eCH-0014 «SAGA.ch»

Titre	SAGA.ch
Code	eCH-0014
Type	norme d'interopérabilité
Stade	appliquée
Version	4.00
Statut	Annulé
Validation	2007-06-22
Date de publication	2010-01-26
Remplace	SAGA version 3.0 valable depuis le 25 août 2005
Langues	allemand, français
Auteurs	Groupe spécialisé Technologie Josef Schmid, président du GS, Unité de stratégie informatique de la Confédération (USIC) Frank Koch, Microsoft Suisse SARL Daniel Muster, Bit Pattern Security Ernest Peter, NetConsult SA Daniel Gabi, Chancellerie fédérale suisse Erich Vogt, SignPool Group SA André von Arx, Oracle Software (Suisse) SARL Martin Weiss, Ergonomics SA Ralf Kastmann Hans Ulrich Bucher, Avataris SA
Editeur / Distributeur	Association eCH, Amthausgasse 18, 3011 Berne T 031 560 00 20, F 031 560 00 25 www.ech.ch / info@ech.ch
Autres personnes ayant participé à l'élaboration	Grégoire Hernan, Conférence suisse sur l'informatique (CSI) Robert Insley, Sun Microsystems Suisse SA Manuel Michaud, HP Suisse SARL Willy Müller, Unité de stratégie informatique de la Confédération (USIC) Adrian Keller, Software SA

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 et il est accompagné de documents séparés présentant des procédés, méthodes et produits pour le développement de systèmes de cyberadministration. De telles normes favorisent la réalisation de solutions compatibles à un coût avantageux. En effet, les systèmes de cyberadministration ne doivent ainsi pas être développés à partir de zéro puisque l'on peut 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. La normalisation devrait en outre 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 précisant les principaux aspects requis pour atteindre les objectifs 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 et de communication (équipes de cyberadministration).

SAGA.ch a été conçu en référence au document SAGA.de, version 1.1, réalisé en Allemagne par l'administration (voir ci-dessous). On consultera également les normes françaises[1] et britanniques[2] correspondant à SAGA.

Remarque

Référence avec autorisation spéciale aux documents du KBSt (Allemagne).

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

Rédaction: groupe spécialisé Technologie d'eCH

Interlocuteur:

Secrétariat ***eCH***
E-mail: info@eCH.ch

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

[1] Cadre commun d´interoperabilité (CCI) et Référentiel général d'interopérabilité (RGI) des systèmes d'information publics (http://www.thematiques.modernisation.gouv.fr/sommaire.php?id=23)

[2] E-Government Interoperability Framework (http://www.govtalk.gov.uk/schemasstandards/egif_document.asp?docnum=949)

Table des matières

1 Statut du document

Le présent document est annulé. Il a été remplacé par la nouvelle version 5.00 SAGA.ch.

1.1 Aperçu des modifications entre les versions 3.0 et 4.0 de SAGA

La version 4.0 de SAGA.ch se caractérise par les modifications suivantes par rapport à la version 3.0 adoptée par eCH:

- évaluation actualisée des normes existantes reprises dans SAGA.ch et de leurs versions,
- classification et enregistrement des programmes exécutables dans les données, tels que ActiveX et JavaScript,
- prise en compte des prescriptions d'exécution de la loi fédérale sur les services de certification dans le domaine de la signature électronique (SCSE),
- services en temps réel sur le réseau télématique (p. ex. voix sur IP),
- nouveaux formats de données,
- définition plus précise de l'orientation de SAGA.ch.

1.2 Détails des modifications par rapport à SAGA 3.0

Chapitre (v. 4)	Nom	Classification v. 3	Classification v. 4
6.4.1	FTP	vivement recommandé	recommandé (pour le téléchargement de données)
6.4.8	WebDAV	en observation	recommandé
	SCVP	K. 6.5 en observation	supprimé
6.7.1	SIP	--	recommandé
6.7.2	H.323	--	recommandé
6.7.3	Skype	--	non recommandé
6.8.8.1	WS Coordination	--	en observation
	WS Business Transaction	en observation (chap. 6.7)	supprimé
6.8.10.2	BPMN	--	en observation
6.8.10.3	UML 2.0	--	recommandé
7.2.1	CSS 2.1	--	en observation
7.2.2	CSV	vivement recommandé	recommandé
7.2.7	LDIF, nouveau pour les		inchangé

	formats de données		
7.2.9	Microsoft Office 2003 XML	en observation	non recommandé
7.2.10	OASIS ODF	en observation	recommandé
7.2.11	Office Open XML	en observation	recommandé
7.2.13	PDF/A	--	vivement recommandé
7.2.14	PDF/X	--	recommandé
7.2.15	PostScript	vivement recommandé	non recommandé pour l'échange de données
7.6	Composantes exécutables dans des fichiers		
8.4.2	3DES mit 112 Bit	vivement recommandé	recommandé
8.4.2	DES	--	non recommandé
8.7.3	SSH	--	en observation
8.7.4	IPSEC V2.0	--	en observation

1.3 Modifications de la version 3.0 par rapport à la version 1-3 de SAGA

Résumé des améliorations apportées à la version 1-3 de SAGA.ch:

- extension de la description de l'architecture pour une meilleure délimitation des objectifs de SAGA.ch;
- ajout de plusieurs protocoles de communication et formats de données (notamment vidéo et audio);
- ajout d'un paragraphe sur la gestion des clés au chapitre 8 "Sécurité";
- extension des sujets de la gestion des certificats et du contrôle des signatures numériques au chapitre 8 "Sécurité";
- formulation d'exigences minimales envers l'application de cyberadministration pour les cas ou des signatures numériques sont nécessaires;
- ajout d'explications concernant les données et les liaisons authentiques;
- **indication de la version de différents formats et technologies;**
- actualisation des références aux normes;
- **discussion et prise en compte des prises de position reçues;**
- ajout d'une comparaison avec SAGA.de, version 2.0 et d'autres normes européennes de cyberadministration;

- améliorations sur les plans rédactionnel et terminologique.

2 Introduction

2.1 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 organisations 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 sexuellement neutre. Pour simplifier la formulation, nous nous limitons parfois à la forme masculine, mais les deux genres sont toujours concernés.

2.2 Antécédents

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

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

Mais la disponibilité en ligne 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 protocoles et de normes techniques.

La normalisation favorise la réalisation de solutions à des coûts plus avantageux. En effet, les systèmes de cyberadministration 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 ICT. 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.

2.3 Public cible

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.

2.4 Objectif et structure du document

2.4.1 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) communiquer 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.

2.4.2 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.

SAGA.ch est une norme ***eCH***. eCH connaît aussi d'autres types de documents, tels que des bonnes pratiques, des solutions types et des auxiliaires de travail. Ces documents se distinguent des normes sur le plan formel et au niveau du contenu, voir www.ech.ch -> types de documents.

2.4.3 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 ne sont pas centrales pour SAGA.ch et se trouvent par conséquent dans des documents séparés, concernant par exemple les structures d'implémentation,
- 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 5 décrit dans ses grandes lignes un modèle d'interfaces et d'architecture,
- les chapitres 6 à 8 décrivent les normes relatives à ce modèle.

Si certaines technologies sont décrites plus en détail que d'autres dans ce document, cela ne signifie pas qu'elles sont plus importantes. Par exemple, les technologies concernant l'architecture «Web services » et la sécurité informatique sont décrites avec plus de détails dans l'hypothèse qu'elles sont moins connues par le public.

2.5 Services à représenter

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

- aux **particuliers** (G2C Government to Citizen),
- aux **entreprises** (G2B Government to Business),
- aux **organisations** (G2O Government to Organisations), par exemple aux organisations non gouvernementales (ONG),
- aux **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** : échange entre les autorités et les utilisateurs ainsi qu'entre les utilisateurs eux-mêmes, le flux d'information étant bilatéral.
- **Services de transaction** : processus d'affaires entre les autorités et les utilisateurs.

3 L'évolution de SAGA.ch

3.1 Tâche

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

3.2 Origine et développement

Le contenu de SAGA.ch se fonde sur les expériences d'autres pays, notamment l'Allemagne, la France et l'Angleterre, ainsi que sur les expériences et connaissances personnelles des membres 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.

3.3 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.

4 Classification 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 d'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 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.

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.

5 Limites du système et interfaces

5.1 Composantes

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) ou téléphone portable (mobile).

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

Un **centre de clearing** (centre d'échange de données) 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).

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,
- Telekurs SA pour le trafic des paiements entre les banques en Suisse,
- La Poste.

5.2 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):

- **I1:** terminal - système
- **I2:** système - système
- **I3:** système - centre de clearing

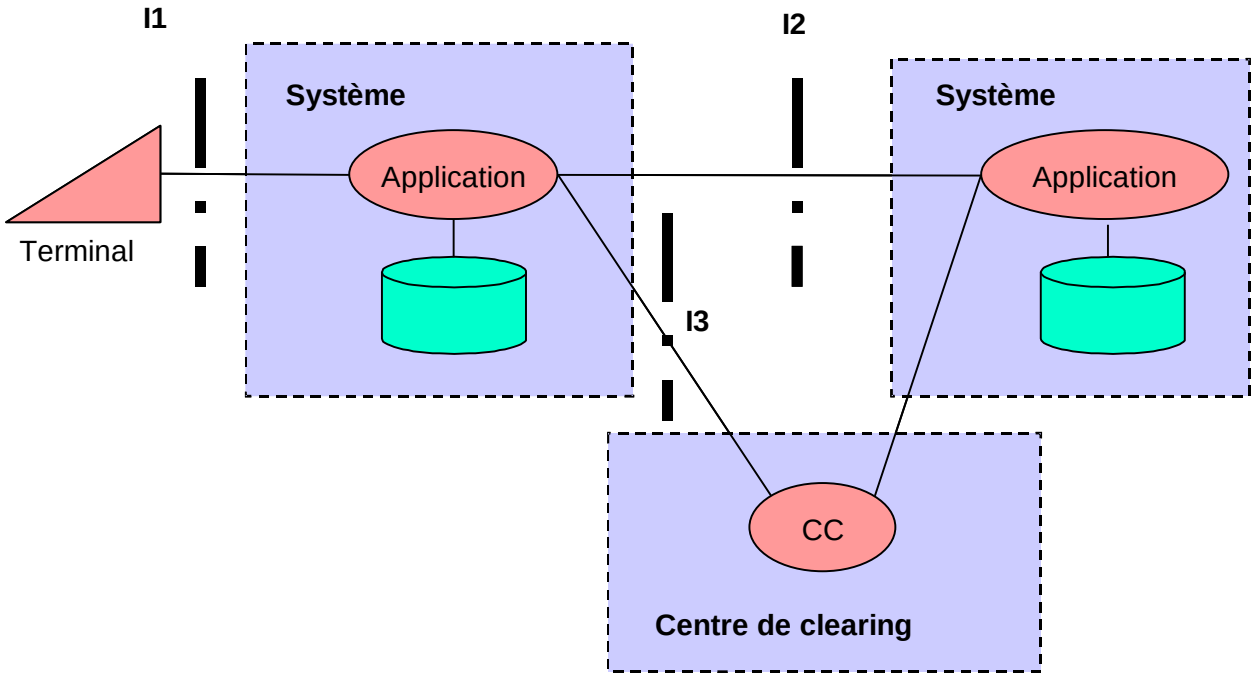

Figure 5-1 Interfaces

La communication et l'échange de données entre les centres de clearing doivent en outre être possibles, comme pour l'interface I3.

Important: Les recommandations présentées ci-après pour la réalisation d'applications de cyberadministration se limitent, 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 I1, I2 et I3. 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; nous ne la traiterons donc pas plus en détail dans ce document.

5.3 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.

5.3.1 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 plate-formes clientes.
- Présentation : définit les formats de présentation et les protocoles pour le client.
- Intergiciel (middleware) / 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.

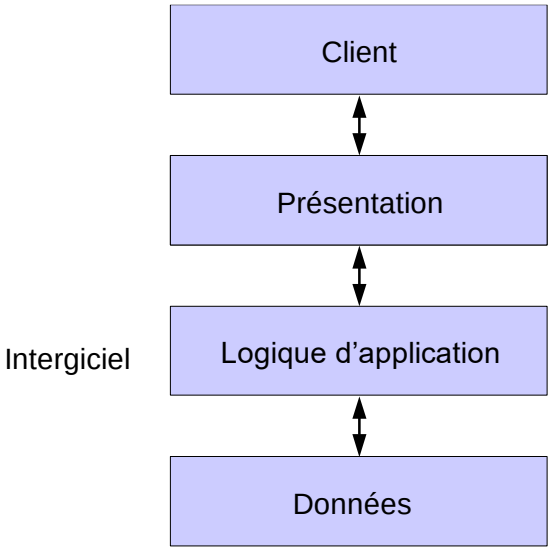

Figure 5-2 Couches de traitement de l'information

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 ceux-ci dépendent, entre autres, du système d'exploitation sous-jacent et des systèmes utilisés pour la gestion des bases de données et de l'information.

En simplifiant, on peut dire que «l'internet peut aussi fonctionner, par exemple, simplement grâce au fait que les protocoles de communication et les contenus de données sont définis. Il n'est pas nécessaire d'indiquer quel système d'exploitation ou quel gestionnaire de bases de données doit être utilisé».

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.

