# **Organisational** and **IT** requirements to be met for secure electronic transmissions in a civil service

Presentation of 27th of October 2017, EURORAI Seville

*Jean-Claude Locatelli*
*IT Auditor at the Audit Office of the Canton of Valais (CH)*

CANTON DU VALAIS
KANTON WALLIS

# Presentation contents

1. Electronic data interchange (EDI)
2. Categories of EDI flows

2.1 Example: audit of administrative measures and criminal sanctions (AMCS)

2.2 Example: audit of reference database (RDB)

3. Civil service requirements for EDI
4. Conclusion

# 1. Electronic data interchange

**Electronic data interchange (EDI)** is the generic term which defines an automatic exchange of information between two entities using standardised messages, from machine to machine.

EDI was originally conceived with the aim of being “paperless” and to automate information processing – rapid availability of complete, dependable information.

In practice, EDI helps to reduce human intervention in information processing, in particular.

# 2. Categories of EDI flows in civil services (1)

Internal flow

Internal EDI flows in civil services may be horizontal or vertical.

Horizontal EDIs correspond to EDIs between departments within the same civil service (Example 1) or between civil services on the same hierarchical level (Example 2).

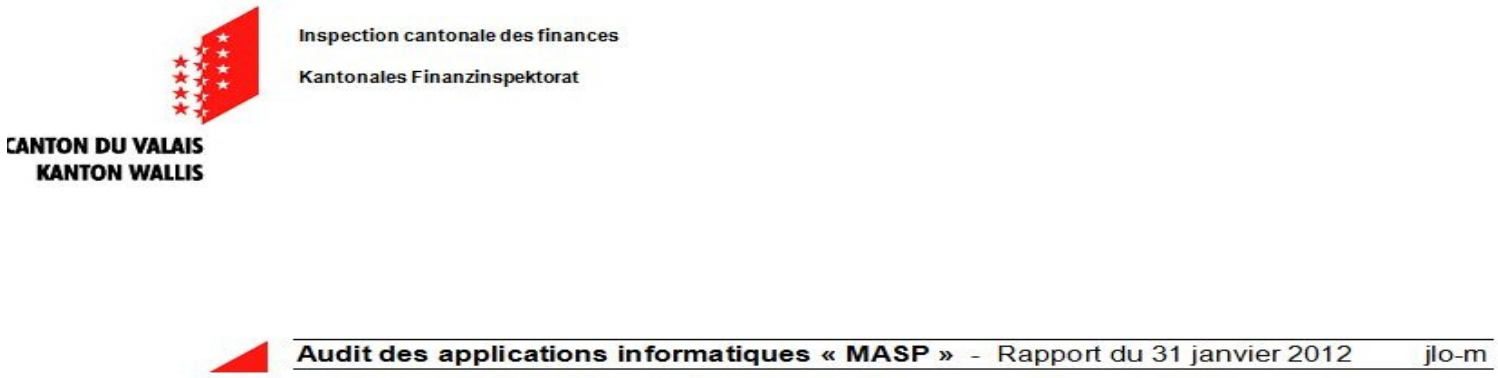
Vertical EDIs correspond to EDIs between civil services on different hierarchical levels. In Switzerland, the Confederation has ordered that regional authorities (cantons) and local authorities (municipalities) use Sedex for EDIs between one another (Example 3).

# 2. Categories of EDI flows in civil services (2)

Example 1: In case of a traffic offence which entails the withdrawal of a vehicle registration certificate, the file has to be transmitted electronically between the police and the road traffic department which imposes the administrative fine, and between the police and the courts which impose the criminal sanction. **For the purposes of EDI, it is necessary to define the common identifiers, or a common register.**

Example 2: Example 1, with the place where the offence was committed being in a canton other than that of the offender's domicile, requires electronic transmission of the administrative file between the police of the canton where the offence was committed and the police of the place of domicile, in order for the administrative fine to be issued. The criminal sanction, on the other hand, is issued in the canton where the offence was committed.

# 2.1 Example of AMCS audit (1)



# 2.1 Example of AMCS audit (2)

Findings

1. The police, the road traffic department and the public prosecutor have recorded the data of the person according to their own administrative rules.

2. The police, the road traffic department and the public prosecutor have all created a file with their own numbering.

3. No common identifier to make the link between the different entities' files.

⇒It was no longer possible to connect the file to an event.

⇒ It was difficult, in some cases even impossible, to link invoices, for instance for taking blood or for an interpreter, which are sent to the police after the incident, to a criminal offence file.

# 2.1 Example of AMCS audit (3)

Main recommendations

1. The offenders' personal data which are in the reference database must appear in the three applications in order to establish the link to the respective persons.

