress Scopes
RFC 7371	Updates to the IPv6 Multicast Adressing Architectures
RFC 7373	IPVIX
RFC 7377	IMAP4 Multimailbox SEARCH Extension

RFC 7381	Enterprise IPv6 Deployment Guidelines
RFC 7427	Signature Authentication in the Internet Key Exchange Version 2 (IKEv2)
RFC 7462	URNs for the Alert-Info Header Field of the Session Initiation Protocol (SIP)
RFC 7463	Shared Appearances of a Session Initiation Protocol (SIP) Address of Record (AOR)
RFC 7572	Interworking SIP and XMPP, Instant Messaging
RFC 7573	Interworking SIP and XMPP, One to One Text Chat Sessions
RFC 7507	TLS Fallback Signaling Cipher Suite Value (SCSV) for Preventing Protocol Downgrade Attacks
RFC 7590	Use of TLS and XMPP
RFC 7621	A Clarification on the Use of Globally Routable User Agent URIs (GRUUs) in the SIP Event Notification Framework
RFC 7622	XMPP Adress Format
RFC 7670	Generic Raw Public-Key Support for IKEv2
RFC 7672	SNMP via DANE
RFC 7692	Compression Extensions for Wegsockets
RFC 7748	Elliptic Curves for Security
RFC 7878	Session Peering Provisioning (SPP) Protocol over SOAP
RFC 7936	Clarifying Registry Procedures for the WebSocket Subprotocol Name Registry
RFC 7957	DISPATCH-Style Working Groups and the SIP Change Process
RFC 7700	Preparation, Enforcement, and Comparison of Internationalized Strings Representing Nicknames
RFC 7702	Interworking between the Session Initiation Protocol (SIP) and the Extensible Messaging and Presence Protocol (XMPP): Groupchat
RFC 7809	Calendaring Extensions to WebDAV
RFC 7816	RPC Security V.3
RFC 7905	ChaCha20-Poly1305 Cipher Suites for Transport Layer Security (TLS)
RFC 7953	Calendar Availability (WebDAV)
RFC 8017	PKCS #1: RSA Cryptography Specifications Version 2.2
RFC 8027	DNSSEC Roadblock Avoidance
RFC 8031	IKEv2 Key Agreement
RFC 8035	Session Description Protocol (SDP) Offer/Answer Clarifications for RTP/RTCP Multiplexing

Normes ISO (www.iso.org)

ISO 7498 2	Information processing systems, Open Systems Interconnection, Basic Reference Model Part 2 Security Architecture
ISO/IEC 7816 all parts 1-4	Identification Cards-Integrated Circuits
ISO/IEC 8859 Teil 1-16	Information technology -- 8-bit single-byte coded graphic character sets
ISO/IEC 9945 Corr.1 2013	Information technology -- Portable Operating System Interface (POSIX®) Base Specifications, Issue 7 (2009; Plus corrigenda 1 2013)
ISO/IEC 10018 2012	Quality management -- Guidelines on people involvement and competence
ISO/IEC 10116 2006	Information technology -- Security techniques -- Modes of operation for an n-bit block cipher (plus Corrigendum1)
ISO/IEC 10646 2014/Amd1-2015/Amd2-2016	Information technology -- Universal Coded Character Set (UCS)
ISO/IEC 10918	Information technology -- Digital compression and coding (6 different parts)
ISO 11172 1-5	Information technology -- Coding of moving pictures and associated audio for digital storage media at up to about 1,5 Mbit/s (plus corrigenda)
ISO 11770 1-6	Information technology -- Security techniques -- Key management (plus corrigenda)
ISO 12234-2 2001	Electronic still-picture imaging -- Removable memory -- Part 2: TIFF/EP image data format
ISO 12639 2001	Graphic technology -- Prepress digital data exchange -- Tag image file format for image technology (TIFF/IT); plus Amd.2007
ISO 13157 1-5 2016	Information technology -- Telecommunications and information exchange between systems -- NFC Security
ISO 13187 2011	Information technology -- Server management command line protocol (SM CLP) specification
ISO 13818 1-11 2016	Information technology -- Generic coding of moving pictures and associated audio information (all 11 parts including corrigenda/amd.)
ISO 14289-1 2014	Document management applications -- Electronic document file format enhancement for accessibility -- Part 1: Use of ISO 32000-1 (PDF/UA-1)
ISO 14443 1-4 2016	Identification cards -- Contactless integrated circuit cards
ISO 14496 1-27 2016	Information technology -- Coding of audio-visual objects (all 27 parts including corrigenda/Amd.); See the MP4 12/14 parts
ISO/IEC 14496-14	Information technology - Coding of audio-visual objects - Part 14: MP4 file format
ISO/IEC 14533 1-2	Processes, data elements and documents in commerce, industry and administration; Part 1 2014, Part 2 2012
ISO 14662 2010	Information technology -- Open-edi reference model

ISO 14721 2012	Space data and information transfer systems -- Open archival information system (OAIS) -- Reference model
ISO 14888 1-3 2016	Information technology -- Security techniques -- Digital signatures with appendix
ISO 15000 1-5-2014	Electronic Business Extensible Markup Language (ebXML)
ISO 15408 1-3-2009	Information technology -- Security techniques -- Evaluation criteria for IT security
ISO 15444 1-13-2016	Information technology -- JPEG 2000 image coding system (13 different parts encluding corrigenda/Amd.)
ISO 15445 2000	Information technology -- Document description and processing languages -- HyperText Markup Language (HTML)
ISO 15489 2016	Information and documentation -- Records management -- Part 1: Concepts and principles
ISO 15693 1-3	Identification cards -- Contactless integrated circuit cards -- Vicinity cards – Parts 1-3 with Amds.2/3 2015
ISO 15836 2009+Corr.1	Information and documentation -- The Dublin Core metadata element set
ISO 15930 1-8 Corr.2011	Graphic technology -- Prepress digital data exchange using PDF
ISO 15489-1 2016	Information and documentation -- Records management -- Part 1: Concepts and principles
ISO 15946 2016	Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves
ISO 15948 2004	Information technology -- Computer graphics and image processing -- Portable Network Graphics (PNG): Functional specification
ISO/IEC 16262-2011	Information technology -- Programming languages, their environments and system software interfaces -- ECMAScript language specification
ISO 16612-2 2010	Graphic technology -- Variable data exchange -- Part 2: Using PDF/X-4 and PDF/X-5 (PDF/VT-1 and PDF/VT-2)
ISO/IEC 17203 2011	Information technology -- Open Virtualization Format (OVF) specification
ISO/IEC 17788 2014	Information technology -- Cloud computing -- Overview and vocabulary
ISO/IEC 17789 2014	Information technology -- Cloud computing -- Reference architecture
ISO/IEC 17826 2016	Information technology -- Cloud Data Management Interface (CDMI)
ISO 18000 1-64	Information technology -- Radio frequency identification for item management (Part 1 bis 64)
ISO 18031 2011	Information technology -- Security techniques -- Random bit generation (plus corrigendum1-2014)
ISO 18033 1-3-2015	Information technology -- Security techniques (partie 1 à 3)