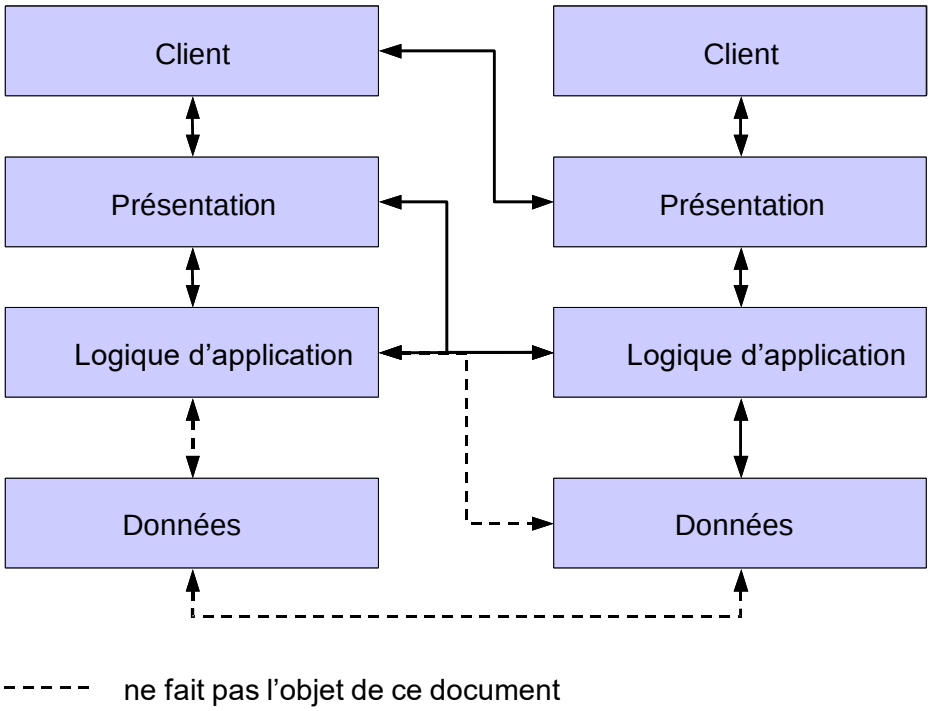

Figure 5-3 Voies de communication possibles

Exception: Le chapitre 6.6.5 Protocoles de serveur d'annuaire selon 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.

5.3.2 Exemple d'architecture à trois niveaux

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

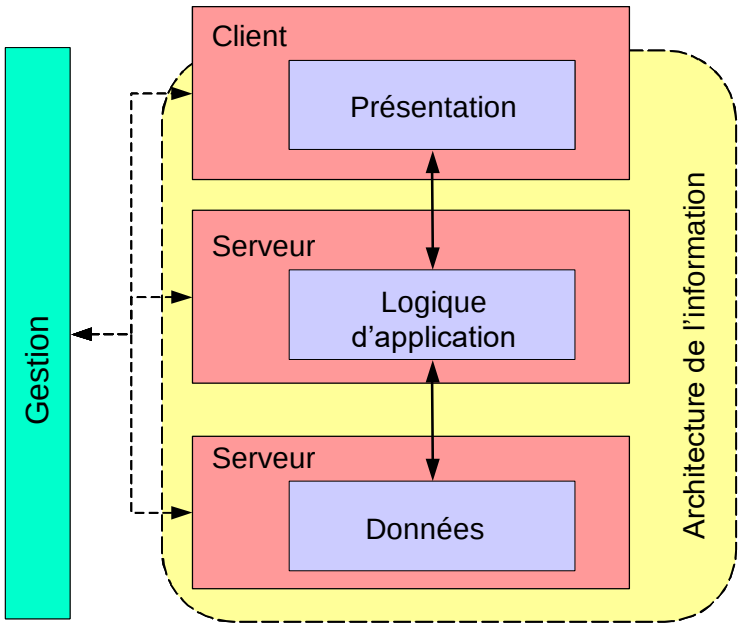

Figure 5-4 Architecture à trois niveaux

Remarque: L'architecture à trois niveaux se rencontre 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 plate-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).

5.3.3 Exemple d'une 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 (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.

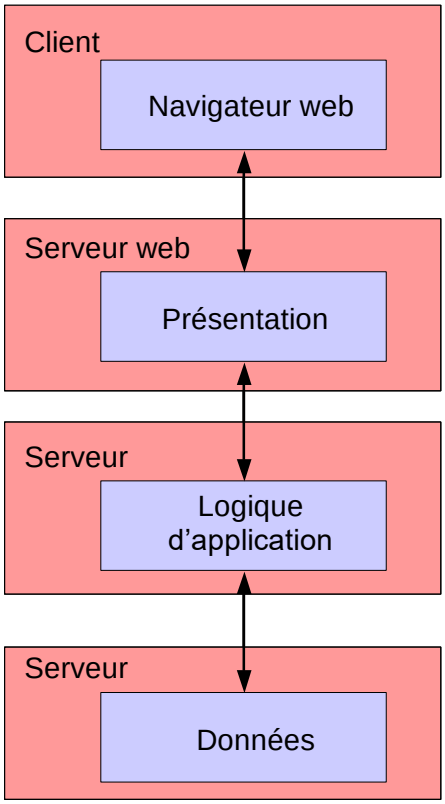

Figure 5-5 Architecture à n niveaux

5.3.4 Remarque concernant l'architecture orientée service (SOA)

L'architecture orientée service (Service-Oriented Architecture, SOA) 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.

6 Protocoles de communication

Dans ce chapitre, nous distinguons entre les protocoles suivants:

- les protocoles de réseau et de transport, cf. chapitre 6.3 Protocoles de réseau et de transport
- les protocoles d'application, cf. chapitre 6.4 Protocoles d'application
- les protocoles de communication mobile, cf. chapitre 6.5Communication mobile
- les protocoles d'accès aux services d'annuaire, cf. chapitre 6.6 "Services d'annuaire"
- les protocoles ou les échanges de données dans le domaine de l'intergiciel (middleware), cf. chapitre 6.7 Web Services (WS).

En outre, nous indiquerons à quelles interfaces I1, I2, I3 (cf. chapitre 5 Limites du système et 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:

I2 **I3**

Selon les recommandations faites, le protocole XY est utilisé aux interfaces I2 (système-système) et I3 (système-centre de clearing), mais non pas à l'interface I1 (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.

6.1 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 8.

6.2 Protocoles de la couche liaison de données

Les protocoles de la couche liaison de données (couche 1 du modèle Internet) ne font pas l'objet de ce document parce que le raccordement des systèmes au réseau incombe aux organisations et opérateurs concernés. C'est pourquoi nous ne donnons ici aucune recommandation à ce propos.

6.3 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].

6.3.1 Pile de protocoles internet

La pile de protocoles internet comprend les protocoles IP, TCP et UDP, ainsi que les protocoles d'application basés sur TCP ou UDP.

I1	I2	I3	
Pile de protocoles internet selon IETF			vivement recommandé

6.3.2 IPv6

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

I1	I2	I3	
IPv6			vivement recommandé

Normes: RFC 2460 et normes s'y rattachant.

6.3.3 IPv4

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

I1	I2	I3	
IPv4			recommandé

Normes: IPv4 (RFC 791, RFC 3232 et normes s'y rattachant), TCP RFC 793, UDP RFC 768

6.4 Protocoles d'application

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

6.4.1 File Transfer Protocol, FTP

Le protocole FTP (File Transfer Protocol) est l'une des principales normes utilisées pour le transfert de fichiers.

I1	I2	I3	
File Transfer Protocol (FTP) pour le téléchargement de fichiers			recommandé

Normes: RFC 959, RFC 2228, RFC 2640

6.4.2 Hyper Text Transfer Protocol, HTTP

HTTP doit être appliqué pour la communication Web. 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.

	I1	I2	I3	
Hyper Text Transfer Protocol (HTTP)				vivement recommandé

Normes: HTTP RFC 1945 et RFC 2616, HTTP State Management Mechanism RFC 2965

6.4.3 Simple Mail Transfer Protocol et 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. Les pièces jointes doivent correspondre aux formats de fichier prescrits par SAGA.ch.

	I1	I2	I3	
Simple Mail Transfer Protocol et format (SMTP et MIME)				vivement recommandé

Normes: RFC 2821, RFC 2822, RFC 2045, RFC 2046, RFC 2047, RFC 2048, RFC 2049 et normes s'y rattachant.

6.4.4 Protocoles d'accès à la messagerie électronique

Il peut arriver que des boîtes aux lettres électroniques soient proposées. On utilisera à ce propos les normes POP3, IMAP4 ou HTTP d'une manière standard pour l'accès aux courriels.

	I1	
POP3, IMAP4, HTTP pour e-mail		vivement recommandé

Normes: POP3 RFC 1939, IMAP4 RFC 2061, HTTP pour e-mail RFC 1945 v.1.0 et RFC 2616 v.1.1

6.4.5 Telnet

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

Telnet	non recommandé

6.4.6 Remote Procedure Call (RPC)

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

	I2	I3
Remote Procedure Call (RPC) avec ports dynamiques		non recommandé

	I2	I3
Remote Procedure Call (RPC) authentifié avec ports fixes		recommandé

Normes: RFC 1050, RFC 1831

6.4.7 Terminal Service et protocoles Thin Client

L'utilisation de Terminal Service et de protocoles Thin Client n'est éventuellement possible qu'à l'interface I1. Terminal Service et les protocoles Thin Client nécessitent toutefois que les deux systèmes soient configurés, gérés et sécurisés par la même institution aux interfaces I1. Leur utilisation n'est donc pas recommandée.

	I1	I2	I3
Terminal Service et protocoles Thin Client			non recommandé

La fonctionnalité client du côté gauche de l'interface I1 est toutefois assurée par le Terminal Server.

6.4.8 Web DAV

Le protocole WebDAV (Distributed Authoring and Versioning) est défini dans le document RFC 2518 et constitue une extension des protocoles HTTP/1.1 selon RFC 2616. 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.

	I1	I2	I3
WebDAV			recommandé

Norme: RFC 2518

6.5 Communication mobile

Au cas où des services seraient offerts par téléphonie mobile , l'échange d'informations devrait s'effectuer à l'aide du protocole WAP (Wireless Access Protocol). WAP a été normalisé à l'origine par le WAP Forum (www.wapforum.org), auquel a maintenant succédé l'organisation Open Mobile Alliance (www.openmobilealliance.org), OMA.

I1	
Wireless Access Protocol	en observation

Normes: toute une série de normes ont été définies pour les protocoles et services apparentés se rapportant au WAP, telle la norme Wireless Application Protocol Architecture (voir aussi annexe A Références et bibliographie). Les normes élaborées et publiées par l'OMA définissent, entre autres, comment les documents XML peuvent être transportés par le protocole WAP.

6.6 Services d'annuaire

6.6.1 LDAPv.3

LDAPv3 (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.

I1	I2	I3	
LDAPv.3			vivement recommandé

Normes: RFC 2251 et normes s'y rattachant.

6.6.2 LDIF

Les données publiées sur la base du protocole LDAP ont souvent le **format** LDIF (LDAP Data Interchange Format).

I1	I2	I3	
LDIF			recommandé

Norme: RFC 2849

6.6.3 LDAP Replication

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

I2 **I3**

LDAP (Version 3) Replication Requirements	en observation

Norme: RFC 3384

6.6.4 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.

I1 **I2** **I3**

Directory Services Markup Language (DSMLv.2.0)	recommandé

Norme: Directory Services Markup Language (DSML) v.2.0, janvier 2002, d'OASIS (www.oasis-open.org).

6.6.5 Protocoles de serveur d'annuaire selon 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

I2 **I3**

Protocoles de serveur d'annuaire selon X.500	recommandé

Normes: X.519 et recommandations de l'UIT (www.itu.org) s'y rattachant.

6.6.6 OCSP

Le protocole OCSP (Online Certificate Status Protocol) permet de déterminer l'état actuel d'un certificat sans accéder à une CRL (Certification Revocation List). OCSP se base sur HTTP.

I1	I2	I3	
Online Certificate Status Protocol (OCSP)			recommandé

Norme: RFC 2560

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 (PKI).

6.7 Protocoles pour un échange d'informations en temps réel

6.7.1 SIP

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

I1	I2	I3	
Session Initiation Protocol (SIP)			recommandé

Norme: le SIP est défini dans plusieurs normes et RFC informatifs. La norme de base RFC 3261 a été actualisée en tant que telle et dans différentes autres normes, dans lesquelles elle a aussi été complétée.

6.7.2 Famille de protocoles H.323

La famille de protocoles H.323 a été développée par l'UIT pour la voix sur IP.

I1	I2	I3	
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 toutefois été actualisés dans différentes autres normes, telles que H.325 ou H.328.

6.7.3 Skype

Skype est un protocole voix sur IP (téléphonie Internet) propriétaire qui n'a pas encore été normalisé.

	I1	I2	I3
Skype			non recommandé

Norme: pas de norme, protocole propriétaire

6.8 Web Services (WS)

6.8.1 Définition

L'appellation «Web Services» prête à confusion pour les non-spécialistes, car sa traduction littérale, c'est-à-dire services internet, ne reflète pas la signification technique que donnent à ce terme les organisations de normalisation (OASIS, WS-I, W3C) et leurs membres. On trouve en outre 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. Couplés de manière souple, ces derniers sont évolutifs et leur interopérabilité est garantie. Leurs interfaces sont définies dans un format déterminé et selon une syntaxe précise.
>
> Ces services sont décrits en XML au moyen du langage WSDL (Web Services Definition Language) et communiquent entre eux par messages en format XML. Ces messages sont transmis à l'aide du protocole SOAP (Simple Object Access Protocol).

6.8.2 Aperçu du système Web Services

Web Services (WS)[5] constitue un système logiciel, ou plutôt intergiciel, comprenant principalement les composantes suivantes:

- le protocole intergiciel utilisé pour l'échange des messages, à savoir le Simple Object Access Protocol, SOAP;
- la description des services du domaine Web Services; le langage WSDL (Web Service Description Language) est utilisé à cet effet;
- le lieu de classement ou de publication du service; UDDI (Universal Description Discovery Integration) peut être utilisé pour le service d'annuaire (directory) où les services du domaine Web Services sont publiés;
- la gestion des transactions.

