SJ2013021314210929

Dokumentresumé:

Bestilt af : DEPCLH den 13-02-2013 15:21:08
Dokumentnr.: 5075
Titel: Banja Luka photo2
Dokumenttype: I
Dokumentdato:
Kontor/enhed: VALG-ENH, Valgenheden
Sagsmedarb.: Nicoline Nyholm Miller, DEPNNM
Indblik:
Versionsnr.: 1
Reg.dato: 10-09-2012
Registreret af: DEPNNM - Nicoline Nyholm Miller

Emneord:

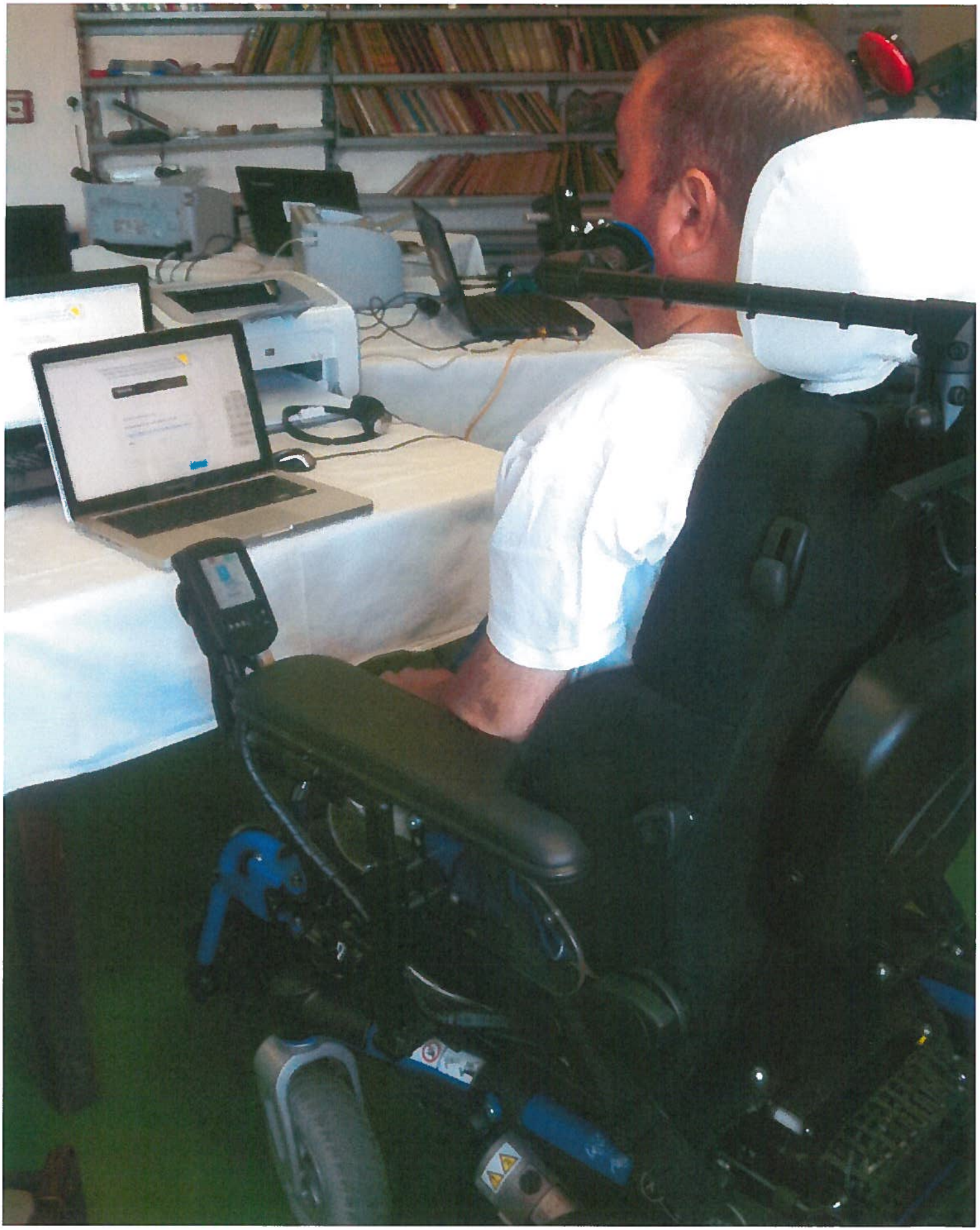
Tekst:

Modtagere:

Oplysninger:

Datoer:

Erindringer:



SJ20130213142107989

Dokumentresumé:

Bestilt af : DEPCLH den 13-02-2013 15:21:07
Dokumentnr.: 5076
Titel: Banja Luka photo1
Dokumenttype: I
Dokumentdato:
Kontor/enhed: VALG-ENH, Valgenheden
Sagsmedarb.: Nicoline Nyholm Miller, DEPNNM
Indblik:
Versionsnr.: 1
Reg.dato: 10-09-2012
Registreret af: DEPNNM - Nicoline Nyholm Miller

Emneord:

Tekst:

Modtagere:

Oplysninger:

Datoer:

Erindringer:


OMCAFÉ
CHIPSY

SJ20130213142106711

Dokumentresumé:

Bestilt af : DEPCLH den 13-02-2013 15:21:06
Dokumentnr.: 5074
Titel: FW: Bosnia--Mock Election Day two
Dokumenttype: I
Dokumentdato: 10-09-2012
Kontor/enhed: VALG-ENH, Valgenheden
Sagsmedarb.: Nicoline Nyholm Miller, DEPNNM
Indblik:
Versionsnr.: 1
Reg.dato: 10-09-2012
Registreret af: DEPNNM - Nicoline Nyholm Miller

Emneord:

Tekst:

Modtagere:
Afsender Mike Summers ,

Oplysninger:

Datoer:

Erindringer:

Christina Løtzsch Hansen

Fra: Mike Summers <mike.summers@everyonecounts.com>
Sendt: 10. september 2012 12:02
Til: Nicoline Nyholm Miller
Emne: FW: Bosnia--Mock Election Day two

Hi Nicoline,

I hope you had a great weekend ☺ I just wanted to take this opportunity to share with you some photos taken on the second day of the Mock election in BiH.

These photos were taken at a home for disabled persons in Banja Luka, Republic of Srpska. This particular, inspirational gentleman has severe Muscular Dystrophy and hence very limited limb movement. He controls his wheelchair using a Bluetooth-enabled, mouth controlled, joystick. We successfully managed to get the joystick to interface with the eLect voting solution so he could navigate the ballot and vote using controls he was familiar with. Great stuff eh?

It was as fantastic and as you can imagine pretty moving moment for us all ☺

Kindest regards,

Mike

Mike Summers
Director of Sales, Worldwide
Everyone Counts, Inc.
Tel: +44 (0) 2076177407
Mobile: +44 (0) 7585800950
Email: mike.summers@everyonecounts.com
Web: www.everyonecounts.com

SJ20130213142111320

Dokumentresumé:

Bestilt af : DEPCLH den 13-02-2013 15:21:10
Dokumentnr.: 4926
Titel: BijlageD_N
Dokumenttype: I
Dokumentdato:
Kontor/enhed: VALG-ENH, Valgenheden
Sagsmedarb.: Nicoline Nyholm Miller, DEPNNM
Indblik:
Versionsnr.: 1
Reg.dato: 10-09-2012
Registreret af: DEPNNM - Nicoline Nyholm Miller

Emneord:

Tekst:

Modtagere:

Oplysninger:

Datoer:

Erindringer:

Bijlage D - Organisatorische bepalingen

***NB:** De hierna organisatorische bepalingen hebben betrekking op de verkiezingssituatie van kracht op de dag van de publicatie van het lastenboek RRN n°3/2008 en voorspellen in geen enkel opzicht latere wijzigingen die zich zouden kunnen voordoen.*

1.1 Inleiding

a. De Federale Overheidsdienst (FOD) Binnenlandse Zaken staat in voor de organisatie van de verkiezingen van de federale Wetgevende Kamers of het federale Parlement, zijnde de Kamer van Volksvertegenwoordigers en de Senaat. Het federale Parlement wordt verkozen voor een termijn van 4 jaar. Het federale Parlement kan steeds vroegtijdig worden ontbonden en dan moeten, vanaf de ontbinding, verkiezingen worden georganiseerd binnen 40 dagen. De verkiezingen van de Kamer van de Senaat worden steeds op dezelfde dag gehouden.

   De laatste verkiezingen van het federale Parlement zijn gehouden op zondag 10 juni 2007. De volgende verkiezingen voor Kamer en Senaat zijn normaal gepland op zondag 17 juli 2011, indien er geen vroegtijdige ontbinding is. De toekomstige verkiezingen voor het federale Parlement zijn dus op normale datum in 2011, 2015, 2019 enz...

   N.B. Na een verkiezing bij vroegtijdige ontbinding van het federale Parlement start een nieuwe volledige termijn van 4 jaar.

   Op de website verkiezingen www.verkiezingen.fgov.be vindt U alle nuttige informaties en documenten over de laatste verkiezingen van het federale Parlement (10 juni 2007), zijnde: de toepasselijke wetgeving, de reglementering, de onderrichtingen, de formulieren, de verkiezingsagenda, de demonstratie van de software voor de inzameling van de kandidatenlijsten en van de verkiezingsresultaten, de toelichtingen over de digitale inzameling van de resultaten, de kandidatenlijsten van de verkiezingen 2007, de toelichtingen over de weergave van het letterwoord of logo en de links naar andere interessante sites, waaronder naar de resultaten op het federaal portaal (www.belgium.be).

b. De FOD Binnenlandse Zaken staat eveneens in voor de organisatie van de verkiezingen van het Europese Parlement en van de Gewest- en Gemeenschapsparlementen (sinds een recente Grondwetswijziging worden de Gewest- en Gemeenschapsraden voortaan Gewest- en Gemeenschapsparlementen genoemd).
   Deze verkiezingen houden dus de stemming in van de Belgische leden voor het Europees Parlement en van de leden voor de diverse regionale Parlementen, zijnde : het Vlaams Parlement, het Waals Gewestparlement, het Brussels Hoofdstedelijk Parlement en het Parlement van de Duitstalige Gemeenschap.
   Deze verkiezingen worden steeds op een vaste datum gehouden voor een termijn van 5 jaar. Deze parlementen kunnen niet vroegtijdig worden ontbonden.

   De laatste verkiezingen voor deze Parlementen zijn gehouden op zondag 13 juni 2004. De toekomstige verkiezingen zijn gepland in juni 2009, in juni 2014, in juni 2019 enz...

Op onze website verkiezingen : www.verkiezingen.fgov.be vindt U alle nuttige informaties en documenten over de laatste verkiezingen terzake (13 juni 2004).

Opmerking :
Ingevolge de zogenaamde "Lambermontakkoorden" uit 2001 is de volledige provinciale en gemeentelijke wetgeving, op enkele uitzonderingen na, overgeheveld van de federale Staat naar de drie Gewesten (Vlaams Gewest, Waals Gewest en Brussels Hoofdstedelijk Gewest). Deze overheveling is geregeld bij de bijzondere wet van 13 juli 2001 houdende overdracht van diverse bevoegdheden aan de Gewesten en Gemeenschappen (Belgisch Staatsblad van 3 augustus 2001).

Hieruit volgt dat vanaf de komende provincie- en gemeenteraadsverkiezingen op zondag 8 oktober 2006, elk van de drie Gewesten uitsluitend bevoegd zijn voor de wetgeving ("decreten" in het Vlaamse Gewest en het Waalse Gewest en "ordonnanties" in het Brussels Hoofdstedelijke Gewest), de reglementering en de organisatie van de provincie- en gemeenteraadsverkiezingen. Deze verkiezingen worden om de 6 jaar georganiseerd.

1.2 De organisatie van de verkiezingen van de federale Wetgevende Kamers

FEDERALE STAAT

Kamer	**Senaat**		
150 rechtstreeks verkozenen	25 Nederlandstaligen 15 Franstaligen	10 Nederlandstaligen 10 Franstaligen 1 Duitstalige	6 Nederlandstaligen 4 Franstaligen
	40 rechtstreeks verkozenen	21 afgevaardigden (1)	10 gecoöpteerden (2)
	Totaal 71 leden (3)		

(1) Komen respectievelijk uit het Vlaams parlement, het Frans Gemeenschapsparlement en het Duitstalig Gemeenschapsparlment.

(2) - De Nederlandstalige gecoöpteerden worden aangewezen door de Nederlandstalige senatoren, die rechtstreeks zijn verkozen of zijn afgevaardigd.
- De Franstalige gecoöpteerden worden aangewezen door de Franstalige senatoren, die rechtstreeks zijn verkozen of zijn afgevaardigd.

(3) Er zijn nog 3 senatoren van rechtswege, met name de kinderen van de Koning : Prins Filip, Prinses Astrid en Prins Laurent.

N.B.: sinds 2006 worden ingevolge Grondwets- en wetsaanpassingen de regionale "Raden" voortaan "Parlementen" genoemd.

a. Samenstelling van de Kamer van Volksvertegenwoordigers

1° De Kamer van Volksvertegenwoordigers telt 150 rechtstreeks verkozen leden (Art. 63 Grondwet).
De zetels worden verdeeld over de kieskringen volgens de bevolkingscijfers. Elke kieskring telt zoveel keer een zetel als de federale deler in het cijfer van de bevolking van de kieskring begrepen is. De federale deler wordt verkregen door het bevolkingscijfer van het Rijk te delen door 150. De overblijvende zetels worden toegewezen aan de kieskringen met het grootste nog niet vertegenwoordigde bevolkingsoverschot.
Een kieskring bestaat uit één of meer administratieve arrondissementen. Voor de verkiezing van de Kamer van Volksvertegenwoordigers zijn er 11 kieskringen. De kieskringen vallen voortaan samen met de provinciegrenzen, behalve voor de kieskringen Leuven en Brussel-Halle-Vilvoorde.
Het cijfer van de bevolking van elke kieskring wordt om de 10 jaar vastgesteld door een volkstelling. De Koning maakt binnen de zes maanden de uitslag ervan bekend. De laatste volkstelling was op 1 oktober 2001 en de resultaten ervan werden in het Belgisch Staatsblad bekendgemaakt op 28 mei 2002. Na die bekendmaking bepaalt de Koning het aantal zetels dat aan elke kieskring toekomt.

2°De verdeling van de leden van de Kamer van Volksvertegenwoordigers over de kieskringen is als volgt :

De 11 kieskringen van de Kamer van Volksvertegenwoordigers			
Nieuwe Provinciale Kieskringen	**Aantal te kiezen leden – kandidaten**	**Aantal kandidaat-opvolgers**	**Hoofdbureau van de Kieskring**
Antwerpen	24	13	Antwerpen
Limburg	12	7	Hasselt
Oost-Vlaanderen	20	11	Gent
West-Vlaanderen	16	9	Brugge
Kieskring Leuven (Vlaams-Brabant) Kieskring B-H-V Waals-Brabant	 7 22 5	 6 12 6	 Leuven Brussel Nijvel
Henegouwen	19	11	Bergen
Luik	15	9	Luik

Luxemburg	4	6	Aarlen
Namen	6	6	Namen
TOTAAL	**150**		

N.B.

- De kandidatenlijsten moeten worden ingediend bij de kieskringhoofdbureaus voor de Kamer en bij de collegehoofdbureaus voor de Senaat op de 29ste dag (tussen 14 en 16 uur) of 28ste dag (tussen 9 en 12 uur) vóór de stemming.
- De voorlopige afsluiting van de kandidatenlijsten in ieder hoofdbureau geschiedt op de 27ste dag vóór de stemming.
- De definitieve afsluiting van de kandidatenlijsten in ieder hoofdbureau gebeurt op de 24ste dag vóór de stemming (ingeval van een beroep bij de rechterlijke macht is dit op de 20ste dag vóór de stemming).
- Het aantal aparte kandidaat-opvolgers bedraagt maximaal de helft van het aantal te kiezen kandidaten plus 1 (cijfers na de komma worden verhoogd naar de volgende eenheid). Er moeten minstens 6 opvolgers zijn.
- Op elk van de lijsten mag noch het verschil tussen het aantal kandidaten-titularissen van elk geslacht, noch het verschil tussen het aantal plaatsvervangende kandidaten van elk geslacht, groter zijn dan één.
  Noch de eerste twee kandidaat-titularissen, noch de eerste twee plaatsvervangende kandidaten van elk van de lijsten mogen van hetzelfde geslacht zijn.

b. Samenstelling van de Senaat

1° De rechtstreeks verkozen senatoren (Art. 67 Grondwet).

De 2 kiescolleges van de Senaat			
Kiescollege	**3 Kieskringen**	**Hoofdbureau van het College**	**Aantal te kiezen leden**
Nederlandstalig	• Vlaams-Gewest (min arr. Halle-Vilvoorde) • Kieskring Brussel-Halle-Vilvoorde	Mechelen	25 (14 opvolgers)
Franstalig	• Waals Gewest • Kieskring Brussel-Halle-Vilvoorde	Namen	15 (9 opvolgers)
		TOTAAL	**40**

De senaat telt 40 rechtstreeks verkozen senatoren :
- 25 senatoren rechtstreeks verkozen door het Nederlandstalig kiescollege
- 15 senatoren rechtstreeks verkozen door het Frans kiescollege

De Vlaamse kieskring omvat het grondgebied van het Vlaamse Gewest, met uitzondering van het administratief arrondissement Halle-Vilvoorde. Daar moeten de stemgerechtigde inwoners van de kieskring Brussel-Halle-Vilvoorde, die hun stem uitbrengen op een lijst die bij het Nederlandse kiescollege is ingediend, worden bijgeteld.
De Waalse kieskring omvat het grondgebied van het Waalse Gewest. Daar moeten de stemgerechtigde inwoners van de kieskring Brussel-Halle-Vilvoorde, die hun stem uitbrengen op een lijst die bij het Franse kiescollege is ingediend, worden bijgeteld.

2° De gemeenschapssenatoren (Art. 67 Grondwet).

Er worden 21 senatoren aangewezen vanuit de regionale Parlementen :

- 10 aangewezen door en uit het Vlaams Parlement
- 10 aangewezen door en uit het Frans Gemeenschapsparlement
- 1 aangewezen door en uit het Duitstalig Gemeenschapsparlement

3° De gecoöpteerde senatoren (Art. 67 Grondwet).

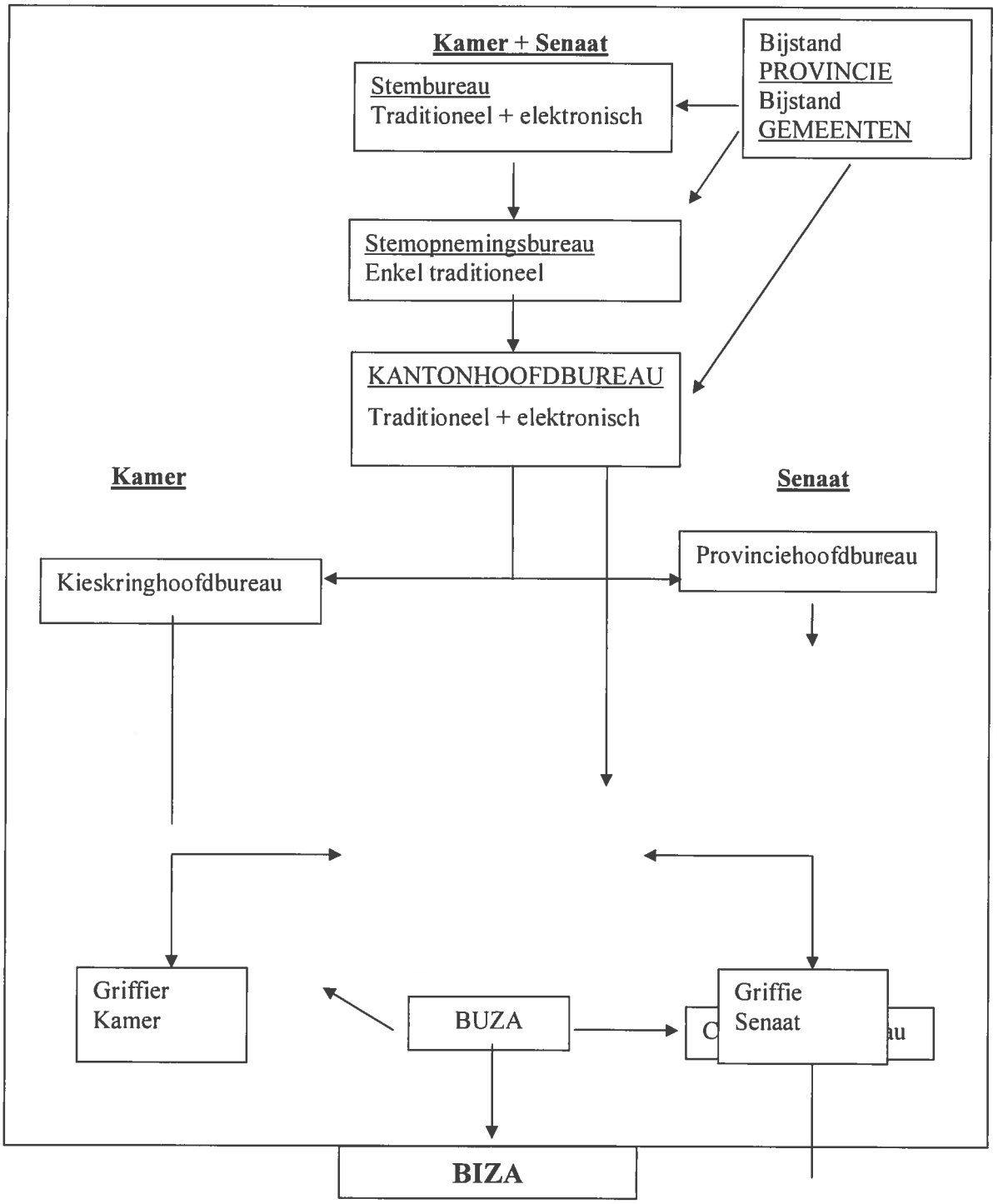
10 senatoren worden aangewezen door de rechtsreeks verkozen senatoren en door de gemeenschapssenatoren. Het gaat hier om een getrapte verkiezing met evenredige vertegenwoordiging. De verdeling is als volgt:

- 6 senatoren worden aangewezen door de 25 rechtstreeks verkozen senatoren van het Nederlandse kiescollege en de 10 Vlaamse Gemeenschapssenatoren
- 4 senatoren worden aangewezen door de 15 rechtstreeks verkozen senatoren van het Franse kiescollege en de 10 Franse Gemeenschapssenatoren.

4° Senatoren van rechtswege (Art.72 Grondwet).

De kinderen van de Koning of, indien er geen zijn, de Belgische nakomelingen van de tot regeren gerechtigde tak van de koninklijke familie, zijn van rechtswege senator wanneer zij de leeftijd van 18 jaar hebben bereikt, voor zover zij de eed van senator hebben afgelegd. Zij zijn pas stemgerechtigd vanaf 21 jaar (hoewel zij dit recht in de praktijk niet uitoefenen) en worden niet meegerekend bij het bepalen van het aanwezigheidsquorum. Momenteel zijn Prins Filip, Prinses Astrid en Prins Laurent senator van rechtswege.

c. Schema Kiesbureaus



d. Toelichtingen bij de kiesbureaus

- Het aantal kiesbureaus en bureauleden bij de komende verkiezingen is een raming die gebaseerd is op de kieswetgeving en op de vorige verkiezingen. Het totale aantal stembureaus en stemopnemingsbureaus kan hoger zijn door een gestegen aantal kiezers in België en door de deelname van de Belgische kiezers in het buitenland.
  Het preciese aantal stem- en stemopnemingsbureaus zal gekend zijn na de opmaak van de officiële kiezerslijst op de 80ste dag vóór de stemming bij normale verkiezingen en op de 40ste dag in het geval van vervroegde verkiezingen. Er komt een gedetailleerde tabel per kieskanton met het aantal kiezers en het aantal kiesbureaus op onze website Verkiezingen (www.verkiezingen.fgov.be).

Soort kiesbureau	Aantal bureaus	Aantal effectieve bureauleden	Aantal plaatsvervangende bijzitters
Collegehoofdbureau (Senaat)	2	12	8
Kieskringhoofdbureau (Kamer)	11	66	44
Geautomatiseerde Kantonhoofdbureau	62	372	248
Traditioneel Kantonhoofdbureau	146	876	584
Geautomatiseerd Stembureau	3.850	30.800	19.250
Traditioneel Stembureau	6.700	40.200	26.800
Stemopnemingsbureau (enkel traditioneel)	4.500	27.000	18.000
TOTALEN	**15.271**	**99.336**	**64.934**

- Elk kiesbureau bestaat normaal uit 6 leden: 1 voorzitter, 1 secretaris en 4 vaste bijzitters (reserve : 4 plaatsvervangende bijzitters).
- De stembureaus zijn gemeenschappelijk bij het traditioneel en elektronisch stemmen voor de verkiezingen van de Kamer en de Senaat.
  Het geautomatiseerd stembureau regelt de elektronische stemming van de kiezers en bestaat uit 8 leden : 1 voorzitter, 1 secretaris, 1 adjunct-secretaris met kennis van informatica en 5 bijzitters.
  Het traditioneel stembureau regelt de stemming met stembiljetten voor de kiezers.
  N.B. In de geautomatiseerde stembureaus tot 800 kiezers blijven deze bureaus uit 6 leden bestaan : 1 voorzitter, 1 secretaris en 4 bijzitters.
- Er zijn aparte stemopnemingsbureaus ("telbureaus") voor de Kamer- en Senaatsverkiezingen, waar meer dan 6 Volksvertegenwoordigers worden gekozen. In alle kieskringen worden de stemopnemingsbureaus gesplitst in een bureau A (telling stembiljetten Kamer) en in een bureau B (telling stembiljetten Senaat), behalve in de

kieskringen Waals-Brabant, Luxemburg en Namen (Art. 149 Kieswetboek).
In de kieskantons met elektronische stemming zijn er geen stemopnemingsbureaus meer. De totalisatie van de stemmen van alle verkiezingen geschiedt dan onmiddellijk op het kantonhoofdbureau.

- Er is één kantonhoofdbureau voor de verkiezingen van de Kamer en Senaat.
  Van de 208 kieskantons in België zijn er 62 kieskantons met elektronische stemming en 146 kieskantons met traditionele stemming. Alle kieskantons in het Brusselse Hoofdstedelijk Gewest en in het Duitstalig kiesgebied zijn geautomatiseerd.

De 62 geautomatiseerde kieskantons :

Provincie Antwerpen : kieskantons van Antwerpen, Arendonk, Boom, Brecht, Duffel, Herentals, Hoogstraten, Kapellen, Kontich, Mechelen Mol, Puurs, Turnhout, Westerlo en Zandhoven
Provincie Limburg : kieskantons van Beringen, Genk, Hasselt, Maasmechelen, Neerpelt, Peer en Voeren
Provincie Oost-Vlaanderen : kieskantons van Dendermonde, Evergem, Kaprijke, Nevele, Sint-Niklaas, Temse, Waarschot, Zele en Zomergem
Provincie West-Vlaanderen : kieskanton van Veurne
Provincie Vlaams-Brabant : kieskantons van Asse, Glabbeek, Haacht, Leuven, Vilvoorde, Zaventem en Zoutleeuw
Administratief arrondissement van Brussel-Hoofstad : kieskantons van Anderlecht, Brussel, Elsene, Schaarbeek, Sint-Jans-Molenbeek, Sint-Gillis, Sint-Joost-Ten-Node en Ukkel
Provincie Henegouwen : kieskantons van Lens en Frasnes-lez-Anvaing
Provincie Luik : kieskantons van Luik, Wezet, Bitsingen, Fléron, Herstal, Grâce-Hollogne, Aywaille, Saint-Nicolas, Seraing, Verlaine, Eupen en Sankt-Vith
Provincie Luxemburg : kieskanton van Durbuy

- Er is een kieskringhoofdbureau voor de verkiezing van de Kamer. Bij de Kamerverkiezingen zijn er 11 kieskringen.
- Het kieskringhoofdbureau (Kamer) vervult eveneens de taken van het provinciehoofdbureau (Senaat).
  Het kieskringhoofdbureau Brussel-Halle-Vilvoorde is provinciehoofdbureau (Senaat) en provinciaal centraal bureau (Kamer-lijstenverbindingen).
  Het provinciehoofdbureau van de provincie Vlaams-Brabant is slechts bevoegd voor het administratief arrondissement Leuven.
  Sinds 2003 zijn de lijstenverbindingen ("apparentering") afgeschaft voor de Kamerverkiezingen.
  De vroegere kieskringen zijn vervangen door de provinciale kieskringen. Er is dus één lijst per politieke formatie binnen een provinciale kieskring.
  Uitzondering :
  Voor de lijsten van de kieskring Brussel-Halle-Vilvoorde en van de kieskring Leuven of van de kieskring Waals-Brabant blijven de lijstenverbindingen bestaan, respectievelijk tussen lijsten van de kieskring Leuven en de kieskring Brussel-Halle-Vilvoorde, enerzijds, en tussen lijsten van de kieskring Brussel-Halle-Vilvoorde en de kieskring Waals-Brabant, anderzijds.

- Er is een collegehoofdbureau voor de verkiezing van de Senaat te Mechelen

(Nederlands kiescollege) en te Namen (Frans kiescollege).

- De gemeenten en de provincies hebben onder meer belangrijke taken bij de organisatie en de logistiek van de kiesbureaus.
- De Federale Overheidsdienst Binnenlandse Zaken (BIZA) staat in voor de algemene organisatie van de verkiezingen.

N.B.

- Door de wet van 7 maart 2002 kan de in het buitenland verblijvende Belg kunnen stemmen voor de federale Parlementsverkiezingen en wordt hij/zij uitgenodigd om een keuze te maken uit de vijf hierna volgende wijzen van stemmen :

  1° de persoonlijke stemming in een Belgische gemeente
  2° de stemming bij volmacht in een Belgische gemeente
  3° de persoonlijke stemming in zijn Belgische diplomatieke of consulaire beroepspost waar de betrokkene is ingeschreven
  4° de stemming bij volmacht in de genoemde post
  5° de stemming per briefwisseling.

  Voor de uitoefening van dit stemrecht vervullen BUZA (FOD Buitenlandse Zaken en de diplomatieke posten) en BIZA (FOD Binnenlandse Zaken) een belangrijke rol, tezamen met de kiesbureaus en de gemeentebesturen.

- Bij de Federale Overheidsdienst Binnenlandse Zaken te Brussel is er een speciaal stemopnemingsbureau voor de telling van de stembiljetten van de Belgische kiezers in het buitenland, die gestemd hebben op een Belgische diplomatieke of consulaire beroepspost. Dit bureau bestaat uit een (algemeen) voorzitter, een (algemeen) secretaris en voor iedere kieskring van de Kamer en de Senaat uit een secretaris en 4 bijzitters (reserve : 4 plaatsvervangende bijzitters) -> Totaal aantal bureauleden : 1 algemeen voorzitter, 1 algemeen secretaris, 14 kieskringsecretarissen, 56 vaste bijzitters (+ 56 plaatsvervangende bijzitters) = 72 (+ 56). Dit speciaal stemopnemingsbureau doet ook de telling van de stembiljetten van de Belgen in het buitenland, die per briefwisseling gestemd hebben in de kieskring Brussel-Halle-Vilvoorde. Hierdoor dient het aantal telbureaus te worden verdubbeld.

e. Enkele belangrijke kiesdata

- **Donderdag.....**
  80ste dag : Opmaak van de kiezerslijst bij verkiezingen op normale datum.

- **Dinsdag .....**
  40ste dag : Opmaak van de kiezerslijst bij vervroegde verkiezingen.

- **Vrijdag .....**
  30ste dag : Ontvangst van de beschermde letterwoorden of logo's tussen 10 en 12 uur bij BIZA en trekking van de nationale volgnummers door de Minister om 12 uur.

- **Zaterdag en zondag .....**

29ste en 28ste dag : Ontvangst van de lijsten voor de controle van de dubbele kandidaturen

- **Dinsdag .....**
  26ste dag : Publicatie in het B.S. van de beschermde letterwoorden of logo's met de nationale volgnummers en mededeling ervan aan de voorzitters van de hoofdbureaus

- **Maandag .....**
  27ste dag : Voorlopige afsluiting van de kandidatenlijsten door de kieskringhoofdbureaus (Kamer) en de collegehoofdbureaus (Senaat)

- **Donderdag .....**
  24ste dag : ° Mededeling van de dubbele kandidaturen aan de voorzitters van de hoofdbureaus
  ° Definitieve afsluiting van de kandidaturen door de kieskringhoofdbureaus (Kamer) en collegehoofdbureaus (Senaat) ublicatie in het B.S. van de nationale nummers

- **Maandag.....**
  20ste dag : Publicatie van de maximumbedragen verkiezingsuitgaven in het B.S. (uiterste datum)

- **Zaterdag .....**
  15de dag : Publicatie in het B.S. van het bericht aan de kiezer (uiterste datum)

- **Zondag .....**
  ° Dag van de stemming
  ° Inzameling van de verkiezingsresultaten.

1.3 De organisatie van de verkiezingen van het Europees Parlement en van de Gewest- en Gemeenschapsparlementen.

a. De Belgische vertegenwoordiging in het Europees Parlement

Europees Parlement
14 vertegenwoordigers uit het Nederlandstalige college
9 vertegenwoordigers uit het Franstalige college
1 vertegenwoordiger uit het Duitstalige college

---

24 verkozenen voor België op een totaal van 732 leden vanaf 13 juni 2004 in de uitgebreide Europese Unie met 25 lidstaten

N.B. Tot 13 juni 2004 had België 25 vertegenwoordigers in het Europese Parlement (14 Nederlandstaligen, 10 Franstaligen en 1 Duitstalige). Het Europees Parlement telt 732 leden uit de 25 lidstaten. Gezien de uitbreiding van de Europese Unie, zal het aantal Belgische vertegenwoordigers aan het Europees Parlement, na de Europese verkiezingen van 2009, 22 vertegenwoordigers bedragen : **13** vertegenwoordigers uit het Nederlandstalige college , **8** vertegenwoordigers uit het Franstalige college en **1** vertegenwoordiger uit het Duitstalige college.

- Voor de verkiezing van het Europees Parlement zijn er 3 kiescolleges en 4 kieskringen:

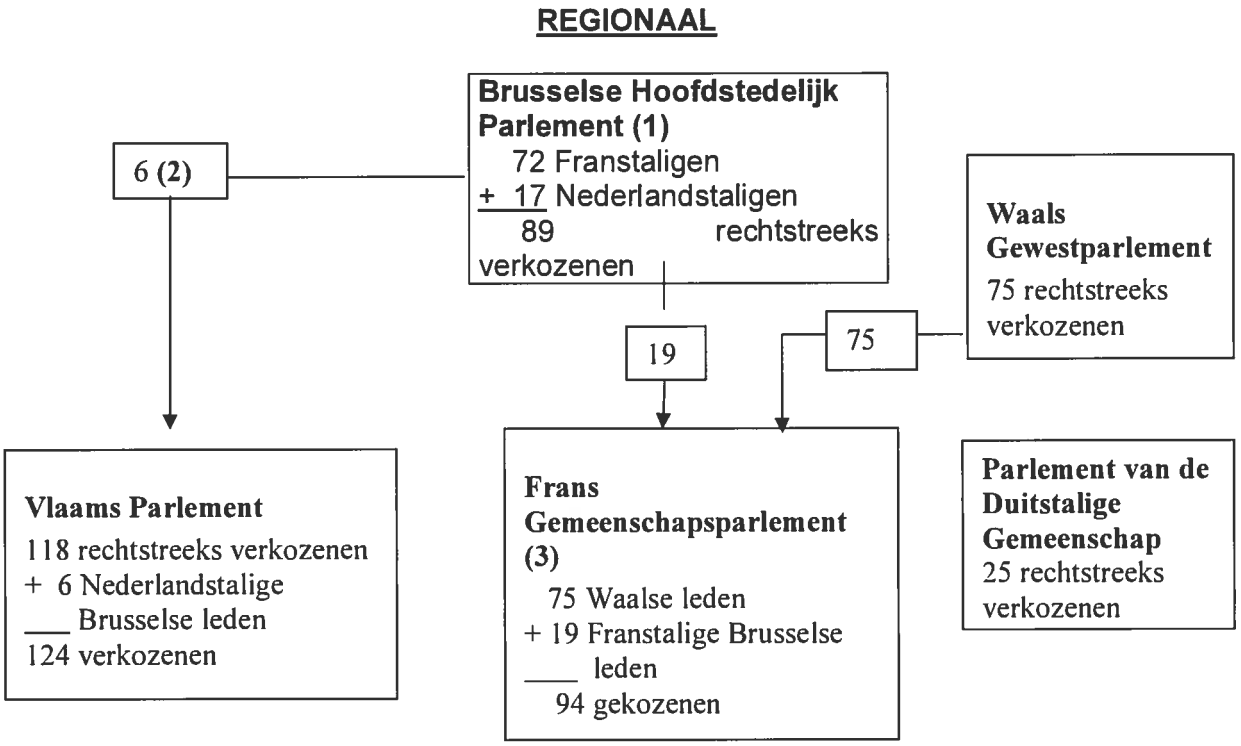
De 3 kiescolleges voor het Europees Parlement			
Kiescollege	**Kiesgebied**	**Hoofdbureau van het College**	**Aantal te kiezen leden**
Nederlandstalig	• Vlaams-Gewest (min arr. Halle-Vilvoorde) • Kieskring Brussel-Halle-Vilvoorde	Mechelen	14 (8 opvolgers)
Franstalig	• Waals Gewest (min 9 Duitstalige gemeenten) • Kieskring Brussel-Halle-Vilvoorde	Namen	9 (6 opvolgers)
Duitstalig	• 9 Duitstalige gemeenten (kantons Eupen en Sankt-Vith)	Eupen	1 (6 opvolgers)

TOTAAL			**24** leden

- Er zijn aparte opvolgers : de helft van het aantal effectieve kandidaten + 1. Er moeten minstens 6 opvolgers zijn.
- De wijziging van de kiescolleges en kieskringen kan bij gewone wet in het federale Parlement.
  Het aantal te verkiezen leden per kiescollege wordt vastgelegd bij koninklijk besluit.

b. Samenstelling van de Gewest- en Gemeenschapsparlementen

N.B. Sinds de Grondwetsherziening van 25 februari 2005 (Belgisch Staatsblad van 11 maart 2005) worden iedere Raad voortaan Parlement genoemd.



(1) Tot de verkiezingen van juni 2004 bestond het Brussels Hoofdstedelijk Parlement uit 75 leden.

(2) Vanaf de verkiezingen in juni 2004 worden de 6 Nederlandstalige Brusselse leden van het Vlaams Parlement rechtstreeks verkozen door de kiezers, die eerst hebben gestemd op een lijst van de Nederlandse taalgroep voor het Brussels Hoofdstedelijk Parlement.

(3) Het Frans Gemeenschapsparlement wordt niet rechtstreeks verkozen, maar wordt samengesteld uit de 75 verkozen leden van het Waals Gewestparlement en uit 19 verkozen leden van de Franse taalgroep in het Brussels Hoofdstedelijk Parlement.

1° Het Vlaamse Parlement (voorheen Vlaamse Raad).

- Het Vlaams Parlement bestaat heden uit 118 rechtstreeks verkozen leden en uit 6 Nederlandstalige leden van het Brussels Hoofdstedelijk Parlement of in totaal uit 124 leden.

N.B. Vanaf de verkiezingen in juni 2004 zijn de 6 Nederlandstalige Brusselse leden van het Vlaams Parlement rechtstreeks verkozen door de kiezers uit het Brusselse Gewest, die eerst hebben gestemd op een lijst van de Nederlandstalige taalgroep voor het Brussels Hoofdstedelijk Parlement.

- De 118 leden uit Vlaanderen worden gekozen in 5 provinciale kieskringen :

	Aantal leden	Aantal opvolgers
1)Antwerpen	33	16
2)Limburg	16	16
3)Oost-Vlaanderen	27	16
4)West-Vlaanderen	22	16
5)Vlaams-Brabant	20	16
	118	
Rechtstreekse verkiezing van leden voor het Vlaams Parlement in het Brussels Gewest	6	
	---	
	124 leden	

- De algemene regel van het aantal opvolgers is dat het aantal opvolgers gelijk moet zijn aan het aantal te verkiezen leden in een kieskring ; doch met een absoluut maximum van 16 opvolgers en met een absoluut minimum van 4 opvolgers.

- Het aantal kandidaten per kieskring is herberekend ingevolge de nieuwe Volkstelling van 1 oktober 2001. Bij besluit van de Vlaamse Regering worden de leden van de Vlaamse Raad verdeeld over de kieskringen.

- Een wijziging van de kieskringen kan slechts met een decreet bij 2/3 meerderheid over in de Vlaamse Raad. Bij stemming op 14 januari 2004 heeft de Vlaamse Raad provinciale kieskringen ingevoerd voor zijn verkiezing. Hierdoor is de apparentering of lijstenverbinding tussen de lijsten binnen éénzelfde provincie ook afgeschaft.

2° Het Waals Gewestparlement (voorheen Waalse Gewestraad).

- Het Waals Gewestparlement bestaat uit 75 rechtstreeks verkozen leden.
- De 75 leden uit Wallonië worden gekozen in 13 kieskringen :

	Aantal leden	Aantal opvolgers
1)Nivelles	8	8
2)Mons	6	6
3)Soignies	4	4
4)Tournai-Ath-Mouscron	7	7
5)Charleroi	9	9
6)Thuin	3	4
7)Arlon-Bastogne-Marche-en-Famenne	3	4
8)Neufchâteau-Virton	2	4
9)Liège	13	13
10) Huy-Waremme	4	4
11) Verviers	6	6
12) Namur	6	6

13)	Dinant-Philippeville	4	4
		---	
		75 leden	

- De algemene regel van het aantal opvolgers is dat het aantal opvolgers gelijk moet zijn aan het aantal te verkiezen leden in een kieskring ; doch met een absoluut maximum van 16 opvolgers en met een absoluut minimum van 4 opvolgers.
- Bij besluit dd. 4 september 2003 van de Waalse Regering is een nieuwe zetelverdeling gebeurd over de kieskringen, rekening houdend met de Volkstelling van 1 oktober 2001 (Belgisch Staatsblad van 12 september 2003 – 2e editie).
- Een wijziging van de kieskringen kan slechts met een decreet bij 2/3 meerderheid in de Waalse Raad. Er is apparentering of lijstenverbinding mogelijk tussen de lijsten binnen éénzelfde provincie.

N.B. Het Frans Gemeenschapsparlement wordt niet rechtstreeks verkozen, maar is samengesteld uit de 75 leden van het Waals Gewestparlement en uit 19 Franstalige leden van het Brussels Hoofdstedelijk Parlement.

3° Het Brussels Hoofdstedelijk Parlement (voorheen Brusselse Hoofdstedelijke Raad).

- De 19 gemeenten (8 kieskantons) van het Brussels Hoofdstedelijke Gewest vormen 1 kiescollege, dat wordt voorgezeten door het Gewestbureau en bestaat uit lijsten van de Franstalige taalgroep en van de Nederlandstalige taalgroep.
  Het Brussels Hoofdstedelijk Parlement, dat vanaf juni 2004 in totaal 89 leden telt, heeft 72 leden die zijn gekozen uit de lijsten van de Franstalige taalgroep en 17 leden die zijn gekozen uit de lijsten van de Nederlandstalige taalgroep. Er worden 16 aparte opvolgers per lijst voorzien.
  Bij de verkiezing in 2004 geschiedde terzelfder tijd en voor de eerste maal de **rechtstreekse verkiezing** van de 6 Brusselse leden, die zetelen in het Vlaams Parlement. Er worden 6 aparte opvolgers per lijst voorzien.

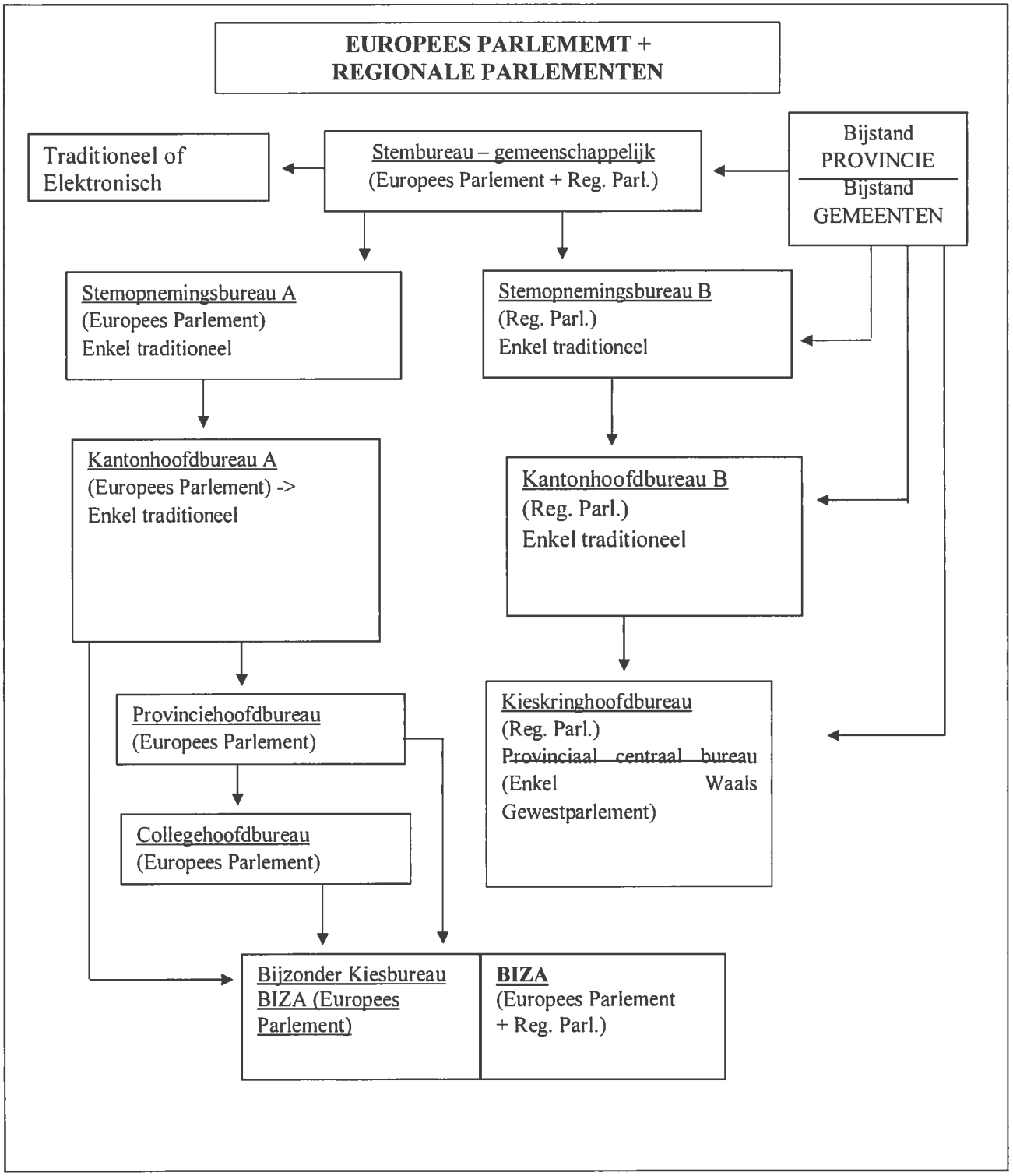
- Het Brussels Hoofdstedelijke Parlement bestond tot juni 2004 uit 75 rechtstreeks verkozen leden, waarvan 64 leden van de Franse taalgroep en 11 leden van de Nederlandse taalgroep.
- Vanaf juni 2004 zijn er dus **89 leden** in het Brussels Hoofdstedelijk Parlement, die rechtstreeks verkozen zijn, met een gewaarborgde vertegenwoordiging van 72 Franstalige leden en 17 Nederlandstalige leden (uitvoering van de Lambermont- en Lombardakkoorden uit 2001).

4° Parlement van de Duitstalige Gemeenschap (voorheen Raad van de Duitstalige Gemeenschap).

- De 9 gemeenten (kieskantons Eupen en Sankt-Vith) van het Duitse taalgebied vormen 1 kiescollege, dat wordt voorgezeten door het Hoofdbureau van het Kiesgebied.
  Het Parlement van de Duitstalige Gemeenschap telt **25 leden**. Er zijn geen aparte opvolgers in dit Parlement.

N.B. De 9 Duitstalige gemeenten zijn : Amel, Büllingen, Burg-Reuland, Bütgenbach, Eupen, Kelmis, Lontzen, Raeren en Sankt Vith.

c. Schema kiesbureaus



N.B. In de elektronische kieskantons is er slechts één kantonhoofdbureau dat de resultaten rechtstreeks overmaakt aan het provinciehoofdbureau- en kieskringhoofdbureau. In deze kieskantons zijn er geen stemopnemingsbureaus meer en komen de resultaten van de geautomatiseerde stembureaus direct naar het kantonhoofdbureau.

d. Toelichtingen bij de kiesbureaus.

Soort kiesbureau	Aantal bureaus	Aantal effectieve bureauleden	Aantal plaatsvervangende bureauleden
Collegehoofdbureau (Europees Parlement)	3	18	12
Provinciehoofdbureau (Europees Parlement)	11	66	44
Kieskringhoofdbureau (Reg. Parl.)	20	120	80
Geautomatiseerd Kantonhoofdbureau	62	372	1.468
Traditioneel Kantonhoofdbureau A (Europees Parlement)	146	876	584
Traditioneel Kantonhoofdbureau B (Reg. Parl.)	146	876	584
Geautomatiseerd Stembureau	3.718	29.744	18.590
Traditioneel Stembureau	6.654	39.924	26.616
Stemopnemingsbureau A (enkel traditioneel – Reg. Parl.)	2.246	13.476	8.984
Stemopnemingsbureau B (enkel traditioneel – Raad)	2.246	13.476	8.984
Bijzonder Kiesbureau FOD BIZA	1	6	4
TOTALEN	**15.253**	**98.954**	**65.950**

- Een kiesbureau bestaat normaal uit 6 leden : 1 voorzitter, 1 secretaris en 4 vaste bijzitters (reserve : 4 plaatsvervangende bijzitters).

- De stembureaus zijn gemeenschappelijk bij het traditioneel en elektronisch stemmen voor de verkiezingen van het Europees Parlement en de Regionale Parlementen.

- Het geautomatiseerd stembureau regelt de elektronische stemming van de kiezers en bestaat uit 8 leden : 1 voorzitter, 1 secretaris, 1 adjunct-secretaris met kennis van informatica en 5 bijzitters.
  Het traditioneel stembureau regelt de stemming met stembiljetten voor de kiezers.

- Er zijn stemopnemingsbureaus A ("telbureaus") voor de verkiezing van het Europees Parlement én stemopnemingsbureaus B voor de verkiezing van de Regionale Parlementen.
  In de kieskantons met elektronische stemming zijn er geen stemopnemingsbureaus meer. De totalisatie van de stemmen van alle verkiezingen geschiedt dan onmiddellijk op het enige kantonhoofdbureau.

- Er is een kantonhoofdbureau A voor de verkiezing van het Europees Parlement én een kantonhoofdbureau B voor de verkiezing van de Regionale Parlementen.
  Dit bureau doet de stemopneming van de stembiljetten van een 3-tal traditionele stembureaus in het kieskanton.
  In de kieskantons met elektronische stemming zijn er geen stemopnemingsbureaus meer. De totalisatie van de stemmen van alle verkiezingen geschiedt dan onmiddellijk op het enige kantonhoofdbureau.
  Van de 208 kieskantons in België zijn er 62 kieskantons met elektronische stemming en 146 kieskantons met traditionele stemming. Alle kieskantons in het Brusselse Hoofdstedelijk Gewest en in het Duitstalig kiesgebied zijn geautomatiseerd.

  Het geautomatiseerd kantonhoofdbureau doet de stemopneming van de stemdiskettes van de geautomatiseerde stembureaus voor het gehele kieskanton (er zijn geen stemopnemingsbureaus of "telbureaus" meer in deze kieskantons).
  Het traditioneel kantonhoofdbureau leidt de telling van de stemmen door de stemopnemingsbureaus in het gehele kieskanton.

- Er is een apart provinciehoofdbureau voor de verkiezing van het Europese Parlement in iedere provinciehoofdplaats. Dit bureau doet de stemopneming in de gehele provincie of kieskring.
  Het provinciehoofdbureau van de provincie Vlaams-Brabant is slechts bevoegd voor het administratief arrondissement Leuven.
  Een apart hoofdbureau van de kieskring Brussel-Halle-Vilvoorde vervult de functies van provinciehoofdbureau te Brussel.
  Het collegehoofdbureau van het Duitstalig kiescollege te Eupen oefent de functies van provinciehoofdbureau uit voor het Duitstalig kiesgebied.

- Er is een collegehoofdbureau voor de verkiezing van het Europees Parlement te Mechelen (Nederlands kiescollege), te Namen (Frans kiescollege) en te Eupen (Duitstalig kiescollege).
  Dit bureau regelt de totale stemopneming van het college, de verdeling van de zetels en de aanwijzing van de gekozenen en de opvolgers.

- Er is een kieskringhoofdbureau voor de verkiezing van de Regionale Parlementen.
  Het kieskringhoofdbureau voor de verkiezing van het Brussels Hoofdstedelijk Parlement wordt Gewestbureau genoemd.

Het kieskringhoofdbureau voor de verkiezing van het Parlement van de Duitstalige Gemeenschap wordt Hoofdbureau van het kiesgebied genoemd.
Dit bureau regelt de totale stemopneming van de kieskring, de verdeling van de zetels en de aanwijzing van de gekozenen en de opvolgers.

- Voor de verkiezing van het Waals Gewestparlement worden de taken van lijstenverbindingen ("apparentering") tussen de kieskringen van een provincie vervuld door het provinciaal centraal bureau, dat het kieskringhoofdbureau in de provinciehoofdplaats is.
  In de provincie Waals-Brabant zijn er geen lijstenverbindingen, mogelijk omdat er slechts 1 kieskring is.
  Bij lijstenverbindingen regelt dit bureau de aanvullende provinciale zetelverdeling en de aanwijzing van de gekozen en opvolgers.