ISO 18092 2013	Information technology -- Telecommunications and information exchange between systems -- Near Field Communication -- Interface and Protocol (NFCIP-1)(plus corrigenda 1 2015)
ISO 19005 1-3-2005/12	Document management - Partie 1 à 3 avec corrigenda
ISO/IEC 19107-2003	Geographic information -- Spatial schema
ISO/IEC 19128-2005	Geographic information -- Web map server interface
ISO/IEC 19136-2007 Part2-2015	Geographic information -- Geography Markup Language (GML)
ISO/IEC 19142-2010	Geographic information -- Web Feature Service
ISO/IEC 19503-2005	Information technology -- XML Metadata Interchange (XMI)
ISO/IEC 19509-2014	Information technology -- Object Management Group XML Metadata Interchange (XMI)
ISO/IEC 19505-2012	Information technology -- Object Management Group Unified Modeling Language (OMG UML)-Part1/2
ISO/IEC 19510-2013	Information technology -- Object Management Group Business Process Model and Notation
19510-2015	Information technology -- Metamodel framework for interoperability (MFI) -- Part 5: Metamodel for process model registration
ISO 19757 all Parts	Information technology -- Document Schema Definition Languages (DSDL)--with corrigenda 2016
ISO 19770-1 2012	Information technology -- Software asset management -- Part 1: Processes and tiered assessment of conformance
ISO 19794 1-11 2015	Information technology -- Biometric data interchange formats (parts 1-11 and corrigenda)
ISO/IEC 19845-2015	Information technology -- Universal business language version 2.1 (UBL v2.1)
ISO/IEC 20802-2 2016	Information technology -- Open data protocol (OData) v4.0 -- Part 2: OData JSON Format
ISO 21481 2012	Information technology -- Telecommunications and information exchange between systems -- Near Field Communication Interface and Protocol -2 (NFCIP-2)
ISO 23081	Information and documentation -- Records management processes; Part 1 2006-Part 2 2009-Part 3 2011
ISO/IEC 24156-2014	Graphic notations for concept modelling in terminology work and its relationship with UML -- Part 1: Guidelines for using UML notation in terminology work
ISO 24517 2008	Document management -- Engineering document format using PDF -- Part 1: Use of PDF 1.6 (PDF/E-1)
ISO 24727 1-	Identification cards -- Integrated circuit card programming interfaces (plus

6	différents amd. et corrigenda)
ISO/IEC 24760 1-3 2016	Information technology -- Security techniques -- A framework for identity management
ISO/IEC 26300	Information technology -- Open Document Format for Office Applications (OpenDocument)- différents corrigenda/amd/parties
ISO/IEC 26429 3-10 2008/9	Digital cinema (D-cinema) packaging
ISO/IEC 2700x	Information technology -- Security techniques -- Information security management systems (voir toutes les partis/corrigenda)
ISO/IEC 27014 2013	Information technology -- Security techniques -- Governance of information security
ISO/IEC 27018 2014	Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
ISO/IEC 29115 2013	Information technology -- Security techniques -- Entity authentication assurance framework
ISO/IEC 29199 1-5 2015	Information technology -- JPEG XR image coding system; différents corrigenda/amds.
ISO/IEC 29500 1-4	Information technology - Document description and processing languages - Office Open XML File Formats
ISO/IEC 32000-2008	Document management -- Portable document format
ISO/IEC 40500-2012	Information technology -- W3C Web Content Accessibility Guidelines (WCAG) 2.0

Normes ITU (www.itu.org)

ITU-T X.509v.3	Information Technology - Open Systems Inter-connections - Public Key and Attribute Certificate Framework
ITU-T X.519	Information Technology - Open Systems Inter-connections – The Directory: Protocol Specification
ITU-T X.525	Information Technology - Open Systems Inter-connections – The Directory: Replication
ITU S.G.13/17	Y3501, 3510, 3520, X1600 et supplémentaires

Normes NIST (www.nist.gov)

FIPS 46-3	DES Digital Encryption Standard
FIPS 81	DES Modes of Operation
FIPS 180-1	SHA Secure Hash Algorithm
FIPS 180-3/4	SHA 224/256/384/512 Secure Hash Algorithm
FIPS 186-2	DSS Digital Signature Standard
FIPS 197	AES Advanced Encryption Standard

Normes OASIS (www.oasis-open.org)

Business Process Execution Language for Web Service v.1.1, December 2003

Directory Services Markup Language (DSML) v.2.0, January 2002

ebXML Collaborative Partner Profile Agreement (CPPA) v.2, June 2002

ebXML Messaging Service Specification v.2.0, April 2002

ebXML Registry Information Model (RIM) v.2.0, March 2002

ebXML Registry Services Specification (RS) v.2.0, February 2002

Extensible Access Control Markup Language (XACML) v.1.0, January 2003

OASIS Open Document Format for Office Applications v.1.0 May 2005

Security Assertion Markup Language (SAML) v.1.1, March 2003

Universal Description, Discovery and Integration (UDDI) v.2.0, February 2003, v.3

Username Token Profile, Working Draft, August 2003

Web Services Atomic Transaction Version 1.1. 12. July 2007

Web Services Business Activity Version 1.1 + errata, 12. July 2007

Web Services Coordination (WS-Coordination) Version 1.1 + errata, 12. July 2007

Web Services Policy 1.5 Framework, 4.September 2007

Web Services Reliable Messaging, Version 1.1, 7. January 2008

Web Services Security Rights Expression Language (REL) Token Profile 1.1, 1st February 2006

Web Services Security SAML Token Profile 1.1, 1st February 2006

Web Services Security UsernameToken Profile 1.1, February 2006

Web Services Security X.509 Certificate Token Profile 1.1 + errata, November 2006

Web Services Security, SOAP Messages Security 1.0, March 2004

Web Services Security, SOAP Messages with Attachments (SwA) Profile 1.1, 1. February 2006

Web Services Trust 1.3, 19. March 2007

Plus de normes OASIS sur oasis.org

Object Management Group (www.omg.org)

Unified Modeling Language (UML)

BPMN 2.0, OMG Final Adopted Specification, January 2011

OMA (www.openmobilealliance.org), WAP Forum (www.wapforum.org)

WTLS, Wireless Transport Layer Security

WAP, Wireless Application Protocol Architecture

WDP, Wireless Datagram Protocol

WSP, Wireless Session Protocol Specification

WTP, Wireless Transaction Protocol

Online Service Computer Interface (www.osci.de)

OSCI-Transport v.1.2/2 Online Service Computer Interface

PC/SC (www.pcscworkgroup.com)

PC/SC	Interoperability Specification for ICCs and Personal Computer Systems

RSA Standards (www.rsa.com)

PKCS#1	RSA Encryption Standard v.2.1
PKCS#3	Diffie-Hellman Key Agreement Standard
PKCS#7	Cryptographic Message Syntax Standard v.1.5
PKCS#11	Cryptographic Token Interface Standard
PKCS#12	Personal Information Exchange Syntax Standard