2. The police file number must be included in the road traffic department's and the public prosecutor's applications.

# 2.1 Example of AMCS audit (4)

Results of the audit report on AMCS by the Canton of Valais Inspectorate of Finances

Based on this report, the various entities (police, road traffic department and public prosecutor) were made aware of:

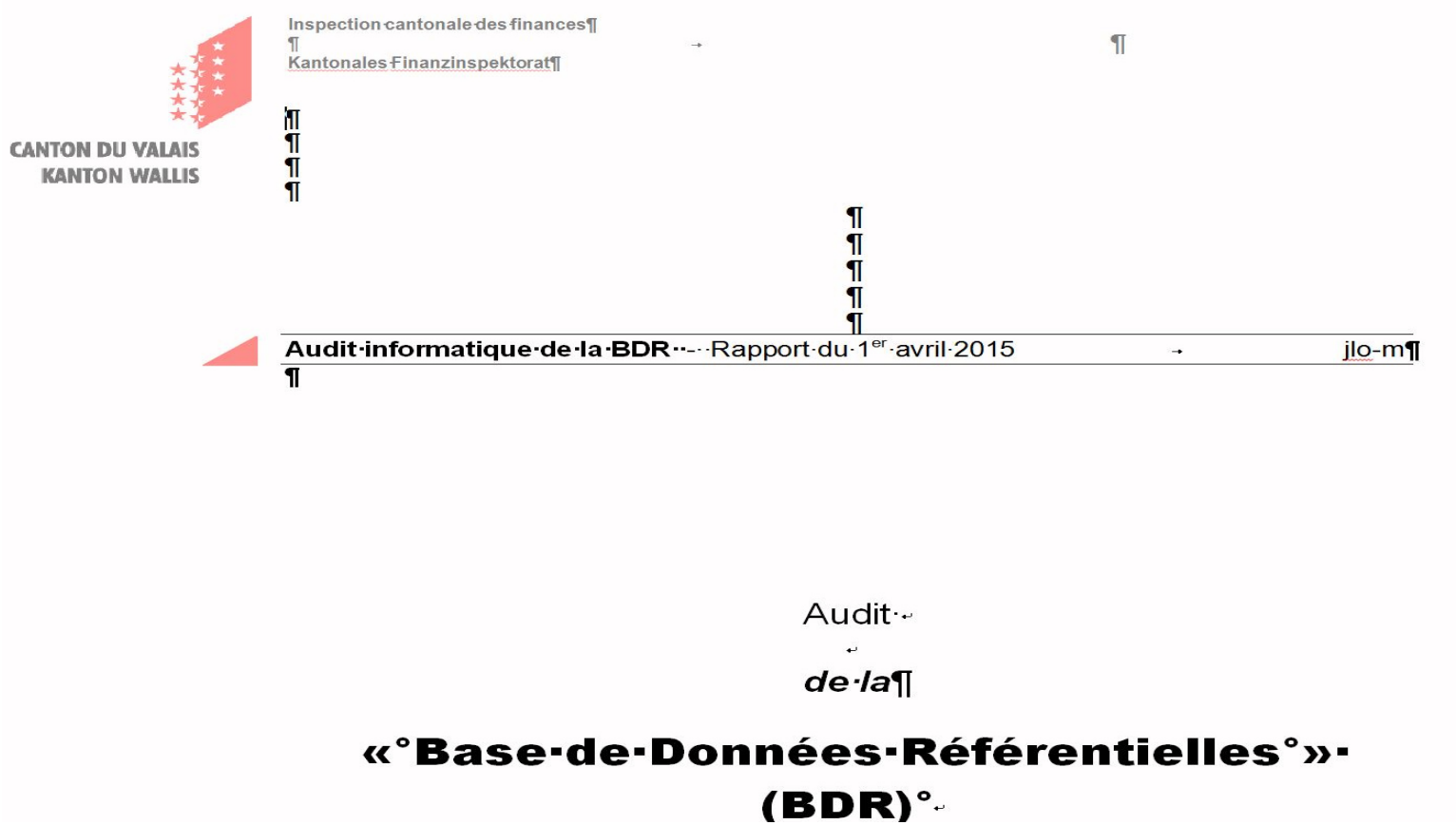
1. The need to collaborate and share information.

2. An increase in productivity in terms of working time, which should put an end to non-collaborative working.

# 2. Categories of EDI flows in civil services (3)

Example 3: In Switzerland, citizens are registered using local applications (municipalities), and for the population census, the data are transmitted to the national government (Confederation) via Sedex. The regional authorities (cantons) monitor the quality of the data transmitted by the local authorities (municipalities).