- Het bijzonder kiesbureau, dat ingesteld wordt bij FOD Binnenlandse Zaken (BIZA), zorgt voor het stemrecht van de Belgen in de Europese Unie die zich hebben geregistreerd als kiezer in België voor het Europees Parlement.
  FOD BIZA staat in voor de algemene organisatie van de verkiezingen.

- De gemeenten en de provincies hebben onder meer belangrijke taken bij de organisatie en de logistiek van de kiesbureaus.

e. Belangrijke kiesdata

- **Donderdag .....** (= 80ste dag vóór de stemming of de 25ste dag van de derde maand vóór de stemming)

Uiterste datum voor aanvraag kiezerslijst door politieke partijen en kandidaten bij aangetekend schrijven aan elke burgemeester van een Belgische gemeente.

- **Vrijdag .....** (= 79ste dag vóór de stemming)

Uiterste datum waarop het bijzonder kiesbureau bij FOD BIZA wordt samengesteld. Het bijzonder kiesbureau regelt het stemrecht van Belgen die wonen in de Europese Unie en deelnemen aan de Europese verkiezingen in België na hun registratie als kiezer. Deze Belgische kiezers in de Europese Unie stemmen enkel per briefwisseling (Het stemrecht van de Belgen in het buitenland met de 5 stemwijzen, zoals bij de federale Parlementsverkiezingen van ....., is niet van toepassing).

- **Donderdag .....** (= 73ste dag vóór de stemming of de eerste dag van de tweede maand vóór de stemming)

Elk college van burgemeester en schepenen maakt de kiezerslijst op die geldt voor alle verkiezingen.

N.B. - De burgers uit de Europese Unie (nu 24 andere lidstaten) die in België verblijven en zich uiterlijk op 31 maart 2009 als kiezer in hun Belgische verblijfsgemeente hebben laten registreren kunnen deelnemen aan de verkiezing van het Europees Parlement (niet aan de Raadsverkiezingen)

- De burgers van de Europese Unie, die de voorwaarden van een Belgische kiezer vervullen (nationaliteit van een lidstaat van de Europese Unie, ingeschreven in een Belgische gemeente, 18 jaar zijn en niet geschorst zijn uit het kiesrecht) hebben passief kiesrecht (= zich kandidaat stellen, dan wel 21 jaar zijn) en actief kiesrecht (= kunnen stemmen).
- Er zijn potentieel ongeveer 500.000 burgers uit de Europese Unie die kunnen deelnemen aan de Europese verkiezingen in België.
- FOD BIZA regelt de gegevensuitwisseling van de kiezers uit de Europese Unie met de andere lidstaten.

- **Dinsdag .....** (= 68ste dag vóór de stemming)

Publicatie van de lijst van de verboden letterwoorden of logo's in het Belgisch Staatsblad door FOD BIZA.

- **Vrijdag .....** (= 65ste dag vóór de stemming)

Indiening van het beschermd letterwoord of logo èn loting van de nationale nummers bij FOD BIZA tussen 10 en 12 uur.

- **Dinsdag .....** (= 61ste dag vóór de stemming)

Publicatie van de beschermde letterwoorden of logo's èn de nationale nummers in het Belgisch Staatsblad.

- **Vrijdag ..... en zaterdag .....** (= 58ste en 57ste dag vóór de stemming)

Indiening van de voordrachtsakten voor de verkiezing van het Europees Parlement bij de 3 collegehoofdbureaus en controle van de dubbele kandidaturen door FOD BIZA.

- **Maandag .....** (= 55ste dag vóór de stemming)

Voorlopige afsluiting van de kandidatenlijsten door de collegehoofdbureaus te Mechelen, Namen en Eupen (Europees Parlement).

- **Donderdag .....** (=52ste dag vóór de stemming)

  - Definitieve afsluiting van de kandidatenlijsten in de collegehoofdbureaus (Europees Parlement), na mededeling en behandeling van eventuele dubbele kandidaturen door FOD BIZA, van verbeterde voordrachtsakten en van bezwaarschriften door kandidaten.
  - Ingeval van beroep bij Hof van Beroep (onverkiesbaarheid kandidaat) of bij Raad van State (taalvereiste), geschiedt de definitieve afsluiting pas op maandag ..... (= 41ste dag vóór de stemming)
  - Na de definitieve afsluiting, loting van de lokale nummers en opmaak van het model-stembiljet met de kandidatenlijsten.

- **Zaterdag ..... en zondag .....** (= 29ste en 28ste dag vóór de stemming)

- Indiening van de voordrachtsakten voor de verkiezing van de Regionale Parlementen (Reg. Parl.) bij de kieskringhoofdbureaus (5 in Vlaanderen, 13 in Wallonië, 1 in Brussels Gewest en 1 in Duitstalig kiesgebied) en controle van de dubbele kandidaturen door FOD BIZA.

- **Maandag .....** (= 27ste dag vóór de stemming)

Voorlopige afsluiting van de kandidatenlijsten (Reg. Parl.) door de kieskringhoofdbureaus.

- **Donderdag .....** (= 24ste dag vóór de stemming)

  - Definitieve afsluiting van de kandidatenlijsten (Reg. Parl.) in de kieskringhoofdbureaus na mededeling en behandeling van eventuele dubbele kandidaturen door FOD BIZA, van verbeterde voordrachtsakten en van bezwaarschriften door kandidaten.
  - Ingeval van beroep bij Hof van Beroep (onverkiesbaarheid kandidaat), geschiedt de definitieve afsluiting pas op maandag ..... (= 20ste dag vóór de stemming)
  - Na de definitieve afsluiting, loting van de lokale nummers en opmaak van het model-stembiljet met de kandidatenlijsten.

- **Donderdag .....** (= 17de dag vóór de stemming)

De verklaringen van lijstenverbindingen bij de voorzitter van het kieskringhoofdbureau in de provinciehoofdplaats (uitsluitend voor het Vlaams Parlement en Waals Gewestparlement – provinciaal centraal bureau voor de "apparentering" – niet meer voor het Vlaams Parlement ingevolge de provincialisering van de kieskringen).

- **Zaterdag .....** (= 15de dag vóór de stemming)

Uiterste datum voor publicatie in het Belgisch Staatsblad van het bericht aan de kiezer door FOD BIZA en verzending van de oproepingsbrieven aan de kiezers door de gemeenten.

- **Dinsdag .....** (= 5de dag vóór de stemming)

De aanwijzing van de getuigen voor de stembureaus en stemopnemingsbureaus (A) bij de voorzitter van het kantonhoofdbureau A voor de verkiezing van het Europees Parlement. De aanwijzing van de getuigen voor de stemopnemingsbureaus B (Reg. Parl.) geschiedt door de voorzitter van het kantonhoofdbureau B.

- **Zondag .....** (= dag van de stemming)

Begeleiding van de stemming en de inzameling van de verkiezingsuitslagen voor het Europees Parlement en voor de Reg. Parl. (Vlaams, Waals, Brussels en Duitstalig) door FOD BIZA. De inzameling van de resultaten voor de Reg. Parl. geschiedt met de medewerking van de regionale administraties.

*
* *

1.4. De organisatie van de gemeenteraads- en van de provincieraadsverkiezingen.

A. De Vlaamse gemeenten en de Vlaamse provincies.

1 Inleiding

Het Agentschap voor Binnenlands bestuur van de Vlaamse Overheid staat in voor de organisatie van de verkiezingen van de provincieraden, districtsraden van de stad Antwerpen, gemeenteraden en OCMW-raden.
In de gemeenten Drogenbos, Kraainem, Linkebeek, Sint-Genesius-Rode, Wemmel, Wezembeek-Oppem (= de zes gemeenten in de Vlaamse rand rond Brussel) en Voeren worden bovendien ook rechtstreeks verkozen: de schepenen, de leden van de raad voor maatschappelijk welzijn en van het vast bureau van het OCMW – zie artikel 15, §2 Nieuwe Gemeentewet, artikel 17bis en 27bis OCMW-wet.

De laatste verkiezing van deze raden had plaats op zondag 8 oktober 2006. Deze verkiezingen worden eens in de zes jaar gehouden. De volgende verkiezing van de provincieraden, districtsraden van de stad Antwerpen, gemeenteraden en OCMW-raden zal plaats hebben in 2012.

2. Het aantal te begeven zetels voor de verschillende raden in 2006

a. Samenstelling van de provincieraden

Voor de verkiezingen van 8 oktober 206 waren de te begeven zetels:

PROVINCIE	***Provincieraadsleden***
ANTWERPEN	84
VLAAMS-BRABANT	84
WEST-VLAANDEREN	84
OOST-VLAANDEREN	84
LIMBURG	75

Het aantal te begeven zetels in de provincieraad wordt bepaald aan de hand van het aantal inwoners van de provincie. Uit de provincieraadleden wordt de deputatie samengesteld.

b. Samenstelling van de Antwerpse districtsraden

Voor de verkiezingen van 8 oktober 206 waren de te begeven zetels:

Antwerpse districten	***aantal districtraadsleden***
Anwerpen	33
Berchem	23
Berendrecht-Zandvliet-Lillo	15
Borgerhout	25
Deurne	27
Ekeren	19
Hoboken	21
Merksem	25
Wilrijk	23

Het aantal te begeven zetels in de districtsraad wordt bepaald aan de hand van het aantal inwoners van het district.

c. Samenstelling van de gemeenteraden

Het aantal te begeven zetels in de gemeenteraden wordt bepaald aan de hand van het aantal inwoners van de gemeenten. Uit de gemeenteraden wordt het schepencollege samengesteld, met uitzondering van Voeren en de zes randgemeenten in de Vlaamse rand rond Brussel waar de schepenen rechtstreeks verkozen worden. Deze randgemeenten zijn Drogenbos, Kraainem, Linkebeek, Sint-Genesius-Rode, Wemmel, Wezembeek-Oppem.

Voor de verkiezingen van 8 oktober 206 waren de te begeven zetels:

	gemeenteraadsleden	***rechtstreeks verkozen schepenen***
AALST	41	
AALTER	25	
AARSCHOT	29	
AARTSELAAR	23	
AFFLIGEM	21	
ALKEN	21	
ALVERINGEM	15	
ANTWERPEN	55	
ANZEGEM	23	
ARDOOIE	21	
ARENDONK	23	

AS	19
ASSE	29
ASSENEDE	23
AVELGEM	21
BAARLE-HERTOG	11
BALEN	27
BEERNEM	23
BEERSE	25
BEERSEL	27
BEGIJNENDIJK	21
BEKKEVOORT	17
BERINGEN	35
BERLAAR	21
BERLARE	23
BERTEM	21
BEVER	11
BEVEREN	35
BIERBEEK	21
BILZEN	31
BLANKENBERGE	25
BOCHOLT	23
BOECHOUT	23
BONHEIDEN	23
BOOM	25
BOORTMEERBEEK	21
BORGLOON	21
BORNEM	27
BORSBEEK	21
BOUTERSEM	19
BRAKEL	23
BRASSCHAAT	33
BRECHT	29
BREDENE	25
BREE	23
BRUGGE	47
BUGGENHOUT	23
DAMME	21
DE HAAN	21
DE PANNE	21
DE PINTE	21
DEERLIJK	21
DEINZE	29
DENDERLEEUW	25
DENDERMONDE	35
DENTERGEM	19
DESSEL	19
DESTELBERGEN	25
DIEPENBEEK	25
DIEST	27
DIKSMUIDE	25
DILBEEK	33
DILSEN-STOKKEM	25
DROGENBOS	15

DUFFEL	25
EDEGEM	27
EEKLO	25
ERPE-MERE	25
ESSEN	25
EVERGEM	31
GALMAARDEN	19
GAVERE	23
GEEL	33
GEETBETS	17
GENK	39
GENT	51
GERAARDSBERGEN	31
GINGELOM	19
GISTEL	21
GLABBEEK	17
GOOIK	19
GRIMBERGEN	31
GROBBENDONK	21
HAACHT	23
HAALTERT	25
HALEN	19
HALLE	31
HAM	21
HAMME	27
HAMONT-ACHEL	23
HARELBEKE	29
HASSELT	41
HECHTEL-EKSEL	21
HEERS	17
HEIST-OP-DEN-BERG	33
HEMIKSEM	21
HERENT	25
HERENTALS	29
HERENTHOUT	19
HERK-DE-STAD	21
HERNE	17
HERSELT	23
HERSTAPPE	7
HERZELE	25
HEUSDEN-ZOLDER	31
HEUVELLAND	19
HOEGAARDEN	17
HOEILAART	21
HOESELT	21
HOLSBEEK	21
HOOGLEDE	21
HOOGSTRATEN	25
HOREBEKE	11
HOUTHALEN-HELCHTEREN	29
HOUTHULST	21
HOVE	19
HULDENBERG	21

HULSHOUT	21	
ICHTEGEM	23	
IEPER	31	
INGELMUNSTER	21	
IZEGEM	29	
JABBEKE	23	
KALMTHOUT	25	
KAMPENHOUT	21	
KAPELLEN	29	
KAPELLE-OP-DEN-BOS	19	
KAPRIJKE	17	
KASTERLEE	25	
KEERBERGEN	23	
KINROOI	21	
KLUISBERGEN	17	
KNESSELARE	19	
KNOKKE-HEIST	31	
KOEKELARE	19	
KOKSIJDE	27	
KONTICH	27	
KORTEMARK	21	
KORTENAKEN	19	
KORTENBERG	25	
KORTESSEM	19	
KORTRIJK	41	
KRAAINEM	23	5
KRUIBEKE	25	
KRUISHOUTEM	19	
KUURNE	23	
LAAKDAL	23	
LAARNE	21	
LANAKEN	27	
LANDEN	23	
LANGEMARK-POELKAPELLE	19	
LEBBEKE	25	
LEDE	25	
LEDEGEM	21	
LENDELEDE	17	
LENNIK	19	
LEOPOLDSBURG	23	
LEUVEN	45	
LICHTERVELDE	19	
LIEDEKERKE	21	
LIER	31	
LIERDE	17	
LILLE	25	
LINKEBEEK	15	3
LINT	19	
LINTER	19	
LOCHRISTI	27	
LOKEREN	33	
LOMMEL	31	
LONDERZEEL	25	

LO-RENINGE	13
LOVENDEGEM	21
LUBBEEK	23
LUMMEN	23
MAARKEDAL	17
MAASEIK	27
MAASMECHELEN	33
MACHELEN	23
MALDEGEM	27
MALLE	23
MECHELEN	41
MEERHOUT	21
MEEUWEN-GRUITRODE	23
MEISE	25
MELLE	21
MENEN	31
MERCHTEM	23
MERELBEKE	27
MERKSPLAS	19
MESEN	7
MEULEBEKE	21
MIDDELKERKE	25
MOERBEKE	17
MOL	31
MOORSLEDE	21
MORTSEL	27
NAZARETH	21
NEERPELT	25
NEVELE	21
NIEL	19
NIEUWERKERKEN	17
NIEUWPOORT	21
NIJLEN	27
NINOVE	33
OLEN	21
OOSTENDE	39
OOSTERZELE	23
OOSTKAMP	27
OOSTROZEBEKE	19
OPGLABBEEK	21
OPWIJK	23
OUDENAARDE	29
OUDENBURG	19
OUD-HEVERLEE	21
OUD-TURNHOUT	23
OVERIJSE	27
OVERPELT	23
PEER	25
PEPINGEN	15
PITTEM	17
POPERINGE	25
PUTTE	25
PUURS	25

RANST	25	
RAVELS	23	
RETIE	21	
RIEMST	25	
RIJKEVORSEL	21	
ROESELARE	37	
RONSE	27	
ROOSDAAL	21	
ROTSELAAR	25	
RUISELEDE	17	
RUMST	23	
SCHELLE	19	
SCHERPENHEUVEL-ZICHEM	27	
SCHILDE	25	
SCHOTEN	31	
SINT-AMANDS	19	
SINT-GENESIUS-RODE	25	5
SINT-GILLIS-WAAS	25	
SINT-KATELIJNE-WAVER	25	
SINT-LAUREINS	17	
SINT-LIEVENS-HOUTEM	21	
SINT-MARTENS-LATEM	19	
SINT-NIKLAAS	39	
SINT-PIETERS-LEEUW	31	
SINT-TRUIDEN	33	
SPIERE-HELKIJN	11	
STABROEK	25	
STADEN	21	
STEENOKKERZEEL	21	
STEKENE	25	
TEMSE	29	
TERNAT	23	
TERVUREN	27	
TESSENDERLO	25	
TIELT	25	
TIELT-WINGE	21	
TIENEN	31	
TONGEREN	29	
TORHOUT	25	
TREMELO	23	
TURNHOUT	33	
VEURNE	21	
VILVOORDE	33	
VLETEREN	13	
VOEREN	15	3
VORSELAAR	19	
VOSSELAAR	21	
WAARSCHOOT	19	
WAASMUNSTER	21	
WACHTEBEKE	17	
WAREGEM	33	
WELLEN	17	
WEMMEL	23	5

WERVIK	25	
WESTERLO	27	
WETTEREN	27	
WEVELGEM	31	
WEZEMBEEK-OPPEM	23	5
WICHELEN	21	
WIELSBEKE	19	
WIJNEGEM	19	
WILLEBROEK	27	
WINGENE	23	
WOMMELGEM	23	
WORTEGEM-PETEGEM	17	
WUUSTWEZEL	25	
ZANDHOVEN	23	
ZAVENTEM	29	
ZEDELGEM	27	
ZELE	27	
ZELZATE	23	
ZEMST	27	
ZINGEM	17	
ZOERSEL	27	
ZOMERGEM	19	
ZONHOVEN	25	
ZONNEBEKE	21	
ZOTTEGEM	27	
ZOUTLEEUW	19	
ZUIENKERKE	11	
ZULTE	23	
ZUTENDAAL	17	
ZWALM	19	
ZWEVEGEM	27	
ZWIJNDRECHT	25	

d. Samenstelling van de rechtstreeks verkozen OCMW-raden

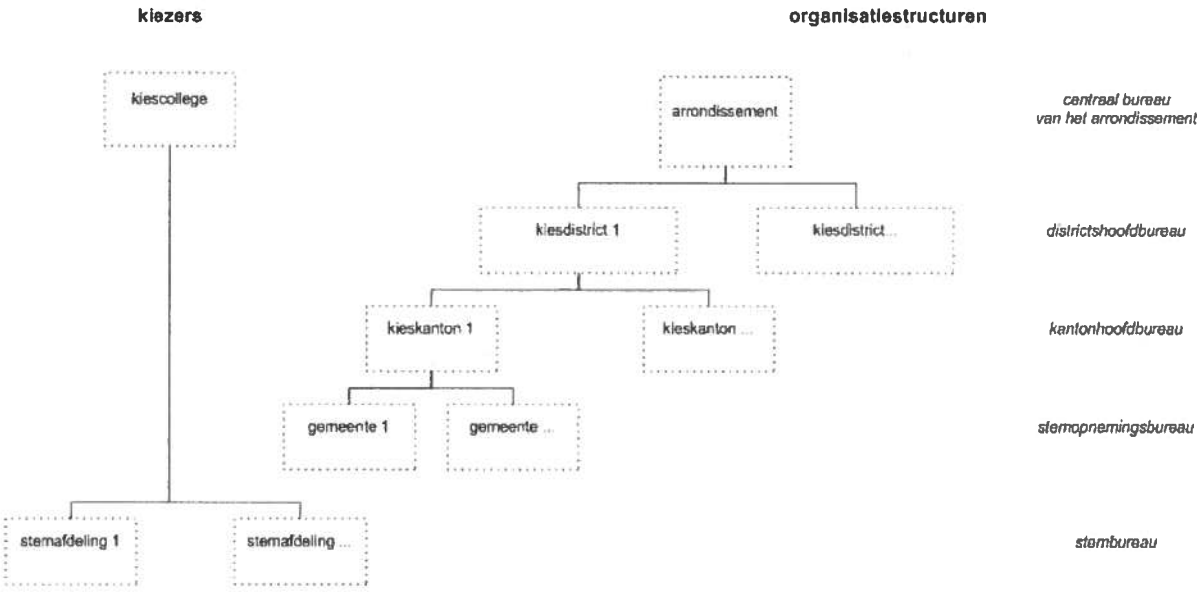
Voor de verkiezingen van 8 oktober 206 waren de te begeven zetels:

GEMEENTE	***OCMW-raadsleden***	***Leden vast bureau***
DROGENBOS	9	3
KRAAINEM	9	3
LINKEBEEK	9	3
SINT-GENESIUS-RODE	11	4
VOEREN	9	3
WEMMEL	9	3
WEZEMBEEK-OPPEM	9	3

Het aantal te begeven zetels in de OCMW-raad wordt bepaald door het aantal inwoners van de gemeente.

3. Organisatie van de verkiezingen: stembureaus

a. Provincieraden



Om ervoor te zorgen dat het stemmen en het verwerken van de stemresultaten van de provincieraadsverkiezingen vlot verlopen worden er een aantal structuren opgericht.

Voor wat betreft de provincieraadsverkiezingen wordt Vlaanderen ingedeeld in een aantal administratieve arrondissementen. Ieder administratief arrondissement wordt op zijn beurt onderverdeeld in een aantal kiesdistricten. Een kiesdistrict bestaat op zijn beurt uit één of meerdere kieskantons.

Een kiesdistrict is een geografische omschrijving van een provinciaal kiescollege. Het is een afgebakend gebied van gemeenten waarbinnen:

- de kandidaatslijsten voor de verkiezingen worden opgesteld
- de zetelverdeling wordt berekend in de eerste fase
- de aanwijzing van de gekozenen gebeurt.

Een administratief arrondissement omvat één of meerder kiesdistricten. In elk arrondissement wordt een centraal bureau van het arrondissement opgericht. Dit bureau heeft een belangrijke taak als er lijstenverbindingen worden aangegaan. Zij aanvaardt de verklaringen van lijstenverbinding, verdeelt in dat geval de zetels over de lijsten en wijst de gekozenen aan.

In de hoofdplaats van elk kiesdistrict wordt een districtshoofdbureau samengesteld. Dit Bureau houdt zich bezig met de aan de stemming voorafgaande verrichtingen en met de algemene telling van de stemmen. Als er geen lijstenverbinding is, dan verdeelt het

districtshoofdbureau de zetels over de lijsten en wijst het de gekozenen aan. De voorzitter houdt toezicht op het geheel van de verrichtingen in het kiesdistrict.

Samenstelling:
- voorzitter
- secretaris
- 4 bijzitters
- 4 plaatsvervangende bijzitters
- eventuele getuigen

Een kiesdistrict omvat een of meerdere kieskantons. Een kieskanton omvat een of meerder gemeenten waarbinnen de stemtellingen voor de provincieraadsverkiezingen worden verzameld.

Tussen de gemeenten van eenzelfde kanton worden ook afspraken gemaakt over hoe de organisatie van de verkiezingen zal verlopen. Bijvoorbeeld kunnen alle gemeenten van een kanton beslissen om over te stappen op geautomatiseerde verkiezingen.

In elk kieskanton is er een kantonhoofdbureau, stemopnemingsbureaus en stembureaus. Als het kiesdistrict slechts één kanton omvat, houdt het districtshoofdbureau terzelfdertijd zitting als kantonhoofdbureau.

Het kantonhoofdbureau is voornamelijk belast met het toezicht op de kiesverrichtingen in het hele kanton. Het verzamelt ook de resultaten van de stemopneming in het kanton.

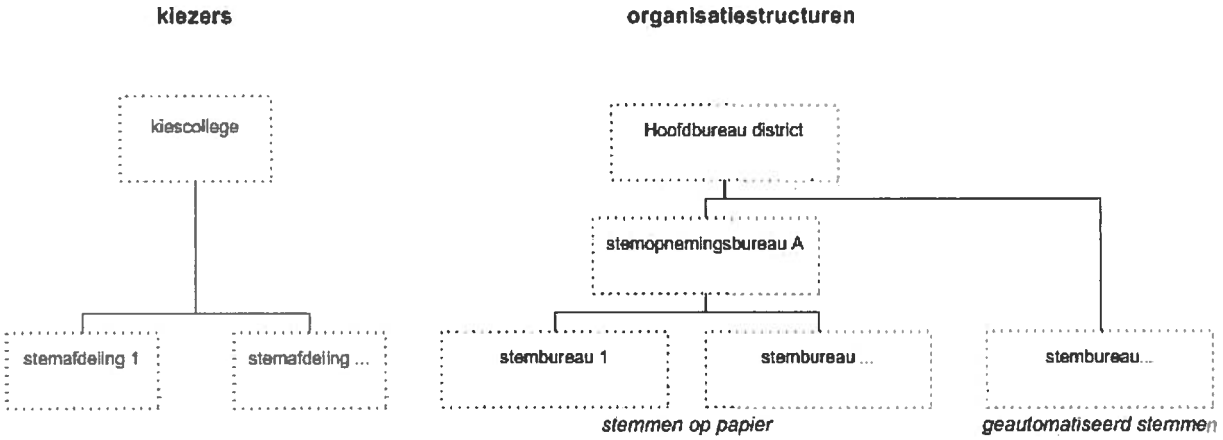
Samenstelling:
- voorzitter
- secretaris
- 4 bijzitters
- 4 plaatsvervangende bijzitters
- eventuele getuigen

In de hoofdplaats van een kieskanton is een stemopnemingsbureau gevestigd. Dit bureau neemt de stembiljetten van de verschillende stembureaus in ontvangst. De stemmen worden geteld en er wordt een proces verbaal van opgesteld. De resultaten worden bezorgd aan de voorzitter van het kantonhoofdbureau. Het stemopnemingsbureau is gevestigd in de kantonhoofdplaats.
Samenstelling:
- voorzitter
- secretaris
- 4 bijzitters
- 4 plaatsvervangende bijzitters
- eventuele getuigen

In de stembureaus kunnen de kiezers hun stem uitbrengen. Na het afsluiten van de kiesverrichtingen stelt het stembureau vast hoeveel stembiljetten in de stembus zijn gestoken, hoeveel er zijn terug genomen en hoeveel er niet zijn gebruikt. De omslag met alle stembiljetten wordt naar het stemopnemingsbureau gebracht. Er worden evenveel stembureaus opgericht als er stemafdelingen zijn.

Samenstelling:
- voorzitter
- secretaris
- 4 bijzitters
- 4 plaatsvervangende bijzitters
- eventuele getuigen

b. Districtsraden (Antwerpen)



Om de praktische organisatie van de districtsraadsverkiezingen vlot te laten verlopen worden een aantal structuren opgezet.

Alle personen die mogen deelnemen aan de districtsraadsverkiezingen van een bepaald district vormen samen het kiescollege van dat district. Vanuit praktische overwegingen kan het kiescollege opgedeeld worden in stemafdelingen. Als er niet meer dan achthonderd kiezers zijn in een gemeente, vormen zij één stemafdeling. Zijn er meer, dan worden ze ingedeeld in stemafdelingen van minstens 150 en maximum 800 kiezers. Deze opdeling wordt gemaakt om het stemmen en de telling te vereenvoudigen.

In elk district wordt er een hoofdbureau geïnstalleerd. Dit hoofd(stem)bureau heeft een coördinerende rol bij de districtsraadsverkiezingen, zowel in de aanloop naar de verkiezingen als tijdens de verkiezingen.

Opdrachten:
- toezien op de werkzaamheden van de stembureaus en de stemopnemingsbureaus
- verzamelen van gegevens van de stemopnemingsbureaus of van gegevensdragers van de stembureaus
- afkondigen van de stemuitslag
- aanvaarden van voordrachten

Samenstelling:

- voorzitter
- eventueel plaatsvervangend voorzitter
- secretaris
- 4 bijzitters
- 4 plaatsvervangende bijzitters
- eventuele getuigen en plaatsvervangende getuigen

Voor elke stemafdeling wordt een stembureau ingericht. In een district kunnen verschillende stembureaus worden opgericht. Een stembureau zorgt voor een vlot verloop van de kiesverrichtingen. In een stembureau komen de kiezers van de overeenkomstige stemafdeling hun stem uitbrengen. Het stembureau voor de gemeenteraadsverkiezingen fungeert eveneens als stembureau voor de districtsraadsverkiezingen.

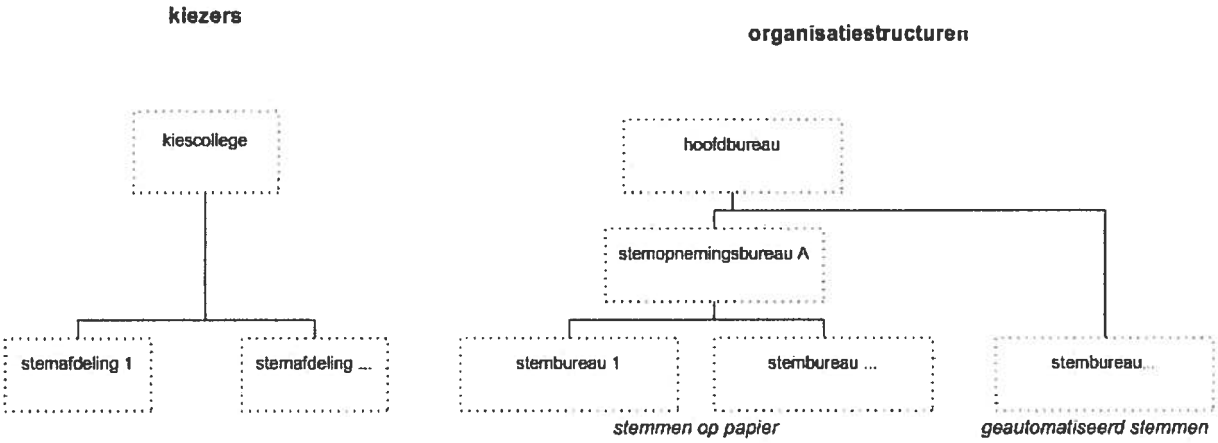
Samenstelling:
- voorzitter
- eventueel plaatsvervangend voorzitter
- secretaris
- 4 bijzitters
- 4 plaatsvervangende bijzitters
- eventuele getuigen en plaatsvervangende getuigen

In een district kunnen verschillende stemopnemingsbureaus worden opgericht. Een stemopnemingsbureau telt de stemmen van maximum 2400 stemgerechtigden. De stemmen van verschillende stembureaus worden daartoe samengevoegd.

Samenstelling:
- voorzitter
- eventueel plaatsvervangend voorzitter
- secretaris
- 2 / 3 / 4 bijzitters (afhankelijk van het aantal te verkiezen raadsleden)
- 2 / 3 / 4 plaatsvervangende bijzitters (afhankelijk van het aantal te verkiezen raadsleden)
- eventuele getuigen en plaatsvervangende getuigen

In districten waar er geautomatiseerd gestemd wordt, worden er geen stemopnemingsbureaus ingericht. De gegevensdragers met de stemmen worden direct door de stembureaus aan het hoofdbureau van het district bezorgd.

c. Gemeente- en OCMW-raden



Om de praktische organisatie van de gemeenteraadsverkiezingen vlot te laten verlopen worden een aantal structuren opgezet.

Alle personen die mogen deelnemen aan de gemeenteraadsverkiezingen van een bepaalde gemeente vormen samen één kiescollege. Vanuit praktische overwegingen kan het kiescollege opgedeeld worden in stemafdelingen. Als er niet meer dan achthonderd kiezers zijn in een gemeente, vormen zij één stemafdeling. Zijn er meer, dan worden ze ingedeeld in stemafdelingen van minstens 150 en maximum 800 kiezers. Deze opdeling wordt gemaakt om het stemmen en de telling te vereenvoudigen.

In elke gemeente wordt er een hoofdbureau geïnstalleerd. Dit hoofd(stem)bureau heeft een coördinerende rol bij de gemeenteraadsverkiezingen, zowel in de aanloop naar de verkiezingen als tijdens de verkiezingen.

Samenstelling:
- voorzitter
- eventueel plaatsvervangend voorzitter
- secretaris
- 4 bijzitters
- 4 plaatsvervangende bijzitters
- eventuele getuigen en plaatsvervangende getuigen

Opdrachten:
- toezien op de werkzaamheden van de stembureaus en de stemopnemingsbureaus
- verzamelen van gegevens van de stemopnemingsbureaus of van gegevensdragers van de stembureaus
- afkondigen van de stemuitslag
- aanvaarden van voordrachten

Voor elke stemafdeling wordt een stembureau ingericht. In een gemeente kunnen verschillende stembureaus worden opgericht. Een stembureau zorgt voor een vlot verloop van de kiesverrichtingen. In een stembureau komen de kiezers van de overeenkomstige stemafdeling hun stem uitbrengen.

Samenstelling:

- voorzitter
- eventueel plaatsvervangend voorzitter
- secretaris
- 4 bijzitters
- 4 plaatsvervangende bijzitters
- eventuele getuigen en plaatsvervangende getuige

In een gemeente kunnen verschillende stemopnemingsbureaus worden opgericht. Een stemopnemingsbureau telt de stemmen van maximum 2400 stemgerechtigden. De stemmen van verschillende stembureaus worden daartoe samengevoegd.

Samenstelling:
- voorzitter
- eventueel plaatsvervangend voorzitter
- secretaris
- 2 / 3 / 4 bijzitters (afhankelijk van het aantal te verkiezen raadsleden)
- 2 / 3 / 4 plaatsvervangende bijzitters (afhankelijk van het aantal te verkiezen raadsleden)
- eventuele getuigen en plaatsvervangende getuigen

In gemeenten waar er geautomatiseerd gestemd wordt, worden er geen stemopnemingsbureaus ingericht. De gegevensdragers met de stemmen worden direct door de stembureaus aan het hoofdbureau bezorgd.

4. Belangrijke data

Zaterdag… (3 maanden voor de verkiezingen)
- Start verkiezingscampagne

Dinsdag… (68 dagen voor de verkiezingen)
- Het schepencollege maakt lijst gemeenteraadskiezers op

Dinsdag… (begin 2e maand voor de verkiezingen)
- Het schepencollege maakt lijsten van voorzitters stem(opnemings)bureaus en (plaatsvervangende) bijzitters stem(opnemings)bureaus op

Zaterdag… (43 dagen voor de verkiezingen)
- Vaststelling en publicatie verboden letterwoorden door Vlaamse Regering

Dinsdag… (40 dagen voor de verkiezingen)
- Overhandiging voorstel tot lijstenvereniging aan Vlaamse Regering

Donderdag… (38 dagen voor de verkiezingen)
- Gemeentebestuur stuurt exemplaren lijst gemeenteraads- en provincieraadskiezers op aan gouverneur en vertegenwoordigers politieke partijen.

Zaterdag… (36 dagen voor de verkiezingen)

- Uiterste datum voor publicatie tabel lijstenverenigingen, letterwoorden en gemeenschappelijke volgnummers

Zondag... (35 dagen voor de verkiezingen)
- College stuurt kiezerslijsten, per stemafdeling aan voorzitter rechtbank van eerste aanleg

Dinsdag... (33 dagen voor de verkiezingen)
- In ontvangst nemen door voorzitter districtshoofdbureau en hoofdstembureau van voordrachten kandidaten en aanwijzingen getuigen – uiterste datum voor mededeling van plaats, dagen en uren.

Vrijdag... (30 dagen voor de verkiezingen)
- Uiterste datum voor aanduiding voorzitters stembureaus + opmaken en opsturen lijst door voorzitter kantonhoofdbureau

Zaterdag... (29 dagen voor de verkiezingen)
- Overhandiging akten van voordracht

Zondag... (28 dagen voor de verkiezingen)
- Overhandiging akten van voordracht + opsturen lijst aan gouverneur

Maandag... (27 dagen voor de verkiezingen)
- Samensteling districtshoofdbureau
- Ingediende voordrachten: inzage – formuleren schriftelijke opmerkingen
- Districtshoofdbureau sluit kandidatenlijst voorlopig af

Dinsdag...(26 dagen voor de verkiezingen)
- Indienen bezwaarschrift tegen aanvaarding van bepaalde kandidaturen bij voorzitter hoofdbureau + kennisgeving

Woensdag... (25 dagen voor de verkiezingen)
- Gemeentebestuur stuurt 2 exemplaren kiezerslijst aan gouverneur

Donderdag... (24 dagen voor de verkiezingen)
- Indienen memorie tot betwisting van onregelmatigheden inzage voorlopig afsluiten kandidatenlijst + indienen verbeteringsakte bij voorzitter hoofdbureau
- Districtshoofdbureau sluit kandidatenlijst definitief af
- Gouverneur geeft voorzitter districtshoofdbureau kennis van meervoudigekandidaatstelingen
- Voorzitter hoofdbureau stuurt definitieve kandidatenlijsten en nummer naar Vlaams minister van Binnenlands Bestuur

Maandag... (20 dagen voor de verkiezingen)
- Hof van beroep behandelt beroepen
- Verspreiding bericht van oproeping in de gemeente
- Districtshoofdbureau maakt stembiljet op en deelt officiële kandidatenlijst (PR) mee

Dinsdag... (19 dagen voor de verkiezingen)

- Voorzitter hoofdstembureau deelt de officiële kandidatenlijst (GR)
- Districtshoofdbureau deelt kandidatenlijsten (PR) mee in geval van beroep

Vrijdag… (16 dagen voor de verkiezingen)
- Voorzitter hof van beroep ontvangt processen-verbaal houdende verklaringen van beroep van voorzitters districtshoofdbureaus

Zaterdag… (15 dagen voor de verkiezingen)
- College stuurt oproepingsbrief aan elke kiezer + toezicht gouverneur
- Provinciegouverneur zendt 2 uittreksels kiezerslijst aan voorzitter kantonhoofdbureau
- Ten minste vijftien dagen vóór de verkiezing doet de Vlaamse Regering in het Belgisch Staatsblad een bericht verschijnen waarbij de dag van de stemming, de uren van opening en sluiting van de stembureaus meegedeeld worden. Dit bericht vermeldt eveneens dat voor elke kiezer bezwaar mogelijk is bij het gemeentebestuur tot twaalf dagen vóór de verkiezing
- College stuurt lijst van mogelijke (plaatsvervangende) bijzitters stembureaus aan voorzitter kantonhoofdbureau – doorsturen naar voorzitters stembureaus

Zondag… (14 dagen voor de verkiezingen)
- Voorzitter kantonhoofdbureau stuurt lijst voorzitters aan voorzitter districtshoofdbureau

Dinsdag… (12 dagen voor de verkiezingen)
- Voorzitters stembureaus duiden (plaatsvervangende) bijzitters stembureaus aan
- Uiterste datum voor indienen bezwaar tegen onjuiste vermeldingen op kiezerslijst bij college

Donderdag… (10 dagen voor de verkiezingen)
- Voorzitter stembureau informeert (plaatsvervangende) bijzitters over hun aanwijzing
- Voorzitter kantonhoofdbureau zendt definitieve lijst voorzitters aan elke voorzitter van de stemafdeling
- Overhandiging verklaringen van lijstenverbinding aan voorzitter districtshoofdbureau

Zaterdag… (8 dagen voor de verkiezingen)
- Voorzitter hoofdbureau verstrekt afschriften van lijst met leden kiesbureaus
- Uiterste datum waarop college uitspraak doet over elk bezwaar
- Aangewezen (plaatsvervangende) bijzitters geven voorzitter stembureau bericht in geval van verhindering

Dinsdag… (5 dagen voor de verkiezingen)
- Voorzitter kantonhoofdbureau wijst stembureaus aan waarvan stembiljetten door elk stemopnemingsbureau onderzocht worden
- Voorzitter hoofdstembureau neemt aanwijzing getuigen in ontvangst
- Voorzitter kantonhoofdbureau geeft kennis aan voorzitters en bijzitters stemopnemingsbureaus van de plaats van de vergadering

Donderdag… (3 dagen voor de verkiezingen)

- Uiterste datum voor aanvraag voor machtiging tot stemming indienen bij burgemeester
- Gemeente maakt stemapparatuur gebruiksklaar voor verkiezing
- Uiterste datum waarop de magnetische geheugendragers aan de voorzitters van de hoofdbureaus bezorgd worden

Vrijdag... (2 dagen voor de verkiezingen)
- Uiterste datum waarop de partijen die beroep instelden tegen beslissingen van het college voor het hof van beroep verschijnen
- Voorzitter hoofdstembureau zendt stembiljetten aan voorzitter van elke stemafdeling

Zaterdag... (1 dag voor de verkizingen)
- Voorzitter hoofdstembureau zendt stembiljetten aan voorzitter van elke stemafdeling
- Voorzitter hoofdbureau overhandigt aan elke voorzitter stembureau omslagen die hem betreffen

Zondag... (dag van de verkiezingen)
- Samenstelling stembureau
- Inzamelen verkiezingsresultaten

B. De Waalse gemeenten en de Waalse provincies.

In het Waalse Gewest, bestaat de gemeenteraad uit rechtstreeks lid in getal veranderlijk in functie van het aantal inwoners van de gemeente (van 7 leden in de gemeenten beneden 1.000 inwoners tot 55 leden in die van 300.000 inwoners en daarboven).

In de Waalse provincies, bestaan de provincieraden uit:

- 56 leden – Provincie Waalse Brabant
- 84 leden – Provincie Henegouwen
- 84 leden – Provincie Luik
- 56 leden – Provincie Luxemburg
- 56 leden – Provincie Namen

<u>OCMW raad van Komen-Waasten.</u>

De leden van de OCMW-raad van Komen-Waasten worden per rechtstreekse verkiezing benoemd.

C. De Brusselse Gemeenten.

De Brusselse Gemeenteraden bestaan uit:

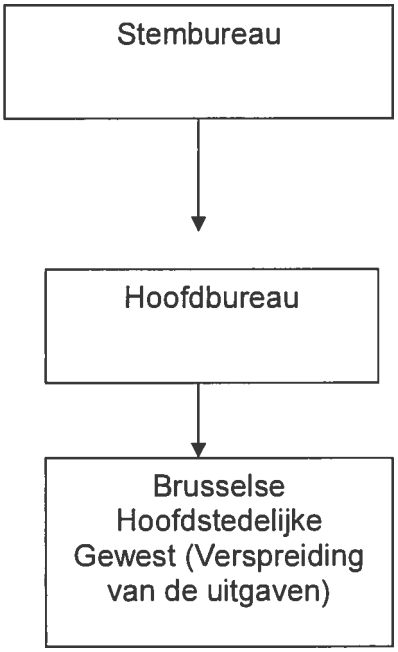
Anderlecht	45
Oudergem	29
Sint-Agathe-Berchem	27
Brussel	47
Etterbeek	35
Evere	31
Vorst	35
Ganshoren	27
Elsene	41
Jette	35
Koekelberg	25
Sint-Jans-Molenbeek	41
Sint-Gillis	35
Sint-Joost-ten-Noode	27
Schaerbeek	47
Ukkel	41
Watermaal-Bosvoorde	27
Sint-Lambrechts-Woluwe	35
Sint-Pieters-Woluwe	33

De kiesbureaus.

In elke gemeente, is er een hoofdbureau dat de voorbereidende verrichtingen, de totalisatie van de stemmen, de verdeling van de zetels, de aanduiding van de parlementslid en de overdracht van de resultaten van de stembureaus naar het Brusselse Hoofdstedelijke Gewest uitvoert.
De stembureaus zijn de kantoren die in elke gemeente worden geplaatst, waar de burgers hun stem uitbrengen (ongeveer 700 stembureaus op het heel grondgebied van het Brusselse Hoofdstedelijke Gewest).

In het Brusselse Hoofdstedelijke Gewest, waar de gemeenteverkiezingen volledig worden geautomatiseerd, zijn er geen stemopnemingsbureaus.

Per gemeente :



Belangrijke kiesdata

Vrijdag ... (44ste dag vóór de verkiezing)
Op deze datum maakt de Regering de verboden letterwoorden bekend in het Belgisch Staatsblad (BGKWB, artikel 23, §1, vijfde tot negende lid). Daar de 43ste dag voorafgaand aan de verkiezing een zaterdag is en bijgevolg een dag is waarop het Belgisch Staatsblad niet verschijnt, zal er de eerste werkdag vóór de 43ste dag gepubliceerd worden.

Donderdag ... (38ste dag vóór de verkiezing)
Uiterste datum waarop het gemeentebestuur twee exemplaren van de lijst van de gemeenteraadskiezers zendt naar de gouverneur van het administratief arrondissement Brussel-Hoofdstad of zijn gemachtigde (BGKWB, artikel 5, eerste en tweede lid). Terzelfder tijd zendt het gemeentebestuur eveneens twee exemplaren van de kiezerslijst naar de Regering (BGKWB, artikel 5, derde lid).

Zondag ... (35ste dag vóór de verkiezing)
Uiterste datum waarop het college van burgemeester en schepenen tegen ontvangstbewijs of in een ter post aangetekende omslag twee voor echt verklaarde uittreksels uit de lijst der kiezers, opgemaakt per stemafdeling, dient te verzenden naar de voorzitter van de rechtbank van eerste aanleg, of, indien in de gemeente geen rechtbank is gevestigd, aan de vrederechter van het kanton (BGKWB, artikel 9, eerste lid).

Zaterdag ... (29ste dag vóór de verkiezing)
Tussen 13 en 16 uur worden de voordrachten van de kandidaten in ontvangst genomen door de voorzitter van het hoofdstembureau (BGKWB, artikel 22,eerste lid).

Zondag ... (28ste dag vóór de verkiezing)

1) Tussen 13 en 16 uur : uiterste tijdstip om de voordrachten van de kandidaten en de verklaringen van bewilliging van hun kandidatuur ter hand te stellen aan de voorzitter van het hoofdstembureau (GKWB, artikel 22, eerste lid en 23, §1, elfde lid).
2) Tussen 13 en 18 uur mogen kandidaten en kiezers die de voordrachten van kandidaten hebben ingeleverd inzage nemen van alle ingediende voordrachten en schriftelijk hun opmerkingen aan het hoofdbureau meedelen (BGKWB, artikel 26, § 1, tweede lid).

Dinsdag ... (26ste dag vóór de verkiezing)
Tussen 13 en 15 uur : indiening van met redenen omklede bezwaarschriften tegen de aanvaarding van bepaalde kandidaturen door zij die de aanvaarde of afgewezen lijsten hebben ingeleverd (of bij hun ontstentenis, een van de erop voorkomende kandidaten), op de plaats aangewezen voor het inleveren van de voordrachten (BGKWB, artikel 26ter, eerste lid). De voorzitter geeft aan de kiezer of kandidaat die de betwiste voordracht heeft ingeleverd, onmiddellijk bij aangetekende brief kennis van het bezwaar, onder vermelding van de aangevoerde redenen (BGKWB, artikel 26ter, tweede lid).

Donderdag ...(24ste dag vóór de verkiezing)
1) Tussen 14 en 16 uur kunnen zij die de aanvaarde of afgewezen lijsten hebben ingeleverd (of een van de erop voorkomende kandidaten) op de plaats aangewezen voor het inleveren van de voordrachten bij de voorzitter van het hoofdbureau tegen ontvangstbewijs een memorie indienen tot betwisting van de onregelmatigheden waarmee bij het voorlopig afsluiten van de kandidatenlijst rekening is gehouden of die de dag na die aansluiting ingeroepen zijn. Wanneer de onregelmatigheid gelegen is in onverkiesbaarheid van een kandidaat, kan een memorie worden ingediend met inachtneming van dezelfde regels (BGKWB, artikel 26quinquies, eerste lid).
In voorkomend geval kunnen bovenvermelde personen een verbeterings- of aanvullingsakte indienen wanneer de voordracht afgewezen is om een van de redenen bedoeld in artikel 26quinquiès, derde lid (BGKWB, artikel 26quinquies, derde lid).
2) Om 16 uur : vergadering van het hoofdbureau, dat de kandidatenlijst definitief afsluit na onderzoek van de stukken die de voorzitter conform de artikelen 26ter, 26quater en 26quiquies van het Brussels Gemeentelijk Kieswetboek ontvangen heeft en na terzake beslist te hebben (BGKWB, artikel 26sexies, eerste en tweede lid). Eventueel, bij verwerping van een kandidatuur wegens onverkiesbaarheid van een kandidaat of bij afwijzing van een bezwaar gegrond op de onverkiesbaarheid van een kandidaat, verzoekt de voorzitter naargelang het geval respectievelijk de kandidaat (of
zijn gemachtigde) of de indiener van het bezwaar (of zijn gemachtigde) op het proces-verbaal een verklaring van beroep te ondertekenen (BGKWB, artikel 26septies).
3) Opeenvolgende lotingen (volledige en onvolledige lijsten) voor de lijsten die geen gemeenschappelijk volgnummer bekwamen ; de kandidatenlijst wordt aangeplakt in dezelfde vorm als het stembiljet met vermelding van de onderrichtingen aan de kiezers en de lijstnummering (BGKWB, artikel 30, zevende lid).
4) In geval van beroep verdaagt het hoofdbureau de om 16 uur geplande verrichtingen

Vrijdag ...(23ste dag vóór de verkiezing)
IN GEVAL VAN BEROEP :
Tussen 11 en 13 uur houdt de voorzitter van het hof van beroep zich in zijn kabinet ter beschikking van de voorzitters van de hoofdbureaus van zijn rechtsgebied om er uit hun handen een uitgifte te ontvangen van de processen-verbaal houdende de verklaringen van

beroep, alsmede alle stukken betreffende de geschillen waarvan de hoofdbureaus kennis hebben gehad.
Bijgestaan door zijn griffier, maakt hij van deze overhandiging akte op. (BGKWB, artikel 26octies en KWB, artikel 125bis).

Maandag ...(20ste dag vóór de verkiezing)
1) Uiterste datum waarop het gemeentebestuur een bericht van oproeping ter openbare kennis dient te brengen in de vorm van een aanplakbiljet (BGKWB, artikel 21, laatste lid)
2) Om 10 uur, zelfs indien die dag een feestdag is, worden de beroepen tegen de afwijzing van een kandidatuur door het hoofdbureau wegens onverkiesbaarheid van een kandidaat of tegen de afwijzing van een bezwaar gegrond op de onverkiesbaarheid van een kandidaat zonder oproeping of dagvaarding voor de eerste kamer van het Hof van Beroep van het rechtsgebied gebracht (BGKWB, artikel 26octies en KWB, artikel 125, derde lid en 125ter, eerste lid). Het beschikkend gedeelte van het arrest wordt telegrafisch ter kennis van de voorzitter van het hoofdbureau gebracht (KWB, artikel 125ter, vijfde lid).
Het dossier van het hof wordt, met een uitgifte van het arrest, binnen acht dagen toegezonden aan de griffier van de vergadering die belast is met het onderzoek van de geloofsbrieven der gekozenen (BGKWB, artikel 26, § 3 en KWB, artikel 125ter, zesde lid)
3) Om 18 uur vergadert het hoofdbureau om te kunnen overgaan tot de verrichtingen bepaald in de artikelen 28 tot 30 zodra het in kennis is gesteld van de beslissingen van het Hof van Beroep (BGKWB, artikel 30ter).
4) Zodra het bureau kennis heeft genomen van de beslissing van het Hof van Beroep stuurt de voorzitter van het hoofdbureau de definitieve kandidatenlijsten en het hun toegekende nummer door aan de daartoe door het MB■G aangewezen ambtenaar.
Deze informatiegegevens kunnen op magnetische drager worden verstuurd voor zover zij echt verklaard zijn (WAS, artikel 17, §1, eerste en tweede lid)

Zaterdag ...(15de dag vóór de verkiezing)
1) Uiterste datum waarop het college van burgemeester en schepenen een oproepingsbrief en een verklarende brochure dient te zenden aan elke kiezer, aan de verblijfplaats die hij op dat ogenblik heeft. (BGKWB, artikel 21, eerste lid).
2) Uiterste datum waarop de Regering een bericht doet verschijnen waarbij de dag van de stemming, de uren van opening en sluiting van de stembureaus meegedeeld wordt. Dit bericht vermeldt eveneens dat voor elke kiezer bezwaar mogelijk is bij het gemeentebestuur tot twaalf dagen vóór de verkiezing (KWB, artikel 107, eerste en tweede lid).
3) De voorzitter van het hoofdbureau verstrekt afschriften van de lijst met de leden van de kiesbureaus van de gemeente aan ieder die er uiterlijk op die datum om verzocht heeft (BGKWB, artikel 17, tweede lid).
4) Datum waarop de kiezer, die afwezig isvan zijn woonplaats omwille van een tijdelijk verblijf in het buitenland en zich bijgevolg in de onmogelijkheid bevindt om zich in het stembureau te melden, een aanvraag moet indienen bij de burgemeester van zijn woonplaats (BKKWB, artikel 42bis, §1, 7°).

Dinsdag ...(12de dag vóór de verkiezing)
1) Uiterste datum waarop elke kiezer de kiezerslijst moet kunnen raadplegen bij de gemeentesecretarie tijdens de diensturen (BGKWB, artikel 3, § 3).
2) Uiterste datum waarop elke kiezer bij het college van burgemeester en schepenen bezwaar kan indienen in verband met de kiezerslijst (BGKWB, artikel 3bis, §§ 1 en 2).

3) Uiterste datum waarop de voorzitter van het stembureau de bijzitters en de plaatsvervangende bijzitters dient aan te wijzen uit de jongste kiezers van de stemafdeling die op de dag van de stemming ten minste dertig jaar oude zijn en kunnen lezen en schrijven. Hij geeft de voorzitter van het hoofdbureau van de gemeente meteen kennis van de aldus gedane aanwijzingen (BGKWB, artikel 14, § 2, en KWB, artikel 95, § 9).

Dinsdag ... (5de dag vóór de verkiezing)
1) Tussen 14 en 16 uur neemt de voorzitter van het hoofdstembureau de aanwijzingen van getuigen in ontvangst. De kandidaten kunnen zoveel getuigen en zoveel plaatsvervangende getuigen aanwijzen als er stembureaus zijn (BGKWB, artikel 22, tweede lid en artikel 25, eerste lid).
2) Onmiddellijk na het verstrijken van de termijn die voor het in ontvangst nemen van de getuigenaanwijzingen is gesteld en ongeacht het aantal aanwezige leden, weert het hoofdstembureau de boventallige getuigen door middel van lotingen (BGKWB, artikel 25, zevende lid).

Zondag ...(Dag van de verkiezing)
Tot op die dag zenden de gemeentebesturen de lijst van de personen die geschrapt dienen te worden van de kiezerslijst, rechtstreeks aan de voorzitters van de stembureaus zodra die zijn aangewezen (BGKWB, artikel 9, derde lid).