Association suisse de normalisation SNV (www.snv.ch)

SN 612030 Interlis Version 1

SN 612031 Interlis Version 2

SNR CWA 14842-3: 2003 Electronic Commerce – Shop presentation and transactions-Part 3: ICT security requirements

SNR CWA 14842-1: 2003 Electronic Commerce – Shop presentation and transactions-Part 1: Regulatory and self-regulatory requirements

Normes WFMC (www.wfmc.org)

XML Process Definition Language (XPDL) Version 2.X

Normes W3C (www.w3C.org)

CSS Cascading Style Sheet Recommendation 2.0, 12 May 1998

HTML 4.01 Specification W3C Recommendation, 24 December1999

PNG Portable Network Graphics, W3C Recommendation, 10 November 2003

RDF Resource Description Framework Model und Syntax Specification Recommendation,

22 February 1999

SOAP v.1.2, June 2003

SVG Scalable Vector Graphic, W3C Recommendation 1.1, 14 January 2003

WSDL Web Services Description Language v.1.1, 15 March 2001

WSDL Web Services Description Language Version 2.0 Part 1: Core Language, 26 June 2007

XHTML Extensible Hypertext Markup Language Recommendation 2.0, August 2002

XKML XML Key Management Specification v.2.0, Draft April 2003

XKMS, XML Key Management Specification (XKMS) Recommendation 2.0, 28 June 2005

XML Encryption and Syntax Processing Recommendation, December 2002

XML Extensible Markup Language (XML) Recommendation v.1.1, November 2003

XML Schema Part 0: Primer Second Edition, W3C Recommendation, 28 October 2004

XML Schema Part 0: Primer, W3C Recommendation, 2nd May 2001

XML Schema Part 1: Structures Second Edition, W3C Recommendation, 28 October 2004

XML Schema Part 1: Structures W3C Recommendation 2nd May 2001

XML Schema Part 2: Datatypes Second Edition, W3C Recommendation, 28 October 2001

XML Schema Part 2: Datatypes W3C Recommendation 2nd May 2001

XML Signature and Syntax Processing Recommendation, February 2002

XML Path Language (XPath) Version 1.0, W3C Recommendation, 16 November 1999

XML Path Language (XPath) 2.0, W3C Recommendation, 23 January 2007

Annexe B – Abréviations

2D	Bidimensionnel
3DES	Triple DES
ACL	Access Control List
ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
AJAX	Asynchronous JavaScript and XML
ANSI	American National Standards Institute
APEC	Asia-Pacific Economic Cooperation
API	Application Programmers Interface
Appl.	Application
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange

OFCOM	Office fédéral de la communication
B2B	Business to Business
B2C	Business to Customer
BGP	Border Gateway Protocol
BMI	(Deutsches) Bundesministerium des Innern
BPEL	Business Process Execution Language
BPEL4WS	Business Process Execution Language for Web Services
BPMN	Business Process Modeling Notation
BSI	Office fédéral (allemand) de la Sécurité dans la technique d'information
BVA	Office fédéral (allemand) de l'administration
CA	Certification Authority, autorité de certification en français
CAPI	1) Common Application Programming Interface 2) Microsoft Crypto API
CBC	Cipher Block Chaining Mode
CEN	Comité Européen de Normalisation
Cert	Certificate
CODEC	Compression Decompression Algorithm
CORBA	Common Object Request Broker Architecture
CPPA	Collaborative Partner Profile Agreement
CRL	Certificate Revocation List
CS	Centre de clearing
CSP	1) Cryptographic Service Provider 2) Certificate Service Provider
CSS	Cascading Style Sheets Language
CSV	Comma Separated Value List
c.à.d.	c'est à dire
DAP	Directory Access Protocol
DB	Data Base, base de données
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DIR	Directory Service
DMZ	Demilitarised Zone
DNS	Domain Name Service, Domain Name Server
DSA	1) Digital Signature Algorithm 2) Directory System Agent
DSML	Directory Services Markup Language
DSS	Digital Signature Standard
DTD	Document Type Definition

DVD	Digital Versatile Disk
DXF	Drawing Exchange Format
ebXML	Electronic Business for XML
EC	Elliptic Curve
ECDSA	Elliptic Curve Digital Signature Algorithm
ECMA International	Association for Standardizing ICT Information and Communication Systems (avant 1994: European Computer Manufacturer Association)
ECM	Enterprise Content Management Systems
ECW	Enhanced Compressed Wavelet
EDI	Electronic Data Interchange
ED/FACT	Electronic Data Interchange for Administration, Commerce and Transport
EIF	European Interoperability Framework
EIS	Enterprise Information System
engl.	Anglais
EPS	Encapsulated Post Script
ERP	Enterprise Resource Planning
ETSI	European Telecommunications Standards Institute
UE	Union européenne
FIPS	Federal (USA) Information Processing Standards
FTP	File Transfer Protocol
FTPD	FTP-Daemon
G2B	Government to Business
G2C	Government to Citizen
G2Con	Government to Consumer
G2G	Government to Government
G2O	Government to Organisation
G-I	Government internal
GIF	Graphic Interchanged Format
GML	Geography Markup Language
GOSIP	Government Open Systems Interconnection Profile
GUI	Graphical User Interface
GZIP	Gnu Zip (Zigzag Inline Package)
HD	High Definition
HMAC	Keyed-Hash Message Authentication Code
Edit.	Editeur
HSM	Hardware Security Module
HTML	Hypertext Markup Language

HTTP	Hypertext Transfer Protocol
HW	Hardware
ICT	Information and Communication Technology
IDA	Interchange of Data between Administrations
IDEA	International Data Encryption Algorithm
IEEE	Institute for Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IHE	Integrating the Healthcare Enterprise
IKE	Internet Key Exchange
IMAP	Internet Message Access Protocol
IMKA	Interministerielle Koordinierungsausschuss für die Informationstechnik in der Bundesverwaltung
IP	Internet Protocol
IPSEC	IP Security Protocol
ISAKMP	Internet Security Association and Key Management Protocol
UPIC	Unité de pilotage informatique de la Confédération
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
IT	Technologie de l'information, Information Technology
ITU	International Telecommunication Union
J2EE	Java 2 Enterprise Edition
JAAS	Java Authentication and Authorization Service
JAXP	Java API for XML
JDBC	Java Database Connectivity
JMS	Java Message Service
JPEG	Joint Photographic Expert Group
JPG	Joint Photographic Expert Group
JTA	Java Transaction API
KBSt	Service de coordination et de conseil du gouvernement fédéral pour les technologies de l'information à l'administration fédérale (Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung) au Ministère de l'intérieur, Allemagne
KoopA	Comité de coopération entre l'Etat fédéral, les Länder et les communes (Kooperationsausschuss ADV Bund/Länder/Kommunaler Bereich), Allemagne
LDAP	Lightweight Directory Access Protocol
LDIF	LDAP Data Information Format
MAC	1) Message Authentication Code 2) Media Access Control
Mbps	Million Bits per second