[4] Pour faciliter la compréhension, nous ne donnons pas ici la traduction littérale de la définition du W3C.

[5] Les informations et les figures suivantes sont tirées, entre autres, de l'ouvrage [GuA]. Nous conseillons au lecteur intéressé, mais ne connaissant pas encore les Web Services, de consulter ce livre, qui sera aussi utile au lecteur d'orientation technique connaissant les bases de XML [ZoT].

6.8.3 Dépendances

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

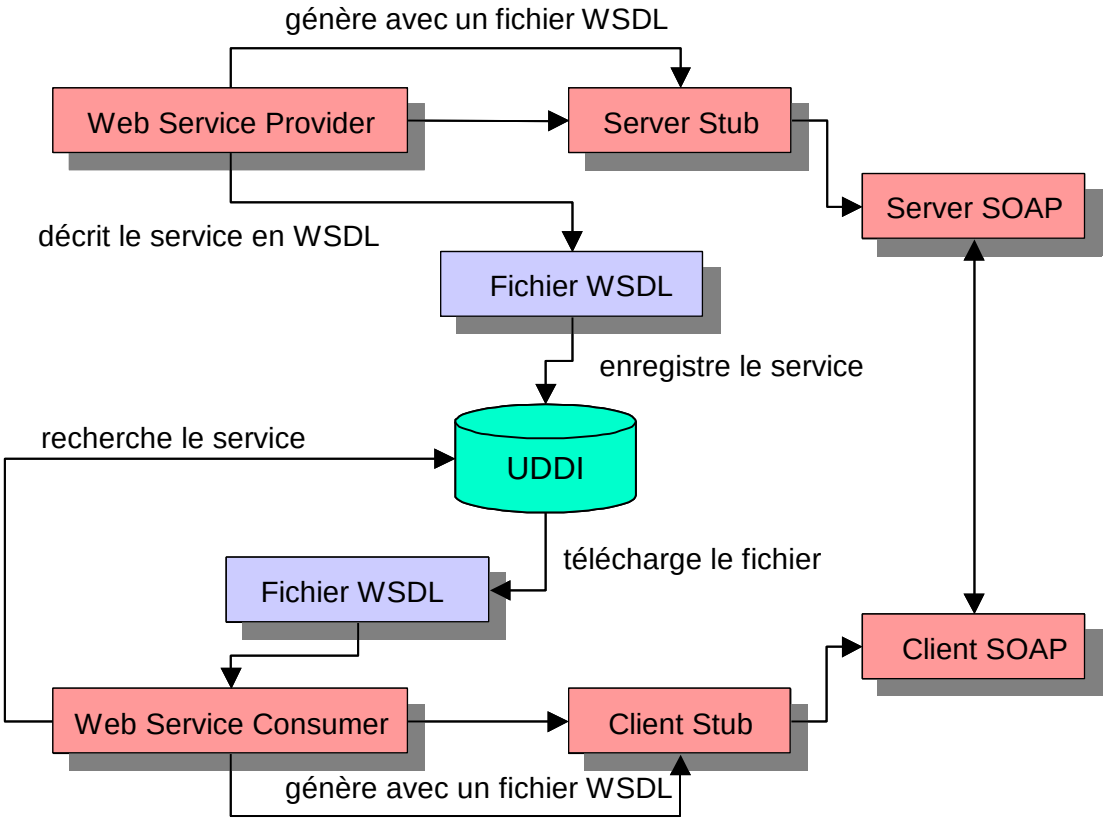

Figure 6-1 Dépendances

- Le fournisseur d'un service Web décrit ce dernier dans un fichier WSDL, qu'il publie ensuite dans un annuaire UDDI.
- Le fournisseur génère la souche serveur (Server Stub) à l'aide du fichier WSDL (la souche serveur est constituée d'un programme et d'une interface individuels à chaque service et résultant des exigences envers ce dernier. Elle représente le lien entre l'intergiciel et les commandes du service à exécuter).
- Le consommateur d'un service Web veut utiliser un service déterminé, qu'il trouve dans un annuaire UDDI. Là, le logiciel client télécharge la description du service. Il génère ensuite la souche client (Client Stub) à l'aide du fichier WSDL.
- Le consommateur Web utilise maintenant le service. Ce dernier est obtenu par l'intermédiaire des souches client et serveur, et à l'aide du protocole SOAP.

6.8.4 Architecture du système Web Services

L'architecture du système Web Services peut être représentée schématiquement de la manière suivante:

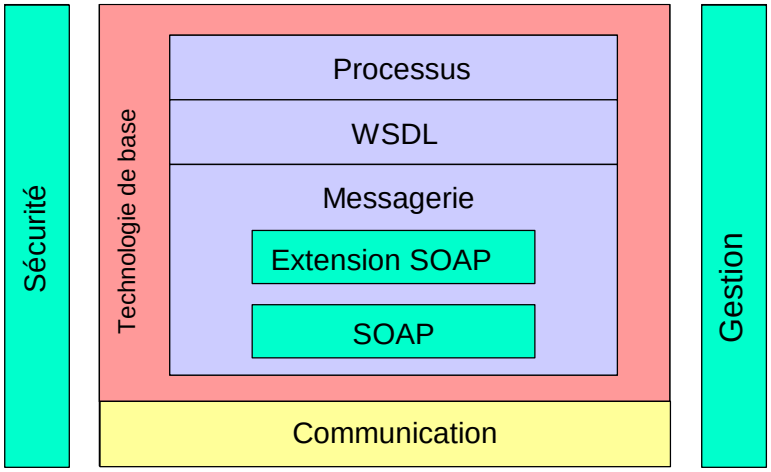

Figure 6-2 Modèle d'architecture

- **Communication:** Dans l'environnement Web Services, le terme de «communication» est utilisé dans une autre acception que par les spécialistes des réseaux. Il s'agit ici d'un protocole d'application selon le modèle internet, par exemple HTTP ou SMTP, qui décrit comment les messages SOAP doivent être transportés sur le réseau.
- **Messagerie:** Cette fonction compose et envoie les messages SOAP, ou les reçoit et les retransmet. Elle pilote aussi la séquence des messages et leur traitement. SOAP constitue la technologie d'échange de messages dans le domaine Web Services. Des extensions peuvent être intégrées dans les messages SOAP pour protéger, entre autres, leur authenticité et leur confidentialité.
- **WSDL:** Comme nous l'avons déjà mentionné, le langage WSDL sert à décrire (définir) les services du domaine Web Services.
- **Processus:** Une fois définis les services du domaine Web Services ainsi que leur mode de publication, il importe encore d'indiquer comment ils doivent se dérouler et avec quelles interactions. Le déroulement de l'ensemble du service doit d'abord être défini sous forme de processus séparés. Ces derniers influencent ensuite le déroulement des différentes transactions et le procédé d'échange de messages.
- **Technologie de base:** Font partie de la technologie de base, entre autres, les formats (XML) et la structure des messages.
- **Gestion:** Les différents services doivent être configurés et administrés.
- **Sécurité:** La sécurité devrait faire partie intégrante de tous les domaines mentionnés ici (communication protégée, messagerie sécurisée, documents WSDL

authentifiés, processus ou transactions fiables, etc.).Les technologies de sécurité possibles dans ces différents secteurs sont mentionnées au chapitre 8 Sécurité.

6.8.5 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 (*envelope*) de l'ensemble du message, dans laquelle il est indiqué d'une manière générale que le fichier XML correspondant représente un message SOAP;
- 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;
- le corps (*body*) du message, qui contient toutes les informations nécessaires pour le destinataire de ce dernier.

SOAP se fonde sur un protocole d'application TCP (voir figure ci-dessous).

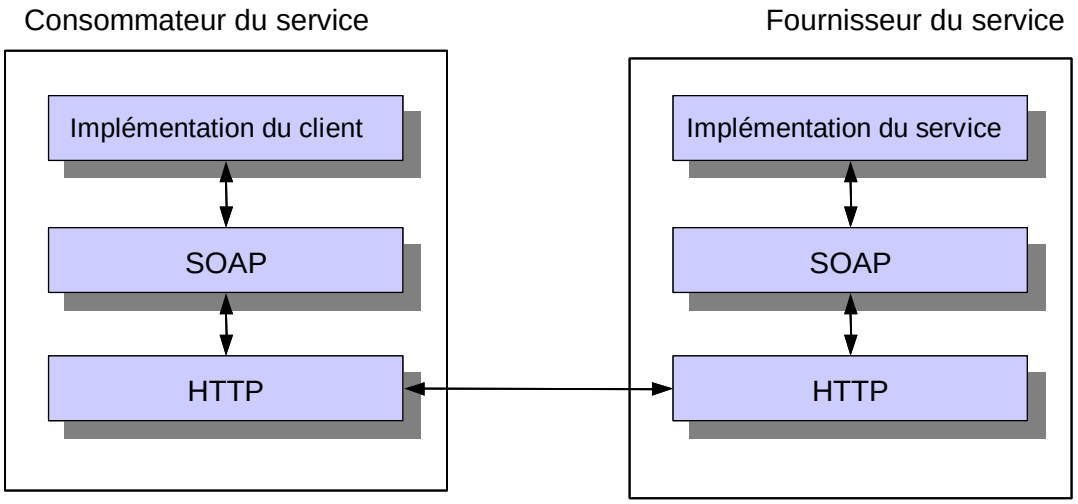

Figure 6-3 Pile de protocoles

Peuvent servir de protocole d'application pour SOAP:

- HTTP,
- SMTP,
- etc.

I1 **I2** **I3**

Simple Object Access Protocol (SOAP)	vivement recommandé

Norme: Simple Object Access Protocol (SOAP) v.1.2, juin 2003, du W3C (www.w3C.org).

6.8.6 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, seul le protocole HTTP ou le Container MIME peuvent être utilisés pour SOAP v.1.1.

Le document WSDL comprend essentiellement les deux éléments suivants:

- **la partie abstraite** (abstract part), qui définit les services et les messages à échanger;
- **la partie concrète** (concrete part), qui indique comment et à l'aide de quelle adresse les messages doivent être échangés.

La «partie abstraite» comprend à son tour les sous-domaines suivants:

- **Types** - Définit le cadre formel des messages, tels que les noms et les formats.
- **Message** - Comprend les noms et les contenus des messages qui sont échangés pour le service correspondant.
- **Operation** - Définit l'opération initiée par les messages.
- **Port Type** - Définit le groupe d'opérations supporté par une interface Web Services.

La «partie concrète» comprend quant à elle les sous-domaines suivants:

- **Binding** - Définit le codage des données et indique le protocole par lequel elles doivent être envoyées.
- **Port** - Spécifie l'adresse du service avec une URI (adresse d'objet détaillée, de syntaxe prédéfinie).
- **Service** - Indique les différentes adresses à l'aide desquelles le service défini ici peut être demandé.

I1	I2	I3

Web Service Description Language (WSDL v.1.1)	vivement recommandé

Web Service Description Language (WSDL v.2.0)	en observation

Norme: WSDL Web Services Description Language v.1.1 15, mars 2001 du W3C (www.w3C.org).

6.8.7 Universal Description, Discovery and Integration (UDDI)

Normalise la publication des services dans le domaine Web Services.

I1	I2	I3

Universal Description, Discovery and Integration (UDDI v.2)	recommandé

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

6.8.8 Protocoles de transaction

A lui seul, SOAP ne suffit pas pour le déroulement de processus d'affaires complexes. C'est pourquoi les protocoles de transaction ci-après ont déjà été conçus et spécifiés:

- WS Coordination
- WS Atomic Transaction (qui constituait auparavant une partie de WS-Transaction)
- WS Business Activity (qui constituait auparavant une partie de WS-Transaction)
- OSCI v1.2

6.8.8.1 WS Coordination

WS Coordination a été conçu et spécifié par OASIS (www.oasis-open.org).

	I1	I2	I3
WS Coordination			en observation

Norme: WS Coordination Protocol (draft), août 2006 d'OASIS (www.oasis-open.org).

6.8.8.2 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 est actuellement en procédure de consultation à OASIS (www.oasis-open.org).

	I1	I2	I3
WS Atomic Transaction			en observation

Norme: Web Services Atomic Transaction (WS Atomic Transaction), août 2006, d' OASIS (www.oasis-open.org), draft.

6.8.8.3 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.

	I1	I2	I3
WS Business Activity			en observation

Norme: Web Services Business Activity, mars 2006, d'OASIS (www.oasis-open.org), draft.

6.8.8.4 OSCI-Transport v.1.2

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.

I1	I2	I3	
OSCI-Transport v.1.2			recommandé

Norme: OSCI a été conçu en Allemagne dans le cadre du concours MEDIA@Komm.

6.8.9 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.

I1	I2	I3	
electronic business using XML (ebXML)			en observation

Normes: les normes concernant ebXML peuvent être obtenues auprès d'OASIS (www.oasis-open.org).

6.8.10 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].

6.8.10.1 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.

Business Process Execution Language (BPEL) v.1.1	recommandé

Norme: Business Process Execution Language for Web Services (BPEL4WS) v1.1, décembre 2003, d'OASIS (www.oasis-open.org).

6.8.10.2 BPMN

BPMN (Business Process Modeling 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. C'est pourquoi nous conseillons, pour une utilisation plus simple de BPMN, le set BPMN réduit selon DIN16566-3 Affaires électroniques — Partie 3: Gestion des processus d'affaires dans l'administration publique; modèle de démarche (www.din.de).

