Les exigences aux niveaux **organisationnel** et **informatique** à retenir pour effectuer des échanges électroniques sécurisés dans une Administration publique

Séminaire EURORAI de Séville du vendredi 27 octobre 2017

Jean-Claude Locatelli
Réviseur informatique à l'Inspection des finances du Canton du Valais (CH)

CANTON DU VALAIS
KANTON WALLIS

Plan de la présentation

1. Echanges de données électroniques
2. Catégories de flux d'échanges de données informatisées (EDI)

   2.1 Exemple Audit sur les Mesures Administratives et Sanctions Pénales (MASP)

   2.2 Exemple Audit sur la Base de Données Référentielles (BDR)
3. Exigences dans les Administrations publiques pour faire de l'EDI
4. Conclusion

1. Echanges de données électroniques

L'Échange de Données Informatisées (EDI) ou échange de données électroniques est le terme générique définissant un échange d'informations automatique entre deux entités à l'aide de messages standardisés, de machine à machine.

L'EDI a été conçu à l'origine dans l'optique du « zéro papier » et afin d'automatiser le traitement de l'information : disposer rapidement d'une information exhaustive et fiable.

Dans la pratique, l'EDI permet de réduire notablement les interventions humaines dans le traitement de l'information.

2. Catégories de flux EDI dans les Administrations publiques (1)

Flux interne

Les EDI à l'intérieur des Administrations publiques peuvent s'effectuer soit selon un flux horizontal ou soit selon un flux vertical.

Les EDI horizontaux correspondent à des EDI à l'intérieur d'une même Administration publique entre différents métiers (Exemple 1) ou entre des Administrations publiques de même niveau hiérarchique (Exemple 2).

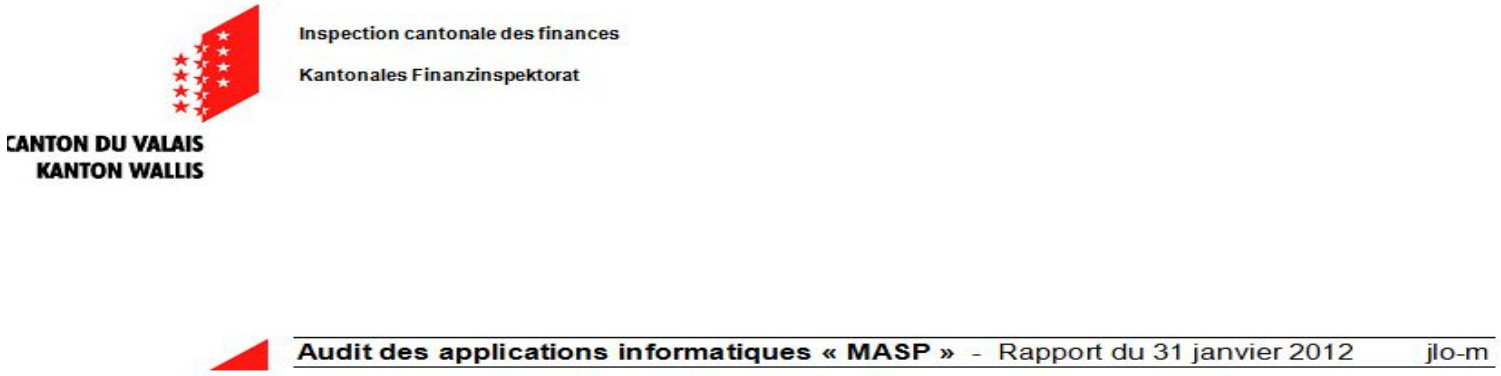
Les EDI verticaux correspondent à des EDI entre des Administrations publiques de niveau hiérarchique différent. En Suisse, l'Autorité gouvernementale (Confédération) a imposé aux autorités territoriales (Cantons) et aux autorités régionales (Communes) d'utiliser le canal Sedex pour effectuer les EDI entre eux (Exemple 3).

2. Catégories de flux EDI dans les Administrations publiques (2)

Exemple 1 : une contravention routière avec un retrait du permis de circulation nécessite une transmission électronique du dossier entre la Police et le Service de la circulation routière qui délivre la sanction administrative et entre la Police et la Justice qui délivre la sanction pénale. **Pour pouvoir réaliser l'EDI, il est nécessaire de définir des identifiants communs ou un registre commun.**

Exemple 2 : L'exemple 1 avec le lieu de l'infraction dans un état (canton) autre que celui du domicile nécessite une transmission électronique du dossier administratif entre les Polices de l'Etat du lieu de l'infraction à celui du lieu de domicile pour établir la sanction administrative. Par contre, la sanction pénale est établie dans l'Etat où l'infraction a été commise.