MD5	Message Digest Algorithm 5
MIME	Multipurpose Internet Mail Extensions
MP3	MPEG Layer 3
MPEG	Moving Pictures Experts Group
MTT	MailTrusT
NFS	Network File System
NGO	Non Government Organisation
NIST	(American) National Institute for Standards and Technology
NSP	Network Security Policy
NTP	Network Time Protocol
OASIS	Organization for the Advancement of Structured Information Standards
OCSP	Online Certificate Status Protocol
ODF	OASIS Open Document Format for Office Applications
OGG	Xiph.org's container format
OMA	Open Mobile Alliance
OMG	Open Management Group
CO	Code des obligations de la Suisse
ORB	Object Request Broker
OS	Operating System (système d'exploitation)
OSCI	Online Services Computer Interface
OSI	Open Systems Interconnect
OSPF	Open Shortest Path First
PC	Personal Computer
PC/SC	Personal Computer/ Smart Card
PCA	Policy Certification Authority
PCM	Pulse Code Modulation
PDA	Personal Digital Assistant
PDF	Portable Document Format
PDF/X	PDF Exchange (Subset of PDF)
PGP	Pretty Good Privacy
PIN	Numéro d'identification personnel, Personal Identification Number
PK	Public Key
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure, infrastructure de clé publique
PKIX	IETF Working Group «Public-Key Infrastructure (X.509)»
PNG	Portable Network Graphics
POP3	Post Office Protocol Version 3

PS	Post Script
QT	QuickTime
RDF	Resource Description Framework
RegTP	Autorité de régulation des télécommunications et de la poste (Regulierungsbehörde für Telekommunikation und Post, Allemagne)
REST	Representational State Transfer
RFC	Request for Comment
RFP	Request for Proposals
RIFF	Resource Interchange File Format
RIP	Routing Information Protocol
RMI	Remote Method Invocation
RPC	Remote Procedure Call
RSA	Rivest Shamir Adleman Public Key
RTF	Rich Text Format
V.	Voir
S1-S3	Interfaces S1, S2 et S3, cf. chap.4.2 du document
S/MIME	Secure Multipurpose Internet Mail Extension
SAGA	Normes et architecture pour applications de cyberadministration
SAGA.ch	Normes et architectures informatiques pour applications de cyberadministration en Suisse
SAML	Security Assertion Markup Language
SASL	Simple Authentication and Security Layer
SEGA	Société Suisse pour le transfert de titres SA
SGML	Standard Generalized Markup Language
SHA	Secure Hash Algorithm
SIP	Session Initiation Protocol
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNV	Association suisse de normalisation (Schweizerische Normenvereinigung)
SOA	1) Service-Oriented Architecture 2) Sarbanes Oxley Act
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Socket Layer
SVG	Scalable Vector Graphic
SW	Software, logiciel
sym.	Symétrique

TAV	Prescriptions techniques et administratives (Technische und Administrative Vorschriften)
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TIFF	Tagged Image File Format
TLS	Transport Layer Security
TSP	Time Stamp Protocol
UDDI	Universal Description, Discovery and Integration
UDP	User Datagram Protocol
UML	Unified Modeling Language
UMTS	Universal Mobile Telecommunication System
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
etc.	etcetera
UTF	Unicode Transformation Format
V.	Version
VPN	Virtual Private Networks
VxD	Virtual Device Driver
OSCSE	Ordonnance sur la signature électronique
W3C	World Wide Web Consortium
WAN	Wide Area Network
WAP	Wireless Application Protocol
WAV	WAVEform audio format
WDP	Wireless Datagram Protocol
WFMC	Workflow Management Coalition
WML	Wireless Markup Language
WMV/A	Windows Media Video/Audio
WS	Web Services
WSDL	Web Services Description Language
WS-I	Web Services Interoperability Organization
WSP	Wireless Session Protocol
WTLS	Wireless Transport Layer Security
WTP	Wireless Transaction Protocol
WWW	World Wide Web
XACML	XML Access Control Markup Language
XHMTL	Extensible Hypertext Markup Language
XKMS	XML Key Management Specification

XLI	X Library Interface
XML	Extensible Markup Language
XPath	XML Path Language
XPDL	XML Process Definition Language
XSDL	XML Schema Definition Language
XSD	XML Schema Definition
XSL	Extensible Stylesheet Language
XSL-FO	XSL Formatting Objects
XSLT	Extensible Stylesheet Language Transformation
SCSE	Loi fédérale sur les services de certification dans le domaine de la signature électronique et autres applications des certificats numériques
ZIP	Zigzag Inline Package

Annexe C – Glossaire

Le glossaire ci-dessous est constitué de termes et explications correspondantes, qui proviennent d'une part du site Internet de l'«Institut für Wirtschaft und Verwaltung» de Berne dont certaines définitions ont été adaptées, et d'autre part à l'ouvrage de D. Muster [Mud]. A noter également que certains termes ont été définis au cours de la rédaction du présent document.

Administration	En relation avec la cyberadministration (eGovernment), le terme «Administration» recouvre l'administration au sens d'une délimitation entre l'exécutif, le législatif, le pouvoir judiciaire et l'Etat considéré au sens large. Formulée d'une manière exclusive, cette notion recouvre tout ce qui ne relève ni de la législation, ni de la jurisprudence. Formulée d'une manière générale, elle s'applique à l'administration publique ou à un organe d'application dirigé par l'Etat et contrôlé par la justice.
AES	Algorithme de cryptage symétrique développé par John Daemen et Vincent Rijmen et reconnu comme norme par le NIST.
Algorithme à clé publique	Algorithme asymétrique de cryptage (cf. Algorithme asymétrique de cryptage), dans lequel une clé ne permet pas de déduction concernant l'autre clé. Une clé est publique d'où son nom (public key) tandis que l'autre est tenue secrète (private Key). Ces méthodes servent à authentifier, à protéger l'intégrité et la communication confidentielle. Elles servent de bases pour élaborer les signatures et certificats digitaux.
Algorithme de cryptage asymétrique	Méthode ou algorithme de cryptage dans laquelle les clés pour le cryptage et le décryptage sont différentes.
Algorithme hash	Un algorithme hash est une fonction hash définie de manière précise, par ex. SHA-1
Algorithme symétrique	Méthode de cryptage dans laquelle les clés de cryptage et décryptage sont identiques.