Business Process Modeling Notation (BPMN) v.1.0	en observation

Norme: BPMN 1.0, OMG Final Adopted Specification, février 2006 de l'Object Management Group (www.omg.org; www.bpmn.org).

6.8.10.3 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.

Unified Modeling Language (UML) v.1.5	recommandé

Unified Modeling Language (UML) v. 2.0	recommandé

Norme: Unified Modeling Language d'Object Management Group (www.omg.org). On utilisera la version 2.0 en cas de doute.

6.8.10.4 XPDL

XML Process Definition Language (XPDL) est une application XML pour la définition de processus et de flux de travail. XPDL a été normalisé par la Workflow Management Coalition (www.wfmc.org), WFMC.

XML Process Definition Language (XPDL)	en observation

Norme: XML Process Definition Language (XPDL), octobre 2002, version 1.0, du WFMC (www.wfmc.org).

6.8.11 Remarque concernant les organismes de normalisation du domaine Web Services

Quatre organismes méritent d'être cités dans l'environnement Web Services:

- Web Services Interoperability Organization (www.ws-i.org)
- OASIS (www.oasis-open.org)
- W3 Consortium (www.w3C.org)
- Business Process Management Initiative (www.bpmi.org)

6.8.12 REST

REST est l'abréviation de «Representational State Transfer» et désigne un type ou un style d'architecture destiné aux systèmes de médias distribués. REST[7] décrit une méthode servant à la conception de systèmes d'information et définissant les interfaces avec les ressources, les composantes et les éléments de données.

REST et Web Services ou les connexions classiques à l'internet peuvent s'exclure mutuellement, sans que ce soit une obligation, cf. [WSA]. Les implémentations REST devraient toutefois utiliser les composantes (protocoles, formats de données) proposées dans ce document. REST n'est toutefois pas encore normalisé définitivement. Par conséquent, nous lui accordons seulement le statut «en observation».

	I1	I2	I3
REST (Representational State Transfer)			en observation

[7] Voir le document [FiR] pour des informations plus détaillées sur REST

6.9 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.

6.10 Remarque

Les protocoles et formats de données de l'environnement Web Services mentionnés ici ainsi que les formats de données du chapitre 7 ne sont en général pas équipés de mécanismes de sécurité ou ceux-ci n'y sont que d'une efficacité très limitée. Si des données confidentielles doivent être transmises, nous recommandons d'utiliser les technologies de sécurité décrites au chapitre 8.

7 Formats de descriptions de fichiers et de données

Ce chapitre 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 I1, I2, I3 les formats correspondants doivent être appliqués. (Pour la définition de I1, I2, I3 cf. 5.2 Interfaces page 20.) Exemple:

> Pour le format de fichier XZ, l'indication suivante est donnée.
>
> **I1** **I3**
>
> Selon les recommandations faites, le format de fichier XZ doit être utilisé à l'interface I1 (terminal-système) et I3 (système-centre de clearing), mais non pas à l'interface I2 (système-système).

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

- documents et descriptions y relatives, cf. chapitre 7.2
- images et graphismes (dans des documents), cf. chapitre 7.3
- multimédia, cf. chapitre 7.4
- divers, cf. chapitre 7.5 et autres

7.1 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 8.

7.2 Documents et descriptions y relatives

7.2.1 CSS (Cascading Stylesheet)

Inventeur	Håkon Wium Lie, Bert Bos pour la version 1, W3C pour la version 2
URL de l'inventeur	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 ou de la forme de contenus. CSS peut servir à la représentation des contenus XML, HTML et XHTML.

Utilisation

Définition de la présentation d'informations en formats XML, HTML et XHTML

I1 **I2** **I3**

CSS (Cascading Stylesheet) v.2	vivement recommandé

Norme: Cascading Style Sheet (CSS), recommandation 2.0, mai 1998 du W3C (www.w3C.org)

CSS (Cascading Stylesheet) v.2.1	en observation

7.2.2 Comma Separated Value (CSV)

Inventeur Borland
URL de l'inventeur 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.

Utilisation

Echange de données de produits et de plate-formes différentes

I1	I2	I3	
Comma Separated Value List (CSV)			recommandé

7.2.3 EPS (Encapsulated Post Script)

Inventeur Adobe Systems
URL de l'inventeur 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.

I1	I2	I3	
EPS (Encapsulated Post Script)			recommandé

7.2.4 GML (Geography Markup Language)

Inventeur Open Geospatial Consortium

URL de l'inventeur www.opengeospatial.org

Le langage GML (Geography Markup Language) est un encodage XML pour l'échange et l'archivage d'informations spatiales, englobant la géométrie et les propriétés des objets géographiques.

Utilisation

Pour la description (sur la base de XML Schema) et l'échange (en XML) d'informations géographiques.

I1	I2	I3

GML 3.0/3.1	En observation

7.2.5 Hypertext Markup Language (HTML)

Inventeur Tim Berners-Lee
URL de l'inventeur www.w3c.org

Hypertext Markup Language (HTML) est un langage normalisé pour la description des pages WWW dans internet ou intranet. Il s'agit d'une application du langage SGML (Standard Generalized Markup Language), donc d'un langage de balisage défini suivant les principes du SGML. Le moyen formel pour cette définition est la DTD (Document Type Definition). SGML a été développé par Charles F. Goldfarb et est défini dans la norme ISO 8879 (voir aussi le commentaire concernant le format de fichier XML, chapitre 7.1.19). SGML définit tant la conception, le contenu et le graphisme de la page que les liens (hyperliens, connexions) avec des pages associées ou étrangères.

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.

I1 **I2** **I3**

Hypertext Markup Language (HTML) v.4.01	vivement recommandé

HTML v.3.1 est recommandé pour les ordinateurs de poche (PDA) et les téléphones portables.

Hypertext Markup Language (HTML) v.3.1	recommandé

Normes: voir IETF (www.ietf.org) RFC 2854.

7.2.6 Interlis

Inventeur Werner Messmer, Josef Dorfschmid
URL de l'inventeur

Le format de données Interlis est utilisé pour la saisie de données géographiques et pour leur échange en Suisse. Il existe deux versions utilisées dans notre pays, à savoir la version 1 (SN 612030) et la version 2 (SN 612031), qui sont des normes de l'Association suisse de normalisation (www.snv.ch).

Utilisation

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

I1 **I2** **I3**

Interlis, version 1	recommandé

La version 1 d'Interlis sera remplacée ces prochaines années par la version 2.

Interlis, version 2	vivement recommandé

7.2.7 LDIF

Les données publiées au moyen de LDAP sont souvent dans le **format** LDIF (LDAP Data Interchange Format).

S1 S2 S3

LDIF	recommandé

Norme: RFC 2849

7.2.8 MIME (Multipurpose Internet Mail Extension)

Inventeur	IETF (N. Borenstein, T. Rose)
URL de l'inventeur	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 (p. ex. Netscape), 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. (RFC 2045, 2046 et normes s'y rapportant)

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.

I1	I2	I3	
Multipurpose Internet Mail (MIME)			vivement recommandé

Normes: RFC 2045, RFC2046 et normes s'y rapportant, de l'IETF (www.ietf.org).

7.2.9 Format XML de Microsoft Office

Inventeur Microsoft

URL de l'inventeur www.microsoft.com

Microsoft a publié les formats de fichiers XML pour Word, 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 plateforme. 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

Echange de données (textes, tableaux, formulaires ou diagrammes)

I1	I2	I3	
Format XML 2003 de Microsoft Office			non recommandé

7.2.10 ODF

Inventeur OASIS

URL de l'inventeur www.oasis-open.org et www.openoffice.org

ODF (Open Document Format) est un format de fichier ouvert et 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. En tant que norme ouverte, qui continue d'être développée sous la direction d'OASIS, ce format permet de nouvelles approches de solutions qui vont au-delà des possibilités des applications traditionnelles de bureautique.

Utilisation

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

I1	I2	I3	
ODF v. 1.0			recommandé

Normes: ISO/IEC 26300 ou à OASIS

7.2.11 Office Open XML Format

Inventeur ecma

URL de l'inventeur www.ecma-international.org

Le format XML Open Office se base sur XML et est un format défini par l'ECMA et pouvant être implémenté librement dans différentes applications et plate-formes. Ce format a été conçu d'emblée de manière à ce que son codage soit compatible avec Microsoft. En tant que norme ouverte, définie sous la direction d'ECMA, ce format permet de nouvelles approches de solutions, qui vont au-delà des possibilités des applications traditionnelles de bureautique.

Utilisation

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

I1	I2	I3	
Format XML Open Office			recommandé

Normes: TC45 - Open Office XML Formats http://www.ecma-international.org/

7.2.12 Portable Document Format (PDF)

Inventeur Adobe Systems
URL de l'inventeur www.adobe.com

Le format PDF de Adobe Systems est un format de fichier polyvalent 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.

En raison de son énorme diffusion sur internet, il peut être considéré comme un standard industriel reconnu dans le monde entier pour la transmission électronique de documents.

Utilisation

PDF (Portable Document Format) est un format de fichier polyvalent 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.

	I1	I2	I3
Portable Document Format (PDF) v.1.4			vivement recommandé

PDF v.1.4 peut être lu à l'aide du programme Acrobat Reader, version 5.0 ou plus.

	I1	I2	I3
Portable Document Format (PDF) v.1.3, 1.5, 1.6, 1.7			recommandé

PDF v.1.3 peut être lu à l'aide du programme Acrobat Reader, version 4.0 ou plus. PDF v.1.5/6/7 peut être lu à l'aide du programme Acrobat Reader, version 6.0/7.0/8.0.

7.2.13 PDF/A

PDF/A est une version normalisée par l'ISO du Portable Document Format. PDF/A (A = archivage) 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. Cette norme est un sous-ensemble de PDF 1.4, qui est spécifié dans ISO 19005-1:2005.

Cette norme spécifie deux niveaux de concordance:

- PDF/A-1a - Level A conformance dans la partie 1
- PDF/A-1b - Level B conformance dans la partie 1 (exigences limitées)

	I1	I2	I3
Portable Document Format (PDF)/A			vivement recommandé

Norme: ISO 19005-1:2005

7.2.14 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.).

PDF/X est normalisée dans les documents ISO suivants:

- ISO 15929 définit l'approche PDF/X dans son ensemble.
- ISO 15930 définit les parties normalisées concrètes.

ISO 15390 est subdivisée en plusieurs sous-normes, la norme ISO 15930-3: PDF/X-3: 2002 étant essentiellement utilisée en Europe.

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) X/3	recommandé

Norme: ISO 15930 Serie

7.2.15 PS (Post Script)

Inventeur Adobe Systems
URL de l'inventeur 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.

I1 I2 I3

Post Script (PS) Level 1-2-3 (comme format d'échange de documentes)	non recommandé

7.2.16 RDF (Resource Description Framework)

Inventeur W3C
URL de l'inventeur 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 information, 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.

I1 I2 I3

RDF (Resource Description Framework)	recommandé

Norme: Resource Description Framework Model and Syntax Specification Recommendation, 22 février 1999, norme du W3C (www.w3C.org)

7.2.17 RTF (Rich Text Format)

Inventeur Microsoft
URL de l'inventeur www.microsoft.com

RTF (Rich Text Format) est un format de fichier spécial, développé pour transférer des textes formatés, avec graphismes, entre différents programmes de traitement de texte. RFT utilise les jeux de caractères ANSI, PC-8, Macintosh et IBM PC pour la présentation et le formatage des documents. Avantage du format RTF: son utilisation conserve le formatage des fichiers texte, même en cas d'échange entre des logiciels de différents fabricants. 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.

I1	I2	I3	
Rich Text Format (RTF), version 1.6			vivement recommandé

Les spécifications peuvent être obtenues auprès de Microsoft (http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnrtfspec/html/rtfspec.asp)

7.2.18 WML (Wireless Markup Language)

Inventeur OMA
URL de l'inventeur www.openmobilealliance.org

WML (Wireless Markup Language) se fonde sur XML et à été développé pour la présentation réduite de textes et d'images sur les téléphones portables. Il utilise WAP comme protocole de transmission.

Utilisation

Pour la présentation de textes et d'images sur des téléphones mobiles et pour leur transmission à partir de ces appareils.

I1	I2	I3	
WML (Wireless Markup Language)			en observation

Contrairement à la version 1, la version 2 de WML est un sous-ensemble de XHTML Basic et intègre les profils CSS Mobile.

7.2.19 XHTML (eXtensible Hypertext Markup Language)

Inventeur W3C
URL de l'inventeur 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 dans le WWW.

I1 I2 I3

eXtensible Hypertext Markup Language (XHTML) v.1.0	vivement recommandé

eXtensible Hypertext Markup Language (XHTML) v.1.1	recommandé

Norme: XHTML 1.0 et 1.1, Extensible Hypertext Markup Language Recommendation 1.1, mai 2001 du W3C (www.w3C.org).

eXtensible Hypertext Markup Language (XHTML) v.2.0	en observation

7.2.20 XML (eXtensible Markup Language)

Inventeur W3C
URL de l'inventeur www.w3C.org

Tout comme HTML, XML (eXtensible Markup Language) est une application SGML (Standard Generalized Markup Language) indépendante des plate-formes. Le développement de XML a commencé en 1996. Ce langage est normalisé par le W3C depuis février 1998. XML est également normalisé dans le RFC 3470.

Les langages de balisage (Markup Languages) servent à interpréter des données et des structures au moyen de marques appelées balises. Les balises sont des règles pour le traitement des contenus qu'elles désignent.

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. Le modèle de format d'un document XML peut être décrit au moyen du langage XSL (eXtensible Style Language). Le schéma XML est lui aussi une application XML et porte le plus souvent l'extension de fichier .xsd.

Concernant XML et notamment les espaces nominatifs XML, nous renvoyons le lecteur au document eCH-0018 d'eCH.