SJ20130213142122406

Dokumentresumé:

Bestilt af : DEPCLH den 13-02-2013 15:21:21
Dokumentnr.: 4925
Titel: Annexe C_bevoting-2_gb
Dokumenttype: I
Dokumentdato:
Kontor/enhed: VALG-ENH, Valgenheden
Sagsmedarb.: Nicoline Nyholm Miller, DEPNNM
Indblik:
Versionsnr.: 1
Reg.dato: 10-09-2012
Registreret af: DEPNNM - Nicoline Nyholm Miller

Emneord:

Tekst:

Modtagere:

Oplysninger:

Datoer:

Erindringer:

BeVoting

Study of Electronic Voting Systems

Part II of the "Studie Geautomatiseerde Stemming Def. Vs 18122006"

Version 1.02

4 December 2007

1 Executive Summary

1.1 Scope of the Study

The Federal and Regional Administrations have requested an independent comparative study of the election systems used abroad and a formulation for the requirements for the voting systems that will be used in Belgium for the elections of 2009 and later. The independent study is executed by a Study Consortium that consists of the following universities: Katholieke Universiteit Leuven, Universiteit Antwerpen, Universiteit Gent, Université catholique de Louvain, Université de Liège, Université Libre de Bruxelles and Vrije Universiteit Brussel.

The Study consists of two parts. The goal of the first part is to present the current state of the art of electronic and Internet voting systems in all their aspects. The state of the art is summarized in a table listing the systems used in various countries, the number of eligible voters, the electoral system, their pros and cons, and the system costs. The first part of the study also evaluates all aspects of the Belgian electoral system, including optical reading of voting ballots, partial electronic voting, and the traditional voting system based on paper ballots.

The goal of the second part of the Study is to propose technical and specific requirements for a new automated voting system for Belgium. The level of detail asked for needs to be such that the report may serve as a technical appendix to the call for tenders for the voting system for the elections of 2009 and later. The system specified in the second part of the Study needs to be compatible with the Belgian and Regional electoral systems.

The English versions 1.0 of the reports for the first and second parts of the Study were formally delivered to the Administrations on 15 April and 12 October 2007, respectively. Version 1.02 of this report was formally delivered to the Administration on 4 December 2007. Annex 13 includes the signatures of the professors who participated in Study Consortium.

Dutch and French versions of this report are also available. The English version of this report rules if inconsistencies should exist in these translations.

1.2 Overview of this Report (Part II of the Study)

The Consortium studied five different eVoting systems. Advantages and drawbacks of each system are presented. It should be kept in mind that the Council of Europe recommends a progressive introduction of eVoting systems to generate trust and confidence among citizens in the use of electronic means for voting systems. This means that one specific system may serve as a preparation step for another. An abstract view on voting systems is given in Figure 1. A voter either marks his[1] vote manually on a paper ballot or by means of a voting machine. The result is a human readable ballot, an encoded ballot, or a combination of both. The ballots may be counted by hand or by machine. They can be processed immediately after the ballot is cast, or at the end of the voting period on Election Day.

In theory, there exist voting systems which correspond with each possible path between the "Voter marks by hand/machine" boxes and the processing boxes but, in

[1] In the remainder of this report, we shall henceforth only use the masculine form in order to simplify the text; it should be clear, however, that we do not discriminate between women and men voters.

practice, only a subset of the paths result in realistic and implementable voting solutions.

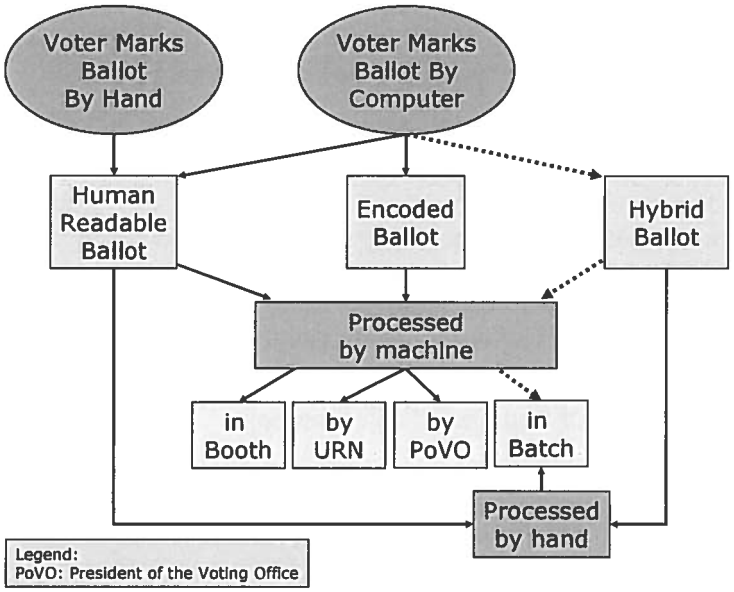


Figure 1: Conceptual View on Voting Systems

The **first** system that is presented in this report is the one preferred by the Consortium (cf. the dotted red line in the above picture). The proposed system is an **improved paper-based voting system** with which the voter casts his vote using a voting computer. The voting computer prints this vote on a paper ballot and represents it also in an encrypted form on a machine readable part of the ballot, namely a barcode or an RFID chip. After the vote is printed, the voter verifies that the printed vote is indeed the vote he has cast with the voting computer. The voter then closes the voting ballot by folding it so that only the machine readable part of the ballot remains visible, or by inserting it in an envelope. In either case, the voter presents it to the president of the voting office to have it inspected for visual marks, after which the voter deposits the ballot into the voting urn of the voting office.

The **second** system is based on paper ballots using **direct optical scanning** to accelerate the tallying of the votes and improve its accuracy.

The **third** system, in this study called the "**thin-client system**", introduces the use of electronic voting machines connected to a local server using a (local and secure) network and with the possibility to produce a paper trail. The paper trail serves to allow the voter to verify the content of his vote. No manipulation of the paper trail by the voter is allowed.

The **fourth** system consists of an **Internet/remote voting system**. This system is the electronic equivalent of postal voting inasmuch as voters can cast their votes from their home, i.e., from an unsupervised environment. This system is foreseen to be used by Belgian citizens living abroad.

Finally, the **fifth** system which has been taken into consideration .is a variant of the remote voting system and consists of the so-called "**kiosk voting**" where the voter casts his vote in a supervised environment (in a polling booth located either at the polling station or in an official building) through electronic voting machines connected to a broader secure network (in this case, national).

The direct optical scan systems are the only systems described in this document with

manual vote casting. The direct optical scanning process needed for counting votes typically requires human interaction. Several of these systems are described in this document; one of them assumes that the voters are themselves responsible for the scanning of their vote. In this variant, paper ballots are transformed immediately into electronic votes and vote counting is done on the electronic votes.

The properties of this variant are, in fact, very similar to the thin client system (third system), where the votes are cast electronically and printed onto paper trails.

The improved paper-based ballots system (first system) has computer based vote casting, but prints out the votes on a paper ballot that serves as a paper trail. The counting is done by reading the machine readable representation of the ballot. This is a manual process aided by automated ballot reading. The ballots are read in batch near the voting offices where they were cast at the end of Election Day.

The thin client system, the kiosk voting and the remote voting system have computer based vote casting and fully automated vote counting.

Many of the remarks made in this report apply equally well to several of the systems, because they only depend on the fact that votes are counted automatically, rather than on the exact counting method being employed.

We now walk through the main steps of the election process and summarize briefly the pros and cons of the different proposals. These remarks are elaborated upon in the following sections:

1. Vote casting

The voter casts his vote, either directly on paper or by using an input/output device connected to a computer. If the vote casting is done by computer, the ballots can be digital. In that case, measures need to be taken to convince the voter that his vote has been entered correctly into the system. One way to achieve this is to produce a paper trail: a paper trail is a copy of the votes that have been cast. This may also be desirable for auditing purposes.

A kiosk voting system, in its basic version, produces no paper trail. Paper trail functionality could easily be added, however. Enforcing the production of a paper copy of the votes is impossible for the remote voting system, since this would require a printer at each voting place, and it may encourage vote selling. This is furthermore not in conformity with the Recommendations of the Council of Europe. The comment on norms 51 and 52 of the Explanatory Report expressly states that in remote e-voting systems based on web applications, in order to protect the secrecy and the anonymity of the vote, the printing, saving and storing functions must be blocked. The same comment states that any possibility of printing, recording or storing of the vote should be banned and technically blocked.

Two systems for the handling of paper ballots are being proposed in this report. In the thin-client system, the paper trails are printed behind a glass window (to prevent physical access to the trails). After visual inspection of the paper trail, the voter presses a button which releases the ballot into a voting urn. Each voting booth is thus equipped with such an urn. In other systems, the printed ballot is taken by the voter and deposited into the urn of the voting office, much in the same way as what is done for traditional manual voting and the classic electronic voting with the magnetic stripe cards. These systems have the disadvantage that voters can leave extraneous marks on the paper ballots and hence invalidate the paper ballots.

2. Vote collecting

The issue here is to ensure the principle of "One person, one vote."

The paper ballot used in manual vote casting makes it relatively easy to ensure that each person votes exactly once: people get one ballot and after marking it, they need to deposit that same ballot in the urn of their voting office under supervision of the voting officers. If the votes are cast using machines, then special measures are required in order to ensure that each person votes no less and no more than one time. *This issue can not be disposed of merely by using electronic means.*

3. Vote counting

The issue here is to ensure that people trust the vote counting process. If the vote counting is fully automated, then one needs to trust the machines and their software (as in the thin client system) or the cryptography (as in the kiosk system and remote voting system). This is sometimes perceived as a disadvantage. On the other hand, fully automated vote counting is very fast, requires only modest investments in hardware, and almost no personnel.

The kiosk voting system and the remote voting system as described further on allow voters to verify that their vote has been included in the final count.

It should be stressed that the conclusion of the Consortium is that, with existing technologies and taking into account both the cost and the advantages and drawbacks of the various solutions which were examined, a fully automated eVoting system is currently not appropriate for Belgium. This is why the proposed solution is an improved paper ballot-based system in which only the casting, reading and counting of the votes is computerized.

2 Contributors to this Document

- Final editor:
  - Danny De Cock (K.U.Leuven)
- Main input contributors (alphabetical order):
  - Technical & Organizational aspects:
    - Antoon Bosselaers (K.U.Leuven)
    - Danny De Cock (K.U.Leuven)
    - Elie Milgrom (UCL)
    - Vincent Rijmen (K.U.Leuven)
  - Legal aspects:
    - Fanny Coudert (K.U.Leuven)
  - Usability & Accessibility aspects:
    - Jan Engelen (K.U.Leuven)
- Other contributors (alphabetical order):
  - Technical & Organizational aspects:
    - Olivier de Marneffe (UCL)
    - Francois Koeune (UCL)
    - Marc Lobelle (UCL)
    - Olivier Pereira (UCL)
    - Bart Preneel (K.U.Leuven)
    - Jean-Jacques Quisquater (UCL)
    - Frederik Vercauteren (K.U.Leuven)

3 Table of Contents

1 Executive Summary 2
1.1 Scope of the Study 2
1.2 Overview of this Report (Part II of the Study) 2
2 Contributors to this Document 6
3 Table of Contents 7
4 Requirements for the second part of the Study 10
4.1 Delivery date 10
4.2 Propose technical and specific norms to compose a specific tender to realize the electronic voting system or of a remote electronic voting system suitable for the Belgian electoral system 10
4.3 Partitioning key to finance the new electronic voting system by the different administrations 10
4.4 Specific criteria for the new voting system 10
4.4.1 Controllable security and integrity of the Elections 10
4.4.2 Guaranteed secrecy of the Vote 10
4.4.3 Usability in Belgium 11
4.4.4 Practical installation in voting offices 12
4.4.5 Promote automating the ballot processing, as opposed to automating casting the vote 12
4.4.6 Verifiability of the system 12
4.4.7 Costs per system 12
4.4.8 Ease of use (user-friendliness, simplicity) 13
4.4.9 Availability (immediate availability in case of advanced elections) 13
4.4.10 Modularity (e.g., 1 canton = 5 municipalities, of which 4 use electronic voting and 1 traditional voting) 13
4.4.11 Open to evolutions and adaptability 13
4.4.12 Storage (volume, space, costs…) 14
4.4.13 Stimulate the willingness of the weakest voter to participate in the voting process (elderly, socially vulnerable voters…) 14
4.4.14 Life cycle of the system 15
5 Specification of the Improved Paper-based Voting System 16
5.1 Terminology & Conventions 21
5.2 High-level description 22
5.2.1 Voter-view on the Voting Procedure with Barcode Ballots 22
5.2.2 Voter-view on the Voting Procedure with RFID Ballots 24
5.2.3 From a Voting Ballot to the Final Election Result 25
5.2.4 Computer Equipment 27
5.3 Basic components of the proposed improved paper-based voting system 41
5.3.1 Boot Credential for the voting computers 41
5.3.2 Voting Token for the voter 42
5.3.3 Paper ballot for the voter 42
5.4 Voting Urn 44
5.5 Verfiying the validity of the ballots 45
5.6 Procedure Details 45
5.6.1 Before Election Day 46
5.6.2 Close to Election Day 53
5.6.3 Start of Election Day 55
5.6.4 End of the voting period on Election Day 56

5.6.5 After the Election Day 58
5.7 Legal Compliance of the Improved Paper-based Voting System 58
5.7.1 Legal Situation of the Voting Ballots 58
5.7.2 The 112 Recommendations of the Council of Europe 60
6 Direct optical scan of voting ballots 72
6.1 Reasons why the consortium did not propose this type of system 72
6.2 Initial remarks 72
6.3 A family of systems 73
6.3.1 Scope 73
6.3.2 Concepts and Terminology 74
6.4 Options and Choices for Direct Optical Scan-based Voting Systems 75
6.4.1 Types of Ballots 75
6.4.2 Where and When to Scan 77
6.4.3 Where and When to Count 79
6.4.4 What to do with the Images of the Scanned Ballots? 79
6.5 Specific Requirements – Hardware, Software, Procedures 79
6.6 Advantages and Drawbacks of Direct Optical Scan Voting Systems 80
6.6.1 Advantages 80
6.6.2 Drawbacks 80
6.6.3 Additional Remarks 81
6.7 Analysis of the Scenarios 81
6.7.1 Hybrid Ballots (Paper-based and Electronic) 82
6.7.2 Storage of the votes in the Machine Manipulated by the Voter 82
6.7.3 Multiple scanning 82
6.7.4 Numbering of Candidates 83
6.8 Compliance of Direct Optical Scan Voting Systems with the CoE Recommendations 83
6.8.1 Legal Standards 83
6.8.2 Operational Standards 86
7 Thin clients e-voting system 89
7.1 Reasons why the consortium did not select this type of voting system 89
7.2 Description 89
7.3 Advantages and disadvantages 90
7.4 Compliance of Thin Clients Voting System with the CoE Recommendations 92
7.4.1 Legal Standards 92
7.4.2 Operational Standards 95
8 Remote/Internet voting based on homomorphic encryption 98
8.1 Reasons why the consortium did not select this type of voting system 98
8.2 Introduction 98
8.3 Functional overview of the remote voting architecture 99
8.3.1 The setup phase 99
8.3.2 Voting phase 100
8.3.3 Tabulation phase 101
8.4 Block Overview of the Remote Voting Architecture 101
8.4.1 Remote voting server architecture 102
8.4.2 Client architecture 104
8.4.3 Remote voting software modules common to client and server 105
8.5 Compliance of Internet/Remote Electronic Voting with the CoE Recommendations 107
8.5.1 Universal Suffrage 108
8.5.2 Equal Suffrage 109
8.5.3 Free Suffrage 109

8.5.4 Secret Suffrage 110
8.5.5 Procedural Safeguards 110
8.5.6 Recommendations of the Council of Europe 111
9 Kiosk voting based on homomorphic encryption 117
9.1 Reasons why the consortium did not select this type of voting system 117
9.2 Description 117
9.3 Compliance of Kiosk Voting with the CoE Recommendations 118
9.3.1 Legal Standards 118
9.3.2 Operational Standards 121
10 Observations of Legal Nature 124
10.1 Introduction 124
10.2 Recommendations of the Council of Europe on eVoting Systems and its Current Implementation in the Belgian System 124
10.2.1 Universal Suffrage 125
10.2.2 Equal Suffrage 127
10.2.3 Free Suffrage 129
10.2.4 Secret Suffrage 130
10.2.5 Procedural Safeguards 132
10.2.6 Verifiability and Accountability 134
10.2.7 Reliability and Security 135
11 General requirements for e-voting systems 137
11.1 Global 137
11.2 Hardware 137
11.3 Software 137
11.4 Communications 140
11.4.1 Physical transportation 140
11.4.2 Telecommunication networks 140
11.5 Organization and procedures 141
12 Annex – Voting Ballots with Different Font Sizes 142

4 Requirements for the second part of the Study

This section contains the checklist for the Study's output requirements as specified in the contract with the Administration.

4.1 Delivery date

The contract specifies 1 September 2007. The title page of this report mentions the date this Study Report has been formally submitted to the Administration.

4.2 Propose technical and specific norms to compose a specific tender to realize the electronic voting system or of a remote electronic voting system suitable for the Belgian electoral system

Section 0 includes a detailed technical description and specific norms of the proposed improved paper-based voting system. This section can be included in the call for tenders as the specification of the new electronic voting system.

4.3 Partitioning key to finance the new electronic voting system by the different administrations

The Consortium proposes to partition the costs for the new electronic voting system in a proportional manner between the Federal and Regional Administrations.

4.4 Specific criteria for the new voting system

4.4.1 Controllable security and integrity of the Elections

The proposed improved paper-based voting system

- provides a paper trail which allows the voter to confirm that the voting computer correctly registered the voter's choice;
- allows the auditing of the complete election by verifying that the paper trails correspond with the machine readable representation of the voter's choice. Moreover, the audit does not need to be exhaustive: checking randomly a small percentage of the ballots is sufficient to ensure a high level of reliability;
- stipulates that the election software of the voting computers is distributed to the presidents of the voting offices before the Election Day and is subject to strict access control procedures. Only authorized people are able to start the voting software on the voting computers. This is explained in more detail in Section 5.6.3.

4.4.2 Guaranteed secrecy of the Vote

The proposed improved paper-based voting system

- consists of voting computers that print out a ballot that serves as paper trail with the voter's choice;
- makes it impossible for the voting computer to link the identity of a voter to a

particular ballot;

- requires that the ballots are mixed before being read, which breaks the chronological order of the ballots that might exist, as voters cast their ballot in a sequential order.

4.4.3 Usability in Belgium

The architecture of the proposed electronic voting system is closely related to the currently used electronic voting system:

- each voting booth is equipped with a voting computer;
- the voter receives a voting token from the president of the voting office after he has been successfully verified to be an eligible voter;
- the voter marks the parties and candidates of his choice on a computer screen.

What happens next is different from what happens in the magnetic stripe card-based electronic voting system and is similar to what happens in the traditional paper based voting:

- the voter checks the ballot to confirm that it represents his choice;
- the voter protects the secrecy of his choice (by folding the human readable printout of his choice like a booklet, or by inserting the ballot in an envelope);
- the voter presents the voting ballot to the president of the voting office to confirm that it does not contain any visible marks;
- the voter inserts the voting ballot in the voting urn;
- at the end of Election Day, the voting urns are emptied, and their content mixed, before the ballots are read.

The production of election results is also very similar to the totalization mechanism of the classic electronic voting system, which makes that the exact same totalization procedures as for the classic electronic voting system can be used.

The Belgian territory is subdivided into disjoint sections that are relevant to the election type. The exact mapping of these sections varies depending on the type of elections (European, Federal, Provincial, Regional, Local, etc.), and is outside the scope of this document.

The proposed electronic voting system therefore introduces more abstract concepts based on Totalization Centers that gather and process partial election results. The number of Totalization Centers is not fixed, but it is assumed that there will be at least three totalization centers (First, Second, Final): the first Totalization Center is situated at municipality level, where the Second, possibly Third, Fourth, etc., are situated at higher levels. The Final Totalization Center is situated at national level. Voting ballots are read at the end of Election Day by Ballot Reading Centers, and are decrypted by Ballot Decryption Centers (cf. below), before they are added to the municipality's score. The Ballot Reading Centers can be located at each voting office, or they may be located in the neighborhood of a set of voting offices to which location the voting urns have to be transported at the end of Election Day. The exact definition and roles of these Totalization Centers is discussed in detail in Section 5.1.

The proposed improved paper-based voting system significantly differs from the paper trail systems that have been tested in the past in Belgium and that proved unusable: the "paper trail" in the proposed voting system is not an add-on, but serves

as the record of the voter's cast votes, i.e. as a voting ballot. The paper trail in the proposed system directly results from the voter's actions using the voting computer. The voter hides the human readable text with the voter's choice of the ballot, after which the ballot is inspected for marks by the president of the voting office; the voter eventually deposits the ballot in the voting urn.

4.4.4 Practical installation in voting offices

Section 5.2.4.2 describes how the voting computers are to be installed in the voting offices.

4.4.5 Promote automating the ballot processing, as opposed to automating casting the vote

The voting computers of the proposed improved paper-based voting system produce, based on the choices specified by the voter, paper ballots which consist of a machine readable and a human readable part, both representing the voter's choice.

At the end of the voting period on Election Day, the voting urns are transported form the voting offices to the Ballot Reading Center to which they have been associated, where the voting urns are emptied and their content mixed, and the machine readable part of each of the ballots that contains encrypted information is read. Once the ballots have been read, this information is digitally signed with the eID card of the president of the Ballot Reading Center, and transferred in its digital form to the Ballot Decryption Center for further processing. All information sent from the Ballot Decryption Center to the First Totalization Center and from one Totalization Center to another is transmitted electronically using a communication channel which protects the integrity of the transferred information. Specifying which transport medium to use for this transmission is beyond the scope of this document. Such transmission must obviously protect the integrity of the transferred information to avoid modifications of the election results while in transit.

4.4.6 Verifiability of the system

The proposed improved paper-based voting system ensures that:

- The elections are fully auditable, because the paper voting ballots consist of two parts: a human readable part and a machine readable part. Independent auditors can select randomly chosen voting ballots to confirm that the machine readable part of these random samples truly corresponds with the human readable text with the voter's choice;
- The software installed on the computers that are used in the voting offices, ballot reading centers, ballot decryption centers, and totalization centers is open source and publicly available;
- The procedures to initialize and operate the voting computers are published;
- The certification of the software is monitored by duly vetted members of the Administration and auditors.

4.4.7 Costs per system

Price quotations are included where relevant and readily available. These quotations are mentioned exclusive VAT, and refer to small quantities.

4.4.8 Ease of use (user-friendliness, simplicity)

The modus operandi of the voting process does not significantly change compared to the currently used electronic voting system. This implies that the vast majority of the voters will not experience much difficulty transitioning to the proposed improved paper-based voting system. Skeptic users of traditional paper ballot voting will be encouraged to switch to the improved paper-based voting system because of the increased transparency of the electronic voting process.

The user interface of the voting computer also pays attention to the usability of the voting computer by visually impaired people:

- The voting computer is equipped with an **audio output** that can be used to connect ear phones through which the visually impaired and blind people can listen to the information displayed by the voting computer;
- The display of the voting computer can be visualized with a **Braille reader** and **corresponding input device** to allow the voter to walk through the election process at his own pace following a logical menu or tree structure: select election type (provincial, European, etc.), select preferred party, select preferred candidate(s), confirm vote, proceed with next election, etc.; the resulting voting ballot is the same as for other voters.
- The voting computer can use a **specific screen layout** to accommodate the needs of people with poor eyesight.

4.4.9 Availability (immediate availability in case of advanced elections)

There are no special requirements for the deployment of the proposed improved paper-based voting system.

4.4.10 Modularity (e.g., 1 canton = 5 municipalities, of which 4 use electronic voting and 1 traditional voting)

Each municipality can choose to use its preferred voting system. A municipality which decides to use the traditional paper voting mechanism will then simply count the paper ballots by hand. The output of this manual counting is transferred to the First Totalization Center which will totalize the results of this municipality with the results of the other municipalities (if any) within its scope.

4.4.11 Open to evolutions and adaptability

The proposed electronic voting system is open to evolutions:

- The voting software is designed so that it does not depend on the elections themselves: the configuration files of the voting software specify which type of elections, which parties and which candidates will be voted for. If new election types have to be introduced, the voting software may have to be updated accordingly. The procedures to design, validate, test, certify and install this software are specified in this document;
- The issuers of the CDs used to boot the computers of the voting offices, Ballot Reading Centers, Decryption Centers and Totalization Centers can fine-tune which computers may be used in which area. Assume that the citizens living in one municipality would be allowed to cast their vote in another municipality.

In that case, the issuer of the CDs used to boot the voting computers needs then simply to create a configuration file on that CD that contains the information of both municipalities. The citizen voting in the alien municipality would then be given a specific voting token that instructs the voting computer to show the correct election information for this voter. An outside observer will not be able to distinguish the alien's paper ballot from the paper ballot of the native citizens. The Ballot Reading Center will read the machine readable part of the alien's voting ballot in the same manner as all the other ballots. The Ballot Decryption Center will make sure that the alien ballot will contribute to the partial election result of the alien's municipality.

4.4.12 Storage (volume, space, costs...)

The storage requirements for the hardware necessary for the proposed improved paper-based voting system are smaller than those for the current electronic voting hardware because the proposed electronic voting system depends on the following hardware:

- The box to store an LCD screen are easily a factor 2.6 smaller than those to store a CRT screen.
  The dimensions of the box that comes with a typical 19" LCD monitor are: 17 cm deep, 48 cm wide and 48 cm high, which results in 39.168 cm^3.
  The dimensions of a typical 15" CRT monitor are: 50 cm deep, 45 cm wide and 45 cm high, which results in 101.250 cm^3.
- The box to store a voting computer as specified for the proposed improved paper-based voting system is about a factor 23 smaller than the box to store a typical desktop computer.
  The box to store a mini PC as specified in the following sections measures about 15 cm deep, 25 cm wide, 7 cm high, which results in 2.625 cm^3.
  The box of a classic desktop computer measures 25 cm deep, 48 cm wide, 52 cm high, which results in 62.400 cm^3.
- The dimensions of the box to store a printer for the paper ballot are approximately: 25 cm deep, 25 cm wide and 18 cm high, which results in 11.250 cm^3.

Estimated total volume of the hardware storage requirements for the proposed electronic voting system: 53.000 cm^3.

Estimated total volume of the hardware storage requirements of the currently used electronic voting system: 164.000 cm^3.

Conclusion: the storage requirements for the hardware of the proposed improved paper-based voting system are a factor 3 smaller than the requirements for the hardware of the currently used electronic voting system.

4.4.13 Stimulate the willingness of the weakest voter to participate in the voting process (elderly, socially vulnerable voters...)

The proposed improved paper-based voting system takes into account the accessibility and usability requirements that were mentioned in the first part of the Study.

4.4.14 Life cycle of the system

Section 5.2.4.2 specifies the different stages in the deployment of the proposed improved paper-based voting system. These include the design, testing, initialization and certification of the software and its configuration for the computers necessary to manage the elections at the voting offices, Ballot Reading Centers, Ballot Decryption Centers, and Totalization Centers, together with the specification of the users who may boot the voting computer and who may initiate the voting process, etc.

5 Specification of the Improved Paper-based Voting System

The improved paper-based voting system presented in this section allows the voter to cast a vote in a voting booth, and to inspect the resulting paper ballot to confirm that the voting computer on which he cast his vote correctly recorded this vote. The outcome of the elections is based on these paper ballots, which guarantees that the outcome effectively corresponds with the voters' cast votes.

The improved paper-based voting system involves the following actors and devices:

- the president of a voting office;
- a person who is an eligible voter;
- a voting computer with a printer;
- a voting ballot;
- a simple non-computerized voting urn per voting office;
- a Ballot Reading Center where the ballots of the voting urns are read;
- a Ballot Decryption Center that decrypt the information of the voting ballots;
- Totalization Centers where the election results are calculated.

The voting process consists of the following steps: (i) each eligible voter receives a convocation letter for the elections; (ii) a person presents himself with his convocation letter and a proof of his identity (typically an eID card) to the president of the voting office who checks whether that person is an eligible voter. If this is the case, (iii) the president of the voting office provides the voter with a voting token which the voter has to use with the voting computer in the voting booth to start casting his vote. The voter (iv) uses the voting token to start casting his vote (v), and (vi) confirms his vote on the voting computer. The result is (vii) a paper voting ballot which the voter (viii) has to inspect to confirm that it corresponds with the choices he made with the voting computer. Once the voter has confirmed that the printout corresponds with the choices cast on the voting computer, the voter (ix) protects the printout from unauthorized eyes, and (x) presents the resulting ballot to the president of the voting office who (xi) inspects it for visual marks that could identify the voter. If the ballot does not contain such marks (xii), the president of the voting office returns the ballot to the voter who deposits the ballot (xiii) in the voting urn of the voting office. Eventually, (xiv) the president of the voting office returns to the voter the latter's proof of identity, together with his convocation letter.

This system is called "improved paper-based voting system" because this procedure is very similar to the voting procedure with classic paper ballots, as the paper ballots are not completed by hand, but are produces with a voting computer. It is an improved paper-based system because the paper ballot does not need to be counted manually: the voting ballot also includes a machine readable representation of the voter's choice to facilitate the automatic counting of the ballots. Independent auditors can verify that the machine readable representation of the voter's choice of randomly selected ballots correctly correspond with the information printed on the ballot in human readable form.

The improved paper-based voting system comes in two variants. Voting ballots of either variant represent the choice of the voter twice: once in a human readable printout so that the voter can easily verify that the ballot correctly corresponds with

his choice, and once in a machine readable form so that the voting ballots can easily be processed at the end of the Election Day to derive the election result. The machine readable form is encrypted to prevent unauthorized access to the voter's choice.

The barcode ballot (cf. Figure 2) is the first variant (other examples are included in Section 12). The voter receives from the president of the voting office a chip card (a) that serves as voting token to start the voting process. This voting chip card prevents the voter from producing more than one voting ballot: one voting chip card leads to one voting ballot. As soon as the voter presents the voting chip card to the voting computer (b), the voter can start casting his vote (c). Eventually, the voter confirms his choice (d), after which the voting computer prints out a voting ballot and deactivates the voting chip card. The voter receives the voting ballot and removes the voting chip card (e). The ballot consists of two parts: a barcode and a textual printout, each representing the voter's choice, but the information in the barcode can only be accessed by the Ballot Decryption Center (cf. below). After the voter confirms (f) that the printout corresponds with the choices he made with the voting computer, (g) the voter folds the ballot as indicated on the ballot with the dotted lines[2] to hide the human readable text columns from anyone else, especially from the president of the voting office who will inspect the folded ballot for visual marks. Once the voter folded the ballot, the voter leaves the voting booth and (h) shows the folded ballot to the president of the voting office who inspects the ballot for visual marks (i) that could identify the voter. If the ballot does not contain such marks, the president of the voting office returns the folded ballot to the voter (j) who deposits the ballot in the voting urn of the voting office (k). Figure 5 depicts this procedure. Although the voter is encouraged to return the voting chip card, if the voter may forget to do so, he will not be able to reuse the chip card, as it has been deactivated.

2 The voter must fold the ballot at least once (i.e., following the vertical folding indication) to hide the human readable text columns. To prevent spontaneous reopening of the first fold, the voter may also fold it a second time, i.e., following the horizontal folding instruction.

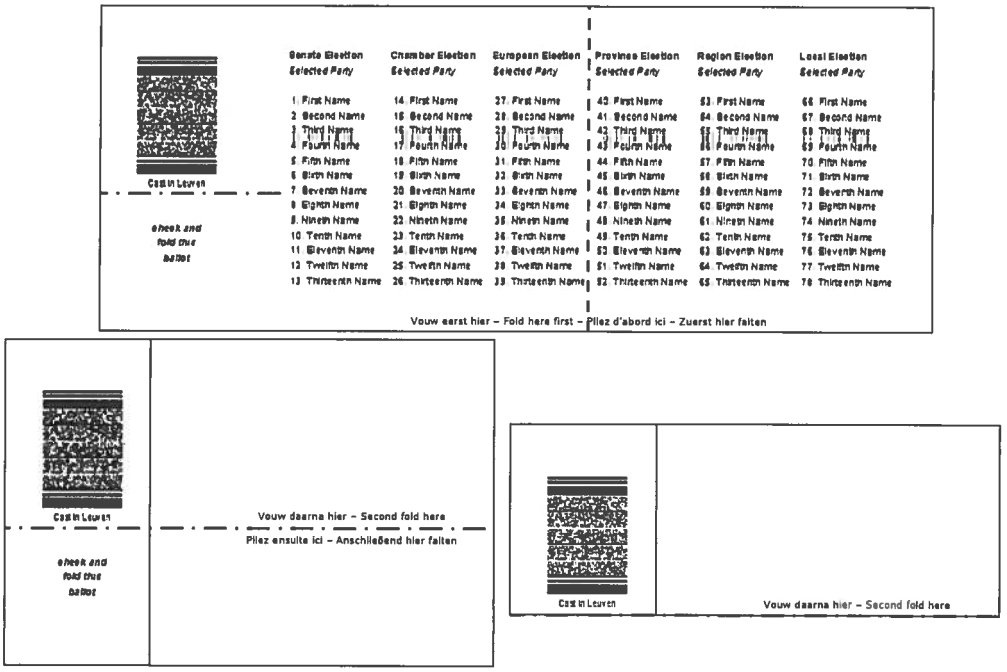
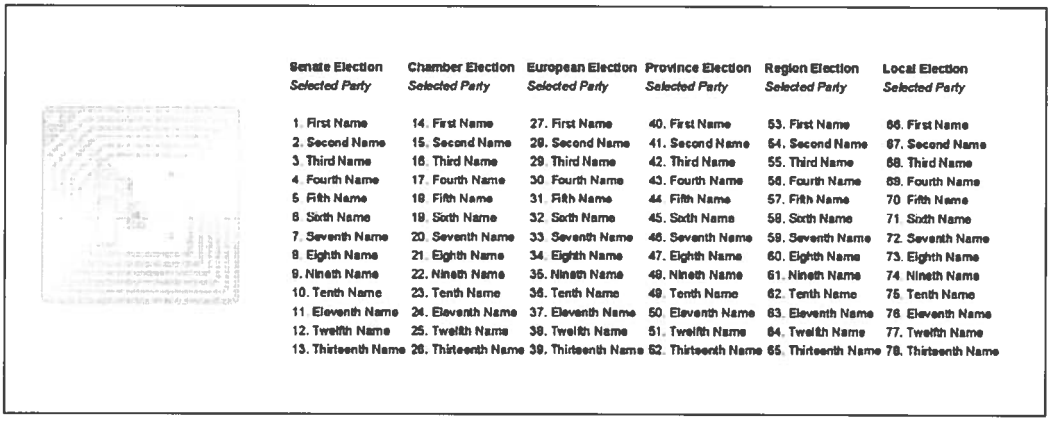


Figure 2: Above: a barcode ballot as produced by the voting computer. Below, left: the ballot that is folded once. Below, right: the ballot that is folded twice



Senate Election *Selected Party*	Chamber Election *Selected Party*	European Election *Selected Party*	Province Election *Selected Party*	Region Election *Selected Party*	Local Election *Selected Party*
1. First Name	14. First Name	27. First Name	40. First Name	53. First Name	66. First Name
2. Second Name	15. Second Name	28. Second Name	41. Second Name	54. Second Name	67. Second Name
3. Third Name	16. Third Name	29. Third Name	42. Third Name	55. Third Name	68. Third Name
4. Fourth Name	17. Fourth Name	30. Fourth Name	43. Fourth Name	56. Fourth Name	69. Fourth Name
5. Fifth Name	18. Fifth Name	31. Fifth Name	44. Fifth Name	57. Fifth Name	70. Fifth Name
6. Sixth Name	19. Sixth Name	32. Sixth Name	45. Sixth Name	58. Sixth Name	71. Sixth Name
7. Seventh Name	20. Seventh Name	33. Seventh Name	46. Seventh Name	59. Seventh Name	72. Seventh Name
8. Eighth Name	21. Eighth Name	34. Eighth Name	47. Eighth Name	60. Eighth Name	73. Eighth Name
9. Nineth Name	22. Nineth Name	35. Nineth Name	48. Nineth Name	61. Nineth Name	74. Nineth Name
10. Tenth Name	23. Tenth Name	36. Tenth Name	49. Tenth Name	62. Tenth Name	75. Tenth Name
11. Eleventh Name	24. Eleventh Name	37. Eleventh Name	50. Eleventh Name	63. Eleventh Name	76. Eleventh Name
12. Twelfth Name	25. Twelfth Name	38. Twelfth Name	51. Twelfth Name	64. Twelfth Name	77. Twelfth Name
13. Thirteenth Name	26. Thirteenth Name	39. Thirteenth Name	52. Thirteenth Name	65. Thirteenth Name	78. Thirteenth Name

Figure 3: Voting ballot with integrated RFID chip

The RFID ballot (cf. Figure 3) is the second variant. With this variant, (a) the voter receives from the president of the voting office a blank voting ballot together with a blank envelope with which the information printed on the RFID ballot can be hidden from unauthorized people, e.g., from the president of the voting office. The use of such envelope may of course also be replaced by simply folding the ballot. The blank voting ballot is an empty sheet of paper with an embedded RFID[3] chip. Arrived in the voting booth, the voter (b) presents the voting ballot to the voting computer. The voter does so by inserting the ballot paper into the printer of the voting booth. As soon as the voting computer detects the newly presented voting token, the voter can start

[3] An RFID (Radio Frequency Identification) chip is a chip that can be integrated into paper. Strict access control mechanisms prevent unauthorized users to read/write information in such chip.

casting his vote (c). After the voter confirms his vote (d), the voting computer prints out the vote on this sheet of paper in a human readable form, and stores the same vote in the RFID chip of the voting ballot, and ejects the voting ballot from the printer (e). After the voter has confirmed that the printout corresponds with the vote cast on the voting computer (f), the voter inserts the ballot paper in the envelope he received from the president of the voting office, or folds the RFID ballot to hide the human readable information (g). Subsequently, the voter leaves the voting booth and (h) presents the envelope or folded ballot to the president of the voting office for inspection. If the envelope or folded ballot does not contain any visual marks that could identify the voter (i), the president of the voting office returns the ballot (j) to the voter who (k) deposits it in the urn of the voting office. Figure 6 depicts this procedure.

The information that is stored in the machine readable part (i.e., the barcode in the first variant, and the RFID chip in the second) of the voting ballot is identical to the information printed in human readable form on the ballot paper. The information is, however, encrypted to protect the voter's choice from unauthorized access: only the Ballot Decryption Center is able to decrypt the information read from the machine readable part. To prevent that the machine readable part is found unreadable at the Barcode Reading Centers, the voter may present the machine readable part of the ballot to a barcode or RFID reader before depositing the ballot in the voting urn. In this case, the voting urn is equipped with a barcode or RFID reader to which the voter can present the voting ballot's barcode or RFID chip. If this reading turns out that the reader was unable to read the ballot, a second attempt is made to confirm the reading problem. If the problem persists, a troubleshooting procedure is started to determine its cause, and the voter problem resolution procedure is started: the unreadable ballot is destroyed, and the voter can restart the voting process.

At the end of Election Day, the election result is produced with the following procedure: (1) a voting office's voting urn is transported to the Ballot Reading Center that is associated with the voting office. This Ballot Reading Center reads the machine readable part of each of the ballots that were cast during the Election Day. Once the ballots have been read, (2) the Ballot Reading Center transfers the encrypted information read from the voting ballots to the Ballot Decryption Center that is associated with the Ballot Reading Center. The Ballot Decryption Center decrypts (3) the ballots and (4) sends the unencrypted information to the First Totalization Center where partial election results are calculated. These partial results are propagated to higher-layer Totalization Centers to contribute to the final election result. Figure 4 depicts this procedure.

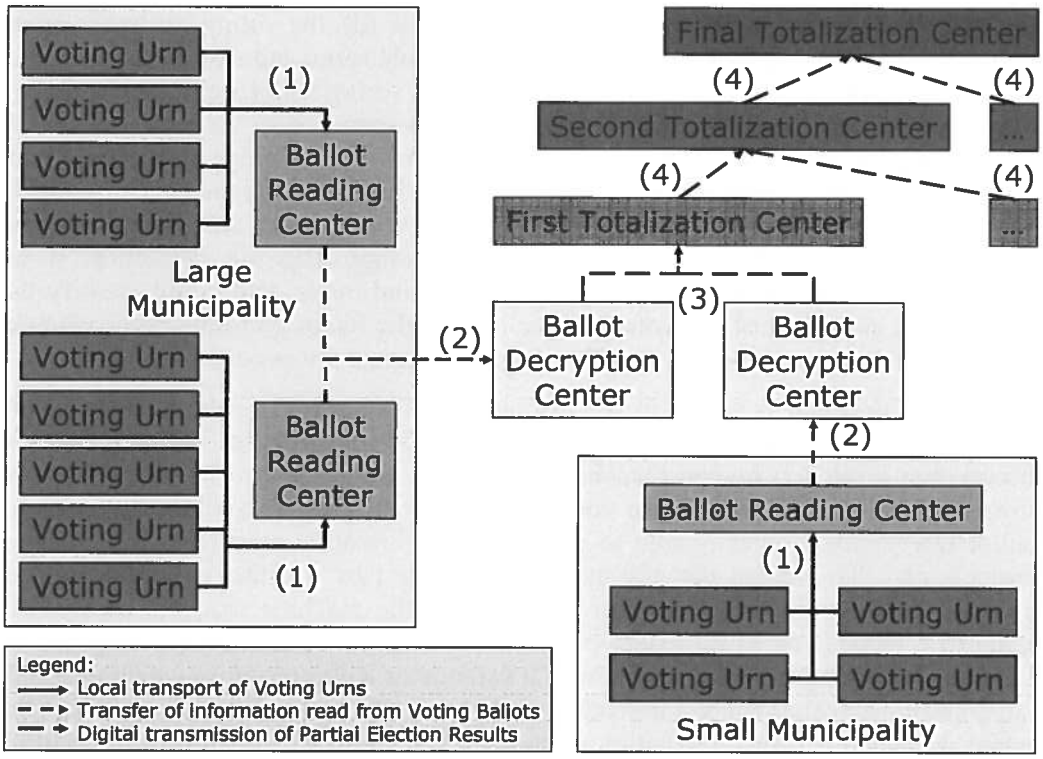


Figure 4: Following a voting ballot from the urn where it was deposited to the Final Totalization Center

At the end of the voting period, the president of a voting office transports his voting urn to the Ballot Reading Center that is associated with his voting office (1). The personnel of the Ballot Reading Center empties the voting urns that arrive and mixes the ballots from these urns to break the chronologic order in which the ballots were deposited in these urn. Subsequently, the personnel of the Ballot Reading Center read the encrypted information that is stored in the machine readable part of each voting ballot. Witnesses make sure that the machine readable part of each voting ballot from each voting urn is read. As soon as all the ballots have been processed, the president of the Ballot Reading Center digitally signs the information that was read from these ballots, and safeguards this signed information on a USB stick that is transported (2) to the Ballot Decryption Center for further processing. Instead of using a USB stick, the president of the Ballot Reading Center may also send an electronic copy of this information to the Ballot Reading Center, e.g., using the Internet.

As soon as a Ballot Decryption Center receives digitally signed information from a Ballot Reading Center, the Ballot Decryption Center verifies the signature on this information. If it is correct, the Center applies the relevant decryption key to the received information. This results in a set of unencrypted votes that have to be processed further on by the First Totalization Center associated with the Ballot Decryption Center. The president of the Ballot Decryption Center therefore digitally signs the list of unencrypted votes, and sends this signed list to the First Totalization Center associated with the Ballot Decryption Center (3). The information sent from the First Totalization Center to the higher level Totalization Centers (4) is digitally signed by the president of the originating Totalization Center.

5.1 Terminology & Conventions

The following terminology is used to avoid inconsistencies and ambiguities:

- Each **voting office** is equipped with a number of voting booths;
- Each **voting booth** is equipped with one voting computer, which includes a touch screen and a printer. A number of voting booths can be reserved for visually impaired people. These voting booths include a voting computer with a Braille reader and a head phone;
- There is one **voting urn** per voting office;
- There are one or more voting offices per municipality;
- The voter receives a **voting token** from the president of the voting office after he has been confirmed to be an eligible voter;
- The voter uses the **touch screen** (or **Braille reader**) to mark the parties and candidates for which and whom he wishes to cast a vote;
- Once the voter confirms that he has completed the voting process, the voting computer prints out the **voting ballot** containing the votes cast both in a human readable and in a machine readable form. The voter confirms that the human readable information corresponds with his vote, after which the voter hides the human readable information;
- The voting ballot may combine a voter's choice for multiple elections, e.g., if the voter has to cast a vote for several elections that are organized on the same day;
- The voter presents the voting ballot to the president of the voting office to confirm that it does not contain any visible marks;
- The voter deposits the voting ballot in the **voting urn**.

The Belgian territory is subdivided in disjoint sections that are relevant to the election type. The exact mapping of these sections varies depending on the type of elections (European, Federal, Provincial, Regional, Local, etc.), and is outside the scope of this document.

The specification in the following sections therefore introduces more abstract concepts based on Totalization Centers where partial results of the elections are gathered or processed. The number of Totalization Centers is not fixed by default, but the following sections assume three Totalization Centers: the First, Second and Final Totalization Center. The first Totalization Center aggregates the election results at municipality level, where the Final Totalization Center aggregates the election results at national level. The encrypted information from a voting ballot is read by the Ballot Reading Centers to which the voting urns are transported at the end of Election Day. this encrypted information is sent from the Ballot Reading Center to the relevant Ballot Decryption Center where the correct decryption key is applied to reveal the unencrypted information of the voting ballots. This unencrypted information is transmitted to the First Totalization Center that is associated with the Ballot Decryption Center, where it contributes to the partial election results of that Totalization Center. Reading the encrypted information from the machine readable part of the voting ballots and decrypting this information takes place at physically distinct locations, whereas the Ballot Decryption and First Totalization Centers may share the same location.

- The **Final Totalization Center** coincides with the Belgian territory; this totalization center is subdivided in several disjoint Totalization Centers, called Second Totalization Centers.
- A **Second Totalization Center** covers disjoint parts of the Final Totalization Center. Each of the Second Totalization Centers is subdivided in one or more disjoint Totalization Centers called First Totalization Centers;
- A **First Totalization Center** is associated with one of the Second Totalization Centers. This Totalization Center processes the output of the Ballot Decryption Centers associated with one or more municipalities. A **municipality** is not further subdivided into sub-levels. The First Totalization Center associated with a municipality totalizes the votes that were cast in the voting urns of that municipality. First Totalization Centers may totalize the votes of more than one municipality.
- A **Ballot Decryption Center** processes the information that was electronically received from the Ballot Reading Center within its scope. It decrypts the information read from the machine readable part of the voting ballots read by the Ballot Reading Center, and provides the decrypted information to the First Totalization Center to which it was associated. A Ballot Decryption Center may be assigned to more than one municipality.
- At a **Ballot Reading Center**, the encrypted information of a voting ballot's machine readable part is read and registered on a digital storage medium. The Ballot Reading Center processes all the voting urns of all the voting offices to which it has been associated. A Ballot Reading Center be assigned to more than one municipality;

It may be necessary to subdivide the territory in more than three totalization centers. In that case, one would have, e.g., First Totalization Center → Second Totalization Center → Third Totalization Center → Fourth Totalization Center → Final Totalization Center.

5.2 High-level description

5.2.1 Voter-view on the Voting Procedure with Barcode Ballots

Figure 5 depicts the voting procedure from the voter's perspective when using barcode-based voting ballots. The voter proceeds as follows to cast his vote:

Step 1. A voter receives a personal **convocation letter**.

Step 2. The **voter presents himself** at the voting office which is mentioned on the convocation letter (a). In case a voter decides to vote by proxy, the proxy presents himself at the voting office which is mentioned on the convocation letter, together with the necessary credentials.

Step 3. The president of the voting office confirms that the voter (or his proxy) is an eligible voter. If the voter (or his proxy) is eligible to vote, he receives from the president of the voting office a **voting chip card** (which serves as voting token) with which the voting computer is to be activated. This voting chip card is discussed in more detail in the next sections. The voting computer waits until a voter presents a voting chip card to start the voting process.

Step 4. The personnel of the voting office indicate one of the free voting booths, in which the voter presents the **voting chip card** to the voting computer to initiate

the voting process (b). Once the voting process is initiated, the voter can start casting his vote(s).

Step 5. The voter casts his vote(s) on the voting computer (c) using its touch screen to select the preferred parties and candidates.

Step 6. The voter confirms his choice (d).

Step 7. When the voter finishes, the voting computer prints out a **paper ballot**. This paper ballot encodes the voter's choices in two equivalent forms: a human readable form (printed text) and a barcode that can be processed by a computer.

Step 8. The voter **removes the voting chip card and the paper ballot from the voting computer** (e) and **inspects the human readable information** of the paper ballot (f).

Step 9. If the human readable information corresponds with his choice, the voter folds the ballot such that only the barcode remains visible (g).

Step 10. The voter returns the voting chip card to the president of the voting office and presents him the **folded ballot** for inspection (h).

Step 11. The **president of the voting office inspects** the folded ballot (i), i.e., without unfolding or opening the ballot to confirm that the ballot does not contain any visible marks that could identify the voter.

Step 12. If the ballot contains no visible marks, the president of the voting office **returns the folded voting ballot** to the voter (j).

Step 13. The voter deposits the **folded ballot in the urn** of the voting office (k).

Step 14. The president of the voting office **returns to the voter his proof of identity and his convocation letter**, the latter having been marked to confirm that the voter showed up during the voting period on Election Day, that he has cast a vote, and that this vote has been deposited in the urn.

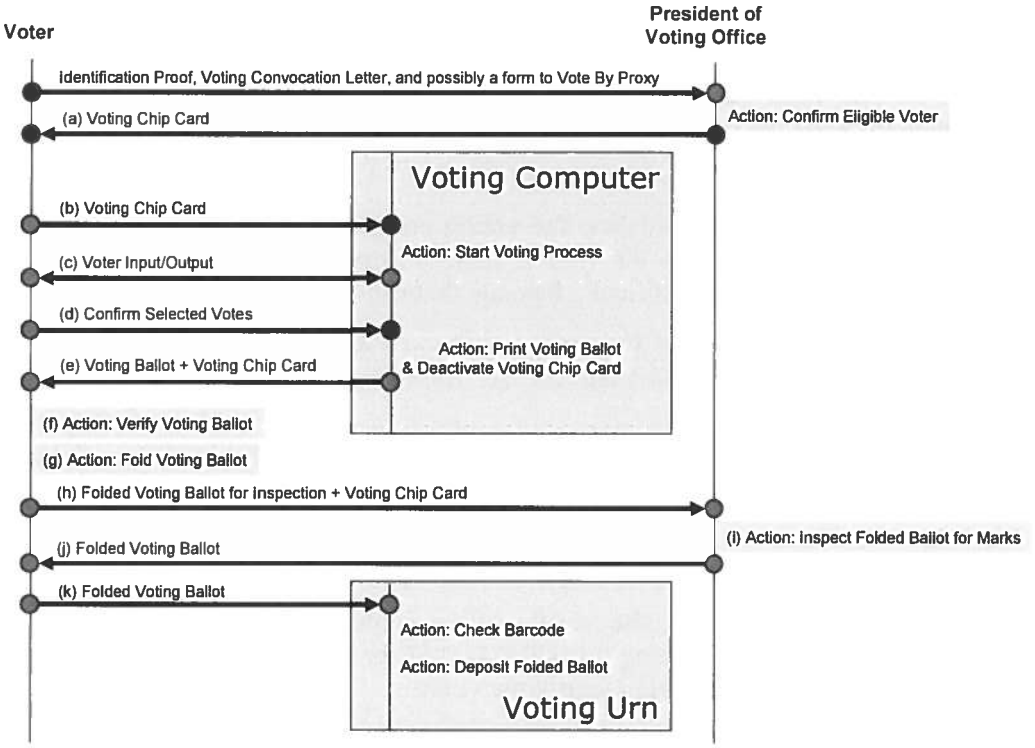


Figure 5: Voting procedure with barcode ballots

5.2.2 Voter-view on the Voting Procedure with RFID Ballots

Figure 6 depicts the voting procedure from the voter's perspective when using RFID-based voting ballots. The voter proceeds as follows to cast his vote:

Step 1. A voter receives a personal **convocation letter**.

Step 2. The **voter presents himself** at the voting office which is mentioned on the convocation letter (a). In case a voter decides to vote by proxy, the proxy presents himself at the voting office which is mentioned on the convocation letter, together with the necessary credentials.

Step 3. The president of the voting office confirms that the voter (or his proxy) is an eligible voter. If the voter (or his proxy) is eligible to vote, he receives from the president of the voting office a **blank paper voting ballot** and a **blank envelope** (optional, as is is also possible to hide the vote printed on the RFID ballot by folding the ballot paper). The voting computer waits until a voter presents a blank voting ballot to start the voting process. The voting computer informs the voter if it should detect a non-blank voting ballot.

Step 4. The personnel of the voting office indicate one of the free voting booths, in which the voter presents the **blank voting ballot** to the voting computer to initiate the voting process (b). Once the voting process is initiated, the voter can start casting his vote(s).

Step 5. The voter casts his vote(s) on the voting computer (c) using its touch screen to select the preferred parties and candidates.

Step 6. The voter confirms his choice (d).

Step 7. When the voter finishes, the voting computer prints the voter's choice on

the **paper ballot**, and writes the encrypted vote to its RFID chip.

Step 8. The voter takes **the paper ballot from the voting computer** (e) and **inspects the printed information** (f).

Step 9. If the printed information corresponds with his choice, the voter inserts the ballot paper in the envelope he received from the president of the voting office (g).

Step 10. The voter **presents the envelope** to the president of the voting office for inspection (h).

Step 11. The **president of the voting office inspects** the envelope with the voting ballot (i), i.e., without opening the envelope, to confirm that the envelope does not contain any visible marks that could identify the voter.

Step 12. If the envelope contains no visible marks, the president of the voting office **returns the envelope with the voting ballot** to the voter (j).

Step 13. The voter deposits the **envelope in the urn** of the voting office (k).

Step 14. The president of the voting office **returns to the voter his proof of identity and his convocation letter**, the latter having been marked to confirm that the voter showed up during the voting period on Election Day, that he has cast a vote, and that this vote has been deposited in the urn.