Assistant de changement de clé publique	Un assistant de changement de clé (publique) est un programme qui décrypte les données à l'aide de l'ancienne clé (privée) et les recrypte avec la nouvelle clé (publique).
Authenticité	Service de sécurité déterminant la responsabilité, définition au chapitre 7.2«Objectifs de protection».
Authentification	Procédure servant à définir l'authenticité.
Benchmark	La notion de «benchmark» est issue du langage des géomètres. Par analogie, le «benchmark» (analyse comparative) sert à comparer des normes spécifiques avec certains objectifs sélectionnés, que ce soit dans des entreprises, des secteurs particuliers ou des produits. Dans l'administration publique, on peut entreprendre de comparer les prestations de domaines différents ou similaires.
Best Practice	Par «best practice» (meilleure pratique), on entend une solution qui, mise en œuvre, a partout fait ses preuves, permettant de comparer des produits, des prestations, des réalisations (informatiques) sur la base de critères de qualité homogènes.
Certificat, numérique	Authentification élaborée à l'aide d'une signature numérique, certifiant qu'une clé publique (cf. algorithme de clé publique) appartient à une entité (cf. entité). Dans le langage parlé, un certificat digital est l'équivalent numérique d'un passeport, ce qui est trompeur. En effet, contrairement à un passeport, un certificat digital ne permet pas à lui seul d'identifier une personne.
Certificate Revocation List	Abrégé CRL, ou liste de révocation; en anglais liste authentifiée par le CA (cf. Certification Authority) des certificats révoqués. L'authentification se fait via signature numérique.
Certification Authority	Abrégé CA, ou autorité de certification; autorité qui procède à l'authentification des clés pour les processus PK, via des certificats (cf. certificat).
Challenge Response	Procédure d'authentification d'un utilisateur ou d'une instance. La personne ou instance procédant à l'authentification doit convaincre (Challenge) la partie adverse qu'elle connaît un secret sans le lui communiquer.
Compresser	En informatique, compresser (compacter, comprimer) signifie éliminer le superflu, donc le plus possible de redondances. Il y a des redondances dans l'information lorsque celle-ci peut être modifiée sans pour autant que sa signification soit transformée. Une information est exempte de redondance, lorsque toute modification apportée à l'information est à l'origine d'une autre signification ou affirmation. Les informations exemptes de redondance n'existe pour ainsi dire pas dans la pratique.
MQTT	Message Queue Telemetry Transport
Confidentialité	Service de sécurité pour la préservation de secrets ou d'informations privées, définition au chapitre 7.2 «Objectifs de protection».
CORBA	Common Object Request Broker Architecture; norme pour une architecture de logiciel standard personnalisé et ses protocoles.
Courbes elliptiques	Algorithme de clé publique proposé séparément par N. Koblitz et V.S. Miller.

DES	Algorithme de cryptage symétrique développé par IBM et à clé de 56 bits.
Diffie Hellmann	Algorithme de clé publique développé par W. Diffie et W. Hellmann.
Disponibilité	Service de sécurité pour la mise à disposition d'informations dans les délais impartis, définition au chapitre 7.2 «Objectifs de protection».
DMZ	Abréviation de «Demilitarised Zone»; zone démilitarisée utilisée dans la sécurité TIC dans le secteur du firewall. Il s'agit de sous-réseaux situés entre le réseau interne et Internet. Partant, ils n'offrent pas autant de sécurité que le réseau interne, sans pour autant être aussi peu sûrs que le réseau externe. C'est là qu'on installe les serveurs qui transmettent les e-mails ou les paquets HTTP entrant et sortants. On installe aussi dans cette zone les serveur web ou ceux qui vérifient que les contenus des paquets HTTP ou e-mail ne soient pas infectés.
e-administration	L'e-administration est la mise en œuvre des technologies de l'information et de la communication (TIC) pour seconder le déroulement de transactions avec l'administration.
e-administration	European Interoperability Framework
EIF	L'e-administration est la mise en œuvre des technologies de l'information et de la communication (TIC) pour seconder le déroulement de transactions avec l'administration
e-business	Commerce électronique ou en ligne: déroulement de processus d'affaire via les technologies de l'information et de la communication (TIC).
e-commerce	Commerce électronique ou cybercommerce englobant une partie de l'e-business, qui traite de l'exécution, par voie électronique, de transactions avec l'administration qui lient juridiquement les parties impliquées. On distingue trois types de transactions: - Business-to-Business (d'entreprise à entreprise) - Business-to-Consumer (d'entreprise à consommateur) - Consumer-to-Consumer (cas spécial où l'entreprise ne sert que d'intermédiaire, p. ex. enchères en ligne).
electronic Public Services (ePS)	Service public électronique: fourniture de prestations de service public à des bénéficiaires de prestations, des privés ou des entreprises via des portails locaux, régionaux ou nationaux.
Entität	Instance dans l'environnement IT munie d'une identité. Il peut s'agir d'un utilisateur, d'un client, d'un serveur, d'un service web, d'un téléphone portable, d'un PDA ou d'un service d'annuaire (liste non exhaustive).
Extensibilité	L'extensibilité est la faculté d'ajouter de nouvelles fonctionnalités ou d'élargir les fonctionnalités existantes dans une application, de manière économique et sans préjudice pour celle-ci.
FIPS	Federal (USA) Information Processing Normes, pour les normes relevant de l'organisation de normalisation NIST.
Flexibilité	La flexibilité est la faculté générale de modifier une architecture existante afin de réaliser une nouvelle exigence pour un coût optimisé.

Fonction hash	Une fonction hash établit à partir d'un fichier une somme de contrôle cryptographique d'une longueur fixe. Connaissant un fichier, on ne peut cependant en prévoir la valeur de la somme de contrôle, ceci à la différence d'une somme de contrôle usuelle. En outre, il est difficile d'établir deux fichiers aboutissant à des valeurs de sommes de contrôle identiques. Ces valeurs sont aussi appelées valeurs hash. Les fonctions hash connues sont SHA-1 et MD5. Ce sont des éléments importants pour élaborer la signature numérique.
GIF	Abréviation pour «Graphics Interchange Format»; principal format d'échange graphique (outre JPEG) pour enregistrer correctement des images avec le navigateur.
Government internal (G-I)	Intragouvernemental; Relations existant entre les organes de l'Etat d'un même niveau, que ce soit dans la Confédération, dans un canton ou dans une commune (terme spécifique à l'USIC au sens de cyberadministration externe).
Government to Business (G2B)	Relations entre l'Etat et l'économie privée faisant appel aux technologies de l'information et de la communication (TIC). Par analogie avec la notion de «Business to Business» (B2B), ce terme décrit ces relations. L'Etat est en relation non seulement avec des personnes physiques mais aussi avec des personnes morales. Le recours à l'électronique peut simplifier ces différentes relations et le traitement des cas les accompagnant.
Government to Citizen (G2C)	Relations entre l'Etat et les citoyens concernant des affaires politiques (utilisation souvent analogue à G2C). Par citoyen au sens politique (citizen), on entend une personne dotée de droits politiques. La notion de «Government to Citizen» recouvre la communication s'établissant via Internet entre l'Etat et le citoyen concernant des affaires politiques. Ce faisant, les citoyens ne sont pas subordonnés à l'Etat; au contraire, ils prennent les décisions, légitimant de la sorte l'activité étatique dans une démocratie.
Government to Consumer (G2Con)	Relations entre l'Etat et des consommateurs ou clients. La notion de «consumer» provient de l'économie privée et désigne, dans le domaine de la cyberadministration, des personnes clientes au sens large. Ce rôle recouvre plusieurs réalités, allant du cas où l'habitant est considéré comme sujet de l'Etat, p. ex. au titre de bénéficiaire de l'aide sociale, de patient ou d'étudiant, jusqu'au cas où l'Etat et ses sujets établissent une relation - peut-être pas forcément volontaire mais cependant classique - de client-fournisseur, c'est-à-dire une relation où le consommateur achète ou fait appel à des biens et prestations publics.
Government to Government (G2G)	Relations existant entre des unités administratives.
Government to Organisation (G2O)	Government to Organisation (G2O) caractérise les relations que tissent la Confédération, les cantons et les communes avec les partenaires de l'économie privée (entreprises) et les organisations de droit public (associations, etc.). Government to Organisation (G2O) est un terme spécifique à l'UPIC (Unité de pilotage informatique de la Confédération) employé pour remplacer le «Government to Business». La notion de G2O englobe celle de G2B et inclut donc les organisations de droit public telles les associations, les syndicats, les partis, etc.