Utilisation

XML définit des structures de données et de documents.

I1 I2 I3

eXtensible Markup Language (XML) v.1.x	vivement recommandé

Norme: Extensible Markup Language (XML), recommandation du W3C (www.w3C.org).

7.2.21 XML Schema

Inventeur W3C
URL de l'inventeur www.w3C.org

XML Schema est aussi une application de XML et sert à décrire le modèle de contenu et à déclarer des éléments tels que des commandes et des ordres de paiement, ou des enregistrements simples, tels que des adresses.

XML Schema est subdivisé par le W3C en trois normes:

- XML Schema Part 0: Primer
- XML Schema Part 1: Structures
- XML Schema Part 2: Datatypes

XML Part 0 vise une description facilement lisible des propriétés de XML Schema et est conçue de manière à ce que l'utilisateur comprenne facilement comment réaliser des schémas XML. XML Schema Part 1 et 2 définissent comment les propriétés et les particularités de la structure et des types de données doivent être décrit dans le schéma XML.

Utilisation

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

I1 **I2** **I3**

XML Schema Part 0,1,2	vivement recommandé

Concernant les normes et les versions, voir le document eCH-0036 du groupe spécialisé XML.

7.2.22 XSL (eXtensible Stylesheet Language)

Inventeur W3C
URL de l'inventeur 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 dans le langage XML;
- XPath (XML Path Language), un langage décrivant comment référencer des éléments XSLT de documents XML ou comment 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 formater des documents XML.

I1 **I2** **I3**

eXtensible Stylesheet Language (XSL) v. 1.0	vivement recommandé

Normes: XSL, Extensible Stylesheet Language Recommendation 1.0, octobre 2001, de W3C (www.w3C.org).

XSL V.2.0 (avec XPath 2.0)	en observation

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.

7.3 Images et graphismes (documents)

7.3.1 GIF (Graphics Interchange Format)

Inventeur Compuserve
URL de l'inventeur 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. **L'utilisation du format GIF est soumise à licence, mais sans frais.**

Les deux versions GIF 87a et 89a doivent être supportées, mais GIF 89a est préférable.

Utilisation

Echange de données

I1	I2	I3	
Graphics Interchange Format (GIF) 87a/89a			vivement recommandé

7.3.2 JPEG (Joint Photografic Expert Group)

Inventeur JPEG (Joint Photografic Expert Group)
URL de l'inventeur: 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. Les formats JPEG sont normalisés par cette commission et en portent le nom. JPEG permet en outre une compression sans perte et la représentation de plus de 16 millions de couleurs. **L'utilisation du format JPEG est soumise à licence, contre paiement ou sans frais selon les conditions.**

Utilisation

Echange de données d' image sous forme comprimée

I1	I2	I3	
Joint Photographic Expert Group (JPEG / JPG)			vivement recommandé

7.3.3 PNG (Portable Network Graphics)

Inventeur W3C
URL de l'inventeur www.w3C.org

PNG (Portable Network Graphics) est un format de fichier développé et normalisé par le World Wide Web Consortium (W3C). Il est du domaine public et devrait à terme remplacer les formats GIF et JPEG et servir à comprimer des images sans diminution importante de la qualité.

Utilisation

Enregistrement comprimé de données d'images.

I1	I2	I3

Portable Network Graphics (PNG)	vivement recommandé

Norme: Portable Network Graphics (PNG), recommandation du 10 novembre 2003, du W3C (www.w3C.org)

7.3.4 SVG (Scalable Vector Graphics)

Inventeur W3C
URL de l'inventeur 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 bi-dimensionnelles, 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

Utilisation

Enregistrement de données vectorielles.

I1	I2	I3

Scalable Vector Graphics (SVG) v.1.1	recommandé

Norme: Scalable Vector Graphics (SVG) 1.1, recommandation du 14 janvier 2003, du W3C (www.w3C.org)

7.3.5 TIFF (Tagged Image File Format)

Inventeur aldus/adobe
URL de l'inventeur 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 version actuelle 5.0 de 1997 offre une intensité de couleur de 24 bits et une compression de données sans perte. La plupart des

programmes graphiques qui traitent des images à base de pixels prennent ce format en charge.

Utilisation

TIFF est utilisé principalement dans l'archivage numérique, parfois aussi pour l'échange sans perte de données d'image (bitmap).

I1 **I2** **I3**

Tagged Image File Format (TIFF) v.5.0	recommandé

7.4 Multimédia

7.4.1 MPEG (Motion Pictures Expert Group)

Inventeur MPEG (Motion Pictures Expert Group)
URL de l'inventeur 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.

7.4.1.1 MPEG-1

MPEG-1 permet des débits de compression atteignant 1,5 mégabit 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

7.4.1.2 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

7.4.1.3 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

I1	I2	I3	
MPEG-4 v.3			recommandé

7.4.2 MP3

Voir chapitre 7.4.1.1.

7.4.3 Ogg

Inventeur Xiph.org Foundation
URL de l'inventeur: 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. Le format bitstream Ogg est normalisé dans le RFC3534.

Utilisation

Echange de données audio et vidéo

I1	I2	I3	
OGG Theora			en observation

OGG Vorbis			en observation

7.4.4 QT (QuickTime)

Inventeur Apple Macintosh
URL de l'inventeur www.apple.com

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

I1	I2	I3	
QT (QuickTime) v.6.5			recommandé

7.4.5 WAV (WAVEform audio format)

Inventeur Microsoft
URL de l'inventeur www.microsoft.com

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 plate-formes. WAV n'est pas soumis à licence et peut être utilisé gratuitement.

Utilisation

Pour l'enregistrement de données audio

I1	I2	I3	
WAV (WAVEform audio format)			recommandé

7.4.6 WMV/A (Windows Media Video/Audio)

Inventeur Microsoft
URL de l'inventeur www.microsoft.com

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

I1	I2	I3	
WMV/A (Windows Media Video/Audio) v.9			recommandé

7.5 Divers

7.5.1 Compression

7.5.1.1 GZIP (Gnu ZIP)

Inventeur Abraham Lempel, Jacob Ziv, Terry Welch
URL de l'inventeur:

GZIP sert à la compression de données sans perte et est une version à source ouverte contenue dans les systèmes d'exploitation UNIX. Il se base sur le même algorithme que ZIP et a été normalisé dans le RFC 1952.

Utilisation

Compression de données sans perte d'information

I1	I2	I3	
GZIP (Gnu Zigzag Inline Package) v.4.3			recommandé

7.5.1.2 ZIP

Inventeur A. Lempel, J. Ziv

Zigzag Inline Package (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. Les logiciels tels que Winzip travaillent avec cette méthode.

Utilisation

Echange de données sous forme comprimée sans perte d'information

I1	I2	I3	
Zigzag Inline Package (ZIP) v.2.0			vivement recommandé

7.5.2 SMS (Short Message Service)

Inventeur SMS Forum
URL de l'inventeur: 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.

I1	I2	I3

SMS (Short Message Service)	recommandé

7.6 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. Les composantes non signées doivent donc être bloquées.

Composantes exécutables non signées, telles que ActiveX, Java Applets	non recommandé

Tous les navigateurs Web ne permettent pas la réception de composantes exécutables ni ne prennent en charge toutes les composantes exécutables mentionnées ici. C'est pourquoi nous recommandons de faire en sorte que la lecture des pages Web et que la communication de cyberadministration restent possibles dans ces conditions aussi.

7.6.1 ActiveX

Inventeur Microsoft
URL de l'inventeur www.microsoft.com

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).

I1

Composantes actives signées	recommandé

7.6.2 Java Applets

Inventeur Sun Microsystems
URL de l'inventeur www.sun.com

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.

I1

Composantes Java Applets signées	recommandé

7.6.3 Java Script

Inventeur Brendan Eich, Netscape Communication
URL de l'inventeur www.netscape.com

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.

I1

Composantes JavaScript signées	recommandé

Recommandation: Si l'exécution de composantes actives est autorisée chez le destinataire, ce dernier devrait activer sur son ordinateur un programme actualisé de contrôle de la sécurité des contenus (Content Security).

7.6.4 . Net Assembly

Inventeur Microsoft
URL de l'inventeur www.microsoft.com

Utilisation

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

I1

.Net Assembly signé	en observation

7.6.5 AJAX

Inventeur Jesse James Garrett
URL de l'inventeur

Utilisation

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.

I1

Fichiers AJAX signés	en observation

8 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 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[8] pour les parties impliquées.

La sécurité des données est à considérer comme une composante 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 fortement augmenté au cours des 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 I1, I2 et I3. 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 supplémentaire sont encore à formuler par ***eCH*** et SAGA.ch en plus de celles concernant la stratégie de sécurité informatique[9].

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

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

8.1 Modèle structurel pour la sécurité des données

Le modèle structurel ci-après (figure 8-1) 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 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.

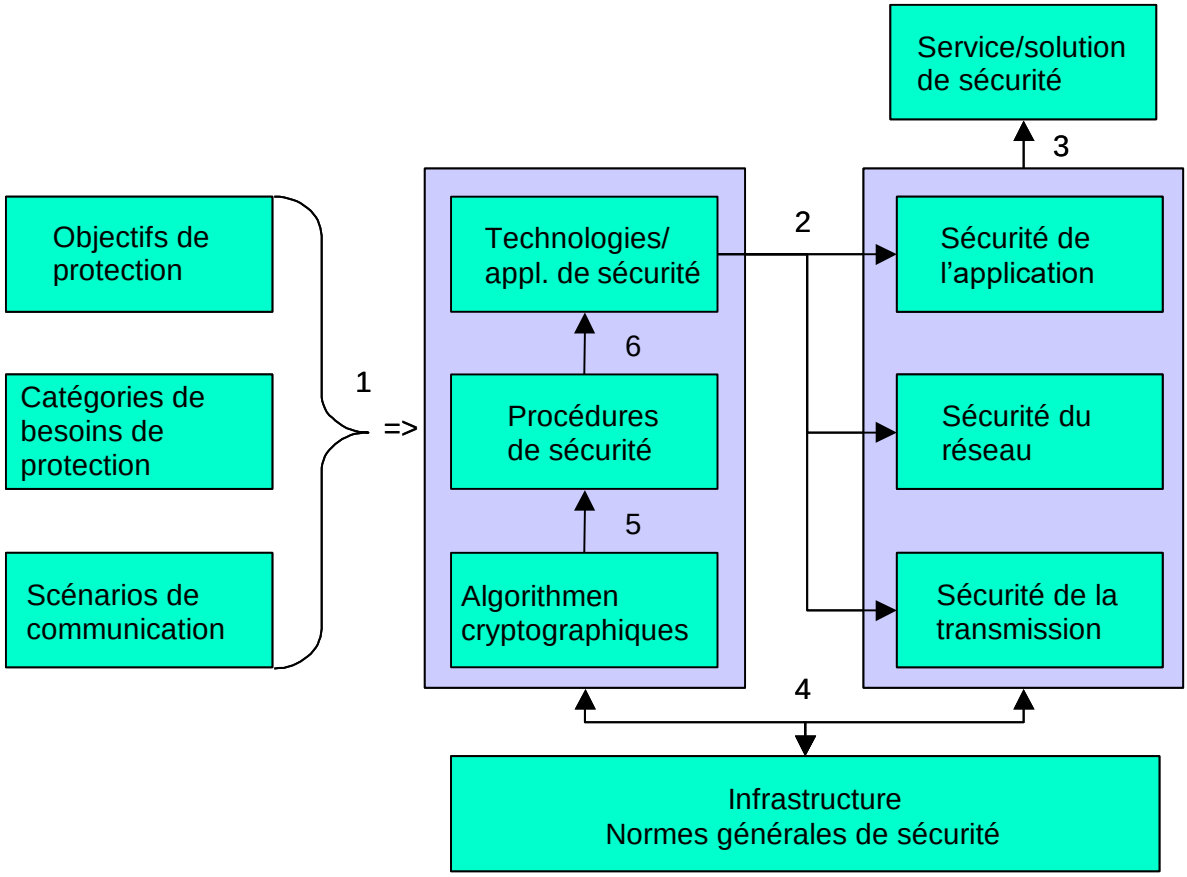

Figure 8-1 Modèle structurel pour les normes de sécurité

Explication de la figure:

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

- authenticité
- confidentialité
- intégrité
- disponibilité.

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

Algorithmes cryptographiques. Dans ce bloc sont définis les algorithmes cryptographiques dont le fonctionnement doit être possible.

Procédures de sécurité. 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. 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)[10]. 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 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 (p. ex. SSL/TLS) du modèle internet architectural (IETF) ou les données d'application elles-mêmes (S/MIME).

Infrastructure et normes générales de sécurité: 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.

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

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,
- 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.

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.

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 de l'USIC. 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.

(La numérotation ci-après se rapporte à la figure 8-1 ci-dessus)

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. La solution de sécurité 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.

Remarque: Le modèle structurel et les normes de sécurité des données que nous présentons ici ne dispense 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.

8.2 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: une information est considérée comme **confidentielle** lorsque ses destinataires croient[11] que personne d'autre ne peut la lire ou la consulter.
  Définition 2: 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: des données sont considérées comme **intègres** lorsque l'on croit pouvoir en percevoir toute modification non autorisée ou non souhaitée par leur propriétaire ou lorsque l'on croit pouvoir les protéger contre toute modification illicite ou involontaire.
  Définition 2: protection de l'exactitude de l'intégrité de l'information ainsi que des méthodes de processus.
- **Authenticité**: protection contre la falsification d'identité ou d'origine
  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: des données ou des informations sont considérées comme **authentiques** lorsque l'on croit savoir de quelle entité elles proviennent.
  Définition 2: 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).