2.1 Exemple Audit MASP (1)



CANTON DU VALAIS
KANTON WALLIS

Inspection cantonale des finances

Kantonales Finanzinspektorat

Audit des applications informatiques « MASP » - Rapport du 31 janvier 2012 jlo-m

Audit

des applications informatiques en relation

avec les mesures administratives et les sanctions

liées à la circulation routière à l'Etat du Valais

2.1 Exemple Audit MASP (2)

Constats

1. la Police, le Service de la circulation routière et le Ministère public ont saisi les données de la personne avec leurs propres règles de gestion

2. la Police, le Service de la circulation routière et le Ministère public ont tous créé un dossier avec leur propre numérotation

3. pas d'identifiant commun pour effectuer la liaison entre les dossiers des différentes entités

⇒ La reconstitution du dossier par rapport à un événement n'était plus possible

⇒ L'attachement des factures comme celle de la prise de sang ou celle de l'interprète arrivées après la survenance de l'événement à la Police à un dossier de sanction pénale était difficile voire dans certains cas plus possible

2.1 Exemple Audit MASP (3)

Principales recommandations

1. Les données personnelles du contrevenant se trouvant dans la base de **données référentielles** doivent être présentes dans les trois applications pour pouvoir faire le lien avec les personnes

2. Le numéro de dossier de la Police doit être repris dans l'application du Service de la circulation routière et dans celui du Ministère public

2.1 Exemple Audit MASP (4)

<u>Effets du rapport d'audit de l'Inspection des finances du Canton du Valais sur les MASP</u>

Ce rapport a permis de faire prendre conscience aux différentes entités (Police, Service de la circulation routière et Ministère public) de :

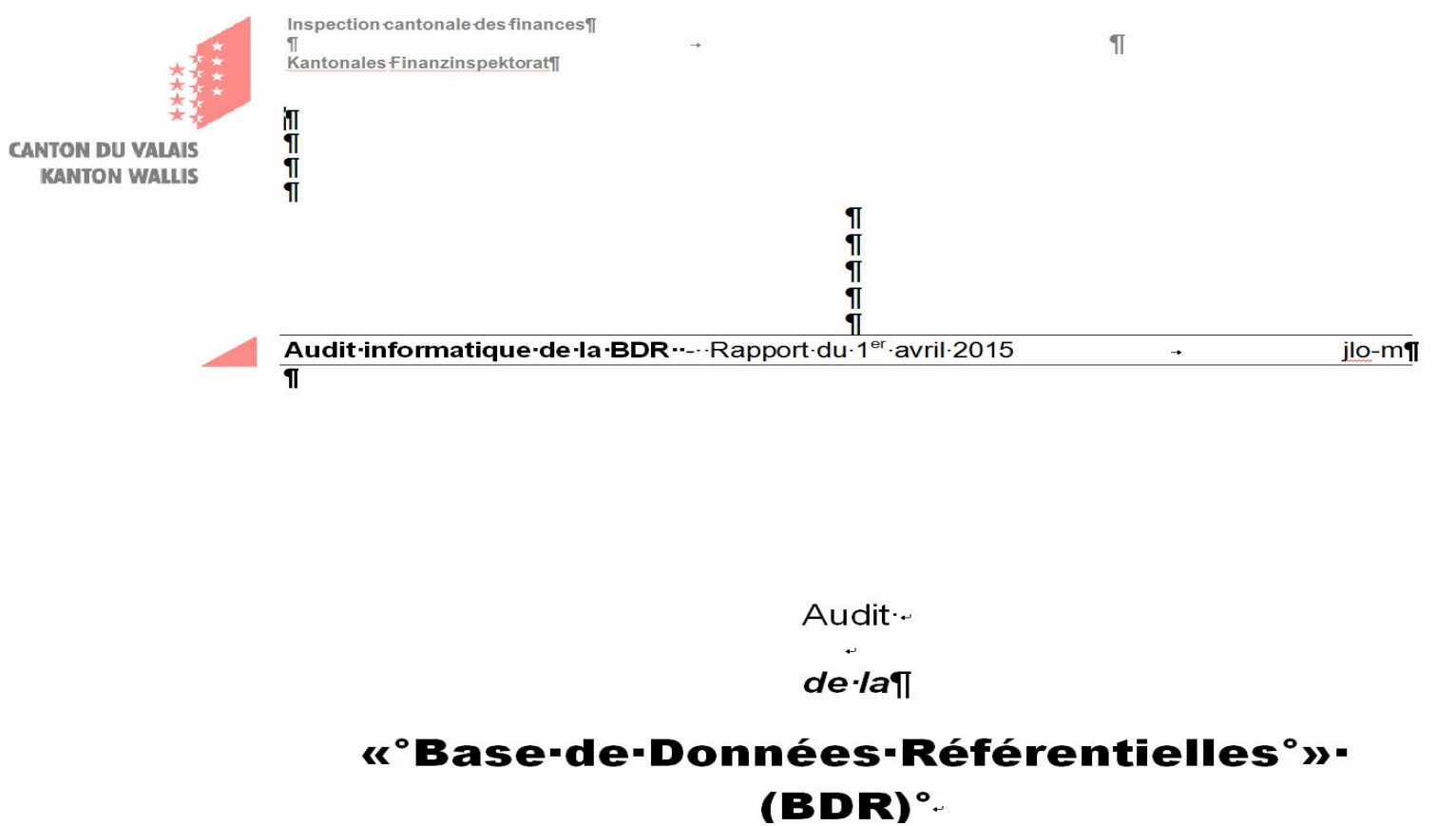
1. la nécessité de collaborer, de partager l'information

