Technicalities of voting, Belgium case.

Slide 1

My name is David Van Kerckhoven and I work for the election department of the Belgian Federal administration.

The purpose of this presentation is to give you a real example of an electronic voting system, which is used in Belgium.

Slide 2

I will talk shortly about the history and the evolution of the electronic voting in Belgium.

Thereafter I'll explain the concept of the Belgian voting system.

I'll say a few words about the security.

And finally there is a conclusion.

Slide 3

An experiment was already held in 2 municipalities in 1991.

But the first real introduction of the electronic voting was in 1994 and was extended in 1999.

This voting system was based on technologies, like a DOS-operating system, floppy drives, etc.

We continued using this system for the next elections.

Since 2012 there is a new voting system, called Smartmatic. This was used during the elections of 2012 and 2014.

The next elections will be held in 2018 and 2019, again with this voting system Smartmatic.

In 2018 there will be municipal elections, the local elections, and in 2019 we will have 3 elections: the European, the federal and the regional elections.

Slide 4

How does a polling station look like in Belgium?

We have a president and his staff, seating at the president's table.

In Belgium we have about 5 voting booths for each polling station and each voting booth contains a voting computer.

So, how does this work? The voter enters the polling station and identifies himself to the president. He gets an activated smartcard (it is like a chip card) and he goes to a voting

booth. There he can start the voting process on the voting computer with his smartcard. After he has made his choice and confirmed his vote, he gets a printed paper trail with his vote converted into a barcode and also into a clear text. When he has checked his vote, he folds his ballot and leaves the voting booth. He goes to the ballot box where he scans the barcode of his paper trail and he put his ballot in the ballot box. The scanned vote will then be encrypted and stored on the USB-stick of the polling station.

If the voter has doubts about the content of his barcode, he can go first to a special voting booth containing a bar code reader. There, he can scan himself the barcode of his ballot. The content of the barcode will be shown on a screen so he can compare it with the printed vote in clear text.

Slide 5

What happens afterwards?

In Belgium we always vote on a Sunday, starting from 8 a.m. until mostly 3 p.m.

So after 3 p.m. the president closes the polling station and goes with the USB-sticks containing all the votes to the main polling station of the canton. A canton in Belgium is a group of municipalities.

There, the USB-stick will be checked and the votes will be transmitted to the central authority, in this case the federal administration of Home Affairs. When we receive some preliminary results from the cantons, we publish them immediately on our website.

Slide 6

How can we secure the voting process?

Our security is based on 3 principles:

- IT security
- A lot of procedures
- And transparency

Slide 7

First point is the IT security.

Because of the fast technological evolutions, in each IT-project there is always a battle between the security people on one side and the hackers on the other side.

At our side we have, of course, the security people of our suppliers and from the administration itself.

But very important, we also have an independent counselling body. Before each election, they will test and verify the software and they will give an advice to us if the software can be used for elections.

And last but not least, in Belgium we have an independent college of experts. In Belgium they play an important role. This college consists of the IT-specialists of the different parliaments. During the last elections in 2014, they consisted of about 22 IT-specialists. For each election, they do a full audit and write a report. Depending on this report, the elections will be approved or disapproved.

Slide 8

Our second point concerns the procedures.

If we can prevent the hackers get physical access to the software, there will be no battle!

Some examples:

When we prepare all the USB-sticks with the software for all the polling stations, we do it in a secured area. This area is protected by access control, there are cameras to supervise, there is a guard 24h a day, etc.

When the USB-sticks are done, (before they leave the secured area) they are put in a sealed envelope and will be accompanied with a security guard on the transport to the local authorities. The president of a polling station may only open the envelope on the day of the elections and all the polling station staff must be present. The corresponding password will arrive in a separate sealed envelope.

Slide 9

The 3rd point is about the transparency.

It is very important that we explain very well to the people how the system works, but also how we work!

On our website we put a lot of documents describing and explaining the voting process. For each election, we have a helpdesk to answer the questions of the people.

And very important! After each election we do a full publication of the source code of our software.

So everyone can verify or ask a specialist to look at our software.

In addition of the confidence we earn, there is also a 2nd benefit:

We can get feedback!

And with this feedback we can improve our system again about the security elements and about our procedures.

So we can learn and do better each time.

Slide 10

In Belgium we have hold experiments with electronic voting since 1991!

Since 2012, we use a new voting system, Smartmatic.

To keep the voting process secure, there are 3 principles:

- IT security
- Procedures
- And Transparency