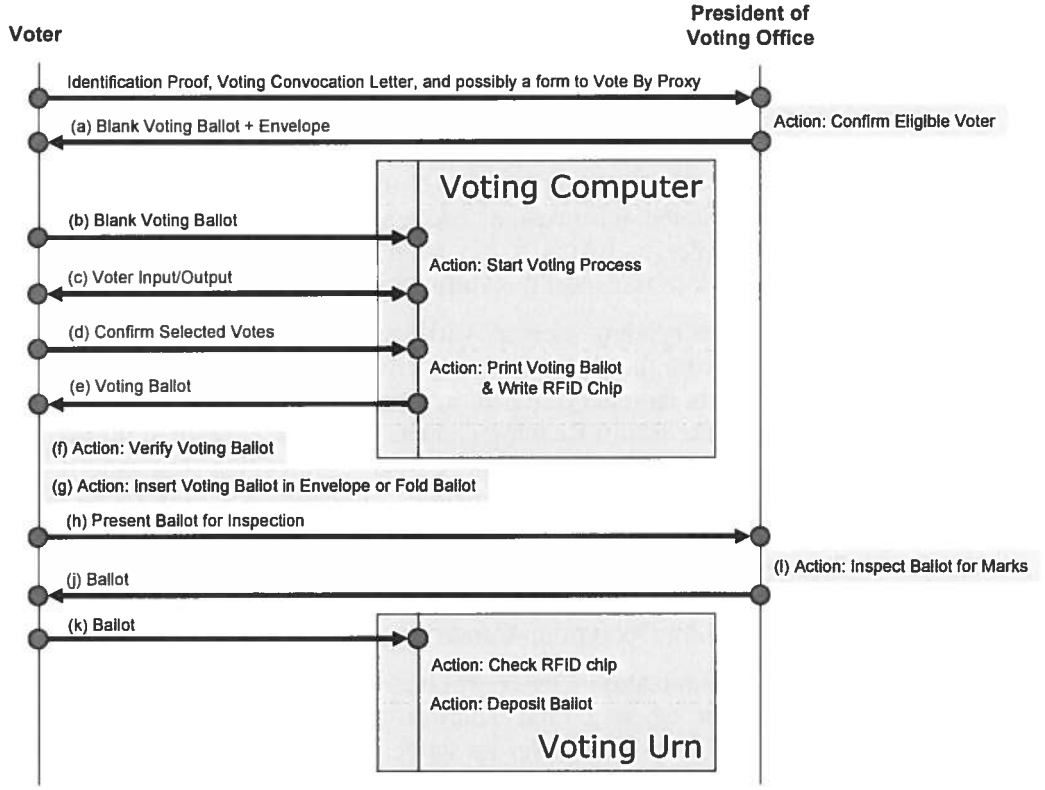


Figure 6: Voting procedure with RFID ballots

5.2.3 From a Voting Ballot to the Final Election Result

At the end of the voting period on Election Day, the following steps are followed to derive the final election result from the voting ballots that were cast during Election

Day. This procedure is also depicted in Figure 4:

Step 1. At the end of Election Day, the president of a voting office transports the voting urn of his voting office to the Ballot Reading Center associated with his voting office (1). Small municipalities may share the services of a Ballot Reading Center, large municipalities may use the services of different Ballot Reading Centers;

Step 2. As soon as a voting urn arrives at a Ballot Reading Center, the urn is emptied, and its content mixed with the content of the other urns that have not yet been processed by the Ballot Reading Center to break the chronological order in which the ballots were deposited in the various urns. The content of different urns can be mixed together, even if the urns originate from different municipalities: the Ballot Decryption Center makes sure that the ballots issued in a particular municipality end up with the Totalization Center responsible for that municipality;

Step 3. The personnel of the Ballot Reading Center uses the appropriate means to read the voting ballots: the information of barcode ballots are read with a barcode reader, the information of RFID ballots is read with RFID readers;

Step 4. As soon as the personnel of the Ballot Reading Center has read the machine readable information of the ballots, the president of the Ballot Reading Center uses his eID card to calculate an electronic signature on this information, after which this signed information is sent (2) to the Ballot Decryption Center. As the content of the urns was mixed before the ballots were read, the list of ballots that will be sent to the Ballot Decryption Center does not refer to the order in which the ballots were cast in the voting offices. The integrity of this transfer is protected using a digital signature calculated with the electronic identity card of the president of the Ballot Reading Center. If the Ballot Reading Center is not able to transfer this signed information through an online connection with the Ballot Decryption Center to which it has been associated, the Ballot Reading Center uses a USB stick to transport this information via courier;

Step 5. The Ballot Decryption Center verifies the digital signature on the information received from the Ballot Reading Centers under its scope. The Ballot Decryption Center sorts the encrypted information of the machine readable part of the ballots read by the Ballot Reading Center. After the encrypted information has been sorted, the Ballot Decryption Center applies the relevant private decryption key to each of the encrypted ballots, tabulating for each municipality under its scope the decrypted voting ballots. After the decryption, the president of the Ballot Decryption Center digitally signs the resulting table with decrypted voting ballots, after which this table is sent to the First Totalization Center associated with this Ballot Decryption Center;

Step 6. Whenever a Totalization Center receives information from a lower layer Totalization Center, or when a First Totalization Center receives information from a Ballot Decryption Center under its scope, the Totalization Center updates its partial election results according to the freshly received information;

Step 7. Each Totalization Center below the Final Totalization Center updates its higher level Totalization Center on a regular basis with a digitally signed update of its partial election result. If a Totalization Center is not able to transfer its partial election result to the higher level Totalization Center to which it has been associated, this digitally signed information is stored on a USB stick or another digital storage medium after which it is transported per courier to the higher level

Totalization Center;

Step 8. The Final Totalization Center publishes the election results based on the partial and final results of the lower level Totalization Centers within its scope.

5.2.3.1 Auditing the Voting and Counting Procedure

Independent auditors may observe the different steps of the production and processing of voting ballots, especially to guarantee that

(i) the voting urns at the beginning of Election Day are empty,

(ii) the voting offices and their personnel operate correctly during Election Day,

(iii) the personnel of the voting offices operates correctly at the end of Election Day,

(iv) all the voting urns are transported from the voting offices to the Ballot Reading Center to which the voting office is associated,

(v) the opening and emptying of the urns proceeds according to the rules,

(vi) the mixing of the voting ballots before reading the encrypted information in the machine readable part of the voting ballots is adequate,

(vii) all the voting ballots have been read,

(viii) the voting official who digitally signs the list of the encrypted voting ballots performs his job correctly,

(ix) the randomized lists are correctly transported from the Ballot Reading Center to the Ballot Decryption Center,

(x) the randomized list with decrypted votes is correctly transported form the Ballot Decryption Center to the First Totalization Center,

(xi) the voting officials of the First Totalization Centers correctly process the information from the Ballot Decryption Centers;

(xii) the different Totalization Centers correctly process the incoming partial election results and the corresponding outgoing partial election results.

The auditors issue official statements (PVs) in which they report their findings, e.g., the number of used voting urns per polling station at the end of the voting period on Election Day, the number of ballots per voting urn, the number of eligible voters per voting office, etc. Whenever partial results are transmitted from one Totalization Center to another, the auditor(s) verify and confirm that the partial result corresponds with the information under their supervision.

5.2.4 Computer Equipment

Figure 7 and Figure 8 illustrate the equipment used in a voting booth of a voting office that uses barcode or RFID ballots, respectively. Figure 9 and Figure 10 show the equipment used at the Ballot Reading Centers that processes barcode and RFID ballots, respectively. Figure 11 and Figure 12 show the hardware necessary at the Ballot Decryption Centers and (First) Totalization Centers.
An overview of this equipment:

- touch screens to communicate with the user of the voting computer;
- normal screens for the Ballot Reading/Decryption Centers;

- mini computers for the voting booths and the different Centers;
- printers to print the voting ballot (depending on the ballot types, the printer can be either a simple ticket printer to print barcode ballots or a slip printer with an RFID module to print and initialize RFID ballots);
- smartcard readers for the voting computers that produce barcode ballots to detect and deactivate the voting chip card;
- smartcard readers with secure PIN pad for the computer systems that will be used by the presidents of the Ballot Reading/Decryption/First Totalization Centers to sign the information that must be sent to the higher-layer Centers;
- Braille readers in the voting booths that will be available to visually impaired voters;
- USB sticks for the Ballot Reading Centers and Ballot Decryption Centers that do not have an online connection with the Centers that will process their information;
- barcode readers for the voting urns and Ballot Reading Centers that process barcode ballots;
- RFID readers for the voting urns and Ballot Reading Centers that process RFID ballots;
- network connections to digitally transfer information from one Center to the other, e.g., from the First Totalization Center to the Second.

The mini computer is required to have an audio output through which visually impaired people may receive audible feedback while they use the voting computer to cast their vote, even in voting booths where no Braille reader is available.

The term "voting computer" refers to the combination of the above mentioned components. Each voting booth consists of one voting computer.

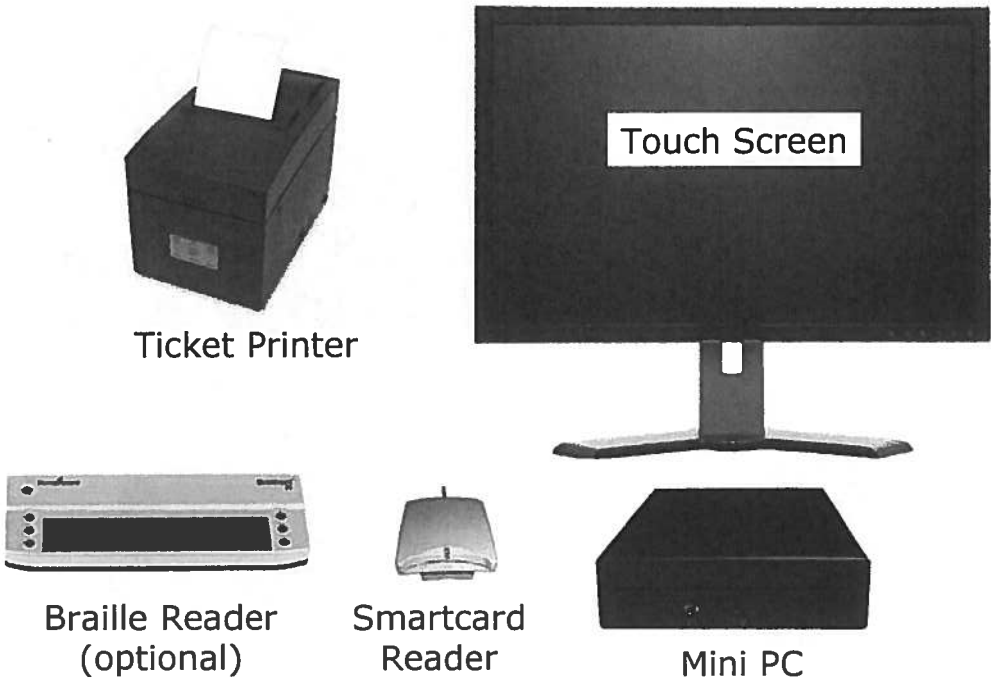


Figure 7: Voting booth equipment when using barcode ballots

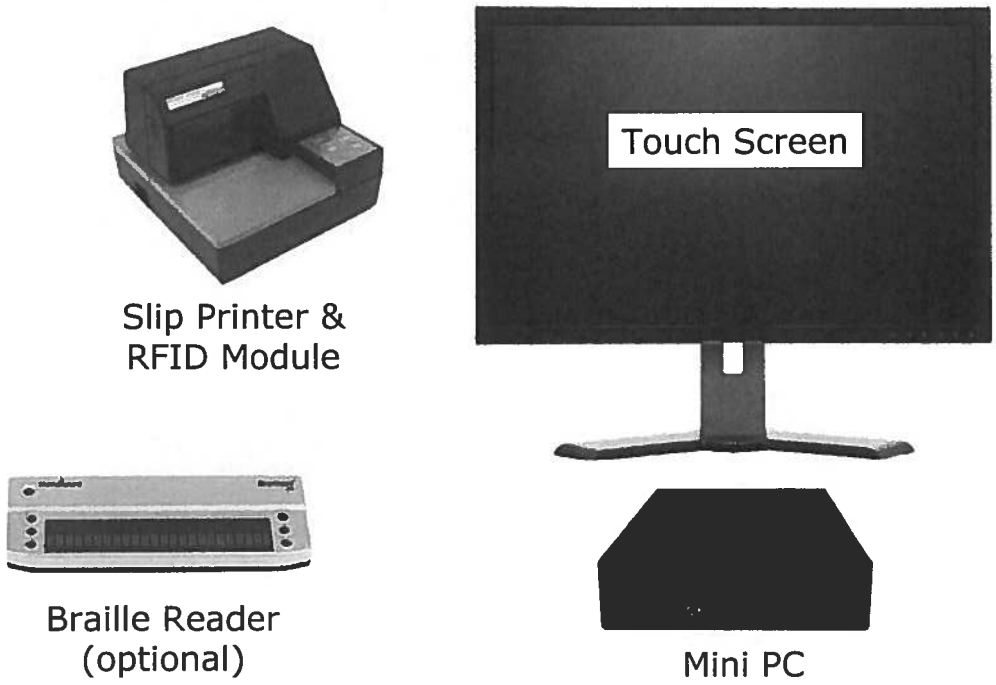


Figure 8: Voting booth equipment when using RFID ballots

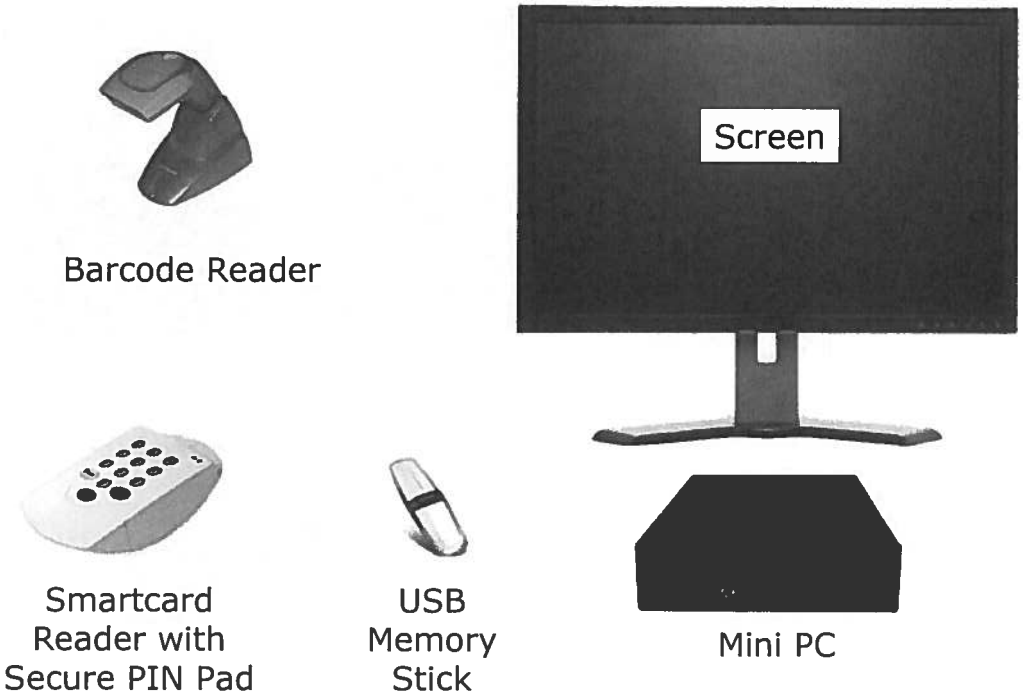


Figure 9: Ballot Reading Center's equipment to process barcode ballots

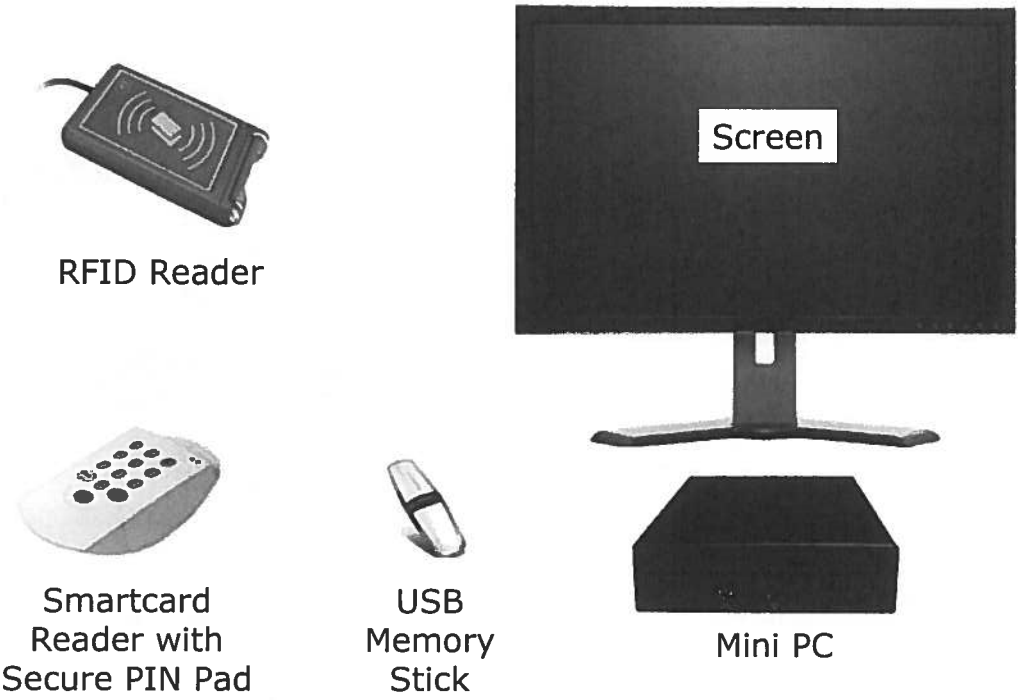


Figure 10: Ballot Reading Center's equipment to process RFID ballots

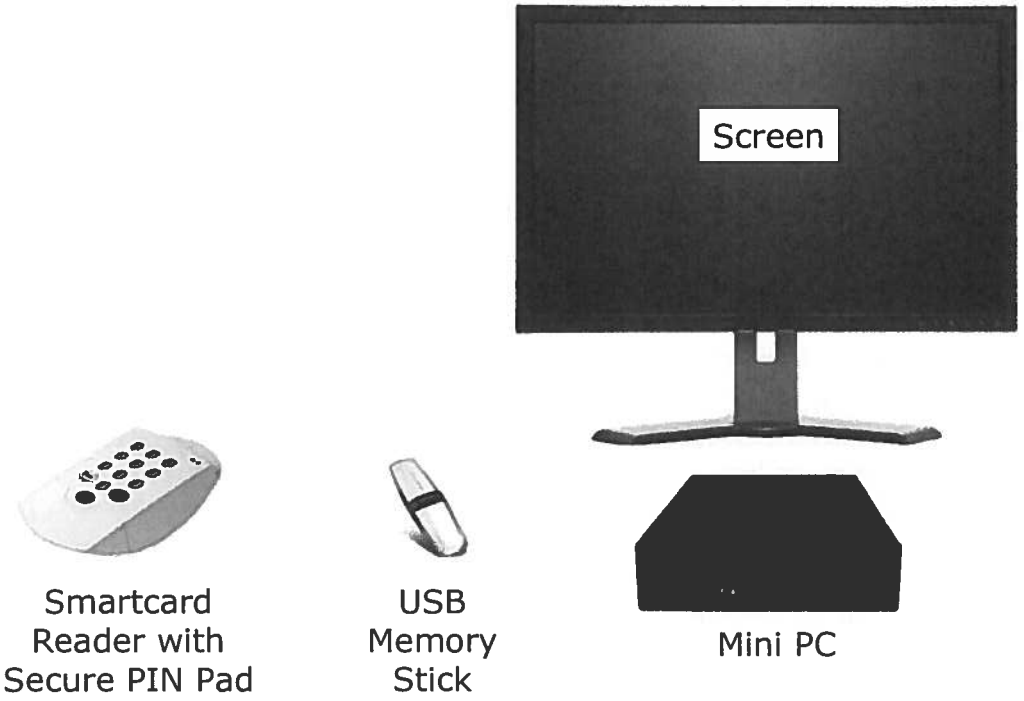


Figure 11: Ballot Decryption Center's equipment

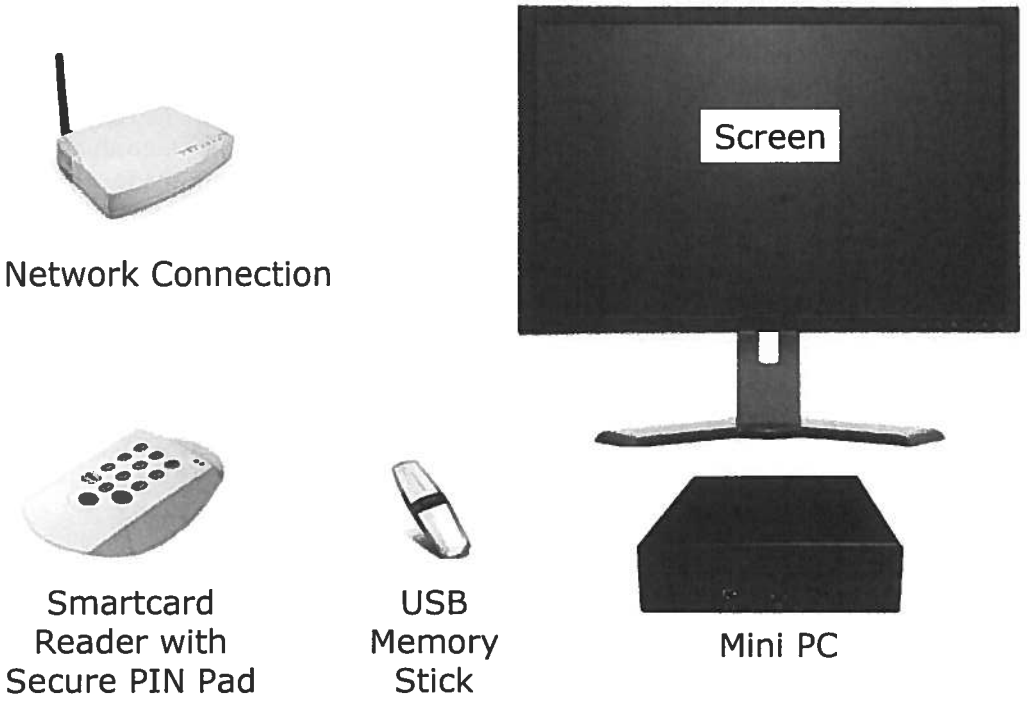


Figure 12: First Totalization Center's equipment

5.2.4.1 Computer Components

Computer System

The computer system that is part of the "voting computer" can be either a custom-

designed dedicated computer or an off-the-shelf computer system.

Advantages and disadvantages of owning the computer system

Advantages of a custom-designed dedicated computer include:

- the custom-made dedicated computer can be designed such that it only includes the hardware components that are strictly necessary for the voting application;
- the designer of the custom-made computer owns and controls the design of this computer, and is in the position to know exactly what operations the device supports, and what operations it cannot support;
- the designer of the custom-made computer system can also include in the design specific measures to avoid advanced side channel analysis attacks on computer hardware (e.g., timing attacks, power analysis, etc), which make it harder for outside observers to successfully launch advanced eavesdropping attacks;
- it is also possible to include hard to tamper with components in the design of the dedicated voting computer so that tampering (e.g., replacing memory chips or adding eavesdropping equipment) becomes nearly impossible;
- the verification of the credentials of the system administrator(s) who will be allowed to install the operating system and the voting software on the voting computer can be incorporated in the firmware of the voting computer.

Disadvantages of designing a custom-made voting computer include:

- the design of a custom made computer system is very complex and thus costly;
- the production costs of such systems will certainly be higher than that of off-the-shelf systems, but the maintenance cost of a custom-made computer system is nearly zero;
- the design and design criteria must be certified, which is a process that may require several months.

Advantages of an off-the-shelf computer system include:

- the Administration may assign a service contract, following a public tendering process, to provide for each election (or for a number of elections) off-the-shelf voting computers;
- there is no need to design and produce dedicated voting computers;
- there is no need to store the computer systems between elections.

Disadvantages of using an off-the-shelf computer system:

- The off-the-shelf computer system may contain hardware that is not strictly necessary for the voting application, e.g., wireless network capabilities. It is then the responsibility of the system administrator (cf. below) to disable the unwanted hardware.

Bootable CDROM with Operating System & Election Software

The voting computers use an open source LINUX operating system. Bootable

CDROMs with the election software[4] are distributed to the presidents of the voting offices, Ballot Reading Centers, Ballot Decryption Centers, and First Totalization Centers. The bootable CDROMs are specially tailored (i.e., simplified) for usage on the computers in the voting booths, at the Ballot Reading Centers, Ballot Decryption Centers and First Totalization Centers[5]. The bootable CDROM only contains the operating system, together with the voting software and its configuration to operate during and after the Election Day, i.e., to cast the votes in the voting booths, to read and decrypt the machine readable parts of the ballots, and to calculate the partial and total election results. Any secret information (e.g., private decryption keys of the Ballot Decryption Center) is not stored on these bootable CDROMs. The secret information is stored on external media, e.g., smartcards or hardware security modules.

The Administration that is in charge of the organization of elections assigns the role of the system administrator who creates this bootable CDROM to a specific actor. This actor is responsible for the fine-tuning of the operating system and the installation and management of the election software and its configuration. The credibility and competence of this actor is a crucial element in the initialization, reliability and trustworthiness of the electronic voting system. After the creation (and testing) of the bootable CDROM, this CDROM can be multiplied in sufficient numbers and be distributed to the relevant recipients (i.e., presidents of the voting offices, Ballot Reading Centers, Ballot Decryption Centers, Totalization Centers). More details on this procedure are included in the following sections.

Examples of off-the-shelf computer systems

There are many providers of small computer systems that are off-the-shelf available. A non-exhaustive (and rapidly changing) list includes:

- PL-01030 from Win Enterprises (http://www.win-enterprises.com/index.php?option=com_content&task=view&id=125&Itemid=59)
- Mini PCs from Avalue Technology Inc (http://www.avalue.com.tw/Box_Computer/mini_pc.cfm)
- Tiny PC Low Cost Embedded system from TK (http://www.ewayco.com/51-embedded-systems-100-PC-mini-ITX-low-cost/01-embedded-systems-100-pc-mini-itx-low-cost.html)

The recommended computer system consists of a compact disk-less and fan-less micro computer with only those input/output connectors that are strictly necessary for the voting application: two (or more) USB connectors (one for a smartcard reader, and one for a USB memory stick), a parallel or additional USB port for the printer, an additional USB port for a Braille reader, a VGA connector for the display, an audio output connectors for the visually impaired people... Figure 13 shows the basic components of such computer system.

---

[4] The term "election software" refers to the combination of all the software and configuration files that are necessary during the election period: voting software on the voting computers, ballot reading software for the Ballot Reading Centers, ballot decryption software for the Ballot Decryption Centers, totalization software for the Totalization Centers.

[5] The specification of the computers used at higher Totalization Centers is outside the scope of this document. As the functionality of the computers used at higher Totalization Centers does not differ from the functionality of the computer at the First Totalization Center, the same hardware could be used if necessary.

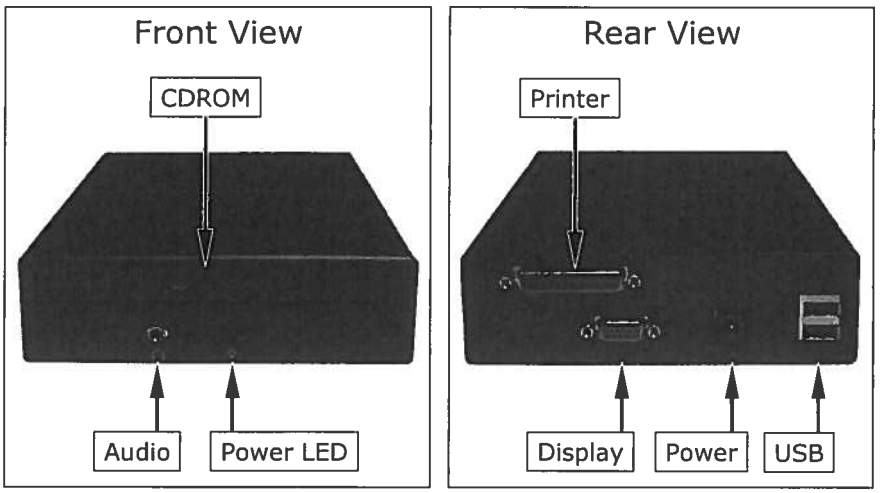


Figure 13: Details of a Mini PC with connectors to connect a printer, display, ear phones, etc.

Price quotations for Fan-less mini pc Win Enterprises

The unit price for a PL-01030 equals 385 USD (information from http://www.embeddedstar.com/weblog/2007/02/04/pl-01030-embedded-computer/). Volume discounts apply.

Price quotations for Mini PC from Avalue Technology

No price information found.

Price quotations for Fan-less mini PC from TK

The unit price for a TK Tiny PC equals 189 USD (information from http://www.ewayco.com/51-embedded-systems-100-PC-mini-ITX-low-cost/11-tk-800mhz-low-cost-pc-embedded-system.html)
Volume discounts apply.

Display & User-input Device of a Voting Booth

The voting computer communicates with its user through a visual display or a tactile display in the form of a Braille reader for visually impaired people.

The display may be combined with an input device, e.g., a classic CRT (Cathode Ray Tube) screen with a light pen, or an LCD (Liquid Crystal Display) touch screen with or without an inductive stylus. Which display type to choose from is largely determined by the input device used by the user. Several options are discussed in the following section.

The magnetic stripe card-based voting computers expect the voters to point to the screen with a light pen. A light pen is a computer input device in the form of a light-sensitive wand used in conjunction with the voting computer's CRT monitor. It allows the user to point to displayed objects, or draw on the screen, in a similar way to a touch screen but with greater positional accuracy. A light pen can work with any CRT-based monitor, but not with LCD screens, projectors or other display devices.[6] The popularity of CRT screens is diminishing rapidly and there is only one major

[6] http://en.wikipedia.org/wiki/Lightpen

manufacturer apparently left in the US: the company Fastpoint7.

For any next generation of voting machines, the light pen is no longer an option as modern computer screens are not CRT-based anymore. It is therefore suggested to use a touch screen to accept and process user input. The voting computer would present a grid with tick boxes that represents a logical menu structure: the main menu displays the elections which the voter has to cast a vote for (if there is more than one election on Election Day). Once the voter has selected the election he is going to cast a vote for, the list of parties is shown. After selecting the preferred party, the voter gets a list of the candidates running for this party and he selects the preferred candidates. Each of the screens that are displayed to the voter comply with the usability recommendations specified below, i.e., the voter has the possibility to cancel casting the vote at any time; he can go back to the previous screen, etc.

Touch screens rate around 200 Euro in small quantities.

Printing Ballot Papers

Each voting booth is equipped with a printer with which the voting ballot is printed. The two ballot types (barcode ballot and RFID ballot) impose specific requirements: the barcode ballot can be produced using any ordinary printer that is commonly available. The RFID ballot, however, requires a specific printer type, namely a slip printer or a ticket printer with an RFID module. This module serves two functions. It first detects the presence of a voting ballot to start the voting process with the voting computer, and it writes the voter's choice (in encrypted form) in the RFID chip that is embedded in the voting ballot.

The human readable vote that is printed on the paper ballot is printed using a printer for paper ribbons or standard paper. There are several options for these printers:

1. a printer as those used to print train tickets and airline boarding passes,
2. a straightforward label printer,
3. a printer as those used to print receipts in a supermarket,
4. an off-the-shelf laser printer, or
5. a slip printer with RFID module.

The first printer type is extremely robust (i.e., very large mean time between failures, with metal casing, an internal chamber to store a ribbon of 1.000 empty voting tickets), and is capable of producing voting tickets in a fully automated manner, i.e., once the voting ballot has been printed, the printer drops the voter's ballot in an easy to reach tray from which the voter can collect his ballot for further inspection. Printers of this type are high quality and therefore rather expensive: 2.000 Euro. Ticket printers may also be equipped with a barcode and/or RFID module (at an extra cost of 150 Euro, each) to confirm that the barcode printed on the paper ballot is correctly encoded, or to initialize the RFID chip embedded in the voting ballot with the voter's encrypted vote. The following figure gives an example of this type of printer:

[7] http://www.fastpoint.com/main.html

Figure 14: Dedicated Ticket Printer, usable for barcode ballots and RFID ballots

The second printer type is a dedicated label printer. The individual labels have fixed size, and are stored in an internal chamber when a label roll is used or from an external supply when using tickets as used for the dedicated ticket printer. These printers rate around 700 Euro. The following picture gives an example of this type of printer:

Figure 15: Dedicated Label Printer

The third printer type is less robust (i.e., more error prone) than the previous two, and uses a paper ribbon on a paper roll. This printer's guillotine ensures that the paper trail can easily be detached from the printer. Once the printer finishes printing the voter's ballot paper trail, the voter must detach his ballot from the printer. As the printer uses a paper ribbon on a paper roll, this paper will automatically take its original curved form once printed. Printers of this type are fairly cheap: 300 Euro in small quantities. The following figure gives an example of this type of printer:

Figure 16: Paper ribbon printer

The fourth printer type consists of a straightforward laser printer. These are well known off-the-shelf and cheap products. The typical size of a laser printer's paper chamber holds 150 standard pages. Laser printers are very cheap: less than 200 Euro in small quantities. The following figure gives an example of a laser printer:

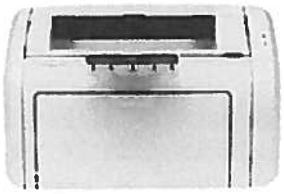


Figure 17: Typical Laser Printer

The fifth printer type is specific to handling RFID ballots. This printer has a built-in RFID module that can detect the presence of the RFID chip embedded in the voting ballot when it is inserted in the printer. These printers are fairly expensive: 800 Euro in small quantities.

Figure 18: Slip Printer with RFID module

5.2.4.2 Life-cycle of the Computers of the Voting Offices, Ballot Reading/Decryption Centers and First Totalization Centers

Computers Boot from CD/DVDROM

The computers used in the voting booths, Ballot Reading Center, Ballot Decryption Center, and the First Totalization Center use the same hardware, namely a mini computer without hard disk or other persistent memory. They boot from CDROM (or DVDROM) drives to avoid the individual installation of these computers. The bootable CDROMs contain the operating system of the computers, their software and configuration files necessary to run the elections.

These bootable CDROMs are specially tailored for usage on the computers in the voting booths, at the Ballot Reading Centers, Ballot Decryption Centers, and First Totalization Centers. This means that the bootable CDROMs only contain the software and configuration files that are relevant to operate during the Election Day, i.e., to allow a voter to cast his vote, to allow the Ballot Reading Centers to read the encrypted votes, to allow the Ballot Decryption Centers to decrypt the encrypted votes, and to allow the First Aggregation Levels to process the output of the Ballot Decryption Centers.

No secret information is stored in the clear on these CDROMs, i.e., privacy-sensitive information is encrypted under the boot credentials of the president of the voting office or Center where the CDROM will be used. Secret information that is necessary to operate correctly during the Election Day, e.g., to allow a Ballot Decryption Center to decrypt the encrypted votes is stored on a persistent medium such as a smartcard or a hardware security module (HSM).

Using such mechanism minimizes the burden to install and manage thousands of computers that are used on Election Day. The voting computers and the computers of the Ballot Reading/Decryption Centers and First Totalization Centers are booted with the same CDROM (it is of course also possible to issue several CDROM types: one specific to voting computers, one for Ballot Reading/Decryption/Totalization Centers). This is achieved by loading these CDROMs with all different versions of the configuration files for each of the locations where the CDROM can be used. Each configuration file is encrypted with the AES using a different key. The boot credentials (cf. below) of the president of the voting office/Ballot Reading/Decryption Center or First Totalization Center that is presented during the computer's boot process contains the information necessary to allow the computer to select the correct configuration file which specifies how the computer will serve. Furthermore, the boot credential contains the key that allows the computer to decrypt this configuration file. One boot credential unlocks one configuration file.

Example: suppose that it is decided to initialize CDROMs for voting computers that can be used in all voting districts of East- and West-Flanders. For each of the voting offices in these two provinces, a separate configuration file is encrypted under a different key and loaded on the CDROMs that will be distributed to the presidents of the voting offices of both provinces. Subsequently, the computers are booted using this CDROM on Election Day. The presidents of the voting offices obtain each their separate boot credentials. When the president of the first voting office of Ghent presents uses her CDROM to boot the voting computers of her voting office, she presents her boot credential to each of the voting computers; the software of each voting computer decrypts and loads the configuration file for this voting office, containing, a.o., the list of candidates for Ghent.

The configuration file of a voting computer is different for each voting office. The file determines the list of elections, parties and candidates that will be shown to the voter in the voting booth. This configuration file also specifies the layout of the screens displayed to the voter and the layout of the printed paper trail. The bootable CDROM is initialized with the election-specific configuration files of the computers in the various locations where these computers will be used. The configuration file of a voting computer that will be used by visually impaired people may, e.g., be configured with a different layout than the voting computers that will be used by the non-visually impaired people. The layout of the voting screens is designed according to the guidelines specified in section 5.6.1.5. Finally, the configuration file specifies which boot credential will be needed to activate the voting computer for the voting process.

Boot Credentials

The president of a voting office shall receive, prior to the Election Day, the secret **boot credentials** that correspond with the voting computers in his voting office. The boot credential determines which configuration files from the bootable CDROM will be activated on the voting computer during Election Day.

This boot credential may consist of a secret pass phrase that must be input on a key pad displayed on the computer screen, or it may consist of the combination of a chip card with PIN if the voting computer is equipped with a smartcard reader. In either case, the president of the voting office must have obtained the correct boot credential for his voting office prior to the Election Day.

A similar procedure is followed to provide the presidents of the Ballot Reading Center, Ballot Decryption Center and First Totalization Center with the boot

credential that enables them to boot their computer equipment with the necessary configuration files.

The different roles in the creation and use of the bootable Election Day CDROMs

We distinguish between 3 different roles.

1. The **system administrator** prepares the bootable CDROM:
   - Removes from the bootable CDROM image all information and software that is not relevant for the election software;
   - Applies the necessary security patches to the operating system of the CDROM image and disables all the computer system's features that will not be necessary for use during Election Day;
   - Loads the voting software for the elections on the CDROM image;
   - Receives the configuration files for the voting software from the initializer and loads these files on the CDROM image;
   - Verifies the conformity of the operating system, voting software and configuration files.
2. The **initializer**:
   - Creates the necessary information for the configuration files of the voting software;
   - Provides the configuration files of the voting software to the system administrator.
3. The **distributor**:
   - Transports the computers to the voting offices, the Ballot Reading Centers, Ballot Decryption Centers, and First Totalization Centers;
   - Sends the bootable Election Day CDROMs to the presidents of the voting offices, Ballot Reading Centers, Ballot Decryption Centers, and First Totalization Centers.

Towards using the Election Day Computers

Figure 19 depicts the typical steps necessary during the initialization of the bootable CDROMs that will be used during Election Day, together with the steps that are necessary to acquire, distribute and use the computers used on Election Day. Each color refers to a particular phase in the life cycle of the voting computers.

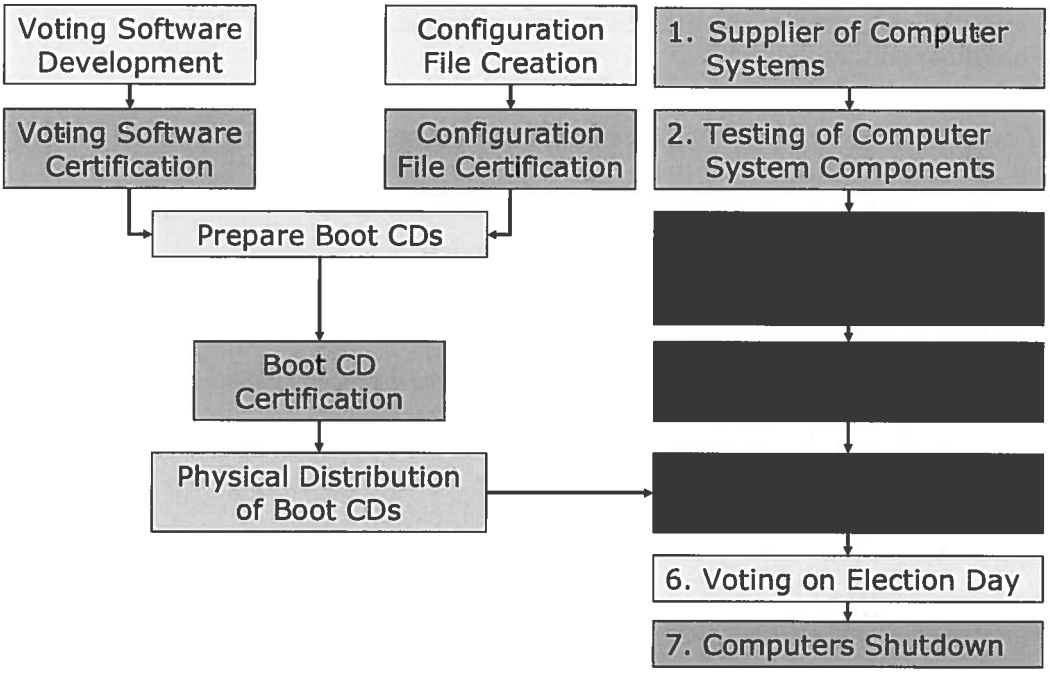


Figure 19: Towards using the Election Day Computers

Two processes happen in parallel: the development, testing and certification of the voting software and configuration files on the one hand, and the acquisition, testing, distribution of the computer systems, etc. on the other hand. Once the voting software and configuration files are certified, they are included in the bootable CDROM that will be distributed to the presidents of the voting offices, Ballot Reading/Decryption/Totalization Centers.

The second process proceeds as follows:

1. **The supplier of the computer systems** that will be used during the Election Day supplies a device that supports the following input/output interfaces:
   - a display;
   - a Braille reader (for the computer systems that will be used by visually impaired voters);
   - a printer interface;
   - a smartcard reader that will be used in the voting offices where barcode ballots will be used and for the computers that will be used in the Ballot Reading/Decryption/First Totalization Centers;
   - a barcode or RFID reader for the computers that will be used at the Ballot Reading Center;

   The supplier shall be asked to disable permanently those interfaces that are not needed for installation or voting purposes, e.g., network interfaces.
2. **Testing of voting computer components**. The supplied hardware is tested to assess the quality of service of the hardware supplier. This includes changing BIOS settings such that the computer systems will only be able to boot from the CDROM drive.
3. **The distributor of the computer systems** delivers the correct computers in the correct municipality. As explained above (section 0), this step is quite

simple as the computers used on Election Day can be used in any voting office or Center that is involved in the election process.

4. **The installation of the computer systems.** The display, printer and auxiliary devices (smartcard reader, barcode reader, etc) shall be connected to the computer as appropriate. The power cord of each of these devices shall be connected to the respective power outlets. The connectors of each of the cables are such that potential cable mismatches can easily be discovered and corrected. At the end of the installation of a computer system, the installer tests the basic functionality of the computer system to confirm that the system's basic functionality operates correctly, more precisely that the display and smartcard, barcode or RFID reader function correctly, and that the printer has been correctly loaded with paper.
5. **Booting the computer system** on Election Day can only be successfully accomplished by the president of the respective voting office or Center. The president activates each of the computers using the bootable CDROM and boot credentials he received prior to the Election Day.

   Whenever the computer boots, or reboots, the president of the voting office or Center where the computer system is used will have to present the boot credential to the computer again. The software of the bootable CDROM will refuse all operation unless this code has successfully been presented. Once activated, the computer system first performs a self-test to confirm that all its components (barcode reader, RFID reader, display, printer...) operate correctly. During this self-test, the computer also checks the integrity of the configuration files.
6. **Casting a vote** is explained in detail above.
7. **The deactivation of the computer system** takes place at the end of the Election Day. All computer systems are collected and centralized at the municipality or higher level to reset their BIOS settings to the factory defaults. Once reset, the computer systems can be disposed of or stored in a secure environment.

5.3 Basic components of the proposed improved paper-based voting system

There are three basic components of the proposed improved paper-based voting system: a **boot credential** used by the president of a voting office to start the voting computers, a **voting token** given to every eligible voter, and the **paper ballot** that is produced by the voting computer when the voter confirms his vote.

5.3.1 Boot Credential for the voting computers

The boot credential for the voting computer consists of either a password to be entered through the voting computer's touch screen or the combination of a chip card with PIN which the president of the voting office receives (through separate letters) a few days prior to the Election Day. If the boot credential is stored on a chip card, the president of the voting office first has to enter the chip card in the voting computer's smart card reader, after which he presents the PIN via the touch screen of the voting computer.

In either case, the president of the voting office receives the secret access credentials a

few days prior to the Election Day.

5.3.2 Voting Token for the voter

The president of a voting office provides a voter with a voting token with which the voter can instruct the voting computer to start the voting process. A voting computer will not start the voting process unless it has been activated with a voting token. This is to avoid double voting: the voting token guarantees that one token results in one voting ballot. The token has three states: NOT_USED_FOR_VOTING, VOTE_BEING_PRINTED and USED_FOR_VOTING.

There are two options for the voting token:

- the voting token is different from the voting ballot, namely a chip card that has to be inserted in the smartcard reader of the voting office, or
- the voting token equals the voting ballot. In this case, the voter presents the voting ballot to the voting computer to start the voting process.

If a voting office uses chip cards as voting token, the president of the voting office receives a pile of chip cards with which the voting computers can be activated. These chip cards are in the NOT_USED_FOR_VOTING state. Each eligible voter receives one chip card to cast his vote. As soon as the voter confirms his choice, the voting computer first changes the state of the chip card into VOTE_BEING_PRINTED, after which it prints out the corresponding voting barcode ballot. It subsequently brings the voting token in the USED_FOR_VOTING state which deactivates the chip card. If the state of a chip card indicates that a voting ballot has already been prepared with that chip card, the voting computer will refuse to start the voting process.

There exists no link between the chip card and the paper ballot. The chip card is only used to guarantee that a voter can produce at most one voting ballot, which makes it impossible to use this chip card to link a voter with a particular ballot.

If a voting office uses voting ballots as the voting token, the president of the voting office receives a pile of voting ballots in the NOT_USED_FOR_VOTING state and a pile of blank envelopes if these ballots have to be inserted into an envelope to protect the secrecy of the voter's choice. An RFID chip is embedded in each of the paper voting ballots. Each eligible voter receives from the president of a voting office a blank voting ballot and a blank envelope (optional) to cast his vote. The voting computer starts the voting process as soon as it detects that the voter has inserted a blank voting ballot in the printer. Once the voter confirms his vote, the voting computer brings the voting ballot in the VOTE_BEING_PRINTED state, prints the vote on the paper ballot, and writes the vote in encrypted form to the RFID chip that is embedded in the paper voting ballot. This brings the voting ballot in the USED_FOR_VOTING state. After the voter has confirmed that the printout corresponds with his vote, the voter folds the paper ballot or inserts it in the blank envelope. This guarantees that the voter's choice cannot be accessed by unauthorized people. If the voter should present a voting ballot of which the RFID chip is in a state different from the NOT_USED_FOR_VOTING, the voting computer will indicate this fact to the voter, after which the voter will not be able to cast a second vote with this voting token.

5.3.3 Paper ballot for the voter

The paper ballot will be produced by a printer as specified above. If the voting token equals the voting ballot (and the voter inserts this ballot himself in the printer), then

the voting computer will print the voter's choice on the paper ballot. If not, the voting computer will print the voter's choice on either a ticket similar to train tickets and airline boarding passes, or on a paper ribbon similar to a supermarket receipt.

If the voting token consists of a chip card, the voting computer produces at the end of the voting process a voting ballot as depicted in Figure 2. In the other case, the voting ballot looks similar to the ballot shown in Figure 3. The details printed on either ballot are specified in the subsequent sections, but can be summarized as follows:

(i) a human readable text with the list of parties and candidates for whom the voter has cast his vote, and

(ii) a machine readable part in which an encrypted version of the voter's choice is stored. The machine readable part makes it easy to read the voting ballots at the end of Election Day.

The voter is expected to inspect the human readable information of the paper ballot to confirm that it corresponds with the votes cast on the voting computer. After this inspection, the voter folds the paper ballot (that was produced after the voter presented the voting chip card to the voting computer) as indicated on the vertical dotted line of the ballot. The result is a folded ballot booklet. In order to make sure that the folded voting ballot does not spontaneously unfold, the ballot can be either folded twice (as indicated in Figure 2 with the horizontal dot-stripe line), or it can be sealed like an envelope with an adhesive strip (Redi-strip closure). The second option is preferred when using a ticket or label printer, because these tickets are fixed size and a ticket or label printer is capable of processing ribbons with tickets/labels of this nature. If it is not possible to use ticket printers, it is not possible to seal the folded ballot like an envelope; in that case, it is recommended to fold the ballot twice, as explained above. Note that the spontaneous unfolding of a folded ballot may not be an issue if the voting urn that collects the voting ballots is not transparent.

If the voting ballot equals the voting token, then the voter insects the human readable information of the paper ballot, and folds the paper ballot or inserts it in the blank envelope if he receives one from the president of the voting office.

After the voter has folded the ballot, or has entered the paper ballot in the blank envelope, he shows it to the president of the voting office so that the latter can confirm that the voter did not add any marks to the voting ballot that could identify the voter. If the ballot contains no visual marks, the president of the voting office returns the ballot to the voter, who deposits it in the voting urn.

Before depositing the ballot in the voting urn, the voter may present the ballot to a barcode or RFID reader. This provides the voter the possibility to immediately detect whether the machine readable part of the ballot (i.e., the barcode or the RFID chip) will be useable at the end of Election Day. if the machine readable part of the ballot turns out to be unreadable, the voting ballot is nullified, and the voter can cast a second time.

The information in the machine readable part of the voting ballot is encrypted to prevent unauthorized access to the voter's choice, e.g., if a third party would take a picture of the barcode, or would read the RFID chip with a personal RFID chip reader. The information is encrypted using a public encryption key of the Ballot Decryption Center to which the voting office is associated. This guarantees that only the Ballot Decryption Center is able to decrypt the information stored in the machine readable part of the voting ballot. It is the responsibility of the Election Authorities to securely generate the key pairs for the different Ballot Decryption Centers. The key pair

generation must in all cases take place in a secure environment to prevent unauthorized parties from decrypting the machine readable parts of a voting ballot.

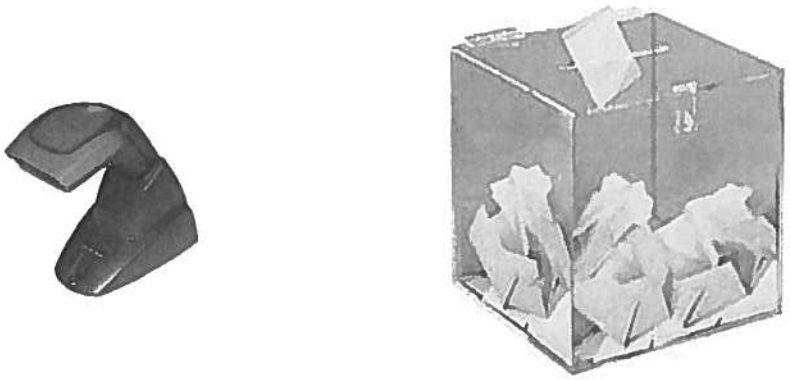
The integrity of the information stored in the machine readable part of the voting ballot (barcode or RFID chip) is protected through a digital signature calculated by the voting computer using the private signing key that corresponds with the voting office. All the voting computers of a voting office share the same signing key to prevent that the voting ballot can be linked with a particular voting computer or voting booth. This signature also prevents the injection of voting ballots that did not originate from one of the voting offices, e.g., from a fraudster. The Election Authorities provide the initializer of the configuration files that are stored on the bootable CDROM used to boot the voting computers with the private signing keys with which the voting computers have to digitally sign the encrypted information of the machine readable part of the ballot. This private signing key is stored in the configuration file of the voting office. This configuration file is encrypted with the AES using a key that is derived from the boot credential of the president of the voting office.

Note that signing the information that is stored in the machine readable part of a voting ballot does not compromise the secrecy of the vote, as all the voting computers in a voting office share the same private signing key, i.e., every voting computer could have been used to produce this signature. The signature links the voting ballot to the voting office, not to the voting booth. It is impossible to link the signed ballot to the voter.

5.4 Voting Urn

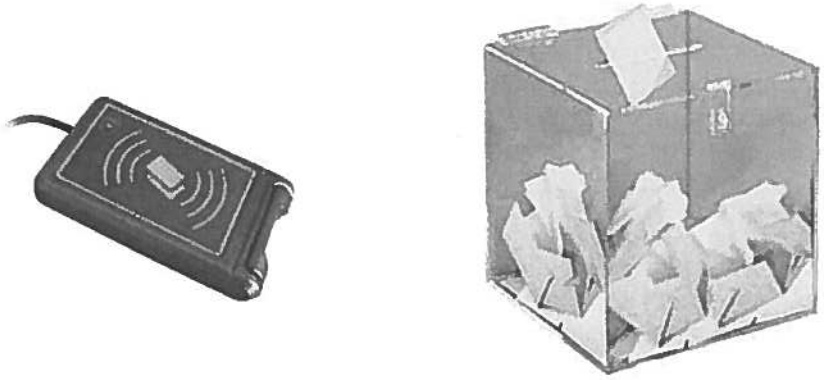
The voting urn collects the ballots that are produced by the voters by means of the voting computers in the voting booths of the voting office. If barcode ballots are used, it is very likely that the folded ballots will unfold spontaneously after they have been inserted in the urn, it is therefore important to use a non-transparent voting urn. The voting urn that is used should be compatible with the models approved by the relevant Royal and Ministerial Decrees on election equipment.

As mentioned earlier, the voter has the possibility to check the validity of the machine readable part of the voting ballot. The voter can present the machine readable part of the voting ballot to a suitable reader (i.e., barcode or RFID reader) to confirm that the machine readable part of the ballot is technically valid. If this is the case, the voter can safely deposit the ballot in the voting urn. However, if this is not the case, the cause of this reading problem must be further diagnosed, and the necessary measures must be taken to resolve the problem. If it is a technical problem, the voter is given a second voting token with which he can cast a vote for the second time.
It should be stressed that the checking the technical validity of the machine readable part of a voting ballot does not compromise the secrecy of the vote, as the information in the machine readable part is encrypted under a key that is only known to the Ballot Decryption Center to which the voting office is associated.
Figure 20 and Figure 21 depicts the hardware necessary for a voting urn when using barcode ballots or RFID ballots, respectively.