Guichet virtuel (www.ch.ch)	Point d'accès Internet structuré en fonction du quotidien de la société, donc de situations vécues. Le concept du guichet virtuel est qu'il s'agit d'un portail Internet dont la structure ne copie pas celle de l'administration ou les processus étatiques (p. ex. www.admin.ch), mais calque à la vie quotidienne de la société.
Haute sécurité	Dans le présent contexte, on parle de haute sécurité si le besoin de protection de l'un des services de sécurité a reçu le statut «très élevé».
HTML	Langage standardisé de description des pages web dans Internet ou Intranet, développé par Charles F. Goldfarb.
HTTP	Le «HyperText Transfer Protocol» repose sur le protocole Internet et facilite l'échange de données pour les utilisateurs. HTTP et HTML ont contribué à l'expansion d'Internet chez les utilisateurs d'ordinateur.
IDEA	Identification Vérification d'identité
IEEE	Institute of Electrical and Electronics Engineers ou Institut des Ingénieurs en Électricité et en Électronique . Comité de normalisation pour les applications électrotechniques, il participe depuis quelques années à la normalisation des algorithmes et des processus liés à la cryptographie de clé publique.
IETF	Internet Engineering Task Force (www.ietf.org). Comité de normalisation pour les protocoles Internet et les services apparentés.
Information	Par information, on entend le savoir ou un descriptif mis à disposition. La mise à disposition de l'information peut revêtir plusieurs formes et caractéristiques, p. ex. fichier livre, dépêche ou article de journal.
Intégrité	Service de sécurité pour détecter les manipulations non désirées, définition au chapitre 7.2 «Objectifs de protection».
Internet	Par Internet, on entend un réseau public d'ordinateurs permettant d'échanger surtout des données à l'aide de protocoles Internet. Les sites peuvent être sélectionnés de manière conviviale à l'aide de l'URI (Uniform Ressource Identifier).
Internet protocol (IP)	L'Internet protocol est issu du réseau Arpanet (réseau américain destiné aux militaires et à la recherche) à la fin des années 60. Il permet à des ordinateurs de communiquer sur de petits tronçons de réseau comme sur des réseaux plus grands.
Interopérabilité	L'interopérabilité technique est la réalisation, sans rupture de média, de services de transaction entre des applications administratives générales.
IPSEC	Abréviation pour IP Security; il s'agit d'une technologie de sécurité normalisée par l'IETF en vue de sécuriser les paquets IP.
ITU/ UIT	L'Union internationale des télécommunications (UIT), autrefois le CCITT, est une organisation internationale chargée de coordonner, normaliser et développer les services de télécommunication. (www.itu.org)
JPEG	1) Joint Photografic Expert Group (JPEG) est une commission qui définit les processus pour comprimer et enregistrer les données d'images et de vidéo. 2) Format de données nommé ainsi en raison du groupe susmentionné.
Mot de passe à utilisation unique	Mot de passe généré à chaque authentification de l'utilisateur, et dépendant donc de l'instant précis. Il n'est donc en principe utilisé qu'une seule fois.

NIST	National Institute of Standards and Technology est un organe de normalisation national des Etats-Unis. (www.nist.gov)
OASIS	Organization for the Advancement of Structured Information Standards. Organisme de normalisation pour Web Services. (www.oasis-open.org).
OMA	Open Mobile Alliance Ltd, a succédé à l'organisation WAP Forum.
OMG	Open Management Group, organisme de normalisation pour CORBA.
PC/SC	Norme pour la connexion de smart cards. Ces normes sont publiées par PC/SC Workgroup. (www.pcscworkgroup.com)
PDF	Produit par l'entreprise Adobe Systems, le format «Portable Document Format» (PDF) est un format de fichier multiple pour présenter des documents et comprenant les polices, les formatages, les couleurs et graphiques de n'importe quel document source, indépendamment du système d'exploitation et du programme utilisé.
PGP	Pretty Good Privacy. Logiciel standardisé développé par P. Zimmermann pour chiffrer et signer les e-mails.
PKCS	Public Key Cryptography Norme. Normes publiées par les RSA Laboratories.
Postscript	Langage de description des pages commercialisé par Adobe System Inc. en 1984, afin d'imprimer et d'enregistrer des graphiques et des textes page par page.
Procédure hash	Une procédure hash est une fonction définie avec précision, ex. SHA-1
Protection des données	Ce terme a différentes significations; d'une part la protection des données contre l'accès non autorisé et, de l'autre, cette même protection au sens de la loi fédérale sur la protection des données (LPD; RS 235.1). La LPD régit notamment la collecte des données personnelles, leur protection, leur traitement, leur publication et leur transmission. Il s'agit ainsi de protéger la personnalité et les droits fondamentaux des personnes qui font l'objet d'un traitement de données.
Public Key Infrastructure	Infrastructure de clé publique ou PKI. Infrastructure nécessaire pour que l'utilisateur puisse échanger des données avec l'algorithme de clé publique tout en garantissant l'authenticité, l'intégrité et la confidentialité. Une PKI se compose notamment d'une autorité de certification (Certification Authority), service d'annuaire où sont publiés les certificats.
Révoquer	Déclarer non valable quelque chose de public et d'attesté (p. ex. une certificat électronique).
Routeur	Elément de gestion d'un réseau, destiné en premier lieu à la communication des données. Il lui incombe notamment de transmettre les paquets de données à l'aide de leurs adresses de destination sur la liaison correcte.
Routing Protocol	Protocole qui aide le routeur à connaître la topologie du réseau afin de permettre le transfert des paquets à destination.
RSA	Système cryptographique à clé publique nommé d'après ses inventeurs Rivest, Shamir et Adleman.
S/MIME	Technologie et norme de sécurité développé par l'IETF pour sécuriser la communication par e-mails.