# 2.2 Example of RDB audit (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 Example of RDB audit (2)

Findings

1. The lack of a cantonal directive for municipalities regarding transmission of residents' data has given rise to data transmission errors which stemmed from the municipalities' IT supplier.

2. The municipalities registered when a resident moved to another municipality, but they didn't notify the new municipality of the move. As a result, residents who didn't register as a resident in the new municipality disappeared from the registers.

3. Data capture in local applications was not secure enough as errors occurred due to the absence of plausibility tests during capture.

# 2.2 Example of RDB audit (3)

Main recommendations

1. Draw up a directive for municipalities and their IT suppliers with the aim of making data capture more secure.

2. Implement administrative rules in order to improve data concordance when residents move to another municipality.

3. Suggest that the municipalities modernise their applications in terms of process orientation and incorporating controls.

**4. Draw up an IT law at civil service level to define roles, responsibilities and controls to be implemented as part of EDI between two civil service departments.**

# 2.2 Example of RDB audit (4)

Results of the audit report on AMCS by the Canton of Valais Inspectorate of Finances

Based on this report, our government became aware of the importance the RDB project has for our civil service and the need to:

1. Set up a working group that brings together expertise from several departments, to get the stagnating RDB project moving again.

2. Draw up a cantonal law and ordinance to determine the source and slave registers and to define how they should function.

# 2. Categories of EDI flows in civil services (4)

External flow

External EDIs correspond to EDIs with different civil service stakeholders (citizens, private enterprises, etc.).

The aim is to implement an e-governance platform in the medium and long term on which the civil service stakeholders can:

- Access the civil service platform by means of strong authentication.

Example 4: The Canton of Valais has implemented a **secure portal (IAM)** to enable citizens to send data electronically to the canton. Each request is monitored by the Chancellery, which provides access to the Canton of Valais' secure portal by registered letter.

A security audit supplied to us by the cantonal IT service was carried out before the IAM portal was released, and made it possible to remedy the various flaws detected.

# 2. Categories of EDI flows in civil services (5)

External flow (continued)

- Access to only those civil service modules to which there is a link.

Example 5: Accountants can access their clients' tax returns and manage the date for filing them. The cantonal tax service defines the accountant's access rights and the latter manages the people authorised to act on his behalf. All the accountant's authorised staff must have requested access to the Canton of Valais' secure portal.

- File, consult and obtain electronic documents in each of the authorised modules.

- Consult the account status for the authorised modules (draft).

# 3. Civil service requirements for EDI (1)

For the purposes of EDI, it is necessary to:

- Control EDI in the civil service, between civil service departments and externally based on a list of needs.
- Draw up a map of applications with the links to the various interfaces.
- Ensure compatibility between the issuing and receiving applications at the data and system levels.

In the Canton of Valais' civil service, these measures form part of the 2015-2025 IT strategy and are in the process of being implemented by the working group responsible for the release strategy.

# 3. Civil service requirements for EDI (2)

For the purposes of EDI, it is necessary to:

- Define the frame of reference for common data and the update process (master-slave), especially at register level.
- Make the capture of reference data in master applications secure by means of a data entry process and by adding screening tests to prevent duplicates and incomplete or erroneous data capture.
- Have the “masters” clean up the common “slave” data.
- Define data quality standards to be attained.
- Define the data (to be anonymised and encrypted) and the access to be validated by the data protection officer.

These measures have been defined as part of the implementation of the Canton of Valais’ RDB following the report by the Canton of Valais Inspectorate of Finances.

# 3. Civil service requirements for EDI (3)

For the purposes of EDI, it is necessary to (continued):

- Define common standards for the electronic transfer of data between civil service departments. E-CH standards have been established at Federal level.

- Channel all requests for IT developments and ensure that they are in accordance with the existing architecture as well as the target architecture. This measure gave rise to a decision by the cantonal government requiring cantonal departments to address their requests for computerisation to the working group responsible for the IT strategy, for validation.

# 3. Civil service requirements for EDI (4)

For the purposes of EDI, it is necessary to (continued):

- Draw up different scenarios for access to the e-governance portal.
- Implement a secure authentication policy.
- Modernise applications in terms of process orientation and incorporating controls, and to replace obsolete systems.

# 4. Conclusion

To sum up, all the measures put forward for the implementation of secure EDI in civil services can only be achieved by drawing up:

- An IT strategy including its organisation and a master plan.
- An e-governance policy which defines standards regarding data traceability, security and authentication.
- An IT law to define roles, responsibilities and controls regarding EDI.

These measures must also be accompanied by a process-orientated reorganisation instead of hierarchical organisation by department.

# THANK YOU FOR YOU ATTENTION