Barcode Reader Ballot Box Copyright:
George Patton Associates, Inc.

Figure 20: Voting urn with barcode ballots



RFID Reader Ballot Box Copyright:
George Patton Associates, Inc.

Figure 21: Voting urn with RFID ballots

5.5 Verfiying the validity of the ballots

As mentioned above, the voter has the possibility to present his ballot to a standalone (RFID or barcode) reader before entering the ballot in the voting urn.
This standalone reader does not store the information read from the machine readable part of the voting ballot. Note that the machine readable information of the ballot is encrypted under a key known only to the Ballot Decryption Center.
Reading the machine readable part of a ballot before entering the ballot in the urn avoids losing votes, as hardware failures (e.g., erroneous barcode printing, unaccessible RFID chip) are detected at the voting office, rather than at the Ballot Reading Center.

5.6 Procedure Details

The procedure to initialize the bootable CDROMs for the voting computers and the computers used at the Ballot Reading/Decryption/First Totalization Centers is

discussed in this section.

5.6.1 Before Election Day

Before the voting computers can be used on the Election Day, the voting computers have to be acquired or obtained, configured, tested and installed.

5.6.1.1 Acquisition of the Voting Computers

As part of the preparation of an election, the voting computers must be acquired or be made available, e.g., using a service contract.

The supplier of the voting computers may specify the BIOS credentials of the voting computers during manufacturing. These credentials typically consist of a password that protects the core features of the computer such as the order in which different boot media are tested (e.g., floppy, CDROM, USB memory stick). Only the system administrators who have the correct BIOS credentials (userid/password will be allowed to manage and configure specific hardware features of the computer system.

5.6.1.2 Design, Development & Testing of the Election Software

The election software is the combination of all the software necessary at the voting booths, Ballot Reading Centers, Ballot Decryption Centers, and (First) Totalization Centers. This software is mostly independent of actual elections: the voting software manages the user input, displays information on the display according to the supplied configuration files, outputs audible information for visually impaired voters, and prints out the paper trail.

The election-specific information (number and names of elections, number and names of parties per election, number and names of these parties, the screen layouts and the layout of the paper ballots) is specified in the configuration files of the election software.

The election software is thus the core that manages the behavior of the voting computer during the voting process.

The creation of this core happens in different steps:

Step 1. Specification of the voting software using state-of-the-art specification methods and tools;

Step 2. Design of the voting software;

Step 3. Validation of the design of the voting software by an external party to confirm that the design corresponds with the software specifications;

Step 4. Development of the voting software;

Step 5. Testing and validation of the voting software using the voting computers that will be used on Election Day.

The development process proceeds to the next step if and only if the current step was completed successfully. If problems or issues are discovered in the current step, the process goes one step back. For instance, if the testing reveals problems, the development step has to be resumed; if the development encounters issues, the design of the voting software may have to be reviewed, which would trigger the validation of the design change, etc.

5.6.1.3 Certification of the Voting Software

Once the voting software and configuration has been successfully tested, the external certification can be started. If necessary, the design-validation-development-testing steps have to be iterated.

Once the certification process of the voting software is finished, the software can be made public and published. The certified version should be digitally signed to avoid unauthorized modifications to this version.

5.6.1.4 The configuration files

The configuration files of a voting computer specify for which elections (e.g., European, Federal, Regional, Local...) the computer will be used, together with the list of parties and their candidates for which the voters will be able to cast their vote electronically. These lists can be specific for each municipality. For instance, for local elections, the local council will be elected. In this case, all bootable CDROMs used with the voting computers that belong to the territory of that local council will share the same configuration file.

The paper ballot that is produced at the end of the voting process consists of two parts: a human readable part and a machine readable part (cf. section 5.3.3 above). The layout of the voting screens and the paper ballots is also specified through the configuration files of the voting computer.

The list of Elections, Parties and Candidates

The configuration file of the voting software enumerates the list of elections, parties and candidates that can be elected during the election. These lists must be encoded in a form that is suitable for use with the voting software, e.g., the Election Markup Language (EML). This encoding may be automated for personnel charged with producing these lists using conversion software (that has to be made available) and that produces outputs compatible with the voting software. Specifying the actual content of the lists of elections, parties and candidates is outside the scope of this document.

The encryption key(s) for the machine readable part of voting ballots

The initializer of the configuration files includes the public encryption key of the Ballot Decryption Centers in the configuration files of the voting computers.

If the initializer created the encryption key pair for the voting office's Ballot Decryption Center, it will provide the private decryption key to the corresponding Center, so that it is able to decrypt the encrypted ballots created by the voting computers of that voting office. The public encryption keys are included in the configuration files that are stored on the bootable CDROM used to start the voting computers.

Preparation of the voting office's signing key

The Election Authorities need to provide the private signing key that must be used by the voting computers of a voting office. This key pair also has to be created in a secure environment to prevent unauthorized parties to get access to this private signing key, which would allow fraudsters to create counterfeit paper ballots.

5.6.1.5 Designing the layout of the voting screens

The configuration files of the voting software also specify the layout of the voting screens. The guidelines specified in the following subsections must be taken into account while designing the layout of the voting screens.

Casting a Vote

The electronic voting systems should be walk-up-and-use. When the voter arrives at the electronic voting system, it should be clear how to operate the electronic voting system and which actions the voter needs to perform to successfully cast a vote. In order to enhance the usability of the voting system, it is possible that the system needs to provide instructions for the user. The instructions should:

- provide clear, simple and easy-to-understand text explanations in combination with indicative pictures of the user-interface for the voting process;
- provide simple and clear task-based instructions for using the system;
- be clearly readable to all users;
- guide the user through the steps of the voting process;
- be field-tested by a set of representable voters prior to the elections;
- provide instructions that are accessible to all potential voters;
- match the instructions to the labeled buttons

Information presentation

The presentation of information on the screen and on the printed ballots should be readable and intuitive to the user. The user should be able to read the instructions and the printed ballots comfortably.

- Typography:
  - consistently use one type of font throughout the voting system;
  - consistently use one type font style throughout the voting system;
  - avoid the use of italic font style on screen displays;
  - select font-type according to function
  - use serif typography to improve line per line reading.
- Color usage:
  - choose a usable and clear background-text contrast;
  - use background color and text color consistently through the entire voting system.
- Language:
  - consistent language use throughout the voting-system;
  - simple and meaningful language for a wide range of users (expertise, education, literacy).
- Labeling:
  - consistently use meaningful and clear labels throughout the voting system;

- use meaningful labels: the label should clearly indicate the function of a button;
- match instructions to the used labels;

- Ballot layout/representation:
  - When people are presented with a sample ballot prior to the elections, the location of each candidate on this ballot should be similar to the location of the candidates on the screen of the voting machines, as people frequently use localization strategies and remember the position the desired candidate is in.

In order to prevent errors due to use of heuristics, the voting system should use the following principles:

- icons (for parties) or pictures (for candidates) that allow voters to easily find their preferred party or candidate;
- a logically ordered list to find the preferred candidate or party;
- fonts that easily allow scanning through the voting screens;
- when providing an overview of all possible candidates or parties, not all candidates of every party should be displayed simultaneously on the screen, as the amount of all available information will be overwhelming and, consequently, the user will experience difficulties finding the needed information. Allow voters to first select the party for which they would like to vote. After selection of the desired party, display all candidates of the selected party for whom one can vote for that election.

Navigation

It is of essential importance that voters are able to confidently and easily navigate through all menus and feel that they have control over the voting process and their vote. Therefore:

- the system should allow users to control the pace of the voting process;
- the system should use controls for navigation that are clear and intuitive (stimulus-response compatibility: they should receive a visual feedback (or audible feedback for visually impaired people) to confirm their action was taken into account, e.g., by highlighting the name of the candidate whom the voter just selected);
- the system should provide clear labels for the various action buttons;
- the controls should be organized in order to prevent accidental completion of the ballot;
- the system must make input as simple as possible (for example, touch the relevant option on the touch screen);
- the system should avoid scroll-bars: all necessary information should fit on one screen;
- the system should provide clear feedback about one's position in the voting process. Breadcrumbs, for example, may provide a clear indication for which election or party one is voting;
- the number of actual steps to any process in the voting system should be

limited to 3: no menus of procedures with a deeper hierarchy of choices than 3 should be used;

- provide easy and simple navigation: back, forward and cancel;
- present a back button in each screen of the electronic voting system (except on the start/first screen and a back button guiding back to the previous election for which one has already cast a definite vote);
- buttons should immediately yield an action and should not be activated by pushing on a start button afterwards;

The system should not jump displays: The pace of change in displays should not be too rapid in order to avoid that voters feel that they lose control over the voting process. Still, it should not be unreasonably slow either.

Navigation Format

Paper analogue navigation

Paper-like navigation for electronic voting systems allows the user to flip the different voting screens in a traditional paper- or book-like manner. One has to flip the pages of the book to the desired party list in order to view the list of candidates for this party. This voting system allows older users to vote in a manner close to that of traditional paper ballot voting, making it easier to use based on habit. The analogy with a book makes the voting system more intuitive to use.

Touch screen

Touch screens are intuitive to use. One simply has to touch the area on the screen on which the desired candidate or option is represented. Still, touch screen voting systems can be troublesome when the user is not familiar with touch screen technology or if the touch screen has not been properly calibrated. To deal with voters who are not familiar with touch screens, the system must initially (or consistently) provide the instruction to touch the desired choice on the touch screen to select that candidate or to perform the presented action. In order to avoid favoring any candidate or party, touch areas should be:

- of equal size for all parties;
- of equal size for all candidates;
- at least :
    - 2 cm by 2 cm (minimally = size of a finger);
    - spaced apart by minimally 3 mm;

The following issues should also be taken into account:

- Possible danger with touch screens: parallax causes the user to push in a location in which he did not intend to push;
- The system should provide feedback when the screen is touched (highlighting and/or sound);
- Avoid scrolling on a touch screen;
- Touch screens do not allow special navigation possibilities: No drag-and-drop, drop-down menu's, multiple windows, double clicks. These actions should be avoided for electronic voting systems because of their non-intuitive nature;

- Limit the amount of hand movements to complete the (voting) tasks:
  - each time a choice has to be made, a part of the screen will be occluded by the hand;
  - avoid arm fatigue;
  - choose the location of the touch areas as intuitive as possible;
- Avoid the representation of the cursor on the screen: users will focus on the screen, not on the cursor;
- Use a bright background for touch screens to diminish the visibility of fingerprints;
- Make sure the room in which the voting system is place is correctly lit in order to avoid glare on the screen. Avoid directing light at the screen;
- The angle of the screen needs to be adapted to the position of the user (also cf. Figure 22):
  - Sitting user: 30°;
  - Standing user: 30°-55°;
  - Ideally the screen should be adaptable by the user himself.

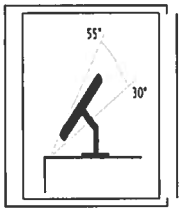


Figure 22: The ideal angle of a touch screen

Verification of the vote

Reviewing the vote

After a voter has selected his preferred candidate(s), he should be given the opportunity to review his choices before confirming his vote for the current election. Therefore, the system must present an overview of the selected candidates and provide two options: 'change votes' and 'confirm votes'. Enough feedback should be provided in the review screen in order to make it clear that a review of the selected votes is presented and that confirmation or corrections are possible. The review screen should have the same layout as the voting screen in which the initial choices were made.

Correcting or changing a vote

When the user, during the casting of the vote or during the review of the vote, decides that he wants to change one or several choices, it should be easy to do so in either phase.

- Removing a vote for a candidate should be possible by selecting the candidate and indicating the wish to remove the vote.
- Erasing all votes in a list of candidates in order to deselect a single candidate should be avoided. Clearing all previously made choices forces the person to recollect all previously selected choices. Erasing the complete ballot should be

offered as an option, but not as a standard way for correcting miscast votes.

- In case only one candidate can be chosen for a specific election, one has to be able to correct a vote by simply choosing another candidate. In this situation, it should be avoided to have to deselect the wrongly chosen candidate before selecting another candidate.
- Allow users to correct their mistakes on the spot, on the same screen in which the review or ballot is presented. Do not ask them to wait for an overview screen at the end of the voting procedure before they can correct a choice. Error recovery should be possible instantaneously; otherwise, voters might forget to apply the correction.
- Make it impossible to over-vote. Remind the voter that votes for candidates of multiple lists are not accepted. This can be achieved by erasing the votes on individual candidates when returning to the screen in which the different lists are presented for selection. This yields the advantage that no over-voting can take place, but has as disadvantage that when one mistakenly returns to the list selection screen, all previously selected votes are deleted.
- Make it impossible to under-vote, i.e., failing to vote for all elections organized on the same day.

5.6.1.6 Testing the voting process, the layout of the paper ballots and the voting screens with representative voters

The layout of the paper ballot, the voting process and the voting screens need to be tested with representative voters before final acceptance and inclusion in the configuration files of the voting computers.

5.6.1.7 Verification of the configuration files for a voting computer

The content of the configuration files of the voting computer, especially the election-specific lists (list of elections, list of parties, lists of candidates) and layouts of the paper ballots and voting screens must be verified carefully before they are copied to the bootable CDROM for the voting computers. Only after positive confirmation that they are correct should one is allowed to proceed with the installation of the configuration files as specified in the next section.

5.6.1.8 Installation of the configuration files for a voting computer on the bootable CDROM

The initializer of the bootable CDROM of the voting computers stores the configuration files on the image of this CDROM. The configuration files are self-contained, i.e., they contain all information that is needed by the voting software.

5.6.1.9 Issuing & Initialization of the Boot Credentials

The initializer of the image of the bootable CDROM for the voting computers specifies who will be able to activate the voting computers on Election Day.

The initializer will create a list of boot credentials with which the voting computer will be booted. Each president of a voting office receives the boot credentials for the voting computers of his voting office.

The boot credentials are generated by the initializer in a secure environment.

5.6.1.10 Initialization of the Voting Tokens

The voting tokens are initialized prior to the Election Day: each voting token is initialized with the "NOT_USED_FOR_VOTING" state.

5.6.1.11 Distribution of the Boot Credentials

Before the Election Day, each president of a voting office, Ballot Reading Center, Ballot Decryption Center and First Totalization Center receives the boot credentials that correspond with the computers of his voting office or Center. This boot credential is used to start the computer with the bootable CDROM sent to the same president. Without this boot credential, it is impossible to use the computer during the Election Day.

This boot credential is to be kept secret, to avoid unauthorized use of the election software.

5.6.1.12 Distribution of the Voting Tokens

A voter receives a voting token from the personnel of the president of a voting office after he is identified as an eligible voter. The voter presents the voting token to the voting computer in order to start the individual voting process in the voting booth.

The voting tokens that are specific to the voting office are distributed to the respective voting offices prior to the Election Day.

Procedural means must ensure that an eligible voter receives exactly one voting token to prevent voting more than once.

5.6.2 Close to Election Day

5.6.2.1 Distribution of the computers

The computers used at the voting offices, Ballot Reading Centers, Ballot Decryption Centers and First Totalization Centers are not linked to a specific location, a sufficient number of computers is distributed to each of these locations prior to the Election Day.

5.6.2.2 Distribution of the bootable CDROMs

The bootable CDROMs that a president of a voting office, Ballot Reading Center, Ballot Decryption Center and First Totalization Center use to start their computers is distributed to these presidents prior to the Election Day. The Boot Credentials of the president of the voting office where a voting computer is booted determine which configuration file from the bootable CDROMs will be used for that voting computer.

5.6.2.3 Installation of the voting computers

The installation of a voting computer is very straightforward: the computer, its display, USB devices and its printer have distinct connectors, so that cable mismatches have a very low probability of occurrence.

5.6.2.4 Accessibility of the Voting Booths and Voting Computer

As voting is a democratic right (sometimes an obligation) for all citizens, having adequate access to the voting activities must be guaranteed to everyone in all

circumstances.

5.6.2.4.1 Specific Accessibility Guidelines

These guidelines have been put together based on documents from:

- a ministerial committee report of the Council of Europe[8]
- information from the GAMAH association[9]
- recommendations of the European Parliament's Disability Intergroup[10].
- the Belgian anti-discrimination act of 2003
- the UK Disabled Rights Commission[11]

1 All authorities (and preferably also the political parties) involved in information distribution via the Internet should respect the Anysurfer guidelines[12] for accessible web page design. Anysurfer testing should be made compulsory for official websites related to the voting process. Attention must be paid to persons who need easy-to-read information.[13]

2 Official websites must also propose an adapted simulation of the electronic voting procedure so that reading impaired persons can try out the procedures before going to the voting place itself.[14]

3 Representative users shall be involved in the design of eVoting systems, particularly to identify constraints and to test ease of use at each main stage of the voting software development process.[15]

4 Consideration shall be given, when developing new products, to their compatibility with existing ones, including those using technologies designed to help people with disabilities.[16]

5 The electronic voting machines must have adapted outputs such as large characters and a synthetic voice (e.g. with headset)[17]. In order to gain experience the development of experimental accessible voting machines and their testing should be stimulated.

6 When producing printed information material (flyers, brochures) related to the elections, authorities should make sure that different accessible formats are

---

8 http://www.cev.ie/htm/report/second_report/pdf/Appendix_6_Recommendation_Rec(2004)11.pdf

9 Résultats de l'enquête – Electeurs à mobilité réduite ou présentant des difficultés de compréhension: citoyens à part entière ou entièrement à part? ed. par GAMAH (October 2006); available at : http://www.gamah.be

10 http://www.edf-feph.org/apdg/Documents/Report_of_the_Disability_Intergroup_meeting_Barriers_to_elections_for_disabled_people.doc

11 http://www.drc.org.uk/docs/10_434_10_434_17_nov_version_.doc

12 http://www.anysurfer.be/

13 Based on Council of Europe guideline nr 63 and on the GAMAH study

14 Based on the Gamah study

15 Based on Council of Europe guideline nr 62 and on the recommendations of the European Parliament's Disability Intergroup (Sarah Gull)

16 Based on Council of Europe guideline nr 64

17 Based on conclusions of the GAMAH study; instead of headsets, GSM based communication (e. g. Bluetooth) may be conceived in the future but will probably be much too complicated for modal users.

available for reading-impaired persons and other disadvantaged groups in the community.[18]

7 Key access standards must not have the appearance of "optional extras": they must be considered core obligations; this should be reflected in any government procurement for voting equipment.[19]

8 Physical access: voters with disabilities should have the choice to vote in voting places providing adequate access. On a longer time scale, administrations should strive to make all voting places accessible to all voters. Voters with disabilities must also be guaranteed the right to be accompanied in the voting booth by a person of their choice. Sufficient accessible parking places must be planned close to the voting places. Chairs must be available for persons who have to wait before casting their vote. The height of voting screens should be adapted for persons in a wheelchair or, better, should be adaptable[20].

9 Polling station personnel should be trained in disability awareness.[21]

10 After every election, care should be taken to collect feedback from voters with disabilities in order to find out what should be improved for the next election!

5.6.3 Start of Election Day

5.6.3.1 Activation and booting of the voting computers

The president of a voting office uses the bootable CDROM and his personal secret boot credential to boot a voting computer.

Each president of a voting office has received such bootable CDROM and these boot credentials prior to Election Day.

It is up to the Election Authorities to decide who gets which boot credentials.

5.6.3.2 Identification of an eligible voter with convocation letter

The personnel of the voting office shall have obtained a list enumerating all eligible voters for this office. Whenever a voter presents himself at a voting office with his convocation letter and his identification documents, the voting office personnel verifies whether that person is an eligible voter, and that he presents himself at the correct voting office. If this is the case, the voter receives a voting token (cf. section 5.6.1.12 above), which will start the individual voting process on the voting computer in the voting booth.

5.6.3.3 Using the voting computer

As soon as the voter presents the voting token received from the personnel of the voting office, the voting computer starts the voting process, showing the first screen of the election. The content and layout of this screen is determined by the

18 Inspired by the Belgian Anti-Discrimination act of 2003 and on DRC guideline 4.2
19 Based on DRC guideline 3.6
20 Based on conclusions of the GAMAH study; incorrect screen height might lead to parallax errors (people touching the wrong buttons)
21 Based on the recommendations of the European Parliament's Disability Intergroup (Sarah Gull)

configuration file of the voting software (cf. section 5.6.1.4 above).

The voter follows the instructions displayed on the voting computer's display and uses the computer's touch screen to cast his vote(s) and to proceed from one screen to the other.

Eventually, the voter confirms his vote(s), after which the voting computer prints out the voting ballot.

5.6.3.4 Verification of the paper ballot by the voter

After the voting computer has printed the paper ballot, the voter inspects the human readable text of this ballot to confirm that the computer effectively encoded the votes he has cast with the voting computer.

Subsequently, the voter folds the paper ballot as indicated on the ballot, or inserts it in the blank envelope, after which he leaves the voting booth and proceeds to the president of the voting office (cf. section 5.3.3 above).

5.6.3.5 Inspecting the voting ballot with respect to marked ballots

The president of the voting office inspects whether the visual parts of the voting ballot contains visual marks. Without opening the ballot.

5.6.3.6 Technical Verification of the Voting Ballot's Machine Readable Part

Before depositing the voting ballot in the voting urn, the voter may present the barcode ballot to the barcode reader of the voting urn, or the RFID ballot to the RFID reader of the voting urn. If this reader indicates that the machine readable part of the ballot cannot be read, the troubleshooting mechanism is activated, and the voter is invited to continue casting his vote.

5.6.3.7 Depositing the ballot in the voting urn

The voter deposits the folded or enveloped voting ballot in the voting urn.

5.6.3.8 Collecting proof of identification and stamped convocation letter

Once the voter has entered the ballot in the voting urn, the voter collects his identification documents and his convocation letter from the voting office's personnel.

5.6.3.9 Random audits during Election Day

During the Election Day, random audits can take place to guarantee that the voting process functions correctly and that all procedures are respected.

5.6.4 End of the voting period on Election Day

At the end of the voting period on Election Day, a specific role is assigned to the independent Auditors of the elections: they have to confirm and witness that all critical operations have been correctly executed, e.g., that all partial results of the lower Totalization Centers are taken into account at the higher Totalization Center.

5.6.4.1 Transporting the voting urns to the Ballot Reading Centers

At the end of the voting period on Election Day, the president of the voting office seals the urn contain the ballots and ensures the local transportation of this urn to the Ballot Reading Center. Sealing the voting urns guarantees that no votes can be inserted in the voting urn after closing the voting office.

5.6.4.2 Shuffling the content of the urns

As soon as the voting urns are collected at the Ballot Reading Centers, the president of this Center will break the seals of the voting urns and collect the ballots contained in each of them. Subsequently, all voting ballots are shuffled to break the chronological order in which they were entered in the urns.

5.6.4.3 Reading the machine readable part of the voting ballots

The machine readable part of each of the voting ballots is electronically read in the Ballot Reading Center. This results in an electronic enumeration of all the ballots that were processed by this Center. This electronic enumeration is digitally signed using the electronic identity card of the president of the Ballot Reading Center who is responsible for reading the encrypted voting ballots. This digitally signed electronic enumeration of encrypted voting ballots is then sent to the Ballot Decryption Center that is associated with this Ballot Reading Center for further processing.

5.6.4.4 Processing the encrypted votes at the Ballot Decryption Center

At the Ballot Decryption Center, the digitally signed electronic enumerations of encrypted votes are decrypted. The Ballot Decryption Center sorts the received encrypted ballots and applies the relevant decryption key to reveal the voting ballot from its encrypted form.

The list of unencrypted voting ballots is provided to the First Totalization Center associated with this Ballot Decryption Center. This list is digitally signed using the electronic identity card of the president of the Ballot Decryption Center before it is sent to the Totalization Center.

5.6.4.5 Processing the partial results of the Counting Center by the First Totalization Center

The voting officials active at the First Totalization Center collect the partial election results from their Ballot Decryption Centers and totalize these results. These lead to partial results which are digitally signed using the electronic identity card of a voting official active at this Center, after which they are provided to the Second Totalization Center.

5.6.4.6 Processing the partial results of the First Totalization Center by the Second Totalization Center

The voting officials active at the Second Totalization Center collect the partial election results from their First Totalization Centers and totalize these results. These lead to partial results which are digitally signed using the electronic identity card of the president of this Center, after which they are provided to the Final Totalization Center.

5.6.4.7 Processing the final results at the Final Totalization Center

The voting officials active at the Final Totalization Center collect the partial election results from the Second Totalization Centers, and totalize these results. As soon as all their partial election results are collected and processed, the final election result is known, after which this can be published.

5.6.5 After the Election Day

5.6.5.1 Auditing the elections

Independent auditors can audit the elections by randomly selecting voting ballots from various Ballot Reading Centers. The task of these auditors consists of verifying whether the human readable text of the paper ballots corresponds with the machine readable part of the paper ballots. They do so by asking the Ballot Decryption Center to decrypt the ballots they randomly selected, after which they verify whether the decrypted information equals the human readable information. This audit guarantees that the voting computers have correctly encoded the voter's choices, assuming that the voters verified the content of the human readable part of the paper ballot before folding it or before it is inserted in the envelope.

5.6.5.2 Resetting the voting tokens

At the end of the election period, the voting chip cards are reset to their NOT_USED_FOR_VOTING state.

5.6.5.3 Resetting the BIOS of the computers

At the end of the election period, the BIOS settings of the computers used at the voting offices, Ballot Reading Centers, Ballot Decryption Centers and First Totalization Centers are reset to their factory defaults. As these computers do not contain any persistent storage media, no further action other than this BIOS reset is necessary.

5.7 Legal Compliance of the Improved Paper-based Voting System

5.7.1 Legal Situation of the Voting Ballots

The voter uses a voting computer to cast his vote. Once he has confirmed his vote, a paper ballot is printed in the form of an unfolded ballot booklet or in the form of an RFID ballot. This ballot consists of two equivalent parts: a machine readable part and a human readable printout of the votes cast by the voter.

The voting computer encrypted the machine readable part of the ballot to protect the anonymity of the voter and to prevent duplication or insertion of votes.

The voter is asked to verify that the human readable printout matches the votes having been cast. If it does, the voter folds the ballot as if it were a booklet, or inserts it in a blank envelope. Once the ballot is folded, only the barcode remains visible. After the RFID ballot is folded or inserted in an envelope, it is no longer visible for the president of the voting office.

The voting office's president checks whether the outer sides of the ballot contain

visual marks that could identify the voter. If the ballot does not contain any such marks, the voting office's president returns the ballot to the voter, who deposits the ballot in the voting urn.

In case the election result is contested, recounting the ballots consists of again reading the machine readable parts of the ballots. It is also possible to recount the ballots on the basis of the human readable part of the ballots (which first need to be opened).

This process raises two main concerns from a legal point of view. The fact that the voter could reveal the content of his vote to third parties between the moment he leaves the voting booth and the moment he inserts his ballot into the urn should be regulated so that the free expression of the voter is guaranteed. Furthermore, the use of a hybrid ballot (i.e., a ballot with a human readable part and a machine readable part in the form of a barcode or an RFID chip) calls for a legal definition of what constitutes an authentic ballot and for a specification of the treatment of invalid ballots when a manual recount is carried out.

Free expression of the voter's will – A risk exists that the voter breaches the secrecy of his vote (because of external pressures) and reveals the content of his vote to third parties between the moment when he exits from the voting booth and the moment he introduces his ballot into the urn. However, this situation remains very similar to the current situation in polling stations which use normal paper ballots. To this effect, Article 143 of the Electoral Law states that it is forbidden to unfold or open a ballot when leaving the voting booth in such way that the content can be seen. If the voter unfolds or opens the ballot, the president of the voting office must take the unfolded ballot, invalidate it and invite the voter to cast a new vote. Similar provisions should apply to these ballots that are produced with a voting computer. Folding a ballot like a booklet, or folding it twice, would prevent spontaneous unfolding of the ballot, but this might increase the voting complexity from the voter's perspective.

Use of hybrid ballots – The use of hybrid ballots, i.e. voting ballots which consist of both a human readable and a machine readable part creates the risk of discrepancies during a recount because electronic ballots cannot be deemed invalid while paper ballots may be invalided if they contain extraneous markings.

With the system proposed a risk exists when it is decided to recount ballots based on the human readable printout, i.e., based on the inner part of the folded barcode ballot or on the human readable text of the RFID ballot. Indeed, when opening the ballot, the re-counter may discover marks on the inner part of the envelope or on the side containing the human readable part of the ballots, or even objects which should lead to the ballot's nullification according to article 157 of the Electoral Law. As mentioned above, these rules are meant to protect the secrecy of the vote and prevent that the ballot could be linked to a voter.

A first possibility consists in deciding that the human readable part of the paper-based ballot ***is*** the authentic ballot. The consequence would be that, from the moment the election is contested and a manual recounting is required, the definitive result will be given based on recounting the human readable parts of the voting ballots, as opposed to the machine readable part of the ballots. Recounting these ballots might require the automated direct optical scanning of the human readable part of the ballots, as this first possibility would rule out the use of the machine readable part of a voting ballot for recounting purposes.

A second possibility would be to give a legal validity only to the machine readable part. The printing of the names of the candidates on the ballot would only have an informative value. The human readable part would only inform the voter of the data

contained into the machine readable part. This solution would not however allow performing the recounting on the basis of the information printed in the ballot, as the only legal ballot is constituted by the machine readable part, namely the barcode of a barcode ballot or the RFID chip of an RFID ballot. In this case, rereading the contested voting ballots using different but interoperable equipment would thus be necessary.

5.7.2 The 112 Recommendations of the Council of Europe

This section evaluates the proposed improved paper-based voting system with respect to the Recommendations of the Council of Europe concerning eVoting systems.

5.7.2.1 Legal Standards

Principles

Universal Suffrage

	Barcode or RFID ballot
1. The voter interface of an eVoting system shall be understandable and easily usable.	Similar to eVoting system currently in use.
2. Possible registration requirements for eVoting shall not pose an impediment to the voter participating in eVoting	Identical to traditional paper ballot voting.
3. eVoting systems shall be designed, as far as it is practicable, to maximize the opportunities that such systems can provide for persons with disabilities.	Similar to eVoting system in use. The proposed system also includes support for blind and bad eyesight people.
4. Unless channels of remote eVoting are universally accessible, they shall be only an additional and optional means of voting.	N.A.

Equal Suffrage

5. In relation to any election or referendum, a voter shall be prevented from inserting more than one ballot into the electronic ballot box. A voter shall be authorized to vote only if it has been established that his ballot has not yet been inserted in the ballot box.	The voting computer requires the presence of a voting token before it can be used by the voter to cast a vote. The presentation of one voting token results in the production of one voting ballot. One voting token = one ballot. Identical to traditional paper ballot voting: the voting ballot is introduced into the urn by the voter after identification and authorization by the President. The ballot booklets are digitally signed by the voting computers, which prevents the insertion of ballot booklets that did not originate from a genuine voting computer.
6. The eVoting system shall prevent any voter from casting a vote by more than one voting channel.	Only one channel is available.
7. Every vote deposited in an electronic ballot box shall be counted, and each vote cast in the election or referendum shall be counted only once.	Not applicable: the voting urn (ballot box) does not perform the counting. It is only a recipient in which the ballots are collected. Appropriate procedural measures and technical safeguards must be installed to prevent loss of voting urns or voting ballots.
8. Where electronic and non-electronic voting channels are used in the same election or referendum, there shall be a secure and reliable method to aggregate all votes and to calculate the correct result.	Similar to eVoting system in use.

Free Suffrage

9. The organization of eVoting shall secure the free	Identical to traditional paper ballot voting, guaranteed by

formation and expression of the voter's opinion and, where required, the personal exercise of the right to vote.	the use of a voting booth. The possibility of revealing the content of the ballot before inserting it into the urn is already forbidden by article 143 of Electoral law.
10. The way in which voters are guided through the eVoting process shall be such as to prevent their voting precipitately or without reflection.	The design of the voting software and process shall ensure that this requirement is met.
11. Voters shall be able to alter their choice at any point in the eVoting process before casting their vote, or to break off the procedure, without their previous choices being recorded or made available to any other person.	The design of the voting software and process shall ensure that this requirement is met. A procedure is available to void a ballot and have the possibility to restart the voting process if a voter claims that the printed ballot does not correspond with the content of his vote.
12. The eVoting system shall not permit any manipulative influence to be exercised over the voter during the voting.	Identical to traditional paper ballot voting; Privacy and free suffrage is guaranteed by voting in the voting booth.
13. The eVoting system shall provide the voter with a means of participating in an election or referendum without the voter exercising a preference for any of the voting options, for example, by casting a blank vote.	Identical to traditional paper ballot voting. The voter may be asked to confirm a blank vote.
14. The eVoting system shall indicate clearly to the voter when the vote has been cast successfully and when the whole voting procedure has been completed.	Satisfied with the printing of the ballot and its insertion into the urn.
15. The eVoting system shall prevent the changing of a vote once that vote has been cast.	The machine readable part of a voting ballot contains the encrypted vote of the voter. The voting computer digitally signs the encrypted vote before it is stored in the machine readable part of the ballot. As a voting computer signs this information, it is impossible to change the voter's choice once the voting computer has produced the ballot. Procedural mechanisms must guarantee that it is impossible to remove voting ballots from a voting urn, and to add ballots after the president of a voting office has sealed the voting urn at the end of Election Day.

Secret Suffrage

16. eVoting shall be organized in such a way as to exclude at any stage of the voting procedure and, in particular, at voter authentication, anything that would endanger the secrecy of the vote.	Identical to traditional paper ballot voting. The voter receives a voting token from the president of the voting office after he has been successfully identified as an eligible voter. The voting token is in no way linked to the voter: any voting token that was issued for use at a voting office will trigger the voting computer to start the voting process.
17. The eVoting system shall guarantee that votes in the electronic ballot box and votes being counted are, and will remain, anonymous, and that it is not possible to reconstruct a link between the vote and the voter.	Identical to traditional paper ballot voting. There is no direct link between a voting ballot and the voter. In particular, there is no information about the voter in the machine readable part of the ballot. At the end of Election Day, all voting ballots of a voting urn are mixed. Mixing these ballots breaks the chronological order between the voting ballots were deposited in the voting urn and , the order in which the Ballot Reading Center reads the machine readable part of each of the voting ballots.
18. The eVoting system shall be so designed that the expected number of votes in any electronic ballot box will not allow the result to be linked to individual voters.	Identical to traditional paper ballot voting. Totals for individual booths or for individual voting offices are not publicly available.
19. Measures shall be taken to ensure that the information needed during electronic processing cannot be used to breach the secrecy of the vote.	There is no direct link between a ballots and the voter. The randomization of ballots prevents establishing indirect links.

5.7.2.2 Procedural Safeguards

5.7.2.2.1 Transparency

20. Member states shall take steps to ensure that voters understand and have confidence in the eVoting system in use.	Each voting ballot contains a human readable part and a machine readable part. Critics of the electronic voting system that is used currently demanded the introduction of a paper trail to strengthen the confidence in the electronic voting system. The human readable part of a voting ballot serves as the paper trail. This trail can be verified by the voter before the voter folds the ballot or inserts the ballot in the envelope. Independent auditors can select a random set of ballot booklets to audit elections by confirming that the machine readable part of these randomly selected ballots corresponds with their human readable part. The voting computers do not contain any secret information that could link the identity of a voter with a particular voting ballot; the voting computers digitally sign the information of a machine readable part of the voting ballots to prevent insertion of alien ballots, this does not allow linking a particular voting ballot to a particular voter.
21. Information on the functioning of an eVoting system shall be made publicly available.	To be achieved by publishing the full specification of the electronic voting mechanism and the vote counting process.
22. Voters shall be provided with an opportunity to practice any new method of eVoting before, and separately from, the moment of casting an electronic vote.	Training facilities should be made available both on the Internet and in the municipalities.
23. Any observers, to the extent permitted by law, shall be able to be present to observe and comment on the electronic elections, including the establishing of the results.	No specific provisions needed. The College of Experts should be kept in charge of this process.

5.7.2.2.2 Verifiability and Auditability

24. The components of the eVoting system shall be disclosed, at least to the competent electoral authorities, as required for verification and certification purposes.	See general requirements.
25. Before any eVoting system is introduced, and at appropriate intervals thereafter, and in particular after any changes are made to the system, an independent body, appointed by the electoral authorities, shall verify that the eVoting system is working correctly and that all the necessary security measures have been taken.	Belgian law stipulates that this should be done by a College of Experts: no specific provisions needed.
26. There shall be the possibility for a recount. Other features of the eVoting system that may influence the correctness of the results shall be verifiable.	Two types of recounts are possible: a. automated recount with different reading equipment and/or software b. manual recount of human readable part of the ballots (unless electronic ballots are considered authentic ballots). The possibilities suggested by the CoE are the following: instruct the eVoting system to recount; transfer the electronic ballot box (voting urn) to a similar but distinct eVoting system and perform the second reading on this system; let the recount be performed by a different system which is interoperable with the eVoting system. This means that the CoE accepts that the recounting of the ballot booklets would involve rereading the machine readable part of a voting ballot.
27. The eVoting system shall not prevent the partial or complete re-run of an election or a referendum.	No specific provisions needed.

5.7.2.2.3 Reliability and Security

28. The member state's authorities shall ensure the reliability and security of the eVoting system.	Can be achieved by means of adequate procedures during pre-voting, voting, and post-voting stages.
29. All possible steps shall be taken to avoid the possibility of fraud or unauthorized intervention affecting the system during the whole voting process.	Can be achieved by means of adequate procedures during pre-voting, voting, and post-voting stages, as well as through the general requirements.
30. The eVoting system shall contain measures to preserve the availability of its services during the eVoting process. It shall resist, in particular, malfunction, breakdowns or denial of service attacks.	Can be achieved by means of adequate procedures during pre-voting, voting, and post-voting stages, as well as through the general requirements. The initializer of the bootable CDROM used for the voting computers can specify more than one boot credential for the CDROM image, such that the CDROMs used for one voting office can also be used in another voting office.
31. Before any electronic election or e-referendum takes place, the competent electoral authority shall satisfy itself that the eVoting system is genuine and operates correctly.	Can be achieved by means of adequate procedures during pre-voting stages, as well as through the general requirements.
32. Only persons appointed by the electoral authority shall have access to the central infrastructure, the servers and the election data. There shall be clear rules established for such appointments. Critical technical activities shall be carried out by teams of at least two people. The composition of the teams shall be regularly changed. As far as possible, such activities shall be carried out outside election periods.	Can be achieved by means of adequate procedures during pre-voting, voting, and post-voting stages, as well as through the general requirements.
33. While an electronic ballot box is open, any authorized intervention affecting the system shall be carried out by teams of at least two people, be the subject of a report; be monitored by representatives of the competent electoral authority and any election observers.	Not applicable: the voting urns (ballot boxes) do not contain any electronic components.
34. The eVoting system shall maintain the availability and integrity of the votes. It shall also maintain the confidentiality of the votes and keep them sealed until the counting process. If stored or communicated outside controlled environments, the votes shall be encrypted.	The information stored in the machine readable part of a voting ballot is encrypted under a key known to the Ballot Decryption Center that is associated with the voting office where the ballot was cast. The voter must fold the barcode or RFID ballot, or insert the RFID ballot in an envelope to hide the human readable part of the ballot from third parties, in particular from the president of the voting office, as this official must inspect the ballot to confirm that it does not contain any marks. It is also possible to fold the human readable part of the barcode booklet, and to glue it together, or even to staple it.
35. Votes and voter information shall remain sealed as long as the data is held in a manner where they can be associated. Authentication information shall be separated from the voter's decision at a pre-defined stage in the e-election or e-referendum.	See general requirements. There is no direct link between a ballot and the voter. The ballots are mixed before their machine readable part is read, which prevents establishing indirect links.

5.7.2.3 Operational Standards

Notification

36. Domestic legal provisions governing an e-election or e-referendum shall provide for clear timetables concerning all stages of the election or referendum, both before and after the election or referendum.	Clear procedures should be defined by the law as regards the use of ballots booklet.
37. The period in which an electronic vote can be cast shall not begin before the notification of an election or a referendum. Particularly with regard to remote eVoting, the period shall be defined and made known to the public well in advance of the start of	No specific provisions needed.

voting.	
38. The voters shall be informed, well in advance of the start of voting, in clear and simple language, of the way in which the eVoting will be organized, and any steps a voter may have to take in order to participate and vote.	Information about the procedure to be followed should be provided to the voter.

Voters

39. There shall be a voters' register which is regularly updated. The voter shall be able to check, as a minimum, the information which is held about him on the register, and request corrections.	No specific provisions needed.
40. The possibility of creating an electronic register and introducing a mechanism allowing online application for voter registration and, if applicable, for application to use eVoting, shall be considered. If participation in eVoting requires a separate application by the voter and/or additional steps, an electronic, and, where possible, interactive procedure shall be considered.	N.A.
41. In cases where there is an overlap between the periods for voter registration and the voting period, provision for appropriate voter authentication shall be made.	N.A.

Candidates

42. The possibility of introducing online candidate nomination may be considered.	N.A.
43. A list of candidates that is generated and made available electronically shall also be publicly available by other means.	The Election Authorities publish the lists of candidates and the layout of the voting screens and voting ballots prior to the elections.

Voting

44. It is particularly important, where remote eVoting takes place while polling stations are open, that the system shall be so designed that it prevents any voter from voting more than once.	N.A.
45. Remote eVoting may start and/or end at an earlier time than the opening of any polling station. Remote eVoting shall not continue after the end of the voting period at polling stations.	N.A.
46. For every eVoting channel, support and guidance arrangements on voting procedures shall be set up for, and be available to, the voter. In the case of remote eVoting, such arrangements shall also be available through a different, widely available communication channel.	Can be achieved by means of adequate procedures during pre-voting stages, by supplying adequate information about the voting process.
47. There shall be equality in the manner of presentation of all voting options on the device used for casting an electronic vote.	Similar to eVoting system currently in use.
48. The electronic ballot by which an electronic vote is cast shall be free from any information about voting options, other than that strictly required for casting the vote. The eVoting system shall avoid the display of other messages that may influence the voters' choice.	Similar to eVoting system currently in use.
49. If it is decided that information about voting options will be accessible from the eVoting site, this information shall be presented with equality.	N.A.
50. Before casting a vote using a remote eVoting system, voters' attention shall be explicitly drawn to the fact	N.A.

that the e-election or e-referendum in which they are submitting their decision by electronic means is a real election or referendum. In case of tests, participants shall have their attention drawn explicitly to the fact that they are not participating in a real election or referendum and shall – when tests are continued at election times – at the same time be invited to cast their ballot by the voting channel(s) available for that purpose.	
51. A remote eVoting system shall not enable the voter to be in possession of a proof of the content of the vote cast.	N.A.
52. In a supervised environment, the information on the vote shall disappear from the visual, audio or tactile display used by the voter to cast the vote as soon as it has been cast. Where a paper proof of the electronic vote is provided to the voter at a polling station, the voter shall not be able to show it to any other person, or take this proof outside of the polling station.	Similar to the eVoting system currently in use. No paper proof remains with the voter. The voting computer produces a paper ballot of which the voter hides the human readable part before leaving the voting booth. The folded ballot booklet is inspected by the president of the voting office, and then inserted by the voter into the voting urn.

Results

53. The eVoting system shall not allow the disclosure of the number of votes cast for any voting option until after the closure of the electronic ballot box. This information shall not be disclosed to the public until after the end of the voting period.	This can be achieved by means of adequate procedures during pre-voting, voting, and post-voting stages, as well as through the general requirements.
54. The eVoting system shall prevent processing information on votes cast within deliberately chosen sub-units that could reveal individual voters' choices.	See general requirements.
55. Any decoding required for the counting of the votes shall be carried out as soon as practicable after the closure of the voting period.	This can be achieved by means of adequate procedures during post-voting stages. The voting urns are collected at the end of the voting period on Election Day, and are assembled at the Ballot Reading Centers. After assembling the urns of different voting offices, the urns are opened and emptied, and their content is mixed to destroy any chronological order that may have been the result of entering the voting ballots one after the other in the individual voting urns. The the machine readable part of the shuffled voting ballots is then read. This results in an electronic copy of the information from such machine readable part, i.e., an encrypted vote. The resulting list enumerates the encrypted ballots that is then digitally signed by the president of the Ballot Reading Center, after which the authenticated list is sent to the Ballot Decryption Center, where the decryption of the encrypted voting ballots will take place.
56. When counting the votes, representatives of the competent electoral authority shall be able to participate in, and any observers able to observe, the count.	Belgian law stipulates that this should be done by a College of Experts and by party witnesses: no specific provisions needed.
57. A record of the counting process of the electronic votes shall be kept, including information about the start and end of, and the persons involved in, the count.	Can be achieved by means of adequate procedures during post-voting stages.
58. In the event of any irregularity affecting the integrity of votes, the affected votes shall be recorded as such.	See also recommendations n°107 and 108: What is considered as authentic vote should be defined by law: the information stored in the machine readable part of a ballot; the human readable part, the whole ballot or it depends on the counting phase (automated counting, manual counting). A problem could occur if a ballot is deemed invalid. However, the solution will consist in defining which of the

	two parts of the ballot booklet is given legal validity.

Audit

59. The eVoting system shall be auditable.	The complete electronic voting system is auditable: (i) the voting computers are booted from a bootable CDROM and run an open source operating system; (ii) the voting software is published once it has been certified by an external auditor; (iii) the voting configuration can be published after it has carefully been verified; (iv) the voting procedure and the procedures to initialize and manage the bootable CDROMs for the voting computers is made publicly available; (v) the mechanism and procedures to read an count ballots can be observed by independent observers; (vi) the voter can confirm that the human readable part of the ballot corresponds with the votes cast by means of the voting computer in the voting booth; (vii) independent auditors may select a random number of randomly chosen ballots to verify that the human readable part of the ballots corresponds with their machine readable part. Also see general requirements.
60. The conclusions drawn from the audit process shall be applied in future elections and referendums.	The recommendations by the College of Experts should be implemented in future elections.

5.7.2.4 Technical Requirements

Accessibility

61. Measures shall be taken to ensure that the relevant software and services can be used by all voters and, if necessary, provide access to altemative ways of voting.	Section 5.6.2.4 includes specific accessibility guidelines for voting systems with respect to this recommendation.
62. Users shall be involved in the design of e-voting systems, particularly to identify constraints and test ease of use at each main stage of the development process.	Section 5.6.2.4 includes specific accessibility guidelines for voting systems which include the involvement of real end-users in the design process of the layout of the voting screens and the voting process.
63. Users shall be supplied, whenever required and possible, with additional facilities, such as special interfaces or other equivalent resources, such as personal assistance. User facilities shall comply as much as possible with the guidelines set out in the Web Accessibility Initiative (WAI).	Section 5.6.2.4 includes specific accessibility guidelines for voting systems with respect to this recommendation.
64. Consideration shall be given, when developing new products, to their compatibility with existing ones, including those using technologies designed to help people with disabilities.	The proposed improved paper-based voting system is a close relative to the currently used electronic voting system.
65. The presentation of the voting options shall be optimized for the voter.	Sections 5.6.1.5 and 5.6.2.4 include specific layout guidelines for voting systems.

Interoperability

66. Open standards shall be used to ensure that the various technical components or services of an e-voting system, possibly derived from a variety of sources, interoperate.	The operating system, voting software and configuration files depend on open standards. The hardware (voting computer, display, pointing device, printer) also uses open market standards to provide its services, which protects against vender-lock in.
67. At present, the Election Markup Language (EML) standard is such an open standard and in order to guarantee interoperability, EML shall be used whenever possible for e-election and e-referendum applications. The decision of when to adopt EML is a matter for member states. The EML standard valid at the time of adoption of this recommendation, and supporting documentation are available on the	The configuration files of the voting software may be encoded using EML.

Council of Europe website.	
68. In cases which imply specific election or referendum data requirements, a localization procedure shall be used to accommodate these needs. This would allow for extending or restricting the information to be provided, whilst still remaining compatible with the generic version of EML. The recommended procedure is to use structured schema languages and pattern languages.	The configuration files of the voting software are localized to accommodate the needs of specific voting offices.

Systems Operation

69. The competent electoral authorities shall publish an official list of the software used in an e-election or e-referendum. Member states may exclude from this list data protection software for security reasons. At the very least it shall indicate the software used the versions, its date of installation and a brief description. A procedure shall be established for regularly installing updated versions and corrections of the relevant protection software. It shall be possible to check the state of protection of the voting equipment at any time.	The software used with the voting computers can be made public prior to the elections. Only the configuration files that contain the signing keys of the voting offices shall be kept secret. All other configuration files can be made public without restriction.
70. Those responsible for operating the equipment shall draw up a contingency procedure. Any backup system shall conform to the same standards and requirements as the original system.	The administration is responsible for the management of the voting computers.
71. Sufficient backup arrangements shall be in place and be permanently available to ensure that voting proceeds smoothly. The staff concerned shall be ready to intervene rapidly according to a procedure drawn up by the competent electoral authorities.	All voting computers of a voting office are interchangeable. The voting computers of a voting office are booted from a bootable CDROM that contains all the relevant information for the elections. This CDROM contains the operating system, voting software, and the configuration file(s) which match the boot credential of the president of the voting office. This means that voting computers of another voting office, or spare voting computers, can be easily used and quickly activated whenever necessary.
72. Those responsible for the equipment shall use special procedures to ensure that during the polling period the voting equipment and its use satisfy requirements. The backup services shall be regularly supplied with monitoring protocols.	Strict access control mechanisms are put in place so that only authorized people can use the voting computers' services and their software during Election Day.
73. Before each election or referendum, the equipment shall be checked and approved in accordance with a protocol drawn up by the competent electoral authorities. The equipment shall be checked to ensure that it complies with technical specifications. The findings shall be submitted to the competent electoral authorities.	The life-cycle description of the voting computers includes the initialization of the bootable CDROM of the voting computers prior to the Election Day, and the restore to factory defaults of the voting computers to their factory defaults after the voting period on Election Day. Disabling unnecessary features or hardware of the voting computers is part of the responsibilities of the system administrator of the voting computers.
74. All technical operations shall be subject to a formal control procedure. Any substantial changes to key equipment shall be notified.	The life cycle of the voting computer includes the certification of t he software, configuration files and bootable CDROMs. Proceeding from one stage to another in the life cycle is subject to successful completion of the previous.
75. Key e-election or e-referendum equipment shall be located in a secure area and that area shall, throughout the election or referendum period, be guarded against interference of any sort and from any person. During the election or referendum period a physical disaster recovery plan shall be in place. Furthermore, any data retained after the election or referendum period shall be stored securely	In between election periods, the voting computers are stored in a secure environment, or returned to their supplier. At the end of the election period, all voting computers are deactivated, i.e., their storage medium is reset in its original state by securely wiping out all information.
76. Where incidents that could threaten the integrity of the system occur, those responsible for operating the	This can be achieved by means of adequate procedures during pre-voting, voting, and post-voting stages, as well

equipment shall immediately inform the competent electoral authorities, who will take the necessary steps to mitigate the effects of the incident. The level of incident which shall be reported shall be specified in advance by the electoral authorities.	as through the general requirements.

Security

General Requirements

77. Technical and organizational measures shall be taken to ensure that no data will be permanently lost in the event of a breakdown or a fault affecting the e-voting system.	None of the voting computers contains critical information that could endanger the whole electronic voting system. Permanent loss of a voting computer has no impact on the operation of other voting computers.
78. The e-voting system shall maintain the privacy of individuals. Confidentiality of voters' registers stored in or communicated by the e-voting system shall be maintained.	It is impossible to link the identity of a voter and the voting ballot which represents this voter's choice: the voting computers are activated using an anonymous voting chip card that can be used only once. The voting computers do not store any information that could identify a voter.
79. The e-voting system shall perform regular checks to ensure that its components operate in accordance with its technical specifications and that its services are available.	The lifecycle of the voting computer includes the self-test of a voting computer whenever the computer is activated.
80. The e-voting system shall restrict access to its services, depending on the user identity or the user role, to those services explicitly assigned to this user or role. User authentication shall be effective before any action can be carried out.	Strict access control mechanisms are put in place to avoid unauthorized access to the voting computer and to its functionalities. The system administrator of the voting computers is responsible for the configuration of the BIOS of the voting computers to guarantee that the computer can only boot from CDROM. Note, however, that a fraudster who obtains a bootable CDROM which can be used to start a voting computer could extract the private signing key(s) of the voting office(s) that are stored in the respective configuration files if the fraudster also obtains the boot credentials of the president of that voting office. It is therefore necessary to put in place organizational safeguards to guarantee that the bootable CDROMs do not become available to unauthorized parties prior to the end of the Election Day. Similar safeguards must protect transporting the voting urns to the Ballot Reading Center to guarantee that no alien ballots .could be injected in a voting urn after having closed the voting office.
81. The e-voting system shall protect authentication data so that unauthorized entities cannot misuse, intercept, modify, or otherwise gain knowledge of all or some of this data. In uncontrolled environments, authentication based on cryptographic mechanisms is advisable.	The privileged information in a voting computer's configuration file is encrypted using a cryptographic key that depends on the boot credential of the president of the voting office, which guarantees that unauthorized access is prevented as long as the boot credentials are kept secret.
82. Identification of voters and candidates in a way that they can unmistakably be distinguished from other persons (unique identification) shall be ensured.	The president of a voting office has an authentic list of eligible voters. Given a person's identification tokens (e.g., identity card), the president of the voting office can confirm the identity of that person, and that he is an eligible voter (or not).
83. E-voting systems shall generate reliable and sufficiently detailed observation data so that election observation can be carried out. The time at which an event generated observation data shall be reliably determinable. The authenticity, availability and integrity of the data shall be maintained.	Not applicable: the voting computers do not comprise of a persistant storage medium, and are unable to log any information.
84. The e-voting system shall maintain reliable synchronized time sources. The accuracy of the time source shall be sufficient to maintain time marks for audit trails and observations data, as well as for	Not applicable: the voting computers operate in a standalone environment without any means to synchronize their system clocks. Because the voting computers do not have a network interface, they are unable to synchronize

maintaining the time limits for registration, nomination, voting, or counting.	their system clock.
85. Electoral authorities have overall responsibility for compliance with these security requirements, which shall be assessed by independent bodies.	Independent auditors need to verify that the correct procedures are correctly executed.