SAGA.ch	Normes et architectures informatiques pour les applications de cyberadministration en Suisse; document élaboré par l'association ***eCH*** qui sous forme compacte présente les directives techniques pour la mise en œuvre des applications de cyberadministration en Suisse.
Service	Dans ce document, un service est une application de cyberadministration concrète et définie de manière précise, traitant une opération complète, telle que la transmission électronique de documents à un tribunal.
Service public	Par service public, on entend le plus souvent la garantie d'une desserte de base en prestations d'infrastructure, ceci dans tout le pays et à des prix convenables. Ces prestations peuvent être aussi bien de nature matérielle (transports, télécommunications, poste, énergie, etc.) qu'immatérielle (santé, formation, culture, etc.), peu importe que ces prestations soient fournies par les collectivités publiques elles-mêmes ou par des privés (sur la base de convention ou mandat de prestations).
Clé de session (Session Key)	Clé temporaire, symétrique et définie par deux ou plusieurs participants pour la durée d'une liaison de communication.
Signature électronique	La signature électronique, aussi appelée numérique, protège l'authenticité et l'intégrité d'un fichier. Elle se base sur la valeur hash (cf. valeur hash) du fichier à protéger et un algorithme PK (cf. algorithme PK). La valeur hash du fichier est chiffrée avec la clé privée. Le résultat qui en sort est désigné comme signature électronique.
Signature numérique	La signature numérique protège l'authenticité et l'intégrité d'un fichier. Elle se base sur la valeur hash (cf. valeur hash) du fichier à protéger et un algorithme PK (cf. algorithme PK). La valeur hash du fichier est chiffrée avec la clé privée. Le résultat qui en sort est désigné comme signature numérique.
Signature, numérique	v. Signature, numérique.
Smart card (carte intelligente)	Élément de plastique standard dans lequel est intégré un microprocesseur qui exécute notamment des opérations cryptographiques.
SOAP	Protocole de logiciel standardisé pour l'échange d'annonces dans le domaine des Web Services.
SSL/TLS	Secure Socket Layer; technologie de sécurité développée par Netscape initialement pour protéger le protocole HTTP. De fait, SSL est devenu une norme. TLS, Transport Layer Security, est une technologie de sécurité normalisée par l'IETF et se basant à presque 95% sur SSL; cependant les deux processus ne sont pas compatibles.
Telnet	Protocole d'application TCP/IP, utilisé pour gérer à distance des serveurs via le réseau.
TIC	Par TIC on entend les technologies de l'information et de la communication. Exemples: Internet, Intranet, Extranet, WAP (Wireless Application Protocol), Email, UMTS (Universal Mobile Telecommunication System).

Transaction	1) Les transactions englobent la résolution de processus liés aux mouvements de marchandises ou à la fourniture de prestations, donc l'ensemble des informations à échanger lors de tels processus. 2) Les informaticiens parlent de transaction pour désigner une action - impliquant plusieurs instances, - dans laquelle des données sont modifiées par des instances différentes, - après laquelle la cohérence des données doit être assurée (sinon l'action doit être annulée).
UDDI	Universal Description Discovery Integration: directory ou annuaire où les services Web sont publiés en langue WSDL. La structure et l'interrogation de cet annuaire ont été normalisées par OASIS (www.oasis-open.org).
UML	UML (Unified Modeling Language) est un langage de description (ou un mode de représentation) de structures et de processus, orienté objet et normalisé. Le déroulement, avec les changements d'état possibles, est décrit dans un diagramme (state chart) indiquant si et comment il est possible de passer d'un état à l'autre.
Use Case (cas d'utilisation)	Un Use Case est une application IT concrète ou un processus concret traité par informatique.
Valeur hash	Valeur d'une somme de contrôle d'un fichier, établie à l'aide d'une fonction hash.
W3C	Comité de normalisation pour XML et les applications s'y référant. (www.w3C.org)
WAP Forum	Ancien comité de normalisation pour le Wireless Application Protocol (WAP). A été intégré dans l'OMA.
Web Services	Définition des Web Services au chapitre 5.9.
WS-I	Web Services Interoperability Organization: comité de normalisation qui cherche à obtenir l'interopérabilité des services Web. (www.ws-i.org)
WSDL	Web Service Description Language: description standard des services web émanant du comité W3C (www.w3C.org)
WTLS	Wireless Transaction Layer Security; technologie de sécurité standardisée par WAP Forum pour protéger le protocole WAP. WTLS se base presque à 95% sur SSL, cependant les deux processus ne sont pas compatibles.
WWW	World Wide Web. Un service Internet pour mettre à disposition des documents reliés les uns aux autres, indépendamment des plates-formes utilisées.
XML	eXtensible Markup Language: version simplifiée du Standard Generalized Markup Language (SGML). Son développement a commencé en 1996 et depuis février 1998, XML est une norme W3C. XML doit permettre l'écriture d'applications SGML par les programmeurs de site Web et ainsi la définition de leurs propres types de documents. XML propose de nombreux mécanismes, devant notamment faciliter l'échange de données dans le réseau.

Annexe D – Modifications par rapport aux versions antérieures

Modifications de SAGA 7.0 à 8.0

La version 8.0 de SAGA.ch se caractérise par les modifications suivantes par rapport à la version précédente d'eCH et la version 7.0:

Chapitre (v.8)	Nom	Classification V.7	Classification V.8
5.4.2	IPv6	Vivement recommandé	Vivement recommandé Texte, RFC complétés
5.5.1	FTP	Recommandé	Recommandé RFC complétés
5.5.2	HTTP	Vivement recommandé	Vivement recommandé V.2 Recommandé, RFC complétés
5.5.3	SMTP	Vivement recommandé	Vivement recommandé RFC complétés
5.5.4	POP3, IMAP4	Vivement recommandé	Vivement recommandé RFC complétés
5.5.6	RPC	Recommandé	Recommandé, RFC complétés
5.5.8	WebDAV	Recommandé	Recommandé, RFC ISO IEC complétés
5.5.9	XMPP	En observation	Recommandé, RFC ISO IEC etc. complétés
5.5.10	CMIS	--	En observation
5.5.11	AMPQ	En observation	Recommandé, ISO/IEC Textes complétés
5.5.13	STOMP	--	En observation
5.7.1	LDAP	Vivement recommandé	Vivement recommandé ISO/IEC RFC Textes complétés
5.7.3	DSML	Recommandé	Recommandé Textes complétés
5.7.4	Protocoles de serveur d'annuaire selon X.500	Recommandé	Recommandé Textes complétés