[11] Nous avons utilisé ici consciemment le verbe «croire» pour bien exprimer le fait qu'il n'existe aucune sécurité absolue. Nous aurions aussi pu dire «pensent» ou «supposent». Nous avons volontairement évité de dire «lorsqu'il est garanti que personne d'autre que ses destinataires ne peut la lire ou la consulter».

- **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: 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 services de sécurité (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 (cryptographie) 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.

8.3 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.

Pour la partie civile de l'administration fédérale, le besoin de protection est fixé dans la NSP (NSP = Network Security Policy de l'Unité de stratégie informatique de la Confédération, l'USIC); pour la cyberadministration, il comprend les quatre catégories suivantes, qui sont tirées de normes internationales et de la proposition allemande (SAGA.de):

Catégorie	Effet des dommages
«aucun»	Aucune protection particulière n'est nécessaire, car aucune conséquence ou seuls des effets très modérés sont à attendre.
«faible à moyen»	Les effets des dommages sont limités et maîtrisables, sans problème de financement.
«élevé»	Les effets des dommages peuvent être considérables et perturber fortement le déroulement du service
«très élevé»	Les effets des dommages peuvent atteindre une ampleur existentielle, catastrophique.

Tableau 8-1 Catégories de besoins de protection

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) une catégorie de besoin de protection selon le tableau ci-dessus (aucun, faible à moyen, etc.) (cette méthode est également appelée classification).

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.

8.3.1 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 y relatives 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 (manuel de protection informatique de base allemand du BSI; http://www.bfd.bund.de/technik/DS-KAP/35.htm).

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.

8.3.2 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.).

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.

Catégorie	Mesures pour assurer l'authenticité
«aucune»	Aucune mesure n'est nécessaire
«faible à moyen»	Nom d'utilisateur et mot de passe, mot de passe à utilisation unique
«élevé»	MAC, HMAC, signatures numériques, transfert de clé avec clés courtes
«très élevé»	MAC, HMAC, signatures numériques, transfert de clé avec clés d'une longueur minimale déterminée et générées selon des critères précis

Tableau 8-2 Catégories de besoin de protection et mesures à prendre pour chacune

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.

8.4 Algorithmes cryptographiques

Ce sous-chapitre définit les algorithmes cryptographiques 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 un algorithme de cryptage asymétrique)
- Cryptographie symétrique
- Stéganographie
- Fonctions hash
- Générateurs de chiffres aléatoires

8.4.1 Cryptographie à clé publique

Les algorithmes suivants de cryptographie à clé publique sont reconnus et utilisés:

- RSA
- Courbes elliptiques (Elliptic Curve Public Key Kryptosystem)
- Diffie-Hellman (Public Key Kryptosystem) [12]

RSA	vivement recommandé

Selon le cas d'application (use case) et le besoin de protection, l'algorithme RSA a seulement le statut «en observation».

Normes: RFC 3447, PKCS#1 v.2.1, IEEE P1363. Le fonctionnement de l'algorithme est décrit dans [Sch] et [Stw].

Diffie-Hellman	recommandé

Selon le cas d'application (use case) et le besoin de protection, l'algorithme Diffie Hellman a seulement le statut «en observation».

Normes: IEEE P1363. Le fonctionnement de l'algorithme est décrit dans [Sch] et [Stw].

Courbes elliptiques	recommandé

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

Normes: IEEE P1363. Le lecteur trouve 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 docu-

[12] La notion d'algorithme Diffie-Hellman est utilisée ici dans sons sens élargi comme le système de cryptage qui génère la clé publique y à partir de la clé publique x selon la formule $y = g^x \bmod p$, p étant un nombre premier, g d'ordre q, q étant aussi un nombre premier

ment [Bek] de RegTP (www.regtp.de) définissent les paramètres et les longueurs de clé pour les algorithmes à clés publiques (pour l'utilisation de signatures électroniques)[13]. Pour RSA, le document ETSI TS 102 176 et al. indique selon quelle méthode les nombres premiers doivent être générés.

8.4.2 Cryptographie symétrique

Les algorithmes suivants devraient être supportés:

- IDEA
- 3DES
- AES

Les données devraient encore être compressées avant le cryptage pour renforcer l'efficacité des algorithmes mentionnés ci-dessus.

IDEA	vivement recommandé

Norme: IDEA n'est pas normalisé, mais cet algorithme est mentionné dans de nombreuses autres normes, telles que SSL et TLS. Son fonctionnement est décrit dans [Sch] et [Stw]. L'utilisation d'**IDEA nécessite une licence payante**.

DES avec clé de 56 bits	non recommandé

3DES avec clé de 112 bits	recommandé

3DES avec clé de 168 bits	vivement recommandé

Norme: FIPS 46-3 pour DES. Le fonctionnement de l'algorithme 3DES est décrit dans [Sch] et [Stw].

AES	vivement recommandé

Norme: FIPS 197

AES permet d'utiliser des clés de longueurs différentes.

Clés de 128 bits	recommandé
Clés de 192 bits	recommandé
Clés de 256 bits	vivement recommandé

[13] Une harmonisation est nécessaire tant entre le document [Bek] de RegTP et SAGA.de qu'entre SAGA.ch et le document [APSES] de l'OFCOM.

Si possible, le cryptage devrait s'effectuer en mode CBC et le «padding» devrait être minimal (cf. [Vau]).	recommandé

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 8.4.5 Générateurs de nombres aléatoires).

8.4.3 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 de droits d'auteur	en observation

8.4.4 Fonction hash

Les fonctions hash suivantes doivent être supportées:

- SHA-1
- MD5
- SHA 256/384/512
- RIPEMD-160

SHA-1	vivement recommandé

Normes: FIPS 180-1, RFC 3174

MD5	recommandé

Non recommandé pour une **protection des données sur une longue durée.** comme pour la signature d'un certificat ou d'un contrat.

Normes: RFC 1321

SHA 256/384/512	recommandé

Normes: FIPS 180-2

SHA 256/384/512 a obtenu un statut moins élevé 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 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.

RIPEMD-160	recommandé

Le document décrivant le fonctionnement de RIPEMD-160 peut être obtenu à l'adresse suivante: http://www.esat.kuleuven.ac.be/~cosicart/pdf/AB-9601/AB-9601.pdf

8.4.5 Générateurs de nombres aléatoires

Les générateurs de nombres aléatoires doivent être installés de façon modulaire afin qu'ils puissent être remplacés.

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.

8.5 Procédures de sécurité

Les procédures de sécurité suivantes sont définies ici:

- authentification en ligne
- signature valable à long terme
- négociation en ligne d'une clé de session

8.5.1 Authentification en ligne

Pour l'authentification en ligne dans l'environnement client-serveur, les différentes technologies suivantes peuvent être appliquées:

- nom d'utilisateur et mot de passe, mot de passe à utilisation unique
- «challenge response»
- Signature numérique
- transfert de clé
- MAC (HMAC)
- authentification biométrique

8.5.1.1 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 une 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. IPSEC permet également l'établissement d'une connexion à l'aide d'un élément secret connu par les deux parties. Cet élément peut aussi être un mot de passe. Voir à ce propos le chapitre 8.5.1.5 MAC (HMAC).

Nom et mot de passe, mot de passe à utilisation unique sur une ligne sécurisée (p. ex. SSL/TLS) ou pour l'établissement d'une connexion IPSEC	recommandé

8.5.1.2 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.

Avec cette procédure, il s'agit de distinguer si une clé de session est négociée ou non pour la protection de la communication. Parmi les protocoles comprenant la négociation d'une clé de session, citons

- SSL/TLS
- IPSEC

Les recommandations du chapitre 8.5.1.4 Transfert de clé s'appliquent par analogie aux procédures Challenge Response qui ne prévoient pas la négociation d'une clé de session pour la protection de la communication.

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

Procédures Challenge Response avec négociation d'une clé de session pour la protection de la communication, sur connexion sécurisée	recommandé

Les recommandations concernant les procédures Challenge Response avec négociation d'une clé de session pour la protection de la communication sont mentionnées dans les chapitres 8.7.1à 8.7.4.

8.5.1.3 Signature numérique

L'authentification s'effectue par le biais d'une signature numérique. Pour celle-ci, une fonction hash et une procédure à clé publique sont nécessaires. Comme fonction hash peuvent être utilisées les procédures définies au chapitre 6.3 Algorithmes cryptographiques. Pour les procédures à clé publique, les algorithmes RSA, Diffie Hellmann ou à courbes elliptiques sont à disposition.

RSA	vivement recommandé

Normes: PKCS#7 1.5, RFC 2315, IEEE P1363

Courbes elliptiques et Diffie-Hellman pour signatures numériques	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); l'algorithme utilisant le système de cryptage à courbe elliptique est appelé Elliptic Curve DSA (ECDSA).

8.5.1.4 Transfert de clé

Dans le système du transfert de clé, un élément secret (suite binaire aléatoire) est crypté avec la clé publique de l'entité à authentifier. Le code qui en résulte est envoyé à cette entité. Si celle-ci peut déterminer l'élément secret, c'est-à-dire décrypter le code reçu et convaincre la partie adverse de la connaissance de cet élément secret, elle est considérée comme authentifiée. Cette procédure d'authentification est souvent combinée avec l'algorithme HMAC.

Cet algorithme est aussi utilisé pour la négociation d'une clé de session sur la base de la clé transférée. Dans S/MIME, c'est cette dernière qui est la clé de session; dans SSL, la clé transférée est utilisée avec d'autres éléments pour générer la clé de session.

RSA	vivement recommandé

Normes: cet algorithme est implémenté 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

Comme système de transfert de clé, citons par exemple ElGamal.

8.5.1.5 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: HMAC RFC 2104. L'algorithme MAC lui-même n'est pas normalisé, mais utilisé en pratique pour la sécurisation des protocoles de routage.

8.5.2 Authentification biométrique

Les systèmes biométriques sont encore peu normalisés et sont rarement utilisés pour l'authentification dans l'environnement informatique.

Authentification biométrique	en observation

8.5.3 Signature électronique 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 (cf. [Mud] pour les problèmes de la conservation à long terme des signatures numériques).

Signature valable à long terme	en observation

Norme: RFC 3126

8.5.4 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, car il permet l'utilisation de l'algorithme de Diffie-Hellmann ou à courbes elliptiques, au choix, pour négocier la clé de session.

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 RFC 2631). (TLS, par exemple, permet de négocier les clés en ligne en utilisant la méthode mentionnée).

Normes: IEEE P1363, PKCS#3, 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 (RFC 2409, 2412).

RSA	en observation

Dans RSA, la négociation des clés se base toutefois sur le transfert des clés tel qu'il est décrit au chapitre 8.5.1.4 clé. Dans ce contexte, nous octroyons à RSA le statut «en observation» parce qu'aucun algorithme n'est encore implémenté dans les technologies de sécurité connues pour la négociation en ligne d'une clé de session avec RSA.

8.6 Données et connexions authentifiées et confidentielles

Il existe, entre autres, les différences suivantes entre les données et les connexions authentifiées:

- Pour les connexions, l'authentification s'effectue en ligne. C'est pourquoi, dans un environnement PKI, toute authentification se basant sur un certificat peut être déclarée non valide si le certificat de l'utilisateur 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 que les données doivent conserver leur authenticité au-delà de la durée de validité du certificat (voir la norme correspondante dans le chapitre 8.5.3 Signature électronique à long terme). La protection de l'authenticité des données nécessite par conséquent un archivage protégé.
- Dans l'environnement PKI, l'authenticité peut aussi être réalisée, pour des connexions authentifiées, par le transfert de clé 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.

Il existe également, entre autres, les différences suivantes entre les données et les connexions protégées au niveau de la confidentialité:

- Pour les connexions confidentielles, les informations ne sont protégées que sur la liaison et peuvent ensuite se trouver en texte clair sur le PC ou le serveur.
- Les données confidentielles sont 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. Cela pose une exigence accrue au système de gestion des clés.

8.7 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)[14]. 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.

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

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

- SSL/TLS
- WTLS
- 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 dans le chapitre 8.4 Algorithmes cryptographiques 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 5.2 Interfaces, page 20). Exemple:

> Pour la technologie de sécurité YZ, nous donnons l'indication suivante.
>
> **I1 I2**
>
> 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).

8.7.1 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. En pratique toutefois, les différents fabricants se sont le plus souvent contentés de réaliser dans leurs produits la protection de HTTP. Bien qu'identiques à 95% environ, SSL et TLS sont incompatibles entre eux.

I1 I2 I3

Secure Socket Layer (SSL) v.3.0	vivement recommandé

Normes: bien qu'il n'existe pour lui qu'un projet de RFC, SSL v.3.0 est considéré comme une norme de fait.

Secure Socket Layer (SSL) v.2.0	non recommandé

Transport Layer Security (TLS)	vivement recommandé

Normes: TLS v.1.0 est défini par l'IETF (www.ietf.org) dans le RFC 2246.

Transport Layer Security (TLS) Extensions	recommandé

Normes: RFC 3546

8.7.2 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.

I1

Wireless Transport Layer Security (WTLS)	recommandé[15]

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.

8.7.3 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.

I1 I2 I3

Secure Shell (SSH)	en observation

Normes: Secure Shell a été adopté par l'IETF (www.ietf.org) depuis janvier 2006 comme norme et est défini dans les RFC 4250 à 4256, 4332, 4344, 4419, 4462 et autres.

8.7.4 IPSEC

IPSEC sert à sécuriser les paquets IP (entre autres pour les applications UDP et TCP). Les normes à son sujet (il y en a plusieurs) ont été spécifiées par l'IETF (www.ietf.org) dans les RFC correspondants. IPSEC doit être supporté et peut être appliqué en même temps que d'autres technologies de sécurité, ceci en particulier lorsque la durabilité de la confidentialité doit être assurée.