2. un gain de productivité au niveau du temps de travail que cela amène de ne plus travailler en silo

2. Catégories de flux EDI dans les Administrations publiques (3)

Exemple 3 : L'enregistrement des citoyens en Suisse s'effectue dans les applications régionales (communes) et la transmission des données à l'Autorité gouvernementale (Confédération) pour le recensement de la population s'effectue via le canal Sedex. L'autorité territoriale (canton) exerce le rôle de contrôleur de la qualité des données transmises par les autorités régionales (communes).

2.2 Exemple Audit BDR (1)



CANTON DU VALAIS
KANTON WALLIS

Inspection cantonale des finances
Kantonales Finanzinspektorat

Audit informatique de la BDR – Rapport du 1er avril 2015 – jlo-m

Audit

de la

« Base de Données Référentielles » (BDR)

2.2 Exemple Audit BDR (2)

Constats

1. L'absence d'une directive cantonale concernant la transmission des données des habitants à l'intention des communes a donné lieu à des erreurs de transmission de données qui dépendaient du fournisseur informatique des communes

2. Les communes enregistraient le départ d'un habitant vers une autre commune, mais celles-ci ne communiquaient pas le déménagement à la nouvelle commune. De ce fait, les habitants qui ne s'annonçaient pas au registre des habitants de la nouvelle commune disparaissaient des registres

3. La saisie des données dans les applications communales n'était pas assez sécurisée et permettait des erreurs du fait de l'absence de tests de plausibilité lors de la saisie

2.2 Exemple Audit BDR (3)

Principales recommandations

1. Etablir une directive pour les communes et leurs fournisseurs informatiques avec le but de sécuriser la saisie des données

2. Mettre en place des règles de gestion afin d'améliorer la concordance des données dans le cadre d'un déménagement dans une autre commune

3. Proposer aux communes de moderniser leurs applications en les orientant processus et en intégrant des contrôles

4. **Etablir une loi informatique au niveau des Administrations publiques pour définir les rôles, les responsabilités et les contrôles à mettre en place dans le cadre des EDI entre deux Administrations publiques**

2.2 Exemple Audit BDR (4)

<u>Effets du rapport d'audit de l'Inspection des finances du Canton du Valais sur les MASP</u>

Ce rapport a permis de faire prendre conscience à notre Gouvernement de l'importance du projet BDR pour notre Administration publique, de la nécessité de :

1. créer un groupe de travail regroupant des compétences de plusieurs métiers pour débloquer le projet BDR qui stagnait

2. établir une loi et une ordonnance cantonale pour déterminer les registres sources et les registres esclaves et pour en définir le fonctionnement

2. Catégories de flux EDI dans les Administrations publiques (4)

Flux externe

Les EDI externes correspondent aux EDI avec les différents partenaires des Administrations publiques (citoyens, entreprises privées, etc.).