Requirements in Pre-Voting

86. The authenticity, availability and integrity of the voters' registers and lists of candidates shall be maintained. The source of the data shall be authenticated. Provisions on data protection shall be respected.	The administration takes care of the compilation of these lists.
87. The fact that candidate nomination and, if required, the decision of the candidate and/or the competent electoral authority to accept a nomination has happened within the prescribed time limits shall be ascertainable.	The administration is responsible for this recommendation.
88. The fact that voter registration has happened within the prescribed time limits shall be ascertainable.	The administration is responsible for this recommendation.

Requirements in the Voting Stage

89. The integrity of data communicated from the pre-voting stage (e.g. voters' registers and lists of candidates) shall be maintained. Data-origin authentication shall be carried out.	Strict user access control mechanisms are enforced when accessing the voting computers. The integrity of the configuration files is verified whenever the voting computer performs its self-test.
90. It shall be ensured that the e-voting system presents an authentic ballot to the voter. In the case of remote e-voting, the voter shall be informed about the means to verify that a connection to the official server has been established and that the authentic ballot has been presented.	The configuration files loaded into the bootable CDROM used by the voting computers are prepared by authorized personnel in a secure environment. The voting software is initialized in such a way that the voting computer truly displays the lists of candidates taking part in the election corresponding to the voting office in which the voter has been authenticated.
91. The fact that a vote has been cast within the prescribed time limits shall be ascertainable.	This has to be guaranteed using procedural and organizational means
92. Sufficient means shall be provided to ensure that the systems that are used by the voters to cast the vote can be protected against influence that could modify the vote.	There is no occasion for exerting influence during the voting process. A voter is alone in the voting booth (except for specific cases of voters with disabilities). Once he leaves the voting booth, his ballot must be folded or put in an envelope so that the votes are not visible (if he fails to do so, the president of the voting office will annihilate the ballot and the voter will be asked to vote again).
93. Residual information holding the voter's decision or the display of the voter's choice shall be destroyed after the vote has been cast. In the case of remote e-voting, the voter shall be provided with information on how to delete, where that is possible, traces of the vote from the device used to cast the vote.	Not applicable: the voting computers do not keep track in any way of the votes that were cast.
94. The e-voting system shall at first ensure that a user who tries to vote is eligible to vote. The e-voting system shall authenticate the voter and shall ensure that only the appropriate number of votes per voter is cast and stored in the electronic ballot box.	The president of the voting office verifies the identity of the voter. Only if he is an eligible voter, the voter receives a voting token with which the voting computer can be activated. No valid voting token = no possibility to cast a vote.
95. The e-voting system shall ensure that the voter's choice is accurately represented in the vote and that the sealed vote enters the electronic ballot box.	The voting computer produces a paper ballot with two parts: a human readable part and a machine readable part. The voter has to verify and confirm that the choice he cast with the voting computer corresponds with the human readable part. Independent auditors have to verify that the machine readable part of randomly selected voting ballots correspond with their respective human readable part.
96. After the end of the e-voting period, no voter shall be allowed to gain access to the e-voting system.	At the end of the voting period on Election Day, all voting computers are deactivated. During the deactivation of a

However, the acceptance of electronic votes into the electronic ballot box shall remain open for a sufficient period of time to allow for any delays in the passing of messages over the e-voting channel.	voting computer, the voting computer's BIOS settings are reset to factory defaults. The voting computers do not contain any persistent storage medium.

Requirements in Post-Voting

97. The integrity of data communicated during the voting stage (e.g. votes, voters' registers, lists of candidates) shall be maintained. Data-origin authentication shall be carried out.	The information sent from the Ballot Reading Centers to their corresponding Ballot Decryption Center, and from the Ballot Decryption Centers to their respective First Totalization Center, and up to the Final Totalization Center is digitally signed using an electronic identity card of the president of the respective Center.
98. The counting process shall accurately count the votes. The counting of votes shall be reproducible.	Official statements (PVs) are issued to report on the different stages of the voting process: from an empty voting urn to the Final Totalization Center.
99. The e-voting system shall maintain the availability and integrity of the electronic ballot box and the output of the counting process as long as required.	This can easily be enforced using the correct procedures with respect to the storage and processing of voting ballots.

Audit

General

100. The audit system shall be designed and implemented as part of the e-voting system. Audit facilities shall be present on different levels of the system: logical, technical and application.	The procedures of the proposed electronic voting system clearly specify the roles and activities of the different auditors that are active before, during and after the Election Day. The election software shall be designed according to specifications which will include provisions for auditing facilities.
101. End-to-end auditing of an e-voting system shall include recording, providing monitoring facilities and providing verification facilities. Audit systems with the features set out in sections II – V below shall therefore be used to meet these requirements.	Since the proposed system is not an end-to-end automated system, this requirement is not fully applicable. Official statements (PVs) report on the monitoring activities of the independent auditors.

Recording

102. The audit system shall be open and comprehensive, and actively report on potential issues and threats.	The audit procedures are open by design.
103. The audit system shall record times, events and actions, including: *a.* all voting-related information, including the number of eligible voters, the number of votes cast, the number of invalid votes, the counts and recounts, etc.; *b.* any attacks on the operation of the e-voting system and its communications infrastructure; *c.* system failures, malfunctions and other threats to the system.	The auditors have to include this information in their official statements (PVs).

Monitoring

104. The audit system shall provide the ability to oversee the election or referendum and to verify that the results and procedures are in accordance with the applicable legal provisions.	The audit mechanisms described in the proposed system permit the verification of the election results, and permit the auditing of the whole Election by randomly selecting voting ballots and verifying whether their machine readable part and human readable text match.
105. Disclosure of the audit information to unauthorized persons shall be prevented.	The disclosure of audit information shall proceed according to the legal provisions.
106. The audit system shall maintain voter anonymity at all times.	There is no link between a voter and a voting ballot. This guarantees that even the auditors will not be able to restore this link.

Verifiability

107. The audit system shall provide the ability to cross-check and verify the correct operation of the e-voting system and the accuracy of the result, to detect voter fraud and to prove that all counted votes are authentic and that all votes have been counted.	The audit procedures include that the auditors have to cross-check the partial election results with the number of voting urns that were tallied and with the respective ballots that were cast with these urns.
108. The audit system shall provide the ability to verify that an e-election or e-referendum has complied with the applicable legal provisions, the aim being to verify that the results are an accurate representation of the authentic votes.	Independent certification of the operating system, the voting software, and configuration files has to take place prior to the elections to verify that they meet the relevant legal requirements.

Other

109. The audit system shall be protected against attacks which may corrupt, alter or lose records in the audit system.	The official statements (PVs) should be digitally signed to prevent undetected modifications of their content.
110. Member states shall take adequate steps to ensure that the confidentiality of any information obtained by any person while carrying out auditing functions is guaranteed.	This requirement must be enforced using organizational means.

Certification

111. Member states shall introduce certification processes that allow for any ICT (Information and Communication Technology) component to be tested and certified as being in conformity with the technical requirements described in this recommendation.	The specified procedures include the necessary certifications of the voting hardware, software, procedures and configuration.
112. In order to enhance international co-operation and avoid duplication of work, member states shall consider whether their respective agencies shall join, if they have not done so already, relevant international mutual recognition arrangements such as the European Cooperation for Accreditation (ECA), the International Laboratory Accreditation Cooperation (ILAC), the International Accreditation Forum (IAF) and other bodies of a similar nature.	The proposed system can be exported to foreign countries which want to boost their citizen's confidence in electronic voting systems.

6 Direct optical scan of voting ballots

6.1 Reasons why the consortium did not propose this type of system

With this voting system, the voter manually marks his choice on a paper ballot. It is the complete ballot that is being optically read. This explains the term "direct reading".

Although it is true that direct optical scan voting systems can be set up in such a way that the voter will see little difference with traditional voting, this comes at the price of making the process very machine-intensive. The most important disadvantage of this system is the fact that scanning is an expensive, relatively slow and error-prone process, especially when dealing with large voting ballots.

Furthermore, the directly scanned images create quite a bulky amount of data to be transported safely and retained for auditing purposes. A much better trade-off can be obtained by asking the voters to enter their vote directly into a computer, thereby greatly reducing the efforts needed later to register the vote.

6.2 Initial remarks

An optical scanner is a device that can read text or illustrations printed on paper and translate the information into a form the computer can use. A scanner works by digitizing an image -- dividing it into a grid of boxes and representing each box with either a zero or a one, depending on whether the box is filled in. The resulting matrix of bits, called a bit map, can then be stored in a file, displayed on a screen, and manipulated by programs.[22]

Direct optical-scan machines use an electronic reader to record the vote, but not to cast it. The machines require voters to mark their choices on a paper ballot, which is then scanned into an electronic reader to record the vote. The paper ballots, however, give officials the ability to catch problems if they examine the ballots through a hand count and compare them against the digital votes.[23]

Direct optical scans are used in voting systems in order to increase the speed and accuracy of the paper-based voting process. The main advantage is that it usually does not imply any substantial modifications in the traditional voting procedure and that it can be subject to "eye-control".

Experimentations of optical scans systems have already been carried out in Belgium in the elections of 2003. They have turned out to be expensive and they have shown important technical limitations. To be read by the optical scanners, ballots could not include more than twenty lists of candidates with a limited number of candidates per list. The system tested also required a previous manual selection of the ballots to

[22] Description extracted from: http://www.webopedia.com/TERM/o/optical_scanner.html

[23] Description extracted from: http://www.wired.com/politics/security/news/2005/07/68097

exclude invalid ballots from the tallying.[24]

The Consortium investigated the use of a different technology. In order to solve the problem of the size of the ballot, the Consortium has investigated numbering the candidates in the paper-based ballot. Finally, the possibility of numbering the ballots in order to reduce fraud has also been considered.

6.3 A family of systems

The systems we describe in this chapter all share a number of common characteristics, described in the "Scope" section below. Still, many different choices may be made, which result in quite different systems, which have specific advantages and drawbacks and which may induce specific requirements with respect to organization and procedures. In other words, this chapter describes a family of optical scan voting systems; political decisions and legal changes would be needed to select a single member of this family as the direct optical scan voting system for Belgium. We recommend a choice among several options.

This chapter presents the major choices to be made if one wishes to implement a direct optical scan voting system, together with the consequences entailed by these choices. The information is provided in order to allow decision makers to make informed choices.

6.3.1 Scope

The basic principles underlying all voting systems based on direct optical scanning covered by the present chapter of this report are the following:

- After having been duly identified and accepted for voting in the voting precinct (voting office), the voter receives a paper ballot.
- In the voting booth, the voter marks the vote on the paper ballot by darkening one ore more areas ("target zones") on the paper ballot next to identifiers of either lists and/or candidates.
- At some point in time, the paper ballot is scanned by a device ("optical reader"), which recognizes which areas on the paper ballot were darkened by the voter and interprets this information to identify for which lists and/or candidates' votes have been expressed. The votes thus identified are processed by means of a computer infrastructure (hardware, software, and communication means). The paper ballots are kept as long as needed in order to allow manual recounts as authorized by law.
- Organizational procedures ensure that a voter may only submit a single ballot per voting box and thus vote only once.
- Organizational procedures allow a voter who has marked the ballot in a way which does not correspond to his intentions (spoiled ballot) to have the ballot annulled and to receive a new blank ballot to start over again.

[24] Belgian Senate, Archives, Demande d'explications de M. Philippe Mahoux au vice-premier ministre et ministre de l'Intérieur sur «le vote électronique» (n° 3-197), 1st April 2004, available on-line at : http://www.senat.be/www/?MIval=/publications/viewPubDoc&TID=50334687&LANG=fr (last accessed 29 August 2007).

Note: The systems under consideration here do not use optical character recognition (OCR) techniques; they also assume that ballots are marked by hand.

6.3.2 Concepts and Terminology

- The **ballot** is a preprinted paper form which is suitable for optical scanning, i.e. it respects constraints relative to design, weight, background color, and size (see later); it may be two-sided, if necessary. If the number of items to print is large, the paper ballot may consist of several (possibly two-sided) ballot **sheets**.
- A **voting item** is an entity for which a vote may be cast during an election: in the current Belgian electoral system, the sole voting items are: **lists** and **candidates**.
- An **identifier** is an accepted means to uniquely and unambiguously designate a voting item. For a list, it may be the full name, an accepted abbreviation, a logo, etc.; for a candidate, it may be the full name, an unambiguous part of the full name, a unique number, a combination of number and (partial) name, etc.
- The paper ballot contains one column per list and, in each column, one row per candidate on the list. The lists and the candidates are designated on the ballot by means of identifiers.
- On the same row and next to each voting item identifier, there is a **target zone** which must be darkened in a specified way and by a specified writing implement in order to indicate a **vote** for this voting item. A target zone may consist of a white spot centered on a black square or of an oval, or of any other means intuitively suitable and legally prescribed to indicate a vote. Users must be instructed to fill the target area completely.

123 Vanpieperzele Jules

Full identifier

123 Vanp. J.

Abbreviated identifier

- The **scanning** of paper ballots may rely on two quite different technologies:
  - **Discrete-sensor** technology: this is an earlier approach, in which the ballot is moved past a row of sensors, which detect which target zones have been darkened, resulting in series of (X, Y) coordinates which are then correlated to voting items by means of appropriate software.
    Prof. D. W. Jones, of the University of Iowa, has very convincingly shown[25] that this technology is error-prone: different readers or the same reader with a different calibration often yield different results. Besides, the resolution is limited to the number of sensors that can be placed on a row, the type of sensor used must fit the marking media used and its color, the systems are sensitive to paper distortion, misalignment, wrinkles, folds, etc.
  - **Pixel-based** technology: in this approach, a pixel image (i.e. digital photograph) of every sheet (and every side of every sheet, if necessary) of the paper ballot is produced and analyzed by means of special-purpose software. It is claimed (mostly by manufacturers) that this technology has none of the

[25] http://www.cs.uiowa.edu/~jones/voting/optical/ (last accessed on October 4, 2007).

drawbacks of discrete-sensor technology[26], even though some of the problems mentioned by Prof. D. W. Jones remain (for instance: how many pixels are needed to consider that a target zone has been effectively marked ?). Still, compared to discrete-sensor technology, where the detection is hardware-based, in this approach the detection is software-based, which greatly increases the potential for reliability and flexibility.

Note: Because of its intrinsic superiority, we shall henceforth only consider optical scan voting systems based on **pixel technology**.

- A **vote set** is the collection of all votes expressed (marked) on a ballot. The purpose of the **scanning** of a ballot is, at least, to identify the vote set it contains, which represents the suffrage expressed by the voter if the scanning is correct.
- The **counting**, **tabulating**, or **tallying** of a vote set consists of adding the votes of the vote set to the current total of votes of the corresponding voting items (lists and/or candidates).
- The scanning and the counting may be realized together, in the same device (the counting obviously following the scanning), or separately (at different stages of the process and in different devices).

6.4 Options and Choices for Direct Optical Scan-based Voting Systems

We now describe a series of options and choices which must be decided upon when designing an optical scan voting system. For each option or choice, we shall present a table with advantages and drawbacks, reflecting our current position on the various items.

6.4.1 Types of Ballots

We distinguish different types of ballots which might possibly be used in the kinds of optical scan voting systems under consideration.

1. **Traditional** Belgian ballots: their size depends on the number of lists and candidates, and may vary between electoral districts. Examples exist of ballots measuring 80 cm by 50 cm. These ballots are supplied to the voter in a folded state and are deposited in the urn again in a folded state to guarantee the confidentiality of the suffrage.
2. **Fixed, standard size** ballots: these are of a size for which scanning devices are readily available (A4, A3, A2 or A1)[27]. The larger the size, the more expensive the scanning device.
3. **Double-sided**, standard size ballots: both sides of a sheet may be used to vote.
4. **Multiple sheet** ballots: consist of several (possibly double-sided) ballot sheets.
5. **"Lotto-style"** ballots: these are fixed, standard size ballots (smaller than A4, similar to normal Lotto forms).

---

[26] http://www.verifiedvoting.org/downloads/OpticalVote-Trakker.pdf (last accessed on October 4, 2007).

[27] A4: 21,0 cm x 29,7 cm A3: 29,7 cm x 42, 0 cm A2: 42,0 cm x 59,4 cm A1: 59,4 cm x 84,1 cm

In all cases where there is not enough room to print the full information on the ballot, abbreviated (but unambiguous) identifiers may be used instead (e.g. a candidate's number and the first letters of his name); the voting booth must then be supplied with posters or election booklets with the full information.

Since the folding of ballots may impair the scanning process, confidentiality must be ensured by other means. In the USA, "secrecy sleeves" or envelopes are used: the voter inserts his ballot in the sleeve or in the envelope before leaving the booth. The ballots must obviously be extracted before scanning.

To prevent simple forms of ballot stuffing, ballots may be stamped before being handed over to voters.

The table below presents the specific advantages and drawbacks of the various types of ballots.

Ballot type		Advantages	Drawbacks
1	**Traditional**	• Well known by everybody: no learning necessary	• Hard to handle • Slow and expensive • Hard to scan by readily available scanning devices (size, folds)
2	**Fixed, standard size**	• Easy handling • Readily available and rather inexpensive scanning devices (if A4 or A3)	• May require abbreviated identifiers for elections with many lists and many candidates: greater risk for errors when marking votes • Sleeve needed for confidentiality
3	**Double-sided**	• More space available than on single-sided ballots	• Risk of forgetting to turn ballot around when voting • Candidates mentioned on the front or back page do not have the same visibility • More complicated scanning process: more expensive • Sleeve needed for confidentiality
4	**Multiple sheet**	• Even more space available • Allows for full identifiers (no abbreviations needed)	• Longer scanning process • One of the sheets may be removed, which would invalidate the ballot • Sleeve needed for confidentiality
5	**"Lotto-style"**	• Easy handling • Cheap scanning devices	• Greater risk of errors when marking (transcribing) votes • The presence and quality of the voting lists must be verified each time a voter enters the voting

			booth • Sleeve needed for confidentiality • Potential for image problem in the public (Election = lottery)

6.4.2 Where and When to Scan

Scanning is the process which produces a pixel-based image of the ballot and which interprets this image in order to extract the vote set it contains.

We examine 4 possibilities:

1. The voting booth is equipped with a scanning device and a visualization screen. The voter scans the ballot sheet(s) himself and the screen displays the scanned image and the vote set which has been detected by the software. If the expressed vote set is incorrect (for instance: votes in more than one list), the vote set and the ballot are voided and the voter is asked to request a new ballot and to start over again. If the expressed vote set is accepted as being legal and if the voter is satisfied that the scanning is accurate, he/she confirms the vote set; otherwise, he/she signals a scanning error to voting officials and will be given a new ballot to use in a different voting booth. Voting officials will then test and, if necessary, replace the voting machine which has produced a scanning error.
2. The voting booth has no scanning equipment: the scanning is done at the voting office (precinct) level in a setup which guarantees voter privacy and allows the same verifications as in the booth-based scanners: the ballot is verified for conformity with election rules and the voter verifies that the scanning and vote set extraction (interpretation) are accurate.

   An example of a system which operates based on this principle is Avante's Optical VOTE-TRAKKER® [28]
3. The voting booth has no scanning equipment: the scanning is done at the voting office (precinct) level and the ballot is only verified for conformity with election rules. If the expressed vote is incorrect (for instance: votes in more than one list), the vote is voided and the voter is asked to request a new ballot and to start over again. The scanning device has two output bins: one for legal ballots and one for incorrect ballots. Many manufacturers produce this type of system.
4. Neither the voting booth nor the voting office have a scanner: the scanning is done at the First Totalization Center after urns have been collected and transported there. Whenever a ballot is detected with an incorrect vote set (for instance: votes in more than one list), the vote set and the ballot are voided. The scanning device has two output bins: one for legal ballots and one for incorrect ballots. Many manufacturers produce this type of system.

The table below summarizes the advantages and the drawbacks of the 4 different approaches to the scanning of ballots.

[28] http://www.avantetech.com/products/elections/optical/ (last accessed on October 4, 2007).

Scan: where and when		Advantages	Drawbacks
1	**Voting booth, by the voter**	• Instantaneous detection of voting mistakes (e.g. over votes) and possibility to ask for new vote • Instantaneous detection of scanning errors by the voter and possibility to signal them and ask for new vote • No need for confidentiality sleeve	• Manipulation of ballot sheet(s) by voter: danger of jamming, etc. • One scanning device per booth: quite expensive • Need to prevent insertion of "fake ballots" • Need to recover information from all voting booths at the end of the voting period
2	**Voting office (precinct), with voter verification**	• Detection of voting mistakes (e.g. over votes) and possibility to ask for new vote • Detection of scanning errors by the voter and possibility to signal them and ask for new vote	• Manipulation of ballot sheet(s) by voter: danger of jamming, etc. • Need for confidentiality sleeve between booth and scanning device: more complex handling • Scanning and verification may take significant time: risk of bottlenecks
3	**Voting office (precinct) without voter verification**	• Detection of voting mistakes (e.g. over votes) and possibility to correct them • Manipulation of ballot sheet(s) by official • Scanning happens quickly	• No possibility to verify the accuracy of the scanning by the voter • Need for confidentiality sleeve between booth and scanning device: more complex handling
4	**Totalization level 1**	• Batch processing of ballots: fewer optical readers needed • No handling of confidentiality sleeve at precinct level	• No possibility to verify the accuracy of the scanning unless multiple scans • Voting mistakes (incorrect votes) can be detected, but not corrected • Need for confidentiality sleeve • Need for transportation of urns

Note: If scanning is done by the voter in the voting booth, it is necessary to make sure that only official ballot sheets and the right number of them are scanned. One way to ensure this would be to have all official ballot marked with a unique identifying number, which would be read during the scanning process. At some point

later in the process, it would be necessary to ascertain that all ballot numbers are indeed numbers corresponding to officially sanctioned ballots and that no number occurs more than once.

6.4.3 Where and When to Count

Counting is the process which adds the votes contained in a vote set to running totals for every vote item (lists and candidates).

We examine 3 possibilities:

1. The counting is realized in the voting booth; this is of course only possible if the voting booth is equipped with a scanning device.
2. The counting is realized at the voting office (precinct) level: this is of course only possible if the voting office is equipped with a scanning device.
3. The counting is realized at the First Totalization Center.

The table below summarizes the advantages and the drawbacks of the 3 different approaches to the counting of votes.

Count: where and when		Advantages	Drawbacks
1	**Voting booth**	• Low volume of information to be transmitted to First Totalization Center	• Voting trends too easy to spot: danger for anonymity
2	**Voting office (precinct)**	• Low volume of information to be transmitted to First Totalization Center	• Voting trends too easy to spot: danger for anonymity
3	**Totalization Center 1**	• Best protection of anonymity: individual or local trends hardest to spot • Best-fitting analogy with manual counting	• Many individual vote sets must be transmitted to Totalization Center 1

6.4.4 What to do with the Images of the Scanned Ballots?

Pixel-based optical scan voting systems produce images of the scanned ballots. Once these images have been processed in order to extract the vote sets they contain, the images themselves are not needed any more for the remainder of the voting process: they can simply be discarded.

Still, it might be useful to keep the set of all pairs consisting of ballot images and the corresponding extracted vote sets in order to measure the accuracy of the scanning and vote sets extracting process and compare it to the accuracy of manual recounts.

6.5 Specific Requirements – Hardware, Software,

Procedures

The only additional requirements for optical scan voting systems, besides those outlined in the chapter on general requirements, have to do with precautions regarding paper handling to prevent jamming and dust avoidance in the scanners themselves. Periodic cleaning, calibration and training of the scanners should be included in the organizational procedures. The correct use of "confidentiality sleeves" (if needed) should be documented and included in the description of the voting procedure.

6.6 Advantages and Drawbacks of Direct Optical Scan Voting Systems

6.6.1 Advantages

- The vote itself is identical or very close to traditional paper ballot voting, which makes it easy to understand and accept. The paper ballot is inherently a voter-verifiable paper trail.
- The counting of votes is automated and proceeds much faster and with a much lower manpower cost than manual counting.
- The paper ballots may be counted manually if a recount is deemed necessary. There are effectively two independent ways to process votes: via the scanning and counting process and via a manual recount.
- A paper ballot is effectively a single-use voting token which ensures that a voter may vote only once.
- In case of equipment failure, voting can proceed in the traditional way while scanning and counting may be delayed until the breakdown is fixed (graceful degradation).
- The processing of postal votes (absentee ballots) can be handled by the same system as regular votes; ballots may even be sent by fax or as image attachments in e-mails (if proper authentication is provided).

6.6.2 Drawbacks

- As is the case for every voting system in which the voter handles a paper ballot, the presence of extraneous markings (currently considered by article 157 of Belgian legislation as grounds for annulment of the ballot and its votes) will sometimes be handled differently by the automated counting process than by a manual count. Indeed, some markings that would be detected by the human eye will be ignored (even though pixel-based technology is much better at detecting them than discrete-sensor technology) while in a manual (re)count, these markings will duly be noticed, which will result in the annulment of the marked ballots. Since there are always a number of ballots with extraneous markings in every election, recounts are statistically bound to produce results which are different from the first (electronic) counts.

  It is a political question to decide what to do in such cases: should the extraneously marked ballots be voided and, if so, what should be done about the undetected extraneously marked ballots which were not subjected to a manual recount.

- The designing, printing, verifying, storing, and distributing of ballots is as costly as in traditional paper ballot voting, which precludes claiming that optical scanning of ballots reduces election costs significantly (except for manpower costs).
- The size of the ballot sheets is usually limited by mechanical considerations imposed by the scanning device; larger scanning areas imply more expensive devices.
- If the processing of ballots is done in batch mode, a reliable mechanical feeder is needed, together with a fast scanner, which may be rather expensive.
- Optical scanning of paper ballots lacks the "hi-tech" gloss of other e-voting systems and may thus be less appealing.
- If ballots with with multiple sheets are used, the president of the voting office has to count the number of sheets in addition to the number of ballots!

6.6.3 Additional Remarks

- In case of a discrepancy between electronically tallied votes and manually (re)counted votes, legislation is needed to determine which of the two results will be accepted as the official (authentic) result.
- Ballots must imperatively be designed by experts to guarantee their legibility both by voters and by scanning devices[29].
- Optical scan voting systems of one kind or another have been used for more than 20 years in the USA and their usage is on the rise (reaching 40% in the 2006 congressional and gubernatorial elections).

6.7 Analysis of the Scenarios

In the first two scenarios, the voter himself scans his ballot either within the voting booth or within a precinct which guarantees his privacy. This enables him to verify the accuracy of the scanning. The "eye control" of party witnesses during the tallying of the vote in the traditional system is here replaced by the "eye control" of the voter himself. This does not however mean that party witnesses and the College of experts are excluded from observation tasks. In the last two scenarios, this option is not given to the voter, the machine only controls that the ballot has been correctly completed and discards incomplete or incorrect ballots.

The last scenario is based on the scanning of the votes at the first totalization center. The difference with the system tested in the elections of 2003 is that a manual elimination of invalid ballots (i.e. with extraneous markings) is not foreseen, the paper ballots are directly scanned and the verification of the validity of the ballot is limited to the correct completion of the ballot. Ballots are not examined to decide whether there are marked in such a way that, according to article 157 of the Election Law, they should be invalidated.

These scenarios present the advantage of reducing the burden of a first manual classification of the ballots as it was the case in the previous testing of optical scan system during the elections of 2003. However, it raises the concern of potential

[29] http://vote.nist.gov/threats/papers/optical_scan_ballot_design.pdf (last accessed on October 4, 2007).

discrepancies between the electronic ballots and paper-based ballots as regards their validity and of the storage of the ballots in the optical scan manipulated by the voter.

6.7.1 Hybrid Ballots (Paper-based and Electronic)

This system results in a situation where the voter actually casts one ballot materialized in two different carriers: a paper ballot and an electronic ballot (the scanned version of the paper-based ballot). The problem is that the optical scan cannot be relied upon to detect invalid ballots, i.e. whether the scanned ballot contains marks or objects inside which would deem them invalid according to article 157 of the Electoral Law makes handling those ballots more expensive. It is worth noticing that the rules invalidating marked ballots are meant to protect the secrecy of the vote and prevent that a ballot could be linked to a voter.

It follows that in case of manual recounting, invalid ballots should be excluded from the tallying. The results of the electronic and manual counting would thus not match. To solve this problem, two possibilities can be considered, identical to those described in section 5.7.1 above.

A first possibility is to acknowledge paper-based ballots as only authentic votes in case a discrepancy occurs. The consequence would be that when the election is contested and a manual recounting is required, authenticate ballots would consists of the paper-based ballots, not the electronic ballots. The results obtained from the tallying of paper-based ballots would produce the final result of the election. It should be noticed that paper ballots are only meant for recounting and that the rules which govern the nullification of ballots are meant to protect the secrecy of the vote (which in this case would override the principle of "one person, one vote", as the secrecy of the vote is more important than the rules that govern the nullification of ballots). The result based on the recount of paper ballots would be in that case the valid result.

A second possibility would consist in giving legal validity to electronic ballots, i.e., the electronic representation of the ballots that is obtained after the direct optical scan. The paper ballot would only serve as a back-up to perform a new recounting. In case the results are contested, the paper ballots would need to be re-scan and automatically recounted. This solution would not however allow performing the recounting on the sole basis of the information contained in the paper ballot, as the only legal ballot is the electronic ballot.

6.7.2 Storage of the votes in the Machine Manipulated by the Voter

In scenarios 1, 2 and 3 of section 6.4.2, the votes are stored on machines directly manipulated by the voters. Technical safeguards should ensure the secrecy of the vote, i.e. that a voter cannot see the content of the vote of the previous voter and that no intermediate totals could be made before the end of the elections. Technical safeguards should as well guarantee the security of the system as long as the machine is directly manipulated by the voter, i.e. to prevent any attack to the software.

6.7.3 Multiple scanning

In case the scanning is performed directly by the voter in the voting booth, measures should be implemented to prevent the voter from scanning his ballot multiple times.

6.7.4 Numbering of Candidates

In order to reduce the size of the ballots, it has been suggested to number the candidates in such a way that only the numbers would appear on the ballot. The voter would be provided with a book (in the voting booth, for instance) where he could check which number corresponds to each candidate.

6.8 Compliance of Direct Optical Scan Voting Systems with the CoE Recommendations

Since the consortium does not propose to retain optical scan voting systems for Belgium, only the general requirements of the Council of Europe will be discussed here, excluding the technical requirements.

6.8.1 Legal Standards

6.8.1.1 Principles

Universal Suffrage

	Direct Optical scan voting systems
1. The voter interface of an eVoting system shall be understandable and easily usable.	Identical to traditional paper ballot voting. The friendliness of the design of the paper ballot should be guaranteed if using a different format for reasons of optical scan features (e.g. numbering of candidates).
2. Possible registration requirements for eVoting shall not pose an impediment to the voter participating in eVoting	Identical to traditional paper ballot voting.
3. eVoting systems shall be designed, as far as it is practicable, to maximize the opportunities that such systems can provide for persons with disabilities.	Identical to traditional paper ballot voting.
4. Unless channels of remote eVoting are universally accessible, they shall be only an additional and optional means of voting.	N.A.

Equal Suffrage

5. In relation to any election or referendum, a voter shall be prevented from inserting more than one ballot into the electronic ballot box. A voter shall be authorized to vote only if it has been established that his ballot has not yet been inserted in the ballot box.	Identical to traditional paper ballot voting: the paper ballot is given to the voter after identification and authorization.
6. The eVoting system shall prevent any voter from casting a vote by more than one voting channel.	Only one channel available.
7. Every vote deposited in an electronic ballot box shall be counted, and each vote cast in the election or referendum shall be counted only once.	To be guaranteed by appropriate procedures, similar to those for traditional paper ballot voting.
8. Where electronic and non-electronic voting channels are used in the same election or referendum, there shall be a secure and reliable method to aggregate all votes and to calculate the correct result.	Traditional counting may easily be merged with electronic scanning and counting at the first totalization center

Free Suffrage

9. The organization of eVoting shall secure the free formation and expression of the voter's opinion and, where required, the personal exercise of the right to vote.	Identical to traditional paper ballot voting. This is guaranteed using voting booths
10. The way in which voters are guided through the eVoting process shall be such as to prevent their voting precipitately or without reflection.	Not applicable: identical to traditional paper ballot voting.
11. Voters shall be able to alter their choice at any point in the eVoting process before casting their vote, or to break off the procedure, without their previous choices being recorded or made available to any other person.	Identical to the classic paper-based voting procedure: a procedure is needed to void a ballot and obtain a new blank one if a voter made a mistake during the marking phase.
12. The eVoting system shall not permit any manipulative influence to be exercised over the voter during the voting.	Identical to traditional paper ballot voting; privacy and free suffrage is guaranteed by the voting booth.
13. The eVoting system shall provide the voter with a means of participating in an election or referendum without the voter exercising a preference for any of the voting options, for example, by casting a blank vote.	Identical to traditional paper ballot voting. If the voter operates the scanner (booth or office), he/she may be asked to confirm a blank vote.
14. The eVoting system shall indicate clearly to the voter when the vote has been cast successfully and when the whole voting procedure has been completed.	Easily satisfied if scanning is done in the booth or in the voting office; otherwise, identical to traditional paper ballot voting.
15. The eVoting system shall prevent the changing of a vote once that vote has been cast.	Depends on the correctness of the election software.

Secret Suffrage

16. eVoting shall be organized in such a way as to exclude at any stage of the voting procedure and, in particular, at voter authentication, anything that would endanger the secrecy of the vote.	Identical to traditional paper ballot voting. There is no direct link between a ballot and the voter.
17. The eVoting system shall guarantee that votes in the electronic ballot box and votes being counted are, and will remain, anonymous, and that it is not possible to reconstruct a link between the vote and the voter.	Identical to traditional paper ballot voting. There is no direct link between a vote set and the voter. The randomization of vote sets prevents establishing indirect links.
18. The eVoting system shall be so designed that the expected number of votes in any electronic ballot box will not allow the result to be linked to individual voters.	Identical to traditional paper ballot voting. Totals for individual booths or for individual voting offices are not publicly available. If ballots are numbered, procedural safeguards should be put in place in order to prevent that a link could be established between the vote and the voter.
19. Measures shall be taken to ensure that the information needed during electronic processing cannot be used to breach the secrecy of the vote.	There is no direct link between a vote set and the voter. The randomization of vote sets prevents establishing indirect links. If the votes were stored in the voting machine, technical safeguards should be implemented to ensure that the content of the vote of the previous voter cannot be displayed on the screen.

6.8.1.2 Procedural Safeguards

Transparency

20. Member states shall take steps to ensure that voters understand and have confidence in the eVoting system in use.	Similar enough to traditional paper ballot voting to guarantee understanding. The possibility of a manual recount should provide confidence.

	In case of opting for ballots with candidates' numbers, the system should be designed so as to be easily understood by the voters.
21. Information on the functioning of an eVoting system shall be made publicly available.	Easily enough to achieve by publishing a description of the working of the scanning devices and of the counting process.
22. Voters shall be provided with an opportunity to practice any new method of eVoting before, and separately from, the moment of casting an electronic vote.	The only need for practicing arises when the voter is expected to operate the scan of the ballot sheet(s) (scanning in booth or office).
23. Any observers, to the extent permitted by law, shall be able to be present to observe and comment on the e-elections, including the establishing of the results.	No specific provisions needed.

Verifiability and Auditability

24. The components of the eVoting system shall be disclosed, at least to the competent electoral authorities, as required for verification and certification purposes.	See general requirements.
25. Before any eVoting system is introduced, and at appropriate intervals thereafter, and in particular after any changes are made to the system, an independent body, appointed by the electoral authorities, shall verify that the eVoting system is working correctly and that all the necessary security measures have been taken.	Belgian law stipulates that this should be done by a College of Experts: no specific provisions needed.
26. There shall be the possibility for a recount. Other features of the eVoting system that may influence the correctness of the results shall be verifiable.	Two types of recounts are possible: • automated recount with different scanning equipment and/or software • manual recount of paper ballots
27. The eVoting system shall not prevent the partial or complete re-run of an election or a referendum.	No specific provisions needed.

Reliability and Security

28. The member state's authorities shall ensure the reliability and security of the eVoting system.	Can be achieved by means of adequate procedures during pre-voting, voting, and post-voting stages.
29. All possible steps shall be taken to avoid the possibility of fraud or unauthorized intervention affecting the system during the whole voting process.	Can be achieved by means of adequate procedures during pre-voting, voting, and post-voting stages, as well as through the general requirements.
30. The eVoting system shall contain measures to preserve the availability of its services during the eVoting process. It shall resist, in particular, malfunction, breakdowns or denial of service attacks.	Can be achieved by means of adequate procedures during pre-voting, voting, and post-voting stages, as well as through the general requirements.
31. Before any e-election or e-referendum takes place, the competent electoral authority shall satisfy itself that the eVoting system is genuine and operates correctly.	Can be achieved by means of adequate procedures during pre-voting stages, as well as through the general requirements.
32. Only persons appointed by the electoral authority shall have access to the central infrastructure, the servers and the election data. There shall be clear rules established for such appointments. Critical technical activities shall be carried out by teams of at least two people. The composition of the teams shall be regularly changed. As far as possible, such activities shall be carried out outside election periods.	Can be achieved by means of adequate procedures during pre-voting, voting, and post-voting stages, as well as through the general requirements.

33. While an electronic ballot box is open, any authorized intervention affecting the system shall be carried out by teams of at least two people, be the subject of a report; be monitored by representatives of the competent electoral authority and any election observers.	Can be achieved by means of adequate procedures during voting and post-voting stages, as well as through the general requirements.
34. The eVoting system shall maintain the availability and integrity of the votes. It shall also maintain the confidentiality of the votes and keep them sealed until the counting process. If stored or communicated outside controlled environments, the votes shall be encrypted.	See general requirements.
35. Votes and voter information shall remain sealed as long as the data is held in a manner where they can be associated. Authentication information shall be separated from the voter's decision at a pre-defined stage in the e-election or e-referendum.	See general requirements. There is no direct link between a vote set and the voter. The randomization of vote sets prevents establishing indirect links. If the votes were stored in the voting machine, technical safeguards should be implemented to ensure that the content of the vote of the previous voter cannot be displayed on the screen.

6.8.2 Operational Standards

6.8.2.1 Notification

36. Domestic legal provisions governing an e-election or e-referendum shall provide for clear timetables concerning all stages of the election or referendum, both before and after the election or referendum.	No specific provisions needed. Clear procedures should be defined by the law as regards the use of optical scans.
37. The period in which an electronic vote can be cast shall not begin before the notification of an election or a referendum. Particularly with regard to remote eVoting, the period shall be defined and made known to the public well in advance of the start of voting.	No specific provisions needed.
38. The voters shall be informed, well in advance of the start of voting, in clear and simple language, of the way in which the eVoting will be organized, and any steps a voter may have to take in order to participate and vote.	No specific provisions needed, besides information about the scanning of ballot sheets (booth or office).

6.8.2.2 Voters

39. There shall be a voters' register which is regularly updated. The voter shall be able to check, as a minimum, the information which is held about him on the register, and request corrections.	No specific provisions needed.
40. The possibility of creating an electronic register and introducing a mechanism allowing online application for voter registration and, if applicable, for application to use eVoting, shall be considered. If participation in eVoting requires a separate application by the voter and/or additional steps, an electronic, and, where possible, interactive procedure shall be considered.	N.A.
41. In cases where there is an overlap between the period for voter registration and the voting period, provision for appropriate voter authentication shall be made.	N.A.

6.8.2.3 Candidates

42. The possibility of introducing online candidate nomination may be considered	N.A.
43. A list of candidates that is generated and made available electronically shall also be publicly available by other means.	N.A.

6.8.2.4 Voting

44. It is particularly important, where remote eVoting takes place while polling stations are open, that the system shall be so designed that it prevents any voter from voting more than once.	N.A.
45. Remote eVoting may start and/or end at an earlier time than the opening of any polling station. Remote eVoting shall not continue after the end of the voting period at polling stations.	N.A.
46. For every eVoting channel, support and guidance arrangements on voting procedures shall be set up for, and be available to, the voter. In the case of remote eVoting, such arrangements shall also be available through a different, widely available communication channel.	Can be achieved by means of adequate procedures during pre-voting stages, by supplying adequate information about the voting process.
47. There shall be equality in the manner of presentation of all voting options on the device used for casting an electronic vote.	Identical to traditional paper ballot voting.
48. The electronic ballot by which an electronic vote is cast shall be free from any information about voting options, other than that strictly required for casting the vote. The eVoting system shall avoid the display of other messages that may influence the voters' choice.	Identical to traditional paper ballot voting.
49. If it is decided that information about voting options will be accessible from the eVoting site, this information shall be presented with equality.	N.A.
50. Before casting a vote using a remote eVoting system, voters' attention shall be explicitly drawn to the fact that the e-election or e-referendum in which they are submitting their decision by electronic means is a real election or referendum. In case of tests, participants shall have their attention drawn explicitly to the fact that they are not participating in a real election or referendum and shall – when tests are continued at election times – at the same time be invited to cast their ballot by the voting channel(s) available for that purpose.	N.A.
51. A remote eVoting system shall not enable the voter to be in possession of a proof of the content of the vote cast.	N.A.
52. In a supervised environment, the information on the vote shall disappear from the visual, audio or tactile display used by the voter to cast the vote as soon as it has been cast. Where a paper proof of the electronic vote is provided to the voter at a polling station, the voter shall not be able to show it to any other person, or take this proof outside of the polling station.	When scanning in the voting booth or office, adequate precautions must be taken to satisfy this requirement.

6.8.2.5 Results

53. The eVoting system shall not allow the disclosure of	Can be achieved by means of adequate procedures during

the number of votes cast for any voting option until after the closure of the electronic ballot box. This information shall not be disclosed to the public until after the end of the voting period.	pre-voting, voting, and post-voting stages, as well as through the general requirements.
54. The eVoting system shall prevent processing information on votes cast within deliberately chosen sub-units that could reveal individual voters' choices.	See general requirements.
55. Any decoding required for the counting of the votes shall be carried out as soon as practicable after the closure of the voting period.	Can be achieved by means of adequate procedures during post-voting stages.
56. When counting the votes, representatives of the competent electoral authority shall be able to participate in, and any observers able to observe, the count.	Belgian law stipulates that this should be done by a College of Experts and by party witnesses: no specific provisions needed.
57. A record of the counting process of the electronic votes shall be kept, including information about the start and end of, and the persons involved in, the count.	Can be achieved by means of adequate procedures during post-voting stages.
58. In the event of any irregularity affecting the integrity of votes, the affected votes shall be recorded as such.	Can be achieved by means of adequate procedures during post-voting stages. (See Rec. n°107 and 108: A problem could occur if a paper ballot is deemed invalid. However, the solution will consist in defining which of the paper or electronic ballot is given legal validity.)

6.8.2.6 Audit

59. The eVoting system shall be auditable.	See general requirements.
60. The conclusions drawn from the audit process shall be applied in future elections and referendums.	The recommendations by the College of Experts should be implemented in future elections.

7 Thin clients e-voting system

7.1 Reasons why the consortium did not select this type of voting system

A very important disadvantage of the thin client voting system is that it ignores some valid concerns from the public about the secrecy and anonymity of the vote. On the one hand, voters are requested to enter their voting token into a reader inside the voting booth before casting their vote. This voting token may consist of the voter's eID card, or a voting token such as described in section 5.3.2 that specifies the proposed improved paper-based voting system. On the other hand, the thin client present in each booth has no computing capabilities: it transmits all data to a couple of servers located in the voting office. Hence, the servers store both the votes and the ID of the voter if an eID card is used as voting token, but should not link this data in any way. This goal is quite difficult to achieve in practice and it will be difficult to prove to the voters that full anonymity is indeed guaranteed.

Another disadvantage of this kind of system is that a major single-point-of-failure is created in the servers. In particular, if it is envisaged at a later stage to connect the servers to a public network, one is producing a tempting target, inviting hackers to bring down the system.

The consortium considers that a fully specified version of the thin client system will resemble the kiosk voting system described below quite closely, except that the kiosk voting system does not rely to the same extent on the security of the servers located in the voting offices. It is felt that ensuring and demonstrating the security of the servers of the thin-client system will be quite hard to achieve.

The thin client voting system uses a paper trail, which allows re-counting votes in case of dispute. However, in contrast to the scheme selected by the consortium, the system under investigation here can only be audited by re-counting all the votes that were cast in the same voting office. There is no possibility to audit a random selection of the votes.

The system does not appear to be much cheaper than any of the other systems under investigation, except for some variants of the optical scanner based system. An informal price quote was requested for a thin client system for 22.000 voting booths with 750 redundant servers (including operating system licenses, but excluding maintenance, software development, hardware installation, pointing device and printer). The quote yielded a cost of 750 USD per voting booth.

7.2 Description

The type of system discussed in this section consists in electronic voting machines connected to a secure network internal to the voting office and provided with a device to print paper trails of the voter's vote. The voting machines are thin clients, connected to two central servers (for redundancy) in the voting office. No specific software is running nor is any information recorded into the thin client. Such thin clients (basically stripped down versions of small footprint personal computers) are used as input/output stations for applications running on the server(s) to which they are connected.

The system requires that the voters authenticate themselves to the software of the thin

client server of the voting office before casting their votes. This authentication is done in the voting booth by having the voter enter his eID-card in a reader. The server software reads the national number from the eID-card and may use the information on the card to decide which lists of candidates need to be displayed (the list of candidates corresponding to the voter's constituency).

Currently, voters are only allowed to cast their vote at the polling station for which they have received a convocation letter: hence there is in fact only one possibility. However, the system may evolve to a configuration where voters can cast their vote at any voting office of their choice. In such a configuration, the server software will need to decide which list of candidates to present to the voter. One important additional complication is the fact that voters may try to vote multiple times by going to different voting offices. This can only be countered by introducing a centralized registration of voters having already cast their votes. All voting offices need to be permanently connected to this central registry. In this study, we do not discuss all the issues that may arise in this hypothetical configuration and we assume the simpler case where a voter must vote in a specific voting office.

If the voter has no eID-card, because it was lost or stolen, a temporary card needs to be issued before the date of the elections. This temporary card may contain only the data needed for the elections.

In order to cast his vote, the voter indicates his choice on the screen of the voting computer in a way similar to the one described in section 5.6.1.5 for the proposed voting system. Subsequently, the vote is printed on a paper trail ticket by a printer in the voting booth. The printer and the printed vote are situated behind a window, such that the voter can see the printed vote, but not touch it. The vote is printed both in human readable form and encoded in a barcode. The barcode is there to allow for a speedier re-count of the votes if needed. The following information is printed:

- Number of the list for which the voter has cast his vote
- If the vote is on the head of the list
- The preferences choices
- The date of the election
- The number of the polling station
- The number of the main polling station
- The barcode

If the printed vote corresponds to the voter's intentions, then the voter confirms the vote by pressing a button. When the button is pressed, the paper printout is dropped automatically in an urn of the voting office. Furthermore, these servers register that this voter has successfully completed the voting procedure.

After the voting period on Election day, the president of the voting office gathers the tickets situated in the urns and puts them together in a bag to be sent to the appropriate totalization office. He then copies the votes registered in both servers on CDs, which are then sent to the appropriate totalization office.

7.3 Advantages and disadvantages

The most important advantages of this kind of systems are related to efficiency: vote casting and vote counting are fully automated. The use of only two servers per voting office and thin clients in the voting booths should help to reduce the investments in hardware. Besides, this kind of system scales up to a certain point: the number of

voting booths per voting office may be increased without needing to install more powerful servers.

The most important disadvantages relate to security and trust.

Firstly, the requirement to insert the eID-card in a reader situated in the voting booth is problematic from the point of view of anonymity. Indeed, the servers store both the national number of the voters and their votes. Since the server needs to ensure that every voter successfully completes the voting procedure exactly once, it is difficult to logically separate the voting information from the identity information. Even the weakest type of correlation between identity and vote is unacceptable, but difficult to avoid, e.g. time of voting is approximately equal to time of identification.

Secondly, the system foresees a double authentication of the voters: once to the president of the voting office, and once to the servers, by using the eID-card. The servers, however, have no means to verify that the card in the reader is genuine; that it belongs to the person in the booth, and that is has not been reported stolen, i.e., a voter could easily present his own eID card to the president of the voting office, and cast with more than one eID card (e.g., using his own and subsequently a second person's card) in the voting booth. The eID-card may have been cloned or stolen. One could imagine that the servers read out also the card number and check whether it was reported as stolen, either based on a recently updated list of stolen eID cards, or after an online query. However, the loss might not have been reported yet. The server could ask the voter to enter his PIN, but that would probably not alleviate the fear that anonymity may be breached.

Even if technical solutions for the problems mentioned are found, there remains the issue that voters have to trust the system. They have to believe that the votes on the paper tickets are the same as the electronic votes. Auditors can verify the correspondence between electronic votes and paper votes only by re-counting all the votes cast in the same voting office.

In the future, the servers of the voting office might go on-line to pass on the results of the vote, or to authenticate voters from a different district. Connecting the servers to the outside world by means of a network introduces vulnerabilities to viruses, hackers, denial-of-service attacks, etc.

Electronic Voter's Register/Filing System

In order to enable the registration of voters through the use of eID cards, a specific file on the servers containing the personal data of voters (national number, voting residence, etc.) will have to be created on the basis of the voter's register. As the national number is planned to be used, this processing is subject both to the Data Protection Act[30] and to the National Register Act of 8 August 1983. The Sector Committee for the National Register, in charge of controlling the compliance with laws governing the National Register, the population registers and the national ID card should be consulted for advice and authorization.

Furthermore, as the authentication procedure and the casting of votes will be managed by the same server, additional security safeguards should be implemented in order to

[30] Act of 8 December 1992 relative to the protection of private life, Belgian Gazette 18 march 1993.

ensure the secrecy of the vote.

7.4 Compliance of Thin Clients Voting System with the CoE Recommendations

Since the consortium does not propose to retain thin client voting systems for Belgium, only the general requirements of the Council of Europe will be discussed here, excluding the technical requirements.

7.4.1 Legal Standards

7.4.1.1 Principles

Universal Suffrage

	Thin Clients Voting System
1. The voter interface of an eVoting system shall be understandable and easily usable.	Similar to eVoting system currently in use. The visual verification of the paper trail is new.
2. Possible registration requirements for eVoting shall not pose an impediment to the voter participating in eVoting	It is not necessary to register for the electronic voting. The identification data could be based on the voters' register
3. eVoting systems shall be designed, as far as it is practicable, to maximize the opportunities that such systems can provide for persons with disabilities.	Similar to eVoting system currently in use.
4. Unless channels of remote eVoting are universally accessible, they shall be only an additional and optional means of voting.	N.A.

Equal Suffrage

5. In relation to any election or referendum, a voter shall be prevented from inserting more than one ballot into the electronic ballot box. A voter shall be authorized to vote only if it has been established that his ballot has not yet been inserted in the ballot box.	To be guaranteed by appropriate technical safeguards.
6. The eVoting system shall prevent any voter from casting a vote by more than one voting channel.	Only one channel available.
7. Every vote deposited in an electronic ballot box shall be counted, and each vote cast in the election or referendum shall be counted only once.	To be guaranteed by appropriate procedures and technical safeguards.
8. Where electronic and non-electronic voting channels are used in the same election or referendum, there shall be a secure and reliable method to aggregate all votes and to calculate the correct result.	Similar to eVoting system currently in use.

Free Suffrage

9. The organization of eVoting shall secure the free formation and expression of the voter's opinion and, where required, the personal exercise of the right to vote.	Identical to traditional paper ballot voting, guaranteed by the use of a voting booth.
10. The way in which voters are guided through the	The voter definitively confirms his vote after the printing

eVoting process shall be such as to prevent their voting precipitately or without reflection.	of the paper trail ticket.
11. Voters shall be able to alter their choice at any point in the eVoting process before casting their vote, or to break off the procedure, without their previous choices being recorded or made available to any other person.	A procedure is needed to separate tickets not validated by the voter.
12. The eVoting system shall not permit any manipulative influence to be exercised over the voter during the voting.	Identical to traditional paper ballot voting. Privacy and free suffrage is guaranteed by the voting booth.
13. The eVoting system shall provide the voter with a means of participating in an election or referendum without the voter exercising a preference for any of the voting options, for example, by casting a blank vote.	Similar to eVoting system currently in use. The voter may be asked to confirm a blank vote.
14. The eVoting system shall indicate clearly to the voter when the vote has been cast successfully and when the whole voting procedure has been completed.	Easily satisfied with the confirmation asked from the voter once the ticket is printed.
15. The eVoting system shall prevent the changing of a vote once that vote has been cast.	Depends on the correctness of the election software and its resistance to tampering.

Secret Suffrage

16. eVoting shall be organized in such a way as to exclude at any stage of the voting procedure and, in particular, at voter authentication, anything that would endanger the secrecy of the vote.	Authentication and voting procedure should be strictly separated. The authentication procedure should finish at the latest before the final confirmation by the voter.
17. The eVoting system shall guarantee that votes in the electronic ballot box and votes being counted are, and will remain, anonymous, and that it is not possible to reconstruct a link between the vote and the voter.	The authentication procedure should finish at the latest before the final confirmation by the voter.
18. The eVoting system shall be so designed that the expected number of votes in any electronic ballot box will not allow the result to be linked to individual voters.	Identical to traditional paper ballot voting. Totals for individual booths or for individual voting offices are not publicly available.
19. Measures shall be taken to ensure that the information needed during electronic processing cannot be used to breach the secrecy of the vote.	Authentication and voting procedure should be strictly separated. The authentication procedure should finish at the latest before the final confirmation given by the voter.

7.4.1.2 Procedural Safeguards

Transparency

20. Member states shall take steps to ensure that voters understand and have confidence in the eVoting system in use.	Voters understands the eVoting system in use and in vast majority trust it; the paper trail strengthens the confidence in the system. The voter is required to trust that his identity is not encoded in any way in the barcode on the paper trail and that it is not associated with his vote in the servers.
21. Information on the functioning of an eVoting system shall be made publicly available.	Easily enough to achieve by publishing a description of the working of the eVoting system and of the counting process.
22. Voters shall be provided with an opportunity to practice any new method of eVoting before, and separately from, the moment of casting an electronic vote.	Training facilities should be made available both on the Internet and in the municipalities.
23. Any observers, to the extent permitted by law, shall be able to be present to observe and comment on the	No specific provisions needed. The College of Experts

e-elections, including the establishing of the results.	should be kept in charge of this process.