[15] 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.

	I1	I2	I3
IP Security (IPSEC)			vivement recommandé

Normes: IPSEC a été normalisé par l'IETF (www.ietf.org) dans les RFC 2402, 2406, 2409, 2412 et dans les recommandations s'y rapportant.

IP Security (IPSEC) version 2.0	en observation

IP Security version 2.0 comporte des faiblesses considérables 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 de la norme 4306 IKE v.2 peut notamment accélérer fortement les attaques de type "Brute Force" ainsi que le contrôle de plausibilité d'un candidat pour une clé.

8.7.5 S/MIME

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

	I1	I2	I3
Secure MIME (S/MIME) v.2.0			vivement recommandé

Norme: RFC 2311 S/MIME Version 2 Message Specification et recommandations s'y rapportant.

Secure MIME (S/MIME) v.3.1	recommandé

Normes: les normes correspondantes sont définies par l'IETF (www.ietf.org) dans le RFC 3851 et les recommandations s'y rapportant.

8.7.6 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.

8.7.6.1 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) (cf. RFC 3275).

Cette norme définit les signatures numériques et les procédures d'authentification avec l'algorithme 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.

	I1	I2	I3
XML Signature			vivement recommandé

Normes: RFC 3275, XML Signature and Syntax Processing Recommendation, février 2002, du W3C (www.w3C.org).

8.7.6.2 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.

	I1	I2	I3
XML Encryption			vivement recommandé

Norme: XML Encryption and Syntax Processing Recommendation, décembre 2002, du W3C (www.w3C.org).

8.7.7 Open PGP

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 est devenu une norme de fait. PGP est normalisé dans le RFC 2440 sous l'appellation Open PGP.

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

I1	I2	I3

Open Pretty Good Privacy (Open PGP) si les certificats X.509v.3 sont supportés	recommandé,

Normes: RFC 2440 pour PGP. RFC 3156 spécifie l'interopérabilité avec S/MIME.

8.7.8 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 pertinence et l'étendue des projets de normes ne peuvent pas encore être évaluées dans leur intégralité.

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

- XML Security (cf. chapitre 8.7.6 XML Security, p. 85)
- SOAP Security
- SAML
- XRML
- XACML
- XKMS
- Sécurité de la transaction (Transaction Security), voir chapitre 8.7.9

8.7.8.1 SOAP Security

SOAP Security est une norme définie par OASIS (www.oasis-open.org) pour l'échange sécurisé d'informations SOAP. 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.509v.3.

I1	I2	I3

SOAP Security	recommandé

Norme: SOAP Messages Security, Working Draft, août 2003, par OASIS (www.oasis-open.org)

8.7.8.2 SAML

Security Assertion Markup Language (SAML) est une norme définie par OASIS (www.oasis-open.org) et fournissant un moyen d'exprimer les informations relatives à l'authentification et à l'autorisation. Ces informations ressemblent à une inscription de fichier journal parce que le message SAML se borne à indiquer l'acte d'authentification et d'autorisation.

I1 **I2** **I3**

Security Assertion Markup Language (SAML)	en observation

Norme: Security Assertion Markup Language (SAML) v1.1, mars 2003, par OASIS (www.oasis-open.org)

8.7.8.3 XRML (eXtensible Rights Markup Language)

Inventeur OASIS (www.oasis-open.org) et ContentGuard (www.contentguard.com)
URL de l'inventeur www.xrml.org (emplacement de la spécification)

XRML est une application 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. XRML est conçu de manière à pouvoir être utilisé dans différents types d'architecture. 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

I1 **I2** **I3**

XRML (eXtensible Rights Markup Language) v.2.0	recommandé

Norme: XRML (eXtensible Rights Markup Language) v.2.0, novembre 2001, ContentGuard (www.contentguard.com) et OASIS (www.oasis-open.org)

8.7.8.4 XACML

XML Access Control Markup Language (XACML) a été normalisé par OASIS (www.oasis-open.org). XACML a été conçu de manière à ce que les règles concernant le contrôle d'accès (access control) puissent être exprimées et enregistrées en format XML.

XML Access Control Markup Language (XACML)	en observation

Norme: Extensible Access Control Markup Language (XACML) v1.0, janvier 2003, par OASIS (www.oasis-open.org)

8.7.8.5 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	en observation

Norme: W3C XML Key Management Specification (XKMS), Recommendation 2.0, 28, juin 2005

8.7.9 Protocole pour services d'horodatage

L'horodatage sert à prouver que certains documents sont mis à disposition à un instant déterminé, et contient entre autres l'indication de la date et de l'heure ainsi qu'une signature. Les services d'horodatage sont fournis par un tiers «digne de confiance» (Trusted Third Party), Le protocole servant à faire appel à un tel service et à fournir le timbre d'horodatage est appelé Time Stamp Protocol (TSP) et est normalisé dans le RFC 3161. Les services d'horodatage sont utilisés, entre autres, pour protéger la validité à long terme des signatures numériques (voir chapitre 8.5.3 Signature électronique à long terme.

Time Stamp Protocol (TSP)	recommandé

Norme: RFC 3161

8.7.10 Sécurité de la transaction

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).

Dans le domaine Web Services, on connaît les protocoles de transaction suivants:

- OSCI Transport
- WS Business Transaction Protocol
- WS-Atomic Transaction et WS Business Activity Security
- ebXML Security

8.7.10.1 OSCI Transport v1.2

Online Service Computer Interface (OSCI) englobe toute une série de protocoles adaptés aux exigences de la cyberadministration et développés par la centrale OSCI. Ces protocoles ont pour but l'assistance des transactions offertes sous forme de services Web et de leur déroulement complet.

Les principaux critères de conception pour le OSCI Transport dans sa version 1.2 étaient les suivants:

- se baser sur des normes (SOAP, Signature XML, XML Encryption),
- rester le plus indépendant possible de la technique sous-jacente, c'est-à-dire du protocole de communication, des plate-formes et des langages de programmation,
- fournir un niveau de sécurité modulable (signatures améliorées ou signatures électroniques qualifiées/accréditées, selon l'application et le besoin).

OSCI-Transport v.1.2	recommandé

Norme: OSCI a été élaboré en Allemagne dans le cadre du concours MEDIA@Komm.

8.7.10.2 WS Transaction Security

Développé et normalisé par le consortium OASIS (www.oasis-open.org) Web Services Business Transaction Protocol présuppose une relation de confiance mutuelle entre les parties concernées . C'est pourquoi OASIS n'a pas prévu de fonctions de sécurité dans cette norme. En principe, des caractéristiques et des mesures de sécurité sont toutefois utilisées dans les transactions, mais il n'existe pas encore de norme à leur propos.

Transaction Security	en observation

8.7.10.3 WS-Atomic Transaction et WS Business Activity Security

La spécification (norme) de WS-Transaction mentionne que la sécurité de la transaction doit être assurée par la sécurisations des messages SOAP.

WS-Atomic Transaction et WS Business Activity Security	en observation

Norme: voir paragraphes 6.8.8.2, 6.8.8.3

8.7.10.4 ebXML Security

electronic business XML (ebXML) est une série de normes créées en commun par le consortium OASIS (www.oasis-open.org) et par UN/CEFACT. Ces deux organismes ont ainsi l'intention de normaliser une infrastructure qui permette la généralisation de l'e-business et en assure l'interopérabilité.

Plusieurs normes du domaine de la sécurité ebXML ont été alors développées ou sont en voie de l'être. L'importance de ces normes de sécurité dans le cadre d'***eCH*** dépendra de deux facteurs:

- le statut (vivement recommandé, recommandé, etc.) qu'ebXML revêtira dans SAGA.ch,
- la sûreté, l'adéquation et/ou la diffusion de ces normes.

ebXML Security	en observation

8.8 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'interfaces avec l'application.

8.8.1 Utilisation de cartes intelligentes (smart cards)

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 cartes HSM, présentant des propriétés équivalentes au niveau de la sécurité, ont le même statut de recommandation que les «smart crypto cards».

ISO/IEC 7816 1-4	vivement recommandé

Remarque: Seule la norme ISO/IEC 7816 4 définit comment transmettre les commandes aux smart cards et les réponses qu'il faut en attendre. Les normes ISO/IEC 7816 1-2 définissent les contacts et les caractéristiques physiques de la carte. Quant à la norme ISO/IEC 7816, elle s'applique au protocole et aux signaux de transmission envoyés à la smart card et en revenant.

Les normes ISO/IEC 7816 1-4 sont mentionnées ici afin de rendre SAGA.ch compatible avec [a006d]. Dans [a006d], les exigences de la Confédération concernant les smart cards elles-mêmes et leurs contacts sont définies. (informations concernant les cartes à puce, cf. [RwEw]).

PC/SC	vivement recommandé

PKCS#11	vivement recommandé

MS Crypto API (Crypto Service Provider) pour la connexion des smart cards	recommandé

MS Crypto-API Service est une interface logicielle pour smart cards inséré dans les derniers systèmes d'exploitation Windows de Microsoft.

Pour les systèmes UNIX, tels que HP Unix, Solaris ou Linux, ainsi que pour les systèmes d'exploitation de Microsoft, les opérations avec la clé privée sur la smart card ou sur des supports de conservation de clés équivalents en matière de sécurité peuvent être lancées via PKCS#11. Cette norme a le statut «vivement recommandée».

8.8.2 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.

LDAPv.3	vivement recommandé

Normes: cf. chapitre 6.6 "Services d'annuaire"

8.8.3 Contenu des certificats et des CRL

8.8.3.1 Généralités

Les formats de certificat sont définis dans les normes X.509v.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 de ces certificats, ceux des CRL et la gestion des certificats sont toutefois définis dans un document séparé.*

8.8.3.2 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.

8.8.3.3 Identification et contenus des certificats

Il y a lieu de contrôler la bonne appartenance non seulement 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].

8.8.3.4 Complément concernant les certificats

Certificats pour serveur	vivement recommandé

Une distinction devrait être établie entre l'authentification et la signature numériques.

La première comprend uniquement l'identification de l'expéditeur. Nous recommandons de bien protéger l'authentification des systèmes de la cyberadministration pour que l'on puisse se fier aux informations qui y sont fournies. L'authentification par clé publique permet d'atteindre un bon niveau de sécurité, mais elle nécessite l'utilisation de certificats.

La seconde 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.
- 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

A l'instant de la correction rédactionnelle de ce document, l'OeDI est en cours de remaniement pour mise en conformité avec l'OSCSE et la SCSE. Dans ce contexte, il est prévu de définir les exigences de sécurité envers les certificats pour fonctions (certificats pour personnes non physiques) pour que la conformité avec la TVA soit assurée.

8.8.4 Signature - Numérisation des processus de cyberadministration

La SCSE et ses prescriptions d'exécution OSCSE et [TAV] sont en vigueur depuis le 1er janvier 2005. Depuis la révision correspondante du Code des obligations (CO), les signatures électroniques sont réglementées depuis le 1er janvier 2005, voir [DigSig]. dans la correspondance commerciale privée entre particuliers, mais pas entre particuliers et autorités ou entre autorités entre elles. La PA (procédure administrative au niveau fédéral) a été révisée suite aux nouvelles lois concernant le Tribunal fédéral. La PA révisée entre en vigueur le 1er janvier 2007. 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.

Au 1er janvier 2007 entreront 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.

8.8.5 Téléchargement de documents contenant des composantes actives (Java, JavaScript, ActiveX) voir 8.12

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.

8.8.6 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: cf. chapitre 6.4 Protocoles d'application et 6.6 "Services d'annuaire".

OCSP	recommandé

Normes: cf. chapitre 6.6 "Services d'annuaire".

8.8.7 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.

8.9 Contrôle 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 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 8.8.3.2 et 8.8.7). 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.

8.10 Gestion des clés

Les tâches ou domaines suivants font partie, entre autres, de la gestion des clés:

- génération des clés,
- conservation des clés,
- interface pour l'accès à la clé ou interface pour lancer une opération avec la clé privée,
- changement de la clé quand celle-ci doit être renouvelée,
- négociation d'une clé de session.

8.10.1 Génération des clés

La norme *ETSI TS 102 176* définit comment doivent être générées les clés pour les différents algorithmes à clé publique. Il définit également les tests que doivent passer les générateurs de chiffres aléatoires.

Ces derniers sont également utilisés pour la génération des clés symétriques.

8.10.2 Conservation des clés

Voir chapitre 8.8.1 Utilisation de cartes intelligentes (smart cards) et norme PKCS#12.

8.10.3 Interface pour les opérations avec la clé (privée)

Voir chapitre 8.8.1 Utilisation de cartes intelligentes (smart cards) et norme PKCS#12.

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 ne devrait être appliqué que dans un environnement de serveur, bien que nous préconisions ici aussi l'utilisation d'une carte HSM.

8.10.4 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 8.6 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 chapitre 8.5.3 Signature électronique à long terme

8.10.5 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 8.5.1.4 et 8.5.4).

8.11 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..

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 par **eCH**, 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 oeuvre 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, par une convention écrite spéciale, 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 toute restriction 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.