	X500		
5.7.5	OCSP	Recommandé	Recommandé Textes complétés
5.8.1	SIP	Recommandé	Recommandé Textes complétés
5.8.2	Famille de protocoles H.323	Recommandé	Recommandé Textes complétés
5.8.3	Skype	Non recommandé	En observation Textes complétés
5.8.4	RTP	Recommandé	Recommandé Textes complétés
5.9.4	SOAP	Vivement recommandé	Vivement recommandé Textes complétés
5.9.6	WSDL V.2	En observation	Recommandé Textes complétés
5.9.8	UDDI	Recommandé	Recommandé Textes complétés
5.9.9.1	WS-Reliable Messaging V.1.1/2	V.1.1 Recommandé V.1.2 en observation	V.1.1/2 Recommandé Textes complétés
5.9.9.2 bis 4	WS-Coordination, Transaction, Business Activity	V.1.1 Recommandé	V.1.1/2 Recommandé Textes complétés
5.9.9.5	OSCI Transport	Recommandé	Recommandé Textes complétés
5.9.10	WSRF	En observation	Recommandé Textes complétés
5.11	SPML	En observation	Recommandé
5.12	ebXML	En observation	Recommandé Textes complétés
5.13	UBL	En observation	Recommandé Textes complétés
5.14	Swissdec/PUCS4.0	--	Recommandé
5.15.1	BPEL	Recommandé	Recommandé Textes complétés
5.15.3	UML	Recommandé	Recommandé Textes complétés
5.15.4	XMI	Recommandé	Recommandé Textes complétés
5.15.5	XPDL	En observation	Recommandé Textes complétés

6.2.1	UTF	Vivement recommandé	Vivement recommandé Textes complétés
6.2.2	CSS	Vivement recommandé	Vivement recommandé Textes complétés
6.2.3	CSV (pour archivage)	Recommandé	Vivement recommandé Textes complétés
6.2.4	SIARD V.2 (archivage)	Recommandé	Vivement recommandé Textes complétés
6.2.6	GML	Recommandé	Recommandé Textes complétés
6.2.7	HTML	Recommandé	Vivement recommandé Textes complétés
6.2.9	WFS	En observation	Recommandé Textes complétés
6.2.10	WMS	En observation	Recommandé Textes complétés
6.2.12	MIME	Vivement recommandé	Vivement recommandé Textes complétés
6.2.13	Format XML de Microsoft Office	Non recommandé	Non recommandé Textes complétés
6.2.14	ODF V.1.1/1.2	En observation	Recommandé
6.2.15	Office Open XML File Formats	Recommandé	Recommandé Textes complétés
6.2.18	PDF UA/VT/E	En observation	Recommandé Textes complétés
6.2.19	PDF/X 1/3/4	En observation	Recommandé Textes complétés
6.2.20	Postscript	Non recommandé	En observation Textes complétés
6.2.23	ATOM	En observation	Recommandé Textes complétés
6.2.26	XHTML V.1 transitional	En observation	Recommandé Textes complétés
6.2.27	XML	Recommandé	Recommandé V.2.0 Textes complétés
6.2.28	XML Schema	Vivement recommandé	Vivement recommandé

			Textes complétés
6.2.29	DSDL	Recommandé	Recommandé Textes complétés
6.2.31	XSLT	En observation	Recommandé V.2.0 Textes complétés
6.2.32	XForms	Recommandé	Recommandé V.2.0 Textes complétés
6.2.35	OAI-PMH	--	Recommandé
6.2.36	Dublin Core	--	Vivement recommandé
6.2.37	Moreq2	--	Vivement recommandé
6.3.3	JPEG 2000	En observation	Recommandé Textes complétés
6.3.6	TIFF (Archivage)	Recommandé	Vivement recommandé Textes adaptés
6.4.1.3	MPEG-4 (Archivage)	Recommandé	Vivement recommandé Textes complétés
6.4.2	MP3	MP3 (sans MP4)	MP3/MP4 Textes complétés
6.4.5	WAVE (Archivage)	Recommandé	Vivement recommandé
6.5.1.3	TAR	Recommandé	Recommandé Textes complétés
6.6.1	JavaScript	Recommandé	Recommandé Textes complétés
7.1.	Modèle structurel pour la sécurité des données		Textes complétés et étendus à ISMS et HERMES
7.4	Gestion de système comme impératif à la sécurité du système	Recommandé	Recommandé Textes complétés
7.5.1	Cryptographie à clé publique	Vivement recommandé	Vivement recommandé Textes complétés
7.5.3	Modes de fonctionnement pour le chiffrement par blocs	Recommandé	Recommandé Textes complétés
7.6.1.3	Signature numérique	Vivement recommandé	Vivement recommandé Textes complétés

7.6.1.5	MAC/HMAC	Vivement recommandé	Vivement recommandé Textes complétés
7.6.1.6	Procédure biométrique	En observation	Non recommandé et nouveau texte
7.6.3	Négociation en ligne d'une clé de session	Recommandé	Recommandé Textes complétés
7.8.x	Anciennement chap.8.8.x	Chap.8.8.x	Est désormais le chap. 7 avec textes complétés
7.8.1	SSL/TLS	TLS V.1.1 Recommandé	TLS Version.1.1 Non recommandé Textes complétés
7.8.3	DTLS	Recommandé	Recommandé Textes complétés
7.8.4	TSP	Recommandé protocole p. services d'horodatage	Recommandé Textes complétés
7.8.6	IPSEC	Vivement recommandé	Vivement recommandé Texte RFC complétés
7.8.7	S/MIME	Recommandé	Recommandé V.3.2 Textes complétés
7.8.9.1	XML Signature	Vivement recommandé	Vivement recommandé Textes complétés
7.8.9.2	XML Encryption	Vivement recommandé	Vivement recommandé Textes complétés
7.8.10	OpenPGP (avec certificats X.509v3)	Recommandé	Recommandé Textes complétés
7.8.11.3	SAML	Vivement recommandé	Vive.recommandé V.2 Textes complétés
7.8.11.7	XACML V.2	Recommandé	Recommandé Textes complétés
7.8.11.11	WS Coordination	Recommandé V.1.1	Recommandé V.1.2 Textes complétés
7.8.11.12	WS Transaction	Recommandé V.1.1	Recommandé V.1.2 Textes complétés
7.8.12	Kerberos	Org.int. Recommandé chap.8.8.4	Organisation interne Recommandé – texte
7.8.13	Oauth V.2	--	En observation

7.8.14	Open ID connect	--	En observation
7.9.1	Utilisation de cartes intelligentes	Recommandé	Recommandé, textes avec ISO/IEC complétés
7.11	Key Management	Recommandé	Recommandé Textes complétés
Chap. 8	Thèmes transversaux (nouveau chapitre)	Chap. 8=Sécurité	Chap. 7=Sécurité Chap. 8=Cloud, IAM, IHE, archivage, Big Data
8.1	Cloud Computing	--	En observation et révision avec le groupe spécialisé Cloud de l'eCH
8.2	IAM	--	En observation avec le groupe spécialisé Review
8.3	IHE	--	IHE Profile Recommandé
8.4	Archivage	--	Utilisation de formats de données compatibles archivage Vivement recommandé
8.5	Big Data	--	Nouveau texte
Adaptions	Références, Annexe	Selon chapitres	Selon chapitres

Des adaptations textuelles ont été effectuées dans un souci de simplifier certaines formulations et d'améliorer la lisibilité.

Modifications SAGA de 6.0 à 7.0

Toutes les modifications sont publiées dans la version 7.