Verifiability and Auditability

24. The components of the eVoting system shall be disclosed, at least to the competent electoral authorities, as required for verification and certification purposes.	See general requirements.
25. Before any eVoting system is introduced, and at appropriate intervals thereafter, and in particular after any changes are made to the system, an independent body, appointed by the electoral authorities, shall verify that the eVoting system is working correctly and that all the necessary security measures have been taken.	Belgian law stipulates that this should be done by a College of Experts: no specific provisions needed.
26. There shall be the possibility for a recount. Other features of the eVoting system that may influence the correctness of the results shall be verifiable.	Three types of recounts are possible: a. automated recount with different software b. automated recount based on the scanning of barcodes c. manual recount of paper ballots The possibilities suggested by the CoE are the following: instruct the eVoting system to recount; transfer the electronic ballot box to a similar but distinct eVoting system and perform the second counting on this system; let the recount be performed by a different system which is interoperable with the eVoting system
27. The eVoting system shall not prevent the partial or complete re-run of an election or a referendum.	Servers are located in each voting office. If part of the election should be re-run, this would be possible at the very level of voting office.

Reliability and Security

28. The member state's authorities shall ensure the reliability and security of the eVoting system.	Can be achieved by means of adequate procedures and technical safeguards during pre-voting, voting, and post-voting stages.
29. All possible steps shall be taken to avoid the possibility of fraud or unauthorized intervention affecting the system during the whole voting process.	Can be achieved by means of adequate procedures and technical safeguards during pre-voting, voting, and post-voting stages, as well as through the general requirements. The network used in the voting offices should be duly secured.
30. The eVoting system shall contain measures to preserve the availability of its services during the eVoting process. It shall resist, in particular, malfunction, breakdowns or denial of service attacks.	Can be achieved by means of adequate procedures and technical safeguards during pre-voting, voting, and post-voting stages, as well as through the general requirements. The use of two servers with replication software contributes.
31. Before any e-election or e-referendum takes place, the competent electoral authority shall satisfy itself that the eVoting system is genuine and operates correctly.	Can be achieved by means of adequate procedures during pre-voting stages, as well as through the general requirements.
32. Only persons appointed by the electoral authority shall have access to the central infrastructure, the servers and the election data. There shall be clear rules established for such appointments. Critical technical activities shall be carried out by teams of at least two people. The composition of the teams shall be regularly changed. As far as possible, such activities shall be carried out outside election periods.	Can be achieved by means of adequate procedures during pre-voting, voting, and post-voting stages, as well as through the general requirements.
33. While an electronic ballot box is open, any	Can be achieved by means of adequate procedures during

authorized intervention affecting the system shall be carried out by teams of at least two people, be the subject of a report; be monitored by representatives of the competent electoral authority and any election observers.	voting and post-voting stages, as well as through the general requirements.
34. The eVoting system shall maintain the availability and integrity of the votes. It shall also maintain the confidentiality of the votes and keep them sealed until the counting process. If stored or communicated outside controlled environments, the votes shall be encrypted.	Votes will be stored encrypted until the tallying of the votes.
35. Votes and voter information shall remain sealed as long as the data is held in a manner where they can be associated. Authentication information shall be separated from the voter's decision at a pre-defined stage in the e-election or e-referendum.	Authentication and voting procedure should be strictly separated. The authentication procedure should finish at the latest before the last confirmation given by the voter.

7.4.2 Operational Standards

7.4.2.1 Notification

36. Domestic legal provisions governing an e-election or e-referendum shall provide for clear timetables concerning all stages of the election or referendum, both before and after the election or referendum.	Clear procedures should be defined by the law.
37. The period in which an electronic vote can be cast shall not begin before the notification of an election or a referendum. Particularly with regard to remote eVoting, the period shall be defined and made known to the public well in advance of the start of voting.	No specific provisions needed.
38. The voters shall be informed, well in advance of the start of voting, in clear and simple language, of the way in which the eVoting will be organized, and any steps a voter may have to take in order to participate and vote.	Information about the procedure to be followed should be provided to the voter.

7.4.2.2 Voters

39. There shall be a voters' register which is regularly updated. The voter shall be able to check, as a minimum, the information which is held about him on the register, and request corrections.	Identical to traditional voting system.
40. The possibility of creating an electronic register and introducing a mechanism allowing online application for voter registration and, if applicable, for application to use eVoting, shall be considered. If participation in eVoting requires a separate application by the voter and/or additional steps, an electronic, and, where possible, interactive procedure shall be considered.	N.A.
41. In cases where there is an overlap between the period for voter registration and the voting period, provision for appropriate voter authentication shall be made.	N.A.

7.4.2.3 Candidates

42. The possibility of introducing online candidate	N.A.

nomination may be considered	
43. A list of candidates that is generated and made available electronically shall also be publicly available by other means.	N.A.

7.4.2.4 Voting

44. It is particularly important, where remote eVoting takes place while polling stations are open, that the system shall be so designed that it prevents any voter from voting more than once.	N.A.
45. Remote eVoting may start and/or end at an earlier time than the opening of any polling station. Remote eVoting shall not continue after the end of the voting period at polling stations.	N.A.
46. For every eVoting channel, support and guidance arrangements on voting procedures shall be set up for, and be available to, the voter. In the case of remote eVoting, such arrangements shall also be available through a different, widely available communication channel.	Can be achieved by means of adequate procedures during pre-voting stages, by supplying adequate information about the voting process. Voters are already allowed to request the help of a member of the polling office.
47. There shall be equality in the manner of presentation of all voting options on the device used for casting an electronic vote.	Similar to eVoting system currently in use.
48. The electronic ballot by which an electronic vote is cast shall be free from any information about voting options, other than that strictly required for casting the vote. The eVoting system shall avoid the display of other messages that may influence the voters' choice.	Similar to eVoting system currently in use.
49. If it is decided that information about voting options will be accessible from the eVoting site, this information shall be presented with equality.	N.A.
50. Before casting a vote using a remote eVoting system, voters' attention shall be explicitly drawn to the fact that the e-election or e-referendum in which they are submitting their decision by electronic means is a real election or referendum. In case of tests, participants shall have their attention drawn explicitly to the fact that they are not participating in a real election or referendum and shall – when tests are continued at election times – at the same time be invited to cast their ballot by the voting channel(s) available for that purpose.	N.A.
51. A remote eVoting system shall not enable the voter to be in possession of a proof of the content of the vote cast.	N.A.
52. In a supervised environment, the information on the vote shall disappear from the visual, audio or tactile display used by the voter to cast the vote as soon as it has been cast. Where a paper proof of the electronic vote is provided to the voter at a polling station, the voter shall not be able to show it to any other person, or take this proof outside of the polling station.	Similar to eVoting system currently in use. No paper proof is provided to the voter since paper trail tickets are inaccessible.

7.4.2.5 Results

53. The eVoting system shall not allow the disclosure of the number of votes cast for any voting option until after the closure of the electronic ballot box. This information shall not be disclosed to the public until	Can be achieved by means of adequate procedures during pre-voting, voting, and post-voting stages, as well as through the general requirements.

after the end of the voting period.	
54. The eVoting system shall prevent processing information on votes cast within deliberately chosen sub-units that could reveal individual voters' choices.	Can be achieved by means of adequate procedures during post-voting stages, as well as through the general requirements.
55. Any decoding required for the counting of the votes shall be carried out as soon as practicable after the closure of the voting period.	Can be achieved by means of adequate procedures during post-voting stages.
56. When counting the votes, representatives of the competent electoral authority shall be able to participate in, and any observers able to observe, the count.	Belgian law stipulates that this should be done by a College of Experts and by party witnesses: no specific provisions needed.
57. A record of the counting process of the electronic votes shall be kept, including information about the start and end of, and the persons involved in, the count.	Can be achieved by means of adequate procedures during post-voting stages.
58. In the event of any irregularity affecting the integrity of votes, the affected votes shall be recorded as such.	Can be achieved by means of adequate technical features during post-voting stages.

7.4.2.6 Audit

59. The eVoting system shall be auditable.	See general requirements.
60. The conclusions drawn from the audit process shall be applied in future elections and referendums.	The recommendations by the College of Experts should be implemented in future elections.

8 Remote/Internet voting based on homomorphic encryption

8.1 Reasons why the consortium did not select this type of voting system

Only a very small number of secure remote voting systems have been fully developed on paper. Almost none have been deployed in practice. Among experts, there appears to be a consensus that these systems still suffer from childhood diseases.

Secondly, it is not certain that the public is ready to accept fully computerized voting systems. Even though mathematical proofs of security exist and can be provided, they cannot be explained in simple terms to laymen. The absence of a paper trail and the need to blindly trust the correctness of program code are often cited as reasons not to adopt systems like this one.

Thirdly, a remote voting system contains client-side applications that help the voter to cast his vote. The security of these applications cannot – within the current state of available technologies – be ensured because of the multitude of viruses, OS version variations, and bugs that are present on home PCs. At the moment, there is not sufficient infrastructure to support voting from home.

Finally, there remain the problems of coercion, vote buying etc., which are difficult to avoid in any remote voting system.

Still, it might be interesting to deploy this kind of voting system for specific voters such as, for instance, Belgians residing abroad. This would allow effective experimentation provided sufficient safeguards are implemented and might pave the way for greater automation of the voting process.

8.2 Introduction

The voting schemes described in this section and the next are based on homomorphic encryption. Using homomorphic encryption, the product of encrypted messages equals the encryption of the sum of the messages. This is useful for electronic voting, where the encrypted message is the vote and hence we do not need to decrypt individual votes in order to get the final tally.
The remote voting system based on homomorphic encryption is depicted in Figure 23. It consists of two main parts: server side components and client side components. The server is operated by election officials and contains mainly the voting server software, the configuration manager software, a web server, and databases. The web server has two distinct functions: it displays election details and it allows for downloading remote voting client software. The voting server executes all the tasks related to server side voting functions. The configuration manager reads the input provided by election officials and formats it and makes it available to other modules.
Voters and (remote) talliers use fixed or mobile Internet devices to connect to the remote voting servers for operations like registration, voting and tallying. Here, a web browser is used for viewing elections details and getting remote voting clients. Registration and Voting Clients are used by voters and the Tallier Client is used by remote talliers for their share of the tally process.

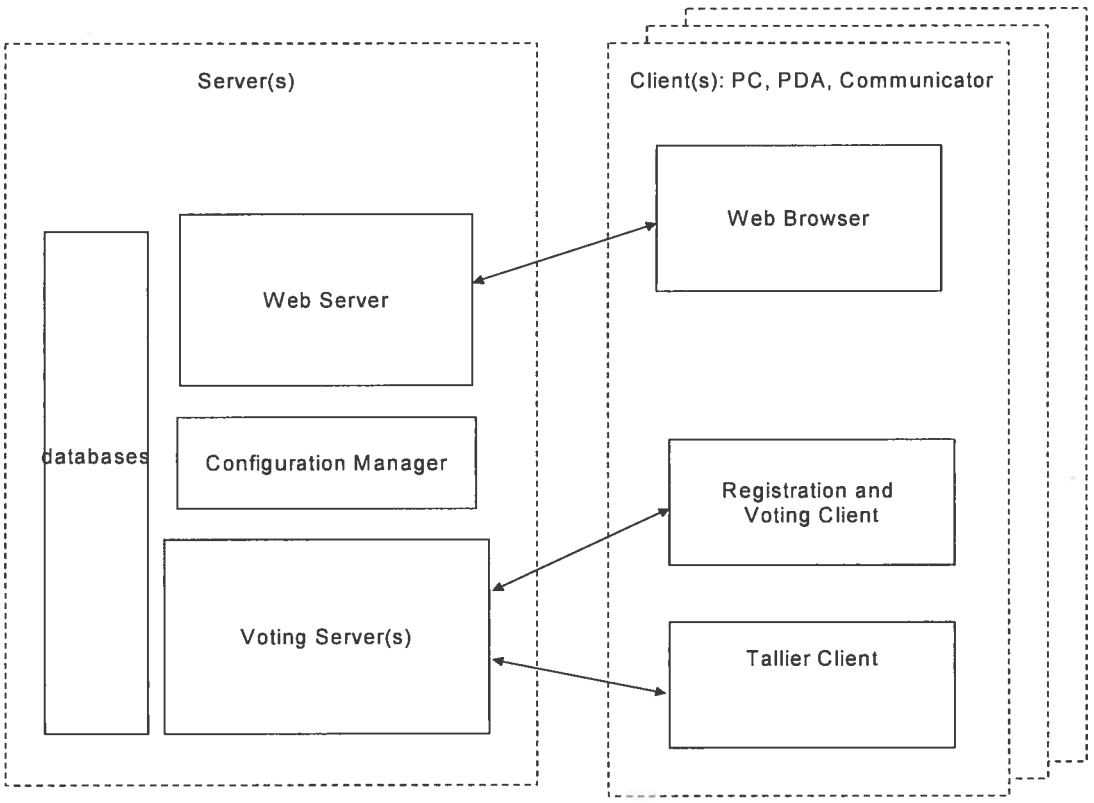


Figure 23: Remote voting architecture based on homomorphic encryption

8.3 Functional overview of the remote voting architecture

In this section we consider the various phases of an election and the relevance of each step to remote voting. The whole election process can be divided into the following three phases:

- Setup phase (pre-election),
- Voting phase (election),
- Tabulation phase (post-election).

8.3.1 The setup phase

This stage involves the initialization of the technical part of the election system (servers) as well as the initialization of the organizational structure. All the necessary election parameters are configured using Configuration Manager tools.

8.3.1.1 The election officials, scrutineers and administrators

The *election officials*, *scrutineers* and *administrators* are appointed. It is assumed that these individuals have been specifically trained to fulfill their obligations and that they fully understand their roles and responsibilities.

Election officials execute all the steps in the election process which need human intervention such as operating the computer systems and supplying the necessary data to the system. In any case, election officials are responsible for the composition of the

various ballot forms and the assignment of types of ballot forms to (classes of) voters.

Scrutineers monitor the election process, both by verifying the actions of the election officials and by performing the necessary checks on the computer systems.

Administrators are privileged users of the remote voting system who ensure the proper functioning of the IT equipment and software used during the whole voting process.

8.3.1.2 Talliers

Furthermore, the *talliers* are appointed. These individuals will be responsible for determining the election result from the votes that were cast. The concrete tasks of the talliers depend heavily on the underlying (cryptographic) protocols. The number of talliers may vary from just one to tens or even hundreds. Depending on underlying (cryptographic) protocols, Tallier keys are generated. That is, either

- Generation of special key-pairs or
- Talliers interact to generate individual shares of a key.

In each case, the "keys" are stored on a smart card or on disc.

8.3.1.3 Voter registration

Finally, the list of registered voters is determined. This part may actually consist of a lengthy and complicated process. An important step in the voter registration process is formed by the initialization of the voter authentication mechanisms to be used during the voting stage.

During voter registration, two possibilities may be used:

- Registration by voters themselves. For example: each voter uses appropriate software to generate a pair of keys as a part of the registration process and submits the key pair's public key to the remote voting server.
- Eligible voters are registered by election officials. For example, by using smart card based authentication, assuming that the smart cards have been issued in a legitimate way. Here, election officials can add the voters' public keys to the voter database without any intervention of individual voters.

All the above operations are performed well before the start time of voting, which is the time at which the voting phase begins and servers start delivering electronic ballots to voters and accepting votes.

8.3.2 Voting phase

The voting phase consists of four steps: voter authentication, ballot production, voting, and ballot validation. To perform these operations, voters use downloaded remote voting client software to connect to the remote voting server over a secure SSL connection through the Internet.

8.3.2.1 Authentication phase

A voter authenticates himself to the remote voting server using the authentication engine.
The Authentication Engine provides an authentication/verification service for the other elements of the system. It offers two basic services:

- An on-line challenge/response protocol to authenticate a voter on a remote

client.

- A signature verification procedure for received signed messages.

With successful authentication, the process continues to ballot production phase.

8.3.2.2 Ballot production phase

At the remote voting server, depending on the authenticated VoterID, the voter's entitlement is checked as well as his voting status. Based on this, a suitable ballot is created and sent back to voter. The appropriate databases are updated to reflect this action.

8.3.2.3 Voting phase

Using the ballot sent to him by the voting server, the voter casts his vote(s) and sends it back to the voting server.

8.3.2.4 Ballot validation phase

At the remote voting server, a check on the VoterID and its Voting Status is carried out. Next, the submitted vote is validated and if successful, the vote is stored in the Bulletin board database. An acknowledgement is sent to the voter in any case.
After the end of the voting period, no more ballots are accepted at the server and the Bulletin board database is ready for the tabulation phase.

8.3.3 Tabulation phase

On the completion of the voting phase the votes need to be counted. Designated and genuine talliers use downloaded voting tallier client software to connect to the remote voting server through a secure SSL connection over the Internet.

- The server tallying software processes all the votes in the database to generate a token.
- Talliers individually connect to the remote voting server and retrieve the token.
- Tallier client software "decrypts" the token.
- Tallier client returns the decrypted token. Tallying server software can be asked to validate the returned token and to discard "false" returns.
- Tallying server software collects returned tokens.
- After receiving at least N out of M (these parameters are configured in the Setup Phase) sub-tally results, the tallying software computes the election result.
- The Tallying software publishes the election result.

The declaration of the result leads to the completion of the total election process.

8.4 Block Overview of the Remote Voting Architecture

The remote voting architecture is divided into appropriate blocks based on their functions in the system. Three parts can be distinguished:

- Server related modules,
- Client related modules, and

- Modules common to both server and client.

Figure 24 gives the notations used for some of the symbols appearing in Figure 25 and.Figure 26

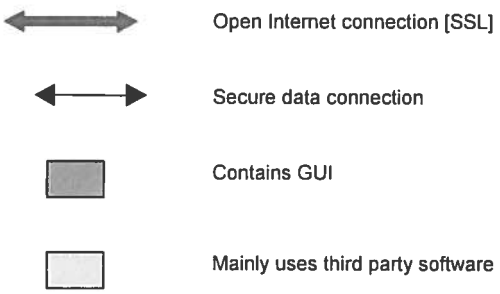


Figure 24: Symbol information

8.4.1 Remote voting server architecture

The remote voting server is presented in Figure 25. The server consists of:

- remote voting server software,
- remote voting configuration software,
- HTML (web) server,
- databases.

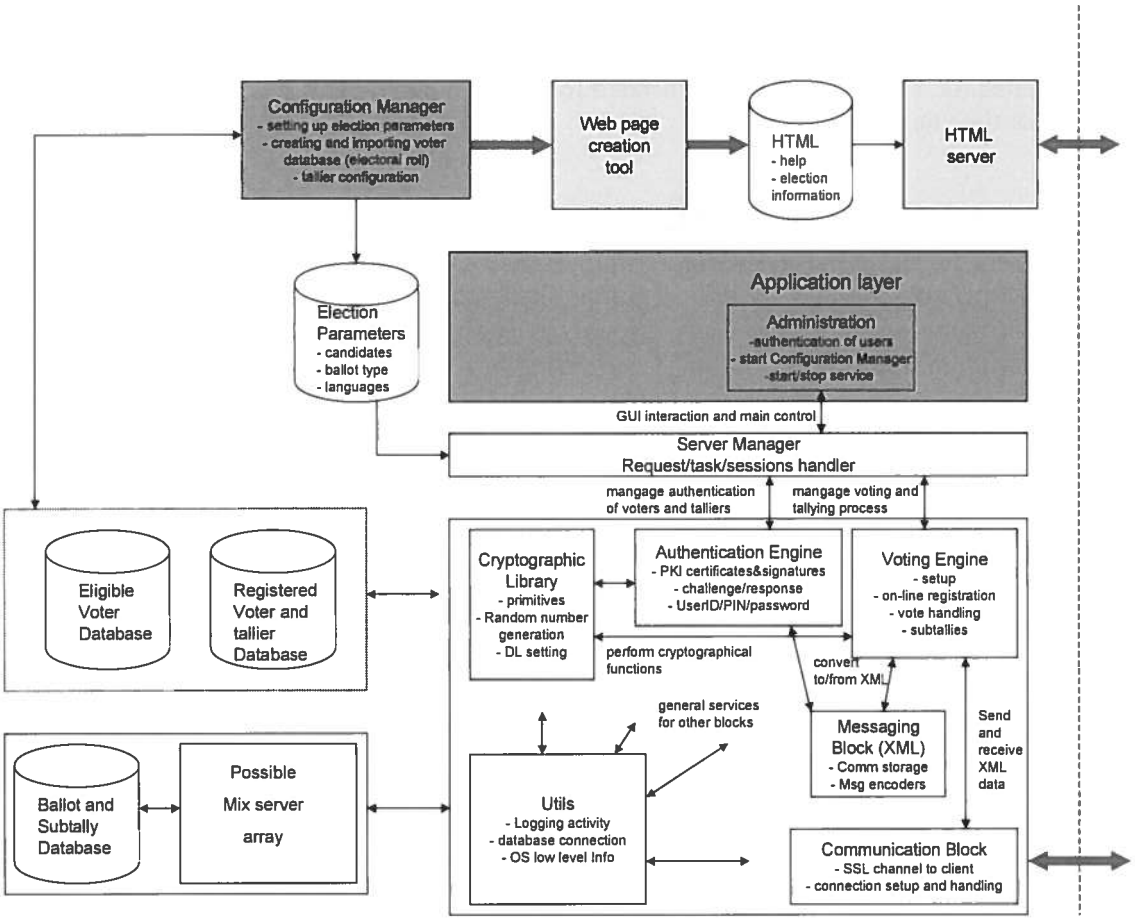


Figure 25: Remote Voting Architecture – Server

8.4.1.1 Administration Block

The Administration Block provides the GUI, by which the election administrators control the Remote voting server. The administration does not have many user functions and the GUI is rather simple. The functions of the administration block are:

- start the server (timer controlled service start-up and termination),
- start logging,
- start the configuration manager,
- display server status,
- user authentication to prevent unauthorized persons trying to operate the system.

8.4.1.2 Server database

The remote voting system requires three databases:

- eligible voters,
- registered voters and talliers, and
- ballot/tally databases.

These may or may not reside on the same computer. The eligible and registered voters databases could also be merged by storing a registration attribute in the eligible voters database. Data storage is also needed for election parameters, election web pages, and for the voters' public keys.

8.4.1.3 Server configuration

There needs to be a software component for configuring the server and election parameters, because each election has many unique properties. When the configuration is finished, it should be impossible for anyone to change the configuration without proper authorization. At least some of the configured parameters will need to be transferred to the Remote voting Web server, which presents election information. However, the configuration utility is not used for that.

8.4.1.4 HTML (web) server

The HTML (web) server is used to make the election web pages available to the voters. Its duties are:

- presenting election information;
- giving information about the Remote voting system;
- allowing the download of suitable remote voting clients for the user's terminal.

8.4.1.5 Other modules

Other modules are common with the client and are described in section 8.4.3.

8.4.2 Client architecture

The Remote voting client is presented in Figure 26. The structure of the software is designed to be as similar as possible to that of the server software, in order to make the maintenance of the code easier. However, there are more important factors to take into account than ease of maintenance, such as: size of client code and running speed of the code. There are also notable differences between client and server, e.g., in GUI, use of specialized cryptographic hardware, database connectivity, and manager blocks. This means that although most of the blocks have identical names and lots of common contents, there are differences inside these blocks. The server's blocks may contain unused client code, but due to the code size and the related download time restrictions, this redundant code must be removed from the client's code.

There are other differences between the client and the server. The election parameters are downloaded from the server and they must have some storage and access method in the client. However, there is no need to have database software in the client, a file or memory object will be sufficient. Also a smart card and a smart card reader will be used only in the client. The server is always a Java application, but the client can be implemented also to be run as Java Applets in a web browser. Even though an application would be used in a client, a web browser is still needed to fully use the system, e.g., some election information is only available from the HTML server.

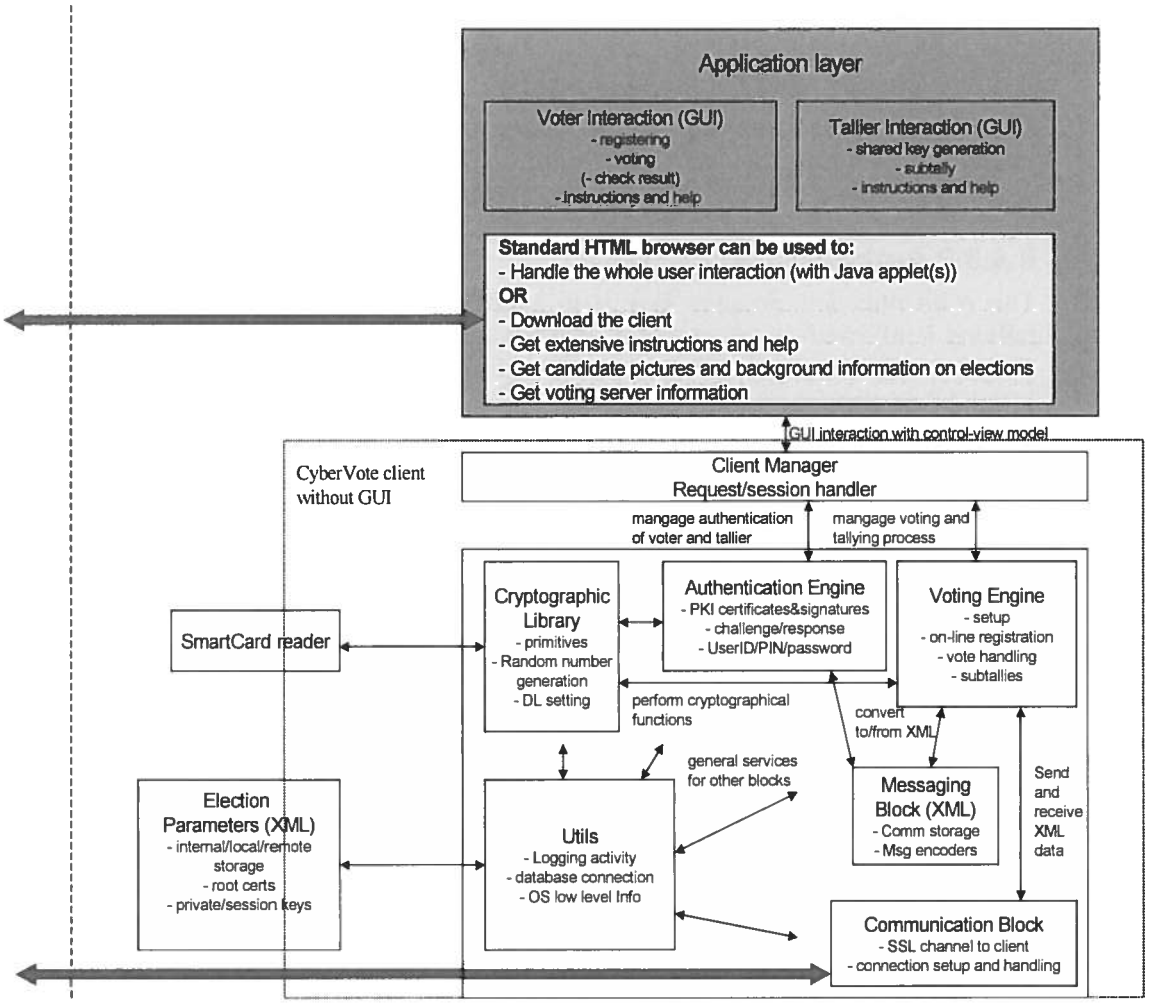


Figure 26: Remote voting architecture – Client

8.4.3 Remote voting software modules common to client and server

The remote voting common software has been divided into different blocks according to the tasks it has to perform. The blocks are:

- Server/Client Manager,
- Authentication Engine,
- Voting Engine,
- Messaging Block,
- Communication Block,
- Cryptographic Library, and
- Utilities.

At the highest layer are the Server/Client Managers, which are responsible for user interaction using the GUI module and which control the operations. Next in the hierarchy come the Authentication and Voting Engines, which provide the main functionality of the server. The rest of the modules are supporting the main

functionality.

8.4.3.1 Server and Client Managers

The Manager blocks are the core of remote voting software. They control the other modules according to the state of the system. They display information to the user and wait for user input. They use the services of other modules through APIs.

8.4.3.2 Authentication Engine

The Authentication Engine's task is to authenticate the user before either voting or tallying is allowed. A client Authentication Engine will initially present its **user ID**. The server Authentication Engine will check the database to determine if the user ID is valid, and then use the designated method to authenticate that user. Authentication is based on a challenge-response protocol, which supports both public key and PIN/password approaches.

8.4.3.3 Voting Engine

The voting engine's task is to handle the functions required by the voting protocols.

8.4.3.4 Communication Block

The communication block is responsible for establishing and maintaining an SSL connection between client and server. As part of this process the server Communication Block presents a certificate to the client so that the server's identity may be confirmed. (Note that the client authentication is handled at the application level by the Authentication Engine). All network traffic between the server and the client is routed through the secure SSL tunnel.

8.4.3.5 Cryptographic Library

The cryptography library will be used mainly for basic operations that are the result of a cryptographic operation. These mathematical operations represent the heart of the cryptographic library. They allow implementing e.g., the homomorphic encryption, but also other public-key algorithms such as digital signatures, the generation of random seeds for keys and key pairs, etc.

- Encryption: the encryption operation protects the confidentiality of the information processed, stored (depending on the application, information may be stored persistently or temporarily) or conveyed from one entity to another.

- Secret-key algorithms: may be used when communicating securely from a web browser to a web server, e.g., using SSLv3.0 or TLSv1.0. Encryption algorithms that can be used in this context include the AES (with 128-bit keys) and 3DES (with 112-bit or 168-bit-keys). The mode of operation for this encryption must be chosen as needed: CBC, CFB, etc.

- Public-key algorithms such as the ElGamal homomorphic encryption protect the confidentiality of a voter's vote.

- Random generation: the security of many cryptographic systems depends upon the generation of unpredictable inputs. Examples include the generation of a secret encryption key, the generation of an ElGamal key pair, the generation of a random seed when encrypting with the ElGamal cryptosystem, etc. The cryptography library gives access to a secure random

(number) generator. Note that this generator must be carefully initialized in order to produce unpredictable output.

- Data integrity (message authentication): the cryptography library provides data integrity operations. Depending on the requirements, these operations rely on no secret information (cryptographic hash functions), on a shared secret (message authentication codes), or on public key cryptography such as digital signatures (using RSA, ElGamal, DSA, etc.).

- Entity authentication (identification): techniques providing identification allow one party (the verifier) to gain assurances that the identity of another (the claimant) is as declared, thereby preventing impersonation. The cryptographic library provides support for zero-knowledge identification protocols, digital signatures and for password-based identification schemes. If necessary for the digital signature scheme, suitable padding schemes are applied before generating the digital signature.

8.4.3.6 Utilities

The functionality that does not fit into any other block is combined into the Utilities Block. The contents of the utilities are, e.g.:

- logging: opening/closing file, writing to file;
- helper functions to use databases;
- getting operating system low level information.

8.5 Compliance of Internet/Remote Electronic Voting with the CoE Recommendations

Since the consortium does not propose to retain Internet/remote electronic voting for Belgium, only the general requirements of the Council of Europe will be discussed here, excluding the technical requirements.

A recent Law Proposal[31] intends to introduce Internet voting as an alternative voting channel for Belgian citizens living abroad. No indications on the system to be used are included. It should be noticed that the Law proposal refers to two different modalities which do not both fit into what the Council of Europe acknowledges as "Remote electronic voting". The first modality consists of casting a vote on a computer at the Embassy or consulate. This option is a modality of kiosk voting and similar to the one suggested in the previous section. The second modality foresees the possibility of casting a vote on a personal computer at home. As mentioned above, the Council of Europe does not acknowledge the first modality as remote electronic voting as long as the vote is cast in a supervised environment and thus does not raise the specific concerns of remote voting regarding the protection of the secrecy of the vote, the freedom of the vote as well as the procedure of identification of the voter.

Internet voting is conceived as an alternative way to cast a vote, but requires the voter

[31] Belgian Parliament, Law Proposal modifying article 180bis of Electoral Code related to the vote of Belgian living abroad and intending to introduce « remote e-voting », doc n° 52K0090, 6 August 2007

to expressly opt for this channel prior to the election.[32] Belgians living abroad are already given the possibility to cast their vote in an unsupervised environment, by postal voting.

The Venice Commission, in its report on the compatibility of remote voting and electronic voting with the standards of the Council of Europe[33], acknowledged the conformity of postal and electronic remote voting with the principles of democratic elections. This body asserts that "their compatibility depends primarily on adequate provision, through national legislation and legal practice, of the prescribed conditions, taking particular account of technical and social conditions."

According to guideline I.3.2. of the Code of Good Practice in Electoral Matters, postal voting should be allowed only where the postal service is safe (in other words, protected from deliberate manipulation) and reliable, in that it operates correctly.[34] Remote electronic voting should ensure the same degree of reliability as postal voting.

8.5.1 Universal Suffrage

The Principle of universal suffrage requires that 'Unless channels of remote eVoting are universally accessible, they shall be only an additional and optional means of voting'. This means that using a single remote electronic voting channel in isolation restricts accessibility. The voter should be protected from a situation where the only means offered for voting is one that is not effectively available to him. This calls for procedural and technical safeguards to ensure that all voters will be able to cast their vote the day of the election. Remote eVoting may start or end at an earlier time than the opening of any polling station. Remote eVoting shall not continue after the end of the voting period at polling stations. Procedural safeguards should be implemented to allow the voter to cast his vote in case a problem occurs with the server.

It follows that every eligible voter shall have access to at least one voting channel and that:

- a contingency procedure shall be drawn up to prepare for the possibility that one or more voting channel where necessary (Recommendations 61b, 70a, 71a);
- the contingency procedure shall include measures for physical disaster recovery (Recommendation 75b);
- staff shall be trained to follow the contingency procedure (Recommendation 71b);
- the eVoting system shall be protected against threats to its availability including: malfunctioning, breakdown and denial of service attacks (Recommendation 30);

---

[32] The current article 180bis of the Electoral Law requires Belgians living abroad to fill out a form where they indicate which voting channel they will use and the municipality where they wish to be registered.

[33] Council of Europe, Venice Commission, Report on the compatibility of remote voting and electronic voting with the standards, adopted at its 58th Plenary Session (Venice, 12-13 March 2004)

[34] European Commission For Democracy Through Law, Report on the compatibility of remote voting and electronic voting with the standards of the council of Europe, adopted on the 12-13 March 2004, pts 15 and 16.

- the availability of each voting channel shall be subject to regular checks (Recommendation 79b).

The timetable for voting channel availability shall be designed to maximize voter access and shall be made public well in advance of the start of the polling period (Recommendations 37, 45).

Finally, it is recommended that the registration procedure does not differ from the existing one in order to avoid confusion amongst voters. The example of France is worth mentioning: in the elections of the Assembly of French living abroad's representatives of June 2006, the complexity of the procedure discouraged many voters living abroad from opting for this voting channel.

8.5.2 Equal Suffrage

The principle of equal suffrage requires that every voter is granted the same number of votes. The Belgian Constitution grants one vote to each eligible voter. In order to avoid multiple voting, the Venice Commission recommends that, when remote voting takes place outside the country, specific safeguards should be implemented, e.g. names of the voters who use remote voting should be crossed out from the lists in a way which prevents them from voting more than once at the polling station during the voting period on Election Day. The Law proposal suggests using either a personal code or a chip card (the eID card) for the authentication procedure.

The use of an electronic authentication procedure calls for the creation of an electronic voter's files which should be able to distinguish eligible voters from other citizens and distinguish those who have successfully cast their votes from those who have not. This may require special attention where multiple voting channels exist and where voter registers may not be up-to-date. However, in the current voting system, Belgians living abroad must opt in advance for one specific channel. This allows establishing separated voter's lists for each voting channel.

8.5.3 Free Suffrage

The free formation and expression of the voter's opinion principle appears to be particularly vulnerable in remote eVoting. It is obvious that the same level of secrecy as the one ensured in voting booths cannot be ensured. Remote Internet voting should thus use the existing standards in postal voting as reference. It appears necessary to ensure the confidentiality of electronic voting with measures comparable to those applicable to postal voting, especially by preventing data manipulation, protecting anonymity to prevent possible disclosure of the elector's wishes, and by maintaining the authenticity and integrity of the votes cast.

Specific safeguards should be implemented in order to ensure that:

- Only the voter should have access to his own vote. Technical safeguards should ensure that the content of the vote cannot be printed or stored on the voter's personal computer, but this appears to be quite difficult to achieve. The confidentiality of the vote is guaranteed by a strict separation of the authentication procedure and the storage of the casting of a vote.
- The eVoting system should not permit any manipulative influence to be exercised over the voter during the vote. The remote voting system described here ensures the same level of guarantee as the current postal voting system.

- The eVoting facilities should not allow the completed ballot to be stored on the voter's device and the vote cast later.
- No one other than the voter should have access to the vote, either on the device or during the transmission to the ballot box. e.g.: sounds which can be associated with a candidate or an option, pop-up screens promoting a particular choice.

8.5.4 Secret Suffrage

With regard to the secrecy of the vote, voters must be able to obtain confirmation of their votes and correct them, if necessary, while respecting the secrecy of suffrage. The system's transparency must be guaranteed. Any violation of secret suffrage should be sanctioned (guideline I.4.d.). It should not be possible to reconstruct the content of any voter's vote and link it to the voter who cast it. The moment of inserting a vote into the electronic ballot box is the latest point in time at which the vote must be separated from the information about who has cast it, without any possibility of ever reconstructing this link. This implies that:

- Anything that would endanger the secrecy of the vote should be excluded at any stage of the voting procedure and, in particular, at voter authentication. Procedural and technical safeguards related to the authentication procedure (sending of personal keys, use of eID cards, etc.) should ensure the respect of the secrecy of the vote.
- At no stage shall the voter's identity and vote be available together in unencrypted form to any person (other than the voter) or system (Recommendations n°16, 19, 34b, 35, 93a, 106), except where required by law and sanctioned by the relevant authority.

The eVoting system shall maintain the privacy of individuals. Confidentiality of voter's registers stored in or communicated by the eVoting system shall be maintained. (Recommendation n°78)

8.5.5 Procedural Safeguards

During the tallying of the votes, transparency is crucial. In Switzerland, the tallying of the vote is realized by a commission constituted by representatives of political parties. This Commission holds the cryptographic keys of the e-urn. In Belgium, the presence of members of the College of experts and of observers from the political parties ensures similar transparency.

As regards transparency, security measures for Internet voting may however make it necessary not to allow the presence of observers in the computer room itself. In that case, measures should be taken in order to give the observers the opportunity to monitor the activities without breaching anonymity.

Where there may be doubt (such as with remote voting), voters shall be educated as to how they may confirm that they are using an authentic channel and that the authentic ballot has been presented (Recommendation n° 90b).

In regard to the system used, this category includes measures that prevent fraudulent or erroneous votes from being recorded[35]. It follows that:

- only votes cast by eligible voters shall be counted, and only permitted number of votes for that voter (Recommendations n°5a, 94);
- votes shall not be recorded outside the polling period. However, provision shall be made for latency in voting channels (Recommendations n° 91, 96).

8.5.6 Recommendations of the Council of Europe

8.5.6.1 Legal Standards

Principles

Universal Suffrage

	Internet/Remote Electronic Voting
1. The voter interface of an eVoting system shall be understandable and easily usable.	Similar to eVoting system currently in use.
2. Possible registration requirements for eVoting shall not pose an impediment to the voter participating in eVoting	A central voters register needs to be created. However, this register could be based on an aggregation of all voters' registers managed by the local authorities. If the voter is required to follow a specific procedure, ease of use for registration should be ensured.
3. eVoting systems shall be designed, as far as it is practicable, to maximize the opportunities that such systems can provide for persons with disabilities.	Similar to eVoting system currently in use.
4. Unless channels of remote eVoting are universally accessible, they shall be only an additional and optional means of voting.	If based on Internet, there is no need for additional voting channels, because the Internet-based system can also be used in, e.g., a kiosk environment using a secure intranet.

Equal Suffrage

5. In relation to any election or referendum, a voter shall be prevented from inserting more than one ballot into the electronic ballot box. A voter shall be authorized to vote only if it has been established that his ballot has not yet been inserted in the ballot box.	To be guaranteed by appropriate technical safeguards at the authentication phase. Multiple voting will be avoided through a permanent update of the central voters' database.
6. The eVoting system shall prevent any voter from casting a vote by more than one voting channel.	A voter registers himself for a particular voting channel, and he has only one vote for this channel.
7. Every vote deposited in an electronic ballot box shall be counted, and each vote cast in the election or referendum shall be counted only once.	To be guaranteed by appropriate procedures and technical safeguards.
8. Where electronic and non-electronic voting channels are used in the same election or referendum, there shall be a secure and reliable method to aggregate all votes and to calculate the correct result.	Identical to voting system in use.

Free Suffrage

[35] McGaley M., Gibson J.P., A critical analysis of the Council of Europe Recommendations on e-voting, available on-line at: http://www.usenix.org/events/evt06/tech/full_papers/mcgaley/mcgaley_html/, last accessed on 31 August 2007

9. The organization of eVoting shall secure the free formation and expression of the voter's opinion and, where required, the personal exercise of the right to vote.	Similar to postal voting.
10. The way in which voters are guided through the eVoting process shall be such as to prevent their voting precipitately or without reflection.	The voter has to confirm his vote before it is cast.
11. Voters shall be able to alter their choice at any point in the eVoting process before casting their vote, or to break off the procedure, without their previous choices being recorded or made available to any other person.	Before the voter has confirmed his vote, he can interrupt the process at any moment. Technical safeguards must ensure that it is not be possible to store the completed ballot on the user's computer. No one should have access to the vote, either on the device or during the transmission to the ballot box
12. The eVoting system shall not permit any manipulative influence to be exercised over the voter during the voting.	Similar to postal voting.
13. The eVoting system shall provide the voter with a means of participating in an election or referendum without the voter exercising a preference for any of the voting options, for example, by casting a blank vote.	Similar to eVoting system currently in use. The voter may be asked to confirm a blank vote.
14. The eVoting system shall indicate clearly to the voter when the vote has been cast successfully and when the whole voting procedure has been completed.	Easily satisfied with the confirmation asked from the voter before the casting of the vote.
15. The eVoting system shall prevent the changing of a vote once that vote has been cast.	Depends on the correctness of the election software.

Secret Suffrage

16. eVoting shall be organized in such a way as to exclude at any stage of the voting procedure and, in particular, at voter authentication, anything that would endanger the secrecy of the vote.	Authentication and voting procedure should be strictly separated. The authentication procedure should finish at the latest before the vote being cast. Homomorphic techniques allow complete anonymity during the storage and counting of votes.
17. The eVoting system shall guarantee that votes in the electronic ballot box and votes being counted are, and will remain, anonymous, and that it is not possible to reconstruct a link between the vote and the voter.	Technical safeguards ensure an electronic separation of the identity of the voter and the content of the vote, at the latest when the vote is introduced into the electronic ballot box
18. The eVoting system shall be so designed that the expected number of votes in any electronic ballot box will not allow the result to be linked to individual voters.	To be defined by technical and procedural safeguards. The use of homomorphic encryption satisfies this requirement.
19. Measures shall be taken to ensure that the information needed during electronic processing cannot be used to breach the secrecy of the vote.	Authentication and voting procedure should be strictly separated. The authentication procedure should finish at the latest before the last confirmation given by the voter.

Procedural Safeguards

Transparency

20. Member states shall take steps to ensure that voters understand and have confidence in the eVoting system in use.	The eVoting system should be clearly explained to the voters.
21. Information on the functioning of an eVoting	Easily enough to achieve by publishing a description of the

system shall be made publicly available.	working of the eVoting system and of the counting process.
22. Voters shall be provided with an opportunity to practice any new method of eVoting before, and separately from, the moment of casting an electronic vote.	Training facilities should be made available both on the Internet and in the municipalities.
23. Any observers, to the extent permitted by law, shall be able to be present to observe and comment on the e-elections, including the establishing of the results.	No specific provisions needed. The College of Experts should be kept in charge of this process. They should also have access to and test sites and information provided for remote eVoting. If it is not possible to allow presence of observers in the computer rooms on basis of security measures, other measures should be taken in order to give the observers the opportunity to monitor the activities.

Verifiability and Auditability

24. The components of the eVoting system shall be disclosed, at least to the competent electoral authorities, as required for verification and certification purposes.	See general requirements.
25. Before any eVoting system is introduced, and at appropriate intervals thereafter, and in particular after any changes are made to the system, an independent body, appointed by the electoral authorities, shall verify that the eVoting system is working correctly and that all the necessary security measures have been taken.	Belgian law stipulates that this should be done by a College of Experts: no specific provisions needed.
26. There shall be the possibility for a recount. Other features of the eVoting system that may influence the correctness of the results shall be verifiable.	The possibilities suggested by the CoE are the following: instruct the eVoting system to recount; transfer the electronic ballot box to a similar but distinct eVoting system and perform the second counting on this system; let the recount be performed by a different system which is interoperable with the eVoting system. In this system, three types of recounts are possible: a. Instruct the eVoting system to recount b. Instruct a new set of talliers to recount c. Automated recount with different software
27. The eVoting system shall not prevent the partial or complete re-run of an election or a referendum.	Identical to traditional system.

Reliability and Security

28. The member state's authorities shall ensure the reliability and security of the eVoting system.	Can be achieved by means of adequate procedures and technical safeguards during pre-voting, voting, and post-voting stages.
29. All possible steps shall be taken to avoid the possibility of fraud or unauthorized intervention affecting the system during the whole voting process.	Can be achieved by means of adequate procedures and technical safeguards during pre-voting, voting, and post-voting stages, as well as through the general requirements.
30. The eVoting system shall contain measures to preserve the availability of its services during the eVoting process. It shall resist, in particular, malfunction, breakdowns or denial of service attacks.	Can be achieved by means of adequate procedures and technical safeguards during pre-voting, voting, and post-voting stages, as well as through the general requirements.
31. Before any e-election or e-referendum takes place, the competent electoral authority shall satisfy itself that the eVoting system is genuine and operates correctly.	Can be achieved by means of adequate procedures and technical safeguards during pre-voting stages, as well as through the general requirements.
32. Only persons appointed by the electoral authority shall have access to the central infrastructure, the servers and the election data. There shall be clear	Can be achieved by means of adequate procedures and technical safeguards during pre-voting, voting, and post-voting stages, as well as through the general requirements.

rules established for such appointments. Critical technical activities shall be carried out by teams of at least two people. The composition of the teams shall be regularly changed. As far as possible, such activities shall be carried out outside election periods.	
33. While an electronic ballot box is open, any authorized intervention affecting the system shall be carried out by teams of at least two people, be the subject of a report; be monitored by representatives of the competent electoral authority and any election observers.	Can be achieved by means of adequate procedures and technical safeguards during voting and post-voting stages, as well as through the general requirements.
34. The eVoting system shall maintain the availability and integrity of the votes. It shall also maintain the confidentiality of the votes and keep them sealed until the counting process. If stored or communicated outside controlled environments, the votes shall be encrypted.	Votes will be stored in encrypted form until the tallying of the votes will be allowed to proceed.
35. Votes and voter information shall remain sealed as long as the data is held in a manner where they can be associated. Authentication information shall be separated from the voter's decision at a pre-defined stage in the e-election or e-referendum.	Authentication and voting procedures should be strictly separated. The authentication procedure should finish at the latest before the last confirmation given by the voter.

8.5.6.2 Operational Standards

Notification

36. Domestic legal provisions governing an e-election or e-referendum shall provide for clear timetables concerning all stages of the election or referendum, both before and after the election or referendum.	Clear procedures should be defined by the law.
37. The period in which an electronic vote can be cast shall not begin before the notification of an election or a referendum. Particularly with regard to remote eVoting, the period shall be defined and made known to the public well in advance of the start of voting.	No specific provisions needed.
38. The voters shall be informed, well in advance of the start of voting, in clear and simple language, of the way in which the eVoting will be organized, and any steps a voter may have to take in order to participate and vote.	Information about the procedure to be followed should be provided to the voter.

Voters

39. There shall be a voters' register which is regularly updated. The voter shall be able to check, as a minimum, the information which is held about him on the register, and request corrections.	Identical to traditional system.
40. The possibility of creating an electronic register and introducing a mechanism allowing online application for voter registration and, if applicable, for application to use eVoting, shall be considered. If participation in eVoting requires a separate application by the voter and/or additional steps, an electronic, and, where possible, interactive procedure shall be considered.	N.A.
41. In cases where there is an overlap between the period for voter registration and the voting period, provision	N.A.

for appropriate voter authentication shall be made.	

Candidates

42. The possibility of introducing online candidate nomination may be considered	N.A.
43. A list of candidates that is generated and made available electronically shall also be publicly available by other means.	N.A.

Voting

44. It is particularly important, where remote eVoting takes place while polling stations are open, that the system shall be so designed that it prevents any voter from voting more than once.	Technical safeguards should ensure that the system will control the eligibility of the voter and that he has not cast a valid vote already. Constant update of the central database is required.
45. Remote eVoting may start and/or end at an earlier time than the opening of any polling station. Remote eVoting shall not continue after the end of the voting period at polling stations.	Can be achieved by means of adequate procedures. In case of impossibility to cast the vote through remote eVoting channel, the voter should be able to cast it in alternative ways.
46. For every eVoting channel, support and guidance arrangements on voting procedures shall be set up for, and be available to, the voter. In the case of remote eVoting, such arrangements shall also be available through a different, widely available communication channel.	Can be achieved by means of adequate procedures during pre-voting stages, by supplying adequate information about the voting process. Voters are already allowed to request the help of a member of the polling office.
47. There shall be equality in the manner of presentation of all voting options on the device used for casting an electronic vote.	Similar to eVoting system currently in use.
48. The electronic ballot by which an electronic vote is cast shall be free from any information about voting options, other than that strictly required for casting the vote. The eVoting system shall avoid the display of other messages that may influence the voters' choice.	Similar to eVoting system currently in use.
49. If it is decided that information about voting options will be accessible from the eVoting site, this information shall be presented with equality.	N.A.
50. Before casting a vote using a remote eVoting system, voters' attention shall be explicitly drawn to the fact that the e-election or e-referendum in which they are submitting their decision by electronic means is a real election or referendum. In case of tests, participants shall have their attention drawn explicitly to the fact that they are not participating in a real election or referendum and shall – when tests are continued at election times – at the same time be invited to cast their ballot by the voting channel(s) available for that purpose.	Confirmation requested from the voter easily achieves this requirement.
51. A remote eVoting system shall not enable the voter to be in possession of a proof of the content of the vote cast.	Technical safeguards should prevent the vote to be printed or stored on the personal computer.
52. In a supervised environment, the information on the vote shall disappear from the visual, audio or tactile display used by the voter to cast the vote as soon as it has been cast. Where a paper proof of the electronic vote is provided to the voter at a polling station, the voter shall not be able to show it to any other person, or take this proof outside of the polling station.	N.A.

Results

53. The eVoting system shall not allow the disclosure of the number of votes cast for any voting option until after the closure of the electronic ballot box. This information shall not be disclosed to the public until after the end of the voting period.	Can be achieved by means of adequate procedures during pre-voting, voting, and post-voting stages, as well as through the general requirements.
54. The eVoting system shall prevent processing information on votes cast within deliberately chosen sub-units that could reveal individual voters' choices.	Can be achieved by means of adequate procedures during post-voting stages, as well as through the general requirements. The centralization of the votes allows mixing all the received votes in one "electronic urn", e.g. with homomorphic encryption.
55. Any decoding required for the counting of the votes shall be carried out as soon as practicable after the closure of the voting period.	Can be achieved by means of adequate procedures during post-voting stages.
56. When counting the votes, representatives of the competent electoral authority shall be able to participate in, and any observers able to observe, the count.	Belgian law stipulates that this should be done by a College of Experts and by party witnesses. Presence of observers may be allowed in the server room (see comment on recommendation n°23)
57. A record of the counting process of the electronic votes shall be kept, including information about the start and end of, and the persons involved in, the count.	Can be achieved by means of adequate procedures during post-voting stages.
58. In the event of any irregularity affecting the integrity of votes, the affected votes shall be recorded as such.	Can be achieved by means of adequate technical features during post-voting stages.

Audit

59. The eVoting system shall be auditable.	See general requirements.
60. The conclusions drawn from the audit process shall be applied in future elections and referendums.	The recommendations by the College of Experts should be implemented in future elections.

9 Kiosk voting based on homomorphic encryption

9.1 Reasons why the consortium did not select this type of voting system

Compared to the remote voting system presented in the previous session, a number of problems disappear. However, many problems remain.

Only a very small number of homomorphic encryption based systems have been fully developed on paper. Almost none have been deployed in practice. Among experts, there appears to be a consensus that these systems still suffer from childhood diseases.

Secondly, it is not certain that the public is ready to accept fully computerized voting systems. Even though mathematical proofs of security exist and can be provided, they cannot be explained in simple terms to laymen. The absence of a paper trail and the need to blindly trust the correctness of program code are often cited as reasons not to adopt systems like this one. Since this system is based on strong cryptography, one could argue that the fears of the public are unfounded. In the future, if the public trust in computerized systems were to increase, then this system could be brought back into consideration.

Still, it might be interesting to deploy this kind of voting system for specific voters such as, for instance, Belgians residing abroad. This would allow effective experimentation provided sufficient safeguards are implemented and might pave the way for greater automation of the voting process.

9.2 Description

Kiosk voting refers to electronic voting systems in which voters must go to a polling station or any official building in order to register their vote on an electronic voting machine connected to a central server situated in a different location. Usually, all the votes are transferred to central servers which do the counting on a centralized basis.

Kiosk voting is not considered to be remote voting by the Recommendations of Council of Europe on eVoting. For the CoE, remote voting is limited to cases where voters cast their vote in an unsupervised environment, that is unsupervised by officials, e.g. at home.[36] This distinction is based on the fact that in a kiosk voting system, the traditional safeguards to guarantee the identity of the voter, the secrecy of the vote, and the free expression of the vote can be maintained. This kind of voting system does not have to face the typical concerns of remote voting, where the vote is cast in an unsupervised environment.

The case analyzed here is based on the scenario described in Section 7 (Thin clients-based eVoting system). However, in this scenario, instead of a local network internal to the polling station, the network is extended to the whole country and links all polling stations to central servers, e.g. in the Ministry of Internal Affairs. This option reduces the possibilities of attacks to the servers, but increases the possibilities of attacks to the network.

Kiosk voting may be implemented by a system similar to that for remote voting based on homomorphic encryption (cf. Section 8). However, there is no need for the voter to

[36] Council of Europe, Recommendation Rec(2004)11, "Explanatory Memorandum", 30 September 2004, p.29

authenticate himself to the voting computer. Instead, the voter authenticates himself to the president of the voting office, and receives from this president a voting token, with which he can activate the voting computer. The client software and configuration files to be used in voting computers are downloaded beforehand, as the voting computer will present the same lists to all voters.