Appendice A – Références et bibliographie

Ouvrages spécialisés

[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, Allemagne
[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, 4. Auflage, 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 stratégie informatique de la Confédération USIC, art. n°. 609.201 (vente comme publication de la Confédération)
[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, 2. Auflage 2002, ISBN 3 9522387 4
[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, 3. Auflage, 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, 1. Auflage 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, Netherland, Lecture Notes in Computer Science No. 2332, pp. 534-545, Springer-Verlag, 2002 ou à: 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
Norme française de cyberadministration	Le cadre commun d´interoperabilité des systèmes d'information publics
SAGA.de	Normen und Architekturen für E-Government-Anwendungen in Deutschland, V.2.0, Bundesministerium des Innern

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
LTF	Loi fédérale du 17 juin 2005 sur le tribunal fédéral (RS 173.110)
OeDI	Ordonnance du DFF du 30 janvier 2002 concernant les données et les informations transmises par voie électronique (RS 641.201.1)
CO	Code suisse des obligations du 30 mars 1911 (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 3 décembre 2004 sur les services de certification dans le domaine de la signature électronique (RS 943.032)
SCSE	Loi fédérale du 19 décembre 2003 sur les services de certification dans le domaine de la signature électronique (RS 943.03)

eCH (www.ech.ch)

eCH-0018	Meilleures pratiques XML
eCH-0036	Documentation pour l'échange de données orienté XML

ECMA (www.ecma-international.org)

Open Office XML Format

ETSI (www.etsi.org)

ETSI TS 102 176 v.1.2.1	Electronic Signatures and Infrastructures (ESI) - Algorithms and Parameters for Secure Electronic Signatures

Normes IEEE (www.ieee.org)

IEEE P1363	Standard for RSA, Diffie-Hellman and related Public-Key Cryptography

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 1180	TCP/IP Tutorial
RFC 1123	Requirements for Internet Hosts - Application and Support
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 1952	GZIP file format specification version 4.3
RFC 2045	Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies
RFC 2046	Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types
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 2104	HMAC Keyed-Hashing for Message Authentication

RFC 2228	FTP Security Extensions
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 und zugehörige
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 2409	The Internet Key Exchange
RFC 2412	The Oakley Key Determination Protocol
RFC 2440	PGP Message Exchange Formats
RFC 2460	Internet Protocol, Version 6 (IPv6)
RFC 2518	HTTP Extensions for Distributed Authoring – WEBDAV
RFC 2560	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP
RFC 2616	Hypertext Transfer Protocol 1.1
RFC 2631	Diffie-Hellman Key Agreement Method
RFC 2634	Enhanced Security Services for S/MIME
RFC 2640	Internationalization of the File Transfer Protocol
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 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 3384	LDAP (version 3) Replication Requirements

RFC 3447	Public-Key Cryptography Standards (PKCS) #1
RFC 3534	The application/OGG Media Type
RFC 3546	Transport Layer Security (TLS) Extensions
RFC 3739	Qualified Certificates Profile
RFC 3850	S/MIME v.3.1 Certificate Handling
RFC 3851	Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1
RFC 3852	Cryptographic Message Syntax
RFC 4180	Common Format and MIME Type for Comma-Separated Values (CSV) Files
RFC 4252	The Secure Shell (SSH) Authentication Protocol
RFC 4253	The Secure Shell (SSH) Transport Layer Protocol
RFC 4306	The Internet Key Exchange (IKE v.2) Protocol

Normes ISO (www.iso.org)

ISO 15929: 2002	Graphic technology -- Prepress digital data exchange -- Guidelines and principles for the development of PDF/X standards
ISO 15930 Series 1-6	Graphic technology -- Prepress digital data exchange
ISO 19005-1: 2005	Document management -- Electronic document file format for long-term preservation -- Part 1: Use of PDF 1.4 (PDF/A-1)
ISO 7498-2	Information processing systems, Open Systems Interconnection, Basic Reference Model Part 2 Security Architecture
ISO/IEC 7816 1-4	Identification Cards-Integrated Circuits

Normes de l'UIT (www.itu.org)

ITU-T X.509v.3	Information Technology - Open Systems Interconnections - Public Key and Attribute Certificate Framework
ITU-T X.519	Information Technology - Open Systems Interconnections – The Directory: Protocol Specification
ITU-T X.525	Information Technology - Open Systems Interconnections – The Directory: Replication

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 180-2	SHA 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

Username Token Profile, Working Draft, August 2003

Web Services Atomic Transaction (WS Atomic Transaction) August 2006

Web Services Business Activity March 2006

Web Services Security, SOAP Messages Security 1.0, March 2004

Web Service Coordination Protocol, August 2006

Object Management Group (www.omg.org)

Unified Modeling Language (UML)

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 Online Service Computer Interface

PC/SC (www.pcscworkgroup.com)

PC/SC	Interoperability Specification for ICCs and Personal Computer Systems

Normes RSA (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), October 2002, Version 1.0

Normes W3C (www.w3C.org)

CSS Cascading Style Sheet Recommendation 2.0 12 May 1998

HTML 4.01 Specification W3C Recommendation 24 December 1999

PNG Portable Network Graphics, W3C Recommendation 10 November 2003

RDF Resource Description Framework Model und Syntax Specification Recommendation 22 February 1999

SOAP Simple Object Access Protocol (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

XHTML Extensible Hypertext Markup Language Recommendation 2.0, August 2002

XKML XML Key Management Specification v.2.0, Draft April 2003

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 200

XML Schema Part 2: Datatypes W3C Recommendation 2nd May 2001

XML Signature and Syntax Processing Recommendation, February 2002

XSL Extensible Stylesheet Language Recommendation 1.0, October 2001

Appendice C – Abréviations

2D	bidimensionnel
3 DES	Triple DES
ACL	Access Control List
ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
AJAX	Asynchronous JavaScript and XML
angl.	anglais
ANSI	American National Standards Institute (Institut américain de normalisation)
APEC	Asia-Pacific Economic Cooperation (Coopération économique de la zone Asie-Pacifique)
API	Application Programmers Interface
Appl.	Application
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
B2B	Business to Business (transactions électroniques entre entreprises)
B2C	Business to Customer (transactions électroniques entre une entreprise et une personne privée)
BGP	Border Gateway Protocol
BMI	Ministère fédéral de l'Intérieur (Allemagne)
BPEL	Business Process Execution Language
BPEL4WS	Business Process Execution Language for Web Services
BPMN	Business Process Modeling Notation
BSI	Office fédéral de sécurité dans la technique de l'information (Allemagne)
BVA	Office de l'administration fédérale (Bundesverwaltungsamt, Allemagne)
CA	Certification Authority, ou autorité de certification
CAPI	1) Common Application Programming Interface 2) Microsoft Crypto API
CBC	Cipher Block Chaining Mode
CC	Centre de clearing
CEN	Comité Européen de Normalisation
Cert	Certificat
cf.	confer, voir
CO	Code des obligations (RS 220)
CODEC	Compression Decompression Algorithm

CORBA	Common Object Request Broker Architecture
CPPA	Collaborative Partner Profile Agreement
CRL	Certificate Revocation List
CSP	Cryptographic Service Provider
CSS	Cascading Style Sheets Language
CSV	Comma Separated Value
DAP	Directory Access Protocol
DB	Data Base, base (banque) de données
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DIR	Directory Service
DMZ	Demilitarised Zone ou zone démilitarisée
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
ECW	Enhanced Compressed Wavelet
Ed.	Editeur
EDI	Electronic Data Interchange
EDIFACT	Electronic Data Interchange for Administration, Commerce and Transport
EIS	Enterprise Information System
EPS	Encapsulated PostScript
ERP	Enterprise Resource Planning
ETSI	Institut européen de normalisation des télécommunications (European Telecommunications Standards Institute)
FIPS	Federal (USA) Information Processing Standards
FTP	File Transfer Protocol
FTPD	FTP-Daemon
G2B	Government to Business (de l'administration aux entreprises)

G2C	Government to Citizen (de l'administration aux citoyens)
G2Con	Government to Consumer (de l'administration aux consommateurs)
G2G	Government to Government (de l'administration à l'administration)
G2O	Government to Organisation (de l'administration aux organisations)
G-I	Government internal
GIF	Graphic Interchange Format
GML	Geography Markup Language
GOSIP	Government Open Systems Interconnection Profile
GUI	Graphical User Interface
GZIP	Gnu Zip (Zigzag Inline Package)
HMAC	Keyed-Hash Message Authentication Code
HSM	High Speed Module
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HW	Hardware (matériel)
ICT	Information and Communication Technology
IDA	Interchange of Data between Administrations
IDEA	International Data Encryption Algorithm
IEEE	Institute for Electrical and Electronic Engineers - Institut des Ingénieurs en Électricité et en Électronique
IETF	Internet Engineering Task Force
IIOP	Internet Inter-ORB Protocol
IKE	Internet Key Exchange
IMAP	Internet Message Access Protocol
IMKA	Comité de coordination interministérielle pour les technologies de l'information à l'administration fédérale (Interministerieller Koordinierungsausschuss für die Informationstechnik in der Bundesverwaltung, Allemagne)
IP	Internet Protocol
IPSEC	IP Security Protocol
ISAKMP	Internet Security Association and Key Management Protocol
ISDN	Integrated Services Digital Network
ISO	Organisation internationale de normalisation
IT	Information Technologie ou technologie de l'information
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 Experts Group
JPG	Joint Photografic 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	millions de bits par seconde
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
NIST	(American) National Institute for Standards and Technology
NSP	Network Security Policy
NT	Network
NTP	Network Time Protocol
OASIS	Organization for the Advancement of Structured Information Standards
OCSP	Online Certificate Status Protocol
OGG	Xiph.org's container format
OMA	Open Mobile Alliance
OMG	Open Management Group
ONG	Organisations non gouvernementales
ORB	Object Request Broker
OS	Operating System
OSCI	Online Services Computer Interface
OSI	Open Systems Interconnect
OSPF	Open Shortest Path First

p. ex.	par exemple
PC	Personal Computer ou ordinateur personnel
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	Personal Identification Number, numéro d'identification personnelle
PK	Public Key
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure, infrastructure à clé publique
PKIX	IETF Working Group «Public-Key Infrastructure (X.509)»
PNG	Portable Network Graphics
PNG	Portable Network Graphics
POP3	Post Office Protocol Version 3
PS	PostScript
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
RFP	Request for Proposals
RIFF	Resource Interchange File Format
RIP	Routing Information Protocol
RMI	Remote Method Invocation
RPC	Remote Procedure Call
RSA	Système cryptographique à clé publique Rivest Shamir Adleman
RTF	Rich Text Format
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
SCSE	Loi fédérale sur les services de certification dans le domaine de la signature électronique (loi sur la signature électronique) (RS 943.03)
SCVP	Simple Certificate Validation Protocol
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	Service-Oriented Architecture
SOA	1) Service-Oriented Architecture 2) Sarbanes Oxley Act
SOAP	Simple Object Access Protocol
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Socket Layer
SVG	Scalable Vector Graphic
SW	Software ou logiciel
sym.	symétrique
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
UE	Union européenne
UML	Unified Modeling Language
UMTS	Universal Mobile Telecommunication System
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USIC	Unité de stratégie informatique de la Confédération (ISB en allemand)
UTF	Unicode Transformation Format

v.	Version
VML	Vector Markup Language
VPN	Virtual Private Networks
VxD	Virtual Device Driver
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 (www.ws-i.org)
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
XSL	Extensible Stylesheet Language
XSL-FO	XSL Formatting Objects
XSLT	Extensible Stylesheet Language Transformation
ZIP	Zigzag Inline Package

Appendice D – Glossaire

Le glossaire ci-dessous se réfère d'une part au site internet de l'«Institut für Wirtschaft und Verwaltung» (www.iwv.ch) 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.
API	Application Programming Interface est un logiciel interface spécifique qui définit p. ex. le choix, la forme et le contenu des paramètres à entrer dans une application.
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 l'identité, définition au chapitre 8.2 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 digital	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.
Clé de session (Session Key)	Clé temporaire, symétrique et définie par deux ou plusieurs participants pour la durée d'une liaison de communication.
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.
Confidentialité	Service de sécurité pour la préservation de secrets ou d'informations privées, définition au chapitre 8.2 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.
Cyberadministration (eGovernment)	Par cyberadministration, on entend le recours à des moyens électroniques interactifs pour assurer la communication à l'intérieur des organes étatiques ainsi qu'entre l'Etat et différents groupes d'intéressés et permettant également à tous les protagonistes impliqués d'intervenir et de participer au débat démocratique.
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 8.2 Objectifs de protection

DMZ	Abréviation de «Demilitarised Zone»; zone démilitarisée utilisée dans la sécurité IT 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-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.
Entité	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).
FIPS	Federal (USA) Information Processing Standards, pour les normes relevant de l'organisation de normalisation NIST.
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)	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.). Terme spécifique à l'USIC 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	International Data Encryption Algorithm, est un algorithme de codage symétrique utilisant une clef de 128 bits. Il a été mis au point au début des années 90 par X. Lai et J. Massey.
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 8.2 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.
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; comité de normalisation national américain. (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 Standard (norme publiée par 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.
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 oeuvre 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).
Signature électronique	voir signature numérique
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. PK Verfahren). La valeur hash du fichier est chiffrée avec la clé privée. Le résultat qui en sort est désigné comme signature numérique.
Smart card (carte intelligente)	Élément de plastique standard dans lequel est intégré un microprocesseur qui exécute notamment des opérations cryptographiques.
SOAP	Simple Object Access Protocol; 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).
Transaction administrative virtuelle	La transaction administrative virtuelle explique comment des affaires officielles peuvent être réglées à l'aide des technologies de l'information et de la communication (TIC).
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)	Processus assisté 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 cf. chapitre 6.8.1, page 33.
WSDL	Web Service Description Language: description standard des services web émanant du comité W3C (www.w3C.org)
WS-I	Web Services Interoperability Organization: comité de normalisation qui cherche à obtenir l'interopérabilité des services Web. (www.ws-i.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 plate-formes utilisées.
XML	eXtensible Markup Language: version simplifiée du Standard Generalized Markup Language (SGML). Son développement à commencé en 1996 et depuis février 1998, XML est une norme W3C. XML offre de nombreux mécanismes qui, entre autres, facilitent l'échange de données dans le réseau.