L'objectif est de mettre en place une plateforme e-Governance à moyen et long terme sur laquelle le partenaire de l'Administration publique pourra :

- accéder à la plateforme de l'Administration publique par le biais d'une authentification forte.
  Exemple 4 : Le Canton du Valais a mis en place un **portail sécurisé (IAM)** pour permettre au citoyen de communiquer des données au canton de manière électronique. Chaque demande est contrôlée par la Chancellerie qui délivre un accès au portail sécurisé de l'Etat du Valais par lettre recommandée.

  Un audit de sécurité mise à notre disposition par le Service cantonal informatique a été réalisé avant la mise en production du portail IAM et a permis de corriger les différentes failles détectées

2. Catégories de flux EDI dans les Administrations publiques (5)

Flux externe (suite)

- accéder uniquement aux modules de l'Administration publique pour laquelle une relation existe

  Exemple 5 : Les fiduciaires peuvent accéder aux déclarations fiscales de leurs clients et gérer le délai des dépôts de ces dernières. Le Service cantonal des contributions définit les droits d'accès de la fiduciaire et celle-ci gère les personnes autorisées pour sa fiduciaire. Toutes les personnes autorisées de la fiduciaire doivent avoir effectué la demande d'accès au portail sécurisé de l'Etat du Valais

- déposer, consulter et obtenir des documents électroniques dans chacun des modules autorisés

- consulter l'état des comptes des modules autorisés (Projet)

3. Exigences dans les Administrations publiques pour faire de l'EDI (1)

Pour pouvoir effectuer de l'EDI, il est nécessaire de :

- maîtriser les EDI dans l'Administration publique, entre Administrations publiques et externes par le biais d'un inventaire des besoins
- établir une cartographie des applications avec les liens avec les différentes interfaces
- s'assurer de la compatibilité entre des applications émettrices et réceptrices au niveau des données et des systèmes

Dans notre Administration cantonale valaisanne, ces mesures sont présentes dans la stratégie informatique 2015-2025 et sont en cours d'élaboration par le groupe de travail de la stratégie de la production

3. Exigences dans les Administrations publiques pour faire de l'EDI (2)

Pour pouvoir effectuer de l'EDI, il est nécessaire de :

- définir les référentiels de données communes et le processus de mise à jour (maître – esclave) surtout au niveau des registres
- sécuriser la saisie des données référentielles dans les applications maîtres par le biais d'une saisie par processus et en y ajoutant des tests de contrôle pour empêcher les doublons et la saisie de données incomplètes ou erronées
- effectuer un nettoyage des données communes « esclave » par les « maîtres »
- définir des normes de qualité de données à atteindre
- définir les données (à anonymiser et à crypter) et les accès à faire valider par le préposé à la protection des données

Ces mesures ont été définies dans le cadre de la mise en place de la BDR du Canton du Valais suite au rapport de l'Inspection des finances

3. Exigences dans les Administrations publiques pour faire de l'EDI (3)

Pour pouvoir effectuer de l'EDI, il est nécessaire de (suite) :

- définir des normes communes pour pouvoir transférer les données de manière informatisée entre les Administrations publiques. Au niveau fédéral, des normes e-CH ont été fixées

- canaliser toutes les demandes de développements informatiques et veiller que celles-ci soient en adéquation avec l'architecture existante et avec l'architecture cible. Cette mesure a donné lieu à une décision du Conseil d'Etat obligeant les services de l'Etat d'adresser la demande d'informatisation au groupe de travail chargé de la stratégie informatique pour validation

3. Exigences dans les Administrations publiques pour faire de l'EDI (4)

Pour pouvoir effectuer de l'EDI, il est nécessaire de (suite) :

- établir les différents scénarii d'accès au portail e-Governance
- mettre en place une politique sécuritaire d'authentification
- moderniser les applications en les orientant processus et en y intégrant des contrôles et remplacer les systèmes obsolescents

4. Conclusion

En résumé, toutes ces mesures proposées pour mettre en place des EDI sécurisés dans les Administrations publiques ne peuvent se faire que par le biais de l'élaboration :

- d'une stratégie informatique avec son organisation et un plan directeur
- d'une politique d'e-Governance avec la définition des normes de traçabilité des données, de sécurité et d'authentification
- d'une loi informatique pour définir les rôles, les responsabilités et les contrôles des EDI

Ces mesures doivent être également accompagnées d'une réorganisation de celles-ci orientée processus en lieu et place d'une organisation hiérarchique par métier

MERCI DE VOTRE ATTENTION