9.3 Compliance of Kiosk Voting with the CoE Recommendations

Since the consortium does not propose to retain kiosk voting for Belgium, only the general requirements of the Council of Europe will be discussed here, excluding the technical requirements.

9.3.1 Legal Standards

9.3.1.1 Principles

Universal Suffrage

	Kiosk voting
1. The voter interface of an eVoting system shall be understandable and easily usable.	Similar to currently used eVoting system.
2. Possible registration requirements for eVoting shall not pose an impediment to the voter participating in eVoting	Similar to currently used eVoting system.
3. eVoting systems shall be designed, as far as it is practicable, to maximize the opportunities that such systems can provide for persons with disabilities.	Similar to currently used eVoting system.
4. Unless channels of remote eVoting are universally accessible, they shall be only an additional and optional means of voting.	N.A.

Equal Suffrage

5. In relation to any election or referendum, a voter shall be prevented from inserting more than one ballot into the electronic ballot box. A voter shall be authorized to vote only if it has been established that his ballot has not yet been inserted in the ballot box.	Similar to currently used eVoting system.
6. The eVoting system shall prevent any voter from casting a vote by more than one voting channel.	Only one channel available.
7. Every vote deposited in an electronic ballot box shall be counted, and each vote cast in the election or referendum shall be counted only once.	To be guaranteed by appropriate procedures and technical safeguards.
8. Where electronic and non-electronic voting channels are used in the same election or referendum, there shall be a secure and reliable method to aggregate all votes and to calculate the correct result.	Identical to voting system in use.

Free Suffrage

9. The organization of eVoting shall secure the free formation and expression of the voter's opinion and, where required, the personal exercise of the right to vote.	Identical to traditional paper ballot voting, guaranteed by the use of a voting booth.
10. The way in which voters are guided through the eVoting process shall be such as to prevent their voting precipitately or without reflection.	The voter has to confirm his vote before it is cast.
11. Voters shall be able to alter their choice at any point in the eVoting process before casting their vote, or to break off the procedure, without their previous choices being recorded or made available to any other person.	Before the voter has confirmed his vote, he can interrupt the process at any moment.
12. The eVoting system shall not permit any manipulative influence to be exercised over the voter during the voting.	Identical to traditional paper ballot voting. Privacy is guaranteed by the voting booth.
13. The eVoting system shall provide the voter with a means of participating in an election or referendum without the voter exercising a preference for any of the voting options, for example, by casting a blank vote.	Similar to currently used eVoting system. The voter may be asked to confirm a blank vote.
14. The eVoting system shall indicate clearly to the voter when the vote has been cast successfully and when the whole voting procedure has been completed.	Easily satisfied with the confirmation asked to the voter before the casting of the vote.
15. The eVoting system shall prevent the changing of a vote once that vote has been cast.	Depends on the correctness of the election software.

Secret Suffrage

16. eVoting shall be organized in such a way as to exclude at any stage of the voting procedure and, in particular, at voter authentication, anything that would endanger the secrecy of the vote.	Authentication and voting procedure should be strictly separated. The authentication procedure should finish at the latest before the vote being cast.
17. The eVoting system shall guarantee that votes in the electronic ballot box and votes being counted are, and will remain, anonymous, and that it is not possible to reconstruct a link between the vote and the voter.	The authentication procedure should finish at the latest before the vote being cast.
18. The eVoting system shall be so designed that the expected number of votes in any electronic ballot box will not allow the result to be linked to individual voters.	To be defined by technical and procedural safeguards.
19. Measures shall be taken to ensure that the information needed during electronic processing cannot be used to breach the secrecy of the vote.	Authentication and voting procedure should be strictly separated. The authentication procedure should finish at the latest before the last confirmation given by the voter.

9.3.1.2 Procedural Safeguards

Transparency

20. Member states shall take steps to ensure that voters understand and have confidence in the eVoting system in use.	Voters understand how the eVoting system works, and the vast majority trusts the system. As conceived in this report, the kiosk voting option would only be implemented in a second phase, e.g., after Belgian voters get used and trust the previous eVoting system. The introduction of kiosk voting would thus be the result of an "adoption" process by Belgian citizens.

21. Information on the functioning of an eVoting system shall be made publicly available.	Easily enough to achieve by publishing a description of the working of the eVoting system and of the counting process.
22. Voters shall be provided with an opportunity to practice any new method of eVoting before, and separately from, the moment of casting an electronic vote.	Visual demonstration of the how the system works as the one published for the last elections could achieve this goal.
23. Any observers, to the extent permitted by law, shall be able to be present to observe and comment on the e-elections, including the establishing of the results.	No specific provisions needed. The College of Experts should be kept in charge of this process.

Verifiability and Auditability

24. The components of the eVoting system shall be disclosed, at least to the competent electoral authorities, as required for verification and certification purposes.	See general requirements.
25. Before any eVoting system is introduced, and at appropriate intervals thereafter, and in particular after any changes are made to the system, an independent body, appointed by the electoral authorities, shall verify that the eVoting system is working correctly and that all the necessary security measures have been taken.	Belgian law stipulates that this should be done by a College of Experts: no specific provisions needed.
26. There shall be the possibility for a recount. Other features of the eVoting system that may influence the correctness of the results shall be verifiable.	The possibilities suggested by the CoE are the following: instruct the eVoting system to recount; transfer the electronic ballot box to a similar but distinct eVoting system and perform the second counting on this system; let the recount be performed by a different system which is interoperable with the eVoting system. In this system, two types of recounts are possible: a. Instruct the eVoting system to recount b. automated recount with different software
27. The eVoting system shall not prevent the partial or complete re-run of an election or a referendum.	Identical to traditional system. Voters are attributed to a specific constituency with a specific list of candidates. In case part of the election would need to be re-run, it should be based on the different lists of candidates.

Reliability and Security

28. The member state's authorities shall ensure the reliability and security of the eVoting system.	Can be achieved by means of adequate procedures and technical safeguards during pre-voting, voting, and post-voting stages.
29. All possible steps shall be taken to avoid the possibility of fraud or unauthorized intervention affecting the system during the whole voting process.	Can be achieved by means of adequate procedures and technical safeguards during pre-voting, voting, and post-voting stages, as well as through the general requirements.
30. The eVoting system shall contain measures to preserve the availability of its services during the eVoting process. It shall resist, in particular, malfunction, breakdowns or denial of service attacks.	Can be achieved by means of adequate procedures and technical safeguards during pre-voting, voting, and post-voting stages, as well as through the general requirements.
31. Before any e-election or e-referendum takes place, the competent electoral authority shall satisfy itself that the eVoting system is genuine and operates correctly.	Can be achieved by means of adequate procedures during pre-voting stages, as well as through the general requirements.
32. Only persons appointed by the electoral authority shall have access to the central infrastructure, the servers and the election data. There shall be clear rules established for such appointments. Critical technical activities shall be carried out by teams of at least two people. The composition of the teams shall	Can be achieved by means of adequate procedures during pre-voting, voting, and post-voting stages, as well as through the general requirements.

be regularly changed. As far as possible, such activities shall be carried out outside election periods.	
33. While an electronic ballot box is open, any authorized intervention affecting the system shall be carried out by teams of at least two people, be the subject of a report; be monitored by representatives of the competent electoral authority and any election observers.	Can be achieved by means of adequate procedures during voting and post-voting stages, as well as through the general requirements.
34. The eVoting system shall maintain the availability and integrity of the votes. It shall also maintain the confidentiality of the votes and keep them sealed until the counting process. If stored or communicated outside controlled environments, the votes shall be encrypted.	Votes will be stored encrypted until the tallying of the votes.
35. Votes and voter information shall remain sealed as long as the data is held in a manner where they can be associated. Authentication information shall be separated from the voter's decision at a pre-defined stage in the e-election or e-referendum.	Authentication and voting procedure should be strictly separated. The authentication procedure should finish at the latest before the last confirmation given by the voter.

9.3.2 Operational Standards

9.3.2.1 Notification

36. Domestic legal provisions governing an e-election or e-referendum shall provide for clear timetables concerning all stages of the election or referendum, both before and after the election or referendum.	Clear procedures should be defined by the law.
37. The period in which an electronic vote can be cast shall not begin before the notification of an election or a referendum. Particularly with regard to remote eVoting, the period shall be defined and made known to the public well in advance of the start of voting.	No specific provisions needed.
38. The voters shall be informed, well in advance of the start of voting, in clear and simple language, of the way in which the eVoting will be organized, and any steps a voter may have to take in order to participate and vote.	Information about the procedure to be followed should be provided to the voter.

9.3.2.2 Voters

39. There shall be a voters' register which is regularly updated. The voter shall be able to check, as a minimum, the information which is held about him on the register, and request corrections.	Similar to traditional voting system.
40. The possibility of creating an electronic register and introducing a mechanism allowing online application for voter registration and, if applicable, for application to use eVoting, shall be considered. If participation in eVoting requires a separate application by the voter and/or additional steps, an electronic, and, where possible, interactive procedure shall be considered.	N.A.
41. In cases where there is an overlap between the period for voter registration and the voting period, provision for appropriate voter authentication shall be made.	N.A.

9.3.2.3 Candidates

42. The possibility of introducing online candidate nomination may be considered	N.A.
43. A list of candidates that is generated and made available electronically shall also be publicly available by other means.	N.A.

9.3.2.4 Voting

44. It is particularly important, where remote eVoting takes place while polling stations are open, that the system shall be so designed that it prevents any voter from voting more than once.	N.A.
45. Remote eVoting may start and/or end at an earlier time than the opening of any polling station. Remote eVoting shall not continue after the end of the voting period at polling stations.	N.A.
46. For every eVoting channel, support and guidance arrangements on voting procedures shall be set up for, and be available to, the voter. In the case of remote eVoting, such arrangements shall also be available through a different, widely available communication channel.	Can be achieved by means of adequate procedures during pre-voting stages, by supplying adequate information about the voting process. Voters are already allowed to request the help of a member of the polling office.
47. There shall be equality in the manner of presentation of all voting options on the device used for casting an electronic vote.	Similar to currently used eVoting system.
48. The electronic ballot by which an electronic vote is cast shall be free from any information about voting options, other than that strictly required for casting the vote. The eVoting system shall avoid the display of other messages that may influence the voters' choice.	Similar to currently used eVoting system.
49. If it is decided that information about voting options will be accessible from the eVoting site, this information shall be presented with equality.	N.A.
50. Before casting a vote using a remote eVoting system, voters' attention shall be explicitly drawn to the fact that the e-election or e-referendum in which they are submitting their decision by electronic means is a real election or referendum. In case of tests, participants shall have their attention drawn explicitly to the fact that they are not participating in a real election or referendum and shall – when tests are continued at election times – at the same time be invited to cast their ballot by the voting channel(s) available for that purpose.	N.A.
51. A remote eVoting system shall not enable the voter to be in possession of a proof of the content of the vote cast.	N.A.
52. In a supervised environment, the information on the vote shall disappear from the visual, audio or tactile display used by the voter to cast the vote as soon as it has been cast. Where a paper proof of the electronic vote is provided to the voter at a polling station, the voter shall not be able to show it to any other person, or take this proof outside of the polling station.	Similar to currently used eVoting system. No paper proof is provided to the voter.

9.3.2.5 Results

53. The eVoting system shall not allow the disclosure of the number of votes cast for any voting option until after the closure of the electronic ballot box. This information shall not be disclosed to the public until after the end of the voting period.	Can be achieved by means of adequate procedures during pre-voting, voting, and post-voting stages, as well as through the general requirements.
54. The eVoting system shall prevent processing information on votes cast within deliberately chosen sub-units that could reveal individual voters' choices.	Can be achieved by means of adequate procedures during post-voting stages, as well as through the general requirements. The centralization of the votes permits to mix all the received votes in one "electronic urn", e.g. with homomorphic encryption.
55. Any decoding required for the counting of the votes shall be carried out as soon as practicable after the closure of the voting period.	Can be achieved by means of adequate procedures during post-voting stages.
56. When counting the votes, representatives of the competent electoral authority shall be able to participate in, and any observers able to observe, the count.	Belgian law stipulates that this should be done by a College of Experts and by party witnesses: no specific provisions needed.
57. A record of the counting process of the electronic votes shall be kept, including information about the start and end of, and the persons involved in, the count.	Can be achieved by means of adequate procedures during post-voting stages.
58. In the event of any irregularity affecting the integrity of votes, the affected votes shall be recorded as such.	Can be achieved by means of adequate technical features during post-voting stages.

9.3.2.6 Audit

59. The eVoting system shall be auditable.	See general requirements.
60. The conclusions drawn from the audit process shall be applied in future elections and referendums.	The recommendations by the College of Experts should be implemented in future elections.

10 Observations of Legal Nature

10.1 Introduction

In 2004, the Council of Europe issued a recommendation on eVoting systems. This text is not binding but "consists of minimum standards which, if followed in an eVoting system, would facilitate compliance with the principles of democratic elections".[37] This part of the report will refer not only to legal standards, but also to operational (relating to the manner in which eVoting hardware and software should be operated and maintained) and technical standards (relating to the construction and operation of eVoting hardware and software) where their compliance could have an influence on the compliance with democratic elections principles.

It is worth noting that, in the opinion of the Council of Europe, despite the fact that "eVoting systems must be designed and operated so as to ensure the reliability and security of the voting process, as is the case with the non-electronic voting systems", "it may be necessary to give more attention to the application of one principle than to that of another. In fact, all the principles are not implemented in the same way in non eVoting systems as, for example, postal voting does not guarantee the freedom of the vote in the same way as traditional voting does. In some circumstances, it could be necessary to balance competing requirements. Taken into account that any electronic voting procedure should afford the same guarantees as paper-based voting systems, their specificities could however require some adaptation of the traditional rules. For instance, the traditional presence of eye witnesses during the tallying of the vote which ensures the respect of the procedures decided by the Law, e.g. that invalid ballots are discarded, should be adapted to electronic environment.

Finally, other laws might need to be taken into account, such as data protection laws and laws on privacy. It is the case for instance, when an electronic voters' register has to be created for the need of electronic authentication. This register should comply with data protection and privacy principles.

10.2 Recommendations of the Council of Europe on eVoting Systems and its Current Implementation in the Belgian System

This section focuses on the way the eVoting system currently in use in Belgium actually complies with the Council of Europe (hereafter, "CoE") Recommendations. This first analysis will provide an overview of the content of the main principles which should govern the design and implementation of any eVoting system and to compare it with the current situation in Belgium.

The five principles of democratic elections (Universal, equal, free, secret and direct suffrage) as they are implemented in traditional voting systems must be applied. Our analysis will mainly focus on the legal requirements, since organizational and technical requirements have been analyzed in other parts of this report. An additional section will focus on procedural safeguards.

---

[37] Council of Europe, Recommendation Rec(2004)11, "Explanatory Memorandum", 30 September 2004, p.26

Legal standards relate to the legal context in which eVoting is deemed legitimate. They intend to ensure the existence of sufficient safeguards to guarantee the five principles identified by the Code of Good Practice in Electoral matters[38] as fundamental in democratic elections: universal, equal, free, secret and direct suffrage.[39] Direct suffrage[40] does not call for specific attention in the context of eVoting and will not be discussed in the present report. This principle is not considered by the CoE Recommendations either.

10.2.1 Universal Suffrage

Universal suffrage means that all human beings have the right to vote and to stand for elections subject to certain conditions.[41] This principle is guaranteed by a strict definition of the restrictions on the right to vote by Electoral law[42] and an open and easy registration procedure. Furthermore, the friendliness of the paper ballot system and its extremely easy use ensures that all voters are able to cast their votes to the best of their knowledge. The introduction of electronic voting could furthermore imply alternative registration procedures and the use of technical means to cast one's vote.

It follows that the introduction of an eVoting system may raise the complexity of the voting process itself. Additional education and training of voters may be required for them to fully understand how to operate the eVoting system.

As a consequence, to be compliant with the principle of universal suffrage, any eVoting system should take into account the following elements:

- the possible registration requirement for eVoting shall not pose an impediment to the voter participating in eVoting;
- the voter interface shall be understandable and easily usable;
- eVoting systems should be designed to maximize the opportunities that such systems can provide for persons with disabilities.

10.2.1.1 Voters' Registration

Belgium's current eVoting system relies on the same voter's register as the one used for paper-based elections. Every municipality puts together a voters' list containing the first name and surname, date of birth, gender, place of main residence and the national register number (Article 10 Election Law). In Belgium, electoral lists are formed on the basis of the municipal population register. As the registration on the municipal population lists is compulsory, the inscription of voters in the register is automatic.

All citizens may, until the twelfth day before the elections, check, at their municipality, whether they are mentioned on the voters' list and whether the

---

[38] Council of Europe, Venice Commission, Code of Good practice in electoral matters (Opinion 190/2002_el) endorsed by Parliamentary Assembly Resolution 1320 (2003).

[39] Council of Europe, Recommendation Rec(2004)11, "Explanatory Memorandum", 30 September 2004, p.25

[40] Direct suffrage means that the ballots cast by the voters directly determine the person(s) elected. See Council of Europe, Recommendation Rec(2004)11, "Explanatory Memorandum", 30 September 2004, p.25

[41] Council of Europe, Recommendation Rec(2004)11, "Explanatory Memorandum", 30 September 2004, p.25

[42] See for Belgium, articles 1, 7 and 7bis of the Electoral Code.

references are correct.

On the day of the election, the list of eligible voters is posted at the polling station (Art. 113 Election Law). Moreover, to be able to vote, voters should present their election card which mentions the date of the election, the polling place and the hours of opening and closing of the polling station. The election card also mentions the first name and the surname, the gender and the main residence of the voter, and if this is the case, also the name of his wife on the voter's list (Article 107 Election Law). No specific registration requirements are necessary for voters who use the eVoting system.

The system currently in use in Belgium thus guarantees a perfect equality between voters who use the paper-based system and voters who use electronic voting machines. It allows the voter to check if the information kept about him/ her is accurate and may request corrections if necessary.

10.2.1.2 Access to Voting Systems

Every eligible voter shall have access to at least one voting channel. This means that when voting machines are used, a contingency procedure shall be drawn to ensure voters will be able to exercise their right to vote in any case, even if the eVoting system becomes inoperative.

The procedure to be followed in case a voting machine fails is currently defined in the polling station President's instructions[43]. The President is required to call the technical assistance, depending on the provider of the machine. If the President's machine fails, the election is suspended until the machine is fixed or replaced. A delegate from the Minister of Internal Affair is in charge of supervising the technical assistance received by the polling station.

10.2.1.3 Friendliness and Usability of the System

The Council of Europe recommends that user interface design (for all interfaces, included vote-casting, registration and administration) shall follow best practice to maximize usability (Recommendations 1b, 61a, 65).[44] This has the following consequences:

- Interfaces shall be understandable and it shall be made clear to voters whether their vote has been recorded correctly (Recommendations 1a, 14, 50). The confirmation asked before the vote is definitively cast and the possibility given to the voter to change his vote before this moment guarantee that voters are aware of the moment when their vote is recorded. Regarding the display of information on voter's options, it is worth noting that the Council of State[45] had acknowledged that the display of the same list of candidates on three different screens may create confusion in the voters. This decision resulted in a modification of the Law concerning the Organization of Computerized

---

[43] Circulaire générale du 4 avril 2007 relative aux élections, adressée aux présidents des bureaux principaux, aux gouverneurs de province et aux administrations communales, pp.12-13

[44] McGaley M., Gibson J.P., A critical analysis of the Council of Europe Recommendations on e-voting, available on-line at: http://www.usenix.org/events/evt06/tech/full_papers/mcgaley/mcgaley_html/, last accessed on 31 August 2007

[45] Council of State, n°93.710, 2 March 2001

Voting (hereafter, "LOCV") in 2003[46] and now, not only the initials of the party should be indicated on the screen, but also the logos, more easily recognizable and identifiable by the voters.

- Voters shall be consulted during the design and testing of vote casting and registration interfaces (Recommendation 62)

- The needs of voters with disabilities shall be taken into account in the design of the interface. Appropriate advocacy groups shall be consulted, and compatibility with relevant products and compliance with relevant standards maximized, to that end (Recommendations 3, 63, 64). Article 9 of the LOCV states that the voter who would experience difficulties when casting his vote may ask for help from the President of the polling station or from another designated member. This exceptional procedure is only allowed for people with physical disabilities which prevent them from entering the voting booth alone. In case of doubt about the veracity of the disability, the President may deny such right to the voter. Polling booths specially designed for people with disabilities are available in at least one out of five polling stations. The buildings where such polling booths are installed should be easily accessible and parking places should be made available.

Furthermore, voters shall be educated in the use of the vote-casting interface and in any steps required in order to participate. This means that:

- Voters shall be given the opportunity to practice using the interface. (Recommendation 22). The new internet-based demonstration published on-line for the past elections[47] gives voters the opportunity to discover how the system works before Election Day.

- Support and guidance shall be available to voters through widely available communication channels (Recommendation 46). In addition to the on-line demonstration, a manual is put at the voter's disposal inside the voting booth.

The survey carried out by the Université Libre de Bruxelles in May 2003[48] has shown that Belgian voters, as a majority, find the current eVoting system user-friendly.

10.2.2 Equal Suffrage

Equal suffrage means that each voter has the same number of votes.[49] Each voter is treated in the same way, no differences are allowed. This principle implies that each

---

[46] Act of 19 February 2003, [*modifiant les lois électorales en ce qui concerne l'indication des partis politiques au-dessus des listes de candidats sur les bulletins de vote pour les élections des Chambres législatives fédérales, du Conseil régional wallon, du Conseil flamand, du Conseil de la Région de Bruxelles-Capitale et du Conseil de la Communauté germanophone*], *M.B. n°97, 21 March 2003.*

[47] See for instance for the municipal elections of October 2006: http://www.bruxelleselections2006.irisnet.be/fr/Content/6/app.rvb, last accessed on 31st August 2007.

[48] See Report "Bevoting. Study of Electronic voting systems. Part I" issued by this Consortium, 15th April 2007, pp. 55-58.

[49] Council of Europe, Recommendation Rec(2004)11, "Explanatory Memorandum", 30 September 2004, p.25

voter is granted with a single vote. Adequate safeguards should thus be implemented to ensure that no voter is able to cast more than one vote (multiple voting) or that one vote is counted more than once. This also implies that when different voting channels are available, all voters should be treated equally and be given the same opportunities.

Equal suffrage is ensured, from a procedural point of view, (1) by a strict identification procedure: the identity of the voter and his right to vote is checked before the casting of the vote, as well as the fact that he/she has not already cast a vote and (2) by the counting procedure, with possibility of recounting if the result is contested.

Three elements should thus be taken into account when implementing an eVoting system in order to fully comply with this principle:

- The identification procedure should prevent multiple voting. This will be particularly relevant in cases of kiosk or Internet voting.
- The system should guarantee that all votes should be counted once and only once.
- Technical safeguards should allow an accurate tallying of the votes.

When different voting channels co-exist, all voters should be treated equally.

10.2.2.1 Identification Procedure

Article 61 of the Belgian Constitution states that every voter is allowed to cast one vote.
This implies that each voter shall only be permitted to insert a single ballot into the ballot box. A voter shall be allowed to vote if it has been established that he has not yet inserted a ballot in the ballot box.

This requirement is complied with thanks to a strict identification procedure. The system of authentication is based on the voter's list issued by the municipality and on the election card where it is indicated that the individual is an eligible voter. Once the vote has been cast, a stamp is put on the election card certifying that voter has cast his vote and preventing him from casting a new vote. [50]

10.2.2.2 All Votes Should be Counted Exactly Once

Equal suffrage also implies that every vote deposited in the urn shall be counted and counted only once. The eVoting system should thus accurately record votes, i.e. ensure that the voter is presented with authentic ballot whose content is actually recorded by the electronic voting machine. The eVoting system must prevent that a ballot is changed or deleted after it was cast by the voter. The result of the elections should be based on the votes that were correctly cast.
In order to guarantee that counting the votes happens correctly, the voting computers, their software and configuration files, and the computers and software that are used to read and count the ballots must be certified by the ministry of internal affairs. This should ensure the reliability and trustworthiness of the system, as wel as the secrecy of the vote (Art. 2§2 LOCV). The system has to be in conformity with the

[50] Instructions du 21 mars 2007 adressées aux présidents des bureaux de vote utilisant le vote automatisé., p.18, http://www.ibz.rrn.fgov.be/fileadmin/user_upload/Elections/fr/forms/tech/instructions_vote_automatise_2007.pdf

requirements determined by Royal Decree.

10.2.2.3 Co-existence of Different Voting Channels

Where electronic and non-electronic voting channels are used in the same election, there shall be a secure and reliable method to aggregate all votes and to calculate the correct result.

Article 180 septies of Electoral Law regulates the procedure to be followed when the postal vote of Belgian citizens living abroad is received in an automated polling station. These ballots should normally be distributed between the counting centers of the canton. In case all polling station of the canton are automated, the ballots are distributed in the counting centers of another canton of the constituency or of the province. If the province is entirely automated, the ballots should be sent to provinces where the vote is not automated. In other cases, the counting should be done manually according to the rules contained in the Electoral Law.

10.2.3 Free Suffrage

Free suffrage means that the voter has the right to form and to express his opinion in a free manner, without any coercion or undue influence.[51]

The traditional safeguards have consisted in isolating the voter when casting his vote and in such way preserve the secrecy of the vote. When the voter finds himself in the voting booth, he is able to make his choice in total freedom. This principle is not absolute; however, voters may also choose to cast their vote either by proxy or through postal voting. In proxy voting, the voter gives a mandate to a trustworthy person to cast his vote. In postal voting, the voter has to cast his vote either at home or at the post office, thus not in an isolated place like a voting booth.

The current electronic voting system used in Belgium relies on a supervised environment (with presence of officials) and on voting booths, i.e. on traditional safeguards, even if proxy voting is admitted. Only one case is admitted for postal voting, for the vote of Belgian citizens living abroad.

10.2.3.1 Free Formation of the Voter's Opinion

The free formation and expression of the voter's opinion is an inner process which is currently guaranteed by the use of a polling booth in order to make sure that no external factors influence the casting of the vote. The most notable threat consists in the so-called "family voting" where one member of the family has gained enough influence to direct the vote of other members of the family.

Another aspect to be taken into account in electronic voting is the possibility to include the display of sounds, images or any other disturbance when the vote is cast. These disturbances are formally forbidden by the Council of Europe. In the current system, the vote-casting interface is free from any information out of the party lists and candidates and as such guarantees the free formation of the voter's opinion.

Finally, the eVoting system shall not allow the disclosure of the number of votes cast for any voting option until after the closure of the electronic ballot box. This

---

[51] Council of Europe, Recommendation Rec(2004)11, "Explanatory Memorandum", 30 September 2004, p.25

information shall not be disclosed to the public until after the end of the voting period. In the current system two guarantees prevent such situation: first of all, the voting machines do not record any vote and thus could not indicate to the voters the number of votes cast earlier. Secondly, the results contained in an e-urn are only made available at the level of the Cantons (art. 151 Electoral Law) in order to prevent a possible identification of the votes cast and the voters.

10.2.3.2 Free Expression of the Voter's Opinion

The eVoting system in use should prevent voters to vote precipitately or without reflection (without enough time to think about it). Voters should be able to alter their choice at any point in the eVoting procedure before the casting of the vote, or to break off the procedure without their previous choice being recorded or made available to any other person. The design of the current voting system where a confirmation is asked to the voter before recording his vote on the magnetic card guarantees the free expression of the voter's opinion (Article 7§4 LOCV). The eVoting system currently in use also permits voters to change their vote before giving the confirmation.

The use of magnetic cards where the vote is recorded (and not on the machine) guarantees that only the voter could have access to the vote. Furthermore, the record of the vote on the magnetic card and its introduction into the e-ballot box guarantee that the vote cast is not changed once it has been cast.

Finally, the possibility of casting a blank vote exists, because it is impossible to cast an invalid vote with an electronic voting system. Note that the Council of Europe recommends to provide a voter with the option to cast an invalid vote or not.[52]

10.2.4 Secret Suffrage

Secret suffrage means that the voter has the right to vote secretly as an individual, and that the state has the duty to protect that right. [53] This is a key point in any eVoting process. Secrecy must apply to the entire procedure:

- At the *pre-voting stage*, where the voter identification procedure should be independent from the rest of the procedure. The traditional identification procedure aims at verifying that the voter is entitled to vote and controls that each voter votes only once. This identification is totally separated from the voting process in itself. Electronic authentication procedures should contain required safeguards to offer the same level of guarantees.

- During the *completion of the ballot*, no marks may be made to the ballot paper which would make it possible to identify the voter. This action is sanctioned by the nullity of the vote during the counting. Despite the fact that electronic voting systems do not allow casting invalid votes, the president is currently required to check whether the card with the magnetic stripe is free from these marks. In any case, the system should guarantee that the voter cannot be linked to the vote cast.

---

[52] Council of Europe, Recommendation Rec(2004)11, "Explanatory Memorandum", 30 September 2004

[53] Council of Europe, Recommendation Rec(2004)11, "Explanatory Memorandum", 30 September 2004, p.25

- Finally, secrecy is required during the *casting and transmission of the ballot* and during the counting and any recounting of the votes. Votes and voter should be totally dissociated during the casting of the vote and once the vote has been cast. The traditional paper-based ballot guarantees by its nature the total anonymity of the vote cast. In eVoting system, technical safeguards should ensure the strict separation between the identification procedure and the storage of the votes cast in such way that they are totally separated.

10.2.4.1 Pre-voting Stage

At the pre-voting stage, the identification procedure currently relies on the control of the identity card of the voter and of his electoral card where its authorization to vote stands. Once this process is complete, the voter is allowed to enter the voting booth to cast his vote. Both identification and voting procedure are physically separated.

The current electronic voting system relies on the traditional procedure. The physical separation thus remains. Where electronic authentication is used, e.g. using eID cards, technical safeguards should be implemented to ensure the separation of both procedures.

10.2.4.2 During the Casting of the Vote

The safeguards implemented in Belgium to guarantee the secrecy of the vote rely on the traditional safeguards used in paper-based voting systems: the identification of the voters is made on a face-to-face basis and the casting of the vote is entirely realized within a polling booth, maintaining the physical separation which can be easily controlled by election officials.

On the other part, the design of the system guarantees, once the vote is cast, a full anonymity of the voter: the content of the vote is recorded on a magnetic stripe on a card which cannot be linked to the voters in any way, the vote is not stored in the voting machine (but even if it were, as the identification process is not automated and totally separated from the casting of the vote, it would be quite difficult to link the voters with the votes) and, finally, all magnetic cards are deposited and mixed into the e-ballot box.

The voter should not be allowed to print the content of his vote or to go outside the polling station with any paper related to his vote.

10.2.4.3 Post-voting stage: Counting and Auditing

In the post-voting stage, before the tallying of the votes, the votes should be stored in such way to guarantee the anonymity and guarantee the secrecy of the vote (Recommendation n°17). In the paper-based system, votes are stored in sealed urns, which guarantee secrecy.

When an electronic voting system is used, the storage of electronic ballots outside a controlled environment should be encrypted in order to guarantee that they cannot be read by unauthorized persons.

As mentioned above, it is impossible to link the identity of a voter to the voter's ballot: the voter's identification follows a face-to-face identification process, and the voting computer only starts the voting process after having detected a magnetic stripe card. This card can be used only once, and is completely anonymous. Once the voter

introduces his magnetic stripe ballot in the voting urn, the vote becomes totally anonymous (except for fingerprints) without any danger of breaking this anonymity during the tallying of the vote or the auditing process.

10.2.5 Procedural Safeguards

The procedural safeguards ensure that all principles of democratic elections are implemented and maintained in an eVoting context. They condition the trust of voters into the system and thus the legitimacy of the elections.

Three main principles ensure the voting procedure to be in conformity with democratic elections principles:

- The procedure should be transparent, i.e. the procedure should be known and understood by the citizens (Recommendations 20, 21). This is currently ensured a.o. by the presence of representatives of political parties and other witnesses during the tallying of the votes.
- The procedure should be reliable and secure (Recommendation 28), i.e. that procedural safeguards should guarantee that the election process is executed according to the principles in place.
- The procedure should be verifiable and accountable. In case the results are contested, the reliability of the counting process should be able to be controlled (accountability) and, if an irregularity is detected, a recount should be possible. In traditional systems, paper ballots can be easily recounted if required.

Electronic voting systems raise a number of issues regarding procedural safeguards. These issues should be addressed in order to guarantee the same level of transparency, reliability, security, verifiability and accountability as in paper-based voting systems. This implies that procedures need to be adapted to the specificities of the new systems in order to generate trust.

10.2.5.1 Transparency

Transparency means that the voting system should be known and understood by the citizens (Recommendation n°20). It allows voters to have confidence in the eVoting system. This usually constitutes a weakness of electronic voting systems since, contrarily to paper-based voting systems, electronic voting systems do not allow citizens to "eye-control" the correct execution of the whole voting process. Alternative control mechanisms should be put in place for the control of the process, normally through the implication of experts with sufficient knowledge to estimate the reliability of the system and its good functioning.

Confidence of the Voters

To increase the understanding of the eVoting system, a virtual demonstration of the procedure to be followed for the casting of the vote has been put on-line. [29] This enables users sufficiently familiarized with new technologies to practice before the election day. However it should be noted that an important part of the population with no access to Internet will not be able to practice. Several municipalities have provided alternative training centers for their citizens.

Full understanding of the system in use is actually required to base voters' confidence. As shown by the previous report issued by this Consortium, the understandability of

the system is achieved, but some organizations have expressed distrust in the system. They claim that one cannot be sure that one's vote will be taken into account by the machine during the tallying of the votes, nor that the votes taken into account are the ones that have been cast by the voters. These organizations basically do not trust the eVoting system and ask for additional guarantees to allow them to see and check that their vote is taken into account. The current eVoting system thus lacks one basic element: the trust of the citizens in the system. However, this argument may be nuanced on the basis of the study of the *Centre d'étude de la vie politique* of the *Université Libre de Bruxelles* conducted through 'exit polls' on May, 18 2003, 88,88% of the voters surveyed actually claim to trust the eVoting system. The lack of confidence seemed to be proper to a group with higher levels of education and older than average. The report concluded that 'computerized voting gave little rise to negative reactions in the areas of user friendliness, societal acceptance and confidence'.[54] Complementary scientific studies may be required to measure the level of confidence in the eVoting system in place.

The solution suggested by these organizations is to include paper trail to the eVoting system, in order to allow a manual recount of the votes and thus increase the trust level to that of the traditional paper ballot voting systems.

It is worth noting that the Council of Europe recommends eVoting systems to be implemented step by step to get citizens used to the system, to the changes it implies and to generate trust.[55]

Control over the Software

In order to increase the transparency of the eVoting system, it is recommended to publish the source code of the software used during the election.[56] This is currently the case in Belgium. However, this disclosure is limited as it takes place only after the election and after the College of Experts had been given the opportunity to certify that the source code published truly corresponds to the software used during the elections.[57]

In that sense, The Council of Europe recommends that observers should have to be provided with an opportunity to have access to relevant software information, to verify electronic safety measures for servers, to inspect and test devices, to have access to test sites and information provided for remote eVoting, to observe cast electronic votes entering the electronic ballot box and verifying that these votes are being correctly counted.

When counting the votes, representatives of the competent electoral authority shall be able to participate to the count and any observers shall be able to observe the counting process.

This control over the elections is currently made in Belgium by the College of Experts

---

[54] See, 1st report delivered by the Consortium, 15.04.2007, pp.66-68.

[55] Council of Europe, Recommendation Rec(2004)11, "Explanatory Memorandum", 30 September 2004, p.35

[56] Council of Europe, Recommendation Rec(2004)11, "Explanatory Memorandum", 30 September 2004, pt.62

[57] See http://www.ecolo.be/index.php?class=home&page=interventions/docs/interparl&fiche=3134&numand=2161)

since 1998. This College is composed of experts designated by the Chamber of representatives, the Senate and the regional legislative bodies. In addition, each political formation that is represented in either Chambers of Parliament by at least two representatives may designate an IT-specialist. These persons control the reliability of electronic voting machines' software, the exact recording of cast votes on the magnetic card and in the polling station's urn, the exact recording of the memory of the computer of the president of the voting office on the storage medium used for the total count of the ballots, the optical reading of issued ballots and controlling electronic voting by printing out the ballots.

Organizational Safeguards

Finally, it is recommended that domestic legal provisions governing an e-election provide clear timetables concerning all stages of the election, both before and after (Recommendation n°36). The period in which an eVote can be cast shall not begin before the notification of an election and the voters shall be informed, well in advance of the start of voting, in clear and simple language, of the way in which the eVoting will be organized, and any steps a voter may have to take in order to participate and vote.

A record of the counting process of the electronic votes shall be kept, including information about the start and end of, and the persons involved in the count

All these requirements are currently met by the Belgian eVoting system. The LOCV defines each step of the procedure which should be followed in great detail. In fact, the Council of State needs to know about infringements of this procedure and its effects on the validity of the electoral process.

10.2.6 Verifiability and Accountability

The Council of Europe specifies that the verifiability of an electronic voting system can be guaranteed by reinstructing the eVoting system to perform a second count; to transfer the electronic ballot box to a similar but distinct eVoting system and perform the recount; to let the recount be carried out by a different system which is interoperable with the eVoting system; to produce, at some stage of the voting process, paper trails of the cast votes and to use these for recounting. It may however not be sufficient to only perform a recount. Other elements may be required to be checked, such as the confirmation that all votes cast have been taken into consideration.

This is actually guaranteed by the use of magnetic cards and thus the possibility to recount these cards if any failure in the system were discovered. Furthermore, since 2003, the voters have been given the possibility to check that the content of the vote recorded on the magnetic card correspond to what he wanted to cast. The voter has thus the possibility to audit the content of the card by himself.

The accountability of the system implies that the components of the eVoting system should be disclosed, at least to the competent electoral authorities, as required for verification and certification purposes and that before any eVoting system is introduced and at appropriate intervals after, an independent body shall verify that the eVoting system is working correctly and that all the necessary security measures have been taken (Recommendations n°24 and 25).

To achieve a complete audit of the system, the Council of Europe recommends that provision shall be made for the observation of all stages of elections to the extent permitted by the law. There shall be a comprehensive audit system designed into the eVoting system to provide information about the functioning of the system at all levels (Recommendations 59, 100, 101, 102, 103, 104, 107, 108). Audit information recorded shall, at a minimum, include: [26]

- the number of votes cast;
- count information (including personnel involved, and enough information to reproduce the count results);
- any suspicious activities which may indicate some kind of attack on the system (including votes affected, if applicable);
- system failures and malfunctions;
- logs of authorized access to the system (including user identity and activities undertaken) (Recommendations 57, 58).

Finally, observers shall be trained about the expected behavior of the system and its operation in order to enable them to make informed judgments about the reliability of election results.

As mentioned above, this audit is currently conducted by the College of experts. Article 5 bis of the LOVC grant them with auditing functions in all stage of the procedure, from day 40 before the election day to 15 days after such day, when they have to deposit their report on the conformity of the elections to the procedures. They thus verify, before any e-election takes place, that the eVoting system is genuine and operates correctly.

10.2.7 Reliability and Security

The reliability and security of the eVoting machines to be used in an eVoting process is crucial to the legitimacy of the elections. The reliability and the security of the machines currently used in Belgium will not be assessed here, as it is not the goal of the legal part. The main recommendations of the Council of Europe to this effect will however be mentioned.

The Council of Europe recommends that all possible steps shall be taken to avoid the possibility of fraud or unauthorized intervention affecting the system during the whole voting process (Recommendation n°29). In that sense, only persons appointed by the electoral authority shall have access to the central infrastructure, the servers and the election data. Clear rules should govern such appointments. Critical technical activities should be carried out by teams of at least two people. The composition of the teams shall be regularly changed. As far as possible, such activities shall be carried out outside election periods (Recommendation n°32).

While an electronic ballot box is open, any authorized intervention affecting the system shall be carried out by teams of at least two people, be the subject to a report, be monitored by representatives of the competent electoral authority and any election observers (Recommendation n°33).

In order to support these requirements, Software engineering best practice shall be followed, including: [26]

- A comprehensive risk assessment shall underpin the decision to introduce eVoting in general and any system in particular. This assessment shall be carried out by individuals with a suitable level of expertise.
- Change management system shall be open and transparent. In particular:
    - All components of the system shall be subject to version control (Recommendation n° 69b).
    - It shall be possible to accurately and reliably determine whether a given component is the version tested and approved for use.
    - Any updates of software, including third-party software such as operating systems, shall be justified before installation.
    - There shall be a bug-tracking system.
    - All of these measures shall follow best practices.
- Compliance with suitable open standards is recommended (Recommendation n° 66).

At least one competent, independent body (certification authority) shall be appointed to assess and certify the system's operation and compliance with these standards. (Recommendation n°111) This is currently the case in Belgium: several external and independent auditing companies have been designated by the Ministry of Internal Affair to carry out the certification.

In the event of any irregularity affecting the integrity of the votes, the affected votes shall be recorded as such.

11 General requirements for e-voting systems

This section of the report describes a number of general requirements which must be satisfied by any e-voting system among the ones under consideration. The four areas which are covered are: hardware, software, communications, and organization and procedures.

These requirements complement and/or augment the requirements set forth in the Recommendations of the Council of Europe on legal, operational, and technical standards for e-voting Rec(2004)11, which we assume will need to be implemented in any e-voting system for Belgium.

11.1 Global

The general requirements for e-voting systems must be clearly stated in a technology-independent way, distinguishing

- functional requirements: which functions must be provided by the system;
- non-functional requirements: accessibility by specific categories of people: elderly, disabled, etc; also security requirements, timing requirements, safety requirements, etc.

The requirements for the components (physical, software, organizational) shall be derived from these general requirements in a demonstrable way.

11.2 Hardware

All computers involved in the election process (pre-voting phases, voting phases, and post-voting phases) shall verifiably fulfill the following requirements:

- The hardware shall be standardized in order to ensure quick and easy replacement in case of breakdown.
- All devices which are not needed for e-voting operation shall be either physically disabled or removed, including communication devices. It shall be possible to ascertain this at any time after installation and during operation.
- Executable programs shall not be contained on removable media (e.g. flash memories).
- Seals shall be apposed to show evidence of possible tampering to auditors.

11.3 Software

Election software (be it at the voting booth, office, or totalization center or be it purpose-made or off-the-shelf) shall verifiably fulfill all requirements for reliable, robust, testable, and maintainable software, including the following ones:

Parameterization

- All election software shall be parameterized by means of data: the election software itself shall be totally independent of specific elections. Parameterization data shall be expressed in a formalism (language) easily understood by election officials.

- Parameterization data which have been prepared during pre-voting stages shall be certified, signed, and protected in a way which prevents tampering and allows verification before and during usage.

Specifications

- All software and all software components (i.e. modules) shall be specified with total accuracy and completeness using appropriate and effective specification methods, languages, and tools prior to implementation. Tenderers shall indicate which specification methods, languages, and tools they intend to use. Specifications shall be made publicly available and comments invited to improve them whenever needed.
- Provisions for testing and auditing shall be included in the specifications, not added as an afterthought.
- Security must be included in the specifications: a vulnerability analysis must be performed; a security policy must be defined to meet the security requirements and security must be built in the specifications in order to remove the vulnerabilities.
- Specifications shall be used to construct comprehensive test suites before actual implementation. The test suites shall be validated with respect to specifications by teams not directly involved in implementation. It shall be possible to test every module in a package independently of the remainder of the package.

Implementation

- Tenderers shall document the software development process they intend to follow, including provisions for quality control and assurance.
- Implementations shall be based on well-known and stable high-level programming languages and on approaches known to enhance the robustness and reliability of software (e.g. modular programming, defensive programming, run-time verification of assertions, etc.).
- Naming conventions for modules, procedures, variables and other significant entities shall be documented and adhered to; such conventions will enhance the human-readability of all election software.
- No code-altering techniques may be used in implementing software: the instructions contained in the code shall remain invariant during execution. Special care shall be taken to prevent accidental or deliberate attempts to modify code during execution (incorrect usage of pointers, buffer or string overflows, etc.).
- Implementers shall produce sufficient evidence that implementations truly satisfy the requirements. Formal program proofs are a possible means to produce such evidence, particularly for the sensitive parts of election software, which are not highly complex in nature.
- Every version of a piece of software shall be identified by a version number. Versions which are to be used during an election must be identified unambiguously, approved and signed by someone with the appropriate level of authority. The signature shall be non-forgeable (or at least extremely hard to forge).

- Every component of election software shall be accompanied by extensive, standardized and uniform documentation, prepared according to prevailing standards. Code shall be adequately commented. The documentation shall be audited by external, accredited auditors.

Certification

- Every component of election software shall be audited by external, accredited auditors, who will certify conformity with the specifications on the basis of evidence produced by the implementers.
- Before execution and at any time during execution of a piece of software involved in the election process, it shall be possible to verify that the piece of software is indeed the one which has been approved and signed.

Operating systems

- The operating systems used in the computers which handle individual votes up to and including the first totalization center shall be stabilized and certified before the election.
- All election-specific software shall be tested with the stabilized and certified versions of the operating systems which will be used.
- Before the election and at any time during the election and before the closing of all election activities, it shall be possible to verify that the versions of the operating systems executed in the various computers are indeed the stabilized and certified ones.
- Operating systems must prevent execution of any software located on removable media.

Tamper resistance

- A tamper-resistant means shall be provided to authenticate both the election specific software and these certified versions of the operating systems.
- Tamper resistance shall not exclusively be dependent on software mechanisms.
- Tamper resistance may be ensured by burning the election specific software, the operating system and all necessary support libraries and code onto a CD-ROM. This CD-ROM will be inserted in a CD-ROM drive which is subsequently closed, locked and sealed.

Audit records

- Software shall produce time-stamped audit records of all operations executed during all phases before, during, and after an election, as well as every error condition encountered and every remedial operation executed to handle such errors. It shall not be possible to stop the recording of audit records or to modify such records.
- Components of an e-voting system will periodically self-test to verify their operation and integrity; these tests will produce audit records and, if needed, real-time alarms to allow effective and timely intervention in case of malfunction. The status of the various components of the e-voting system shall be displayed in real-time.

- Time sources shall be adequately synchronized to maintain correct interpretation of audit trails.
- Audit records shall not contain information about the contents of a vote nor about the identity of a voter.
- Audit records shall be preserved until the election has been validated or for whatever time span is required by legislation.
- Whenever intervention is needed, messages to this effect shall be produced and displayed in a clear and unambiguous manner.

Miscellanea

- The user interfaces to election software shall be designed by experts in man-machine communications. Due attention shall be devoted to the needs of voters with disabilities.
- Whenever individual votes are stored, they shall be randomized in order to protect the anonymity of the suffrage.
- International efforts related to the specification, implementation, and verification of election software shall be taken into account (see e.g. Project P1583 of the IEEE[58]).

11.4 Communications

In the pre-voting phases, voting phases, and post-voting phases, software, data, and/or information will need to be communicated among various components of the overall voting system. Communication may be realized through physical transportation or by means of telecommunication networking facilities.

11.4.1 Physical transportation

Whenever software, parameterization data, or election information (votes, totals, etc.) are to be transported physically from one location to another, the following requirements must be met:

- Information shall be stored on appropriate media and protected in a way that prevents unauthorized access and tampering with contents. WORM (Write Once – Read Many times) media shall be preferred.
- The persons involved in the physical transportation of the media shall not possess keys allowing them to access the contents or tamper with its contents.
- An unbroken chain of custody shall be established in a verifiable way for all communications of sensitive information.

11.4.2 Telecommunication networks

Whenever software, parameterization data, or election information (votes, totals, etc.) are to be transported by means of a telecommunication network from one location to another, the following requirements must be met:

- Preference shall be given to usage of private, demonstrably secure networks.

[58] http://grouper.ieee.org/groups/scc38/1583/

- Whenever private, secure networks are unavailable, end-to-end secured transmission over public networks may be used, provided that the level of security is recognized as sufficient by experts in order to guarantee integrity of communications.

11.5 Organization and procedures

In the case of e-voting, many people will come in contact with hardware, software, and procedures with which they may not be familiar with and for which they may lack the adequate level of "computer literacy".

- Procedures shall be designed and written down by experts in human interactions and in man-machine communications.
- All procedures must be written in precise, but simple to understand language. All specific terminology shall be explained; whenever useful, examples and illustrations shall be provided. Independent tests shall be run to determine whether procedural descriptions actually meet these requirements.
- Adequate training shall be provided sufficiently in advance of the election. On-line learning techniques may be used whenever applicable to minimize cost and nuisance. The efficiency of the training shall be ascertained by means of random tests.
- Tests enabling election officials to verify the integrity of hardware, software, parameterization data and communication means (if any) shall be provided and procedures shall indicate when to apply them. For counting systems, tests shall allow ascertaining that counters have been set to zero before counting begins.
- All material related to confidentiality and security (i.e. keys) shall be handled with special care and attention at all levels. All such material shall only be handled by duly vetted officials, who shall be made aware of the need to protect its integrity and its secrecy.
- Decryption of encrypted information shall always require several partial keys supplied by different vetted officials.
- Contingency plans shall be set up to handle various kinds of breakdowns and failures; backup equipment shall be readily available; procedures shall explicitly mention what to do in case of problem.
- Sensitive data shall be kept available (in encrypted and signed form) on multiple supports to prevent loss in case of equipment or transmission malfunction.
- The complete end-to-end operation of any e-voting system should be tested with representative users in order to verify its feasibility and effectiveness.
- The need for auditing shall not compromise the need for anonymity of the suffrage.

12 Annex – Voting Ballots with Different Font Sizes

The following voting ballots illustrate the number of candidates that could be printed on a voting ballot. The number of columns, the number of lines per column, the exact layout and the font size are flexible parameters.

Senate Election *Selected Party*	Chamber Election *Selected Party*	European Election *Selected Party*	Province Election *Selected Party*	Region Election *Selected Party*	Local Election *Selected Party*
1 First Name	17 First Name	33 First Name	49 First Name	65 First Name	81 First Name
2 Second Name	18 Second Name	34 Second Name	50 Second Name	66 Second Name	82 Second Name
3 Third Name	19 Third Name	35 Third Name	51 Third Name	67 Third Name	83 Third Name
4 Fourth Name	20 Fourth Name	36 Fourth Name	52 Fourth Name	68 Fourth Name	84 Fourth Name
5 Fifth Name	21 Fifth Name	37 Fifth Name	53 Fifth Name	69 Fifth Name	85 Fifth Name
6 Sixth Name	22 Sixth Name	38 Sixth Name	54 Sixth Name	70 Sixth Name	86 Sixth Name
7 Seventh Name	23 Seventh Name	39 Seventh Name	55 Seventh Name	71 Seventh Name	87 Seventh Name
8 Eighth Name	24 Eighth Name	40 Eighth Name	56 Eighth Name	72 Eighth Name	88 Eighth Name
9 Nineth Name	25 Nineth Name	41 Nineth Name	57 Nineth Name	73 Nineth Name	89 Nineth Name
10 Tenth Name	26 Tenth Name	42 Tenth Name	58 Tenth Name	74 Tenth Name	90 Tenth Name
11 Eleventh Name	27 Eleventh Name	43 Eleventh Name	59 Eleventh Name	75 Eleventh Name	91 Eleventh Name
12 Twelfth Name	28 Twelfth Name	44 Twelfth Name	60 Twelfth Name	76 Twelfth Name	92 Twelfth Name
13 Thirteenth Name	29 Thirteenth Name	45 Thirteenth Name	61 Thirteenth Name	77 Thirteenth Name	93 Thirteenth Name
14 Fourteenth Name	30 Fourteenth Name	46 Fourteenth Name	62 Fourteenth Name	78 Fourteenth Name	94 Fourteenth Name
15 Fifteenth Name	31 Fifteenth Name	47 Fifteenth Name	63 Fifteenth Name	79 Fifteenth Name	95 Fifteenth Name
16 Sixteenth Name	32 Sixteenth Name	48 Sixteenth Name	64 Sixteenth Name	80 Sixteenth Name	96 Sixteenth Name

Figure 27: Voting ballot with 96 candidates, font size 7, 6 columns

Senate Election *Selected Party*	Chamber Election *Selected Party*	European Election *Selected Party*	Province Election *Selected Party*	Region Election *Selected Party*	Local Election *Selected Party*	Community Election *Selected Party*
1 First Name	21 First Name	41 First Name	61 First Name	81 First Name	101 First Name	121 First Name
2 Second Name	22. Second Name	42 Second Name	62 Second Name	82 Second Name	102 Second Name	122. Second Name
3 Third Name	23. Third Name	43 Third Name	63 Third Name	83 Third Name	103. Third Name	123. Third Name
4 Fourth Name	24. Fourth Name	44 Fourth Name	64 Fourth Name	84 Fourth Name	104. Fourth Name	124. Fourth Name
5 Fifth Name	25. Fifth Name	45 Fifth Name	65. Fifth Name	85. Fifth Name	105. Fifth Name	125. Fifth Name
6 Sixth Name	26. Sixth Name	46 Sixth Name	66 Sixth Name	86 Sixth Name	106 Sixth Name	126 Sixth Name
7 Seventh Name	27 Seventh Name	47 Seventh Name	67 Seventh Name	87 Seventh Name	107 Seventh Name	127 Seventh Name
8 Eighth Name	28 Eighth Name	48 Eighth Name	68 Eighth Name	88 Eighth Name	108 Eighth Name	128 Eighth Name
9 Nineth Name	29 Nineth Name	49 Nineth Name	69 Nineth Name	89 Nineth Name	109 Nineth Name	129 Nineth Name
10 Tenth Name	30 Tenth Name	50 Tenth Name	70. Tenth Name	90 Tenth Name	110. Tenth Name	130. Tenth Name
11 Eleventh Name	31 Eleventh Name	51 Eleventh Name	71 Eleventh Name	91 Eleventh Name	111 Eleventh Name	131. Eleventh Name
12 Twelfth Name	32. Twelfth Name	52 Twelfth Name	72 Twelfth Name	92 Twelfth Name	112 Twelfth Name	132 Twelfth Name
13 Thirteenth Name	33 Thirteenth Name	53 Thirteenth Name	73 Thirteenth Name	93 Thirteenth Name	113 Thirteenth Name	133 Thirteenth Name
14 Fourteenth Name	34 Fourteenth Name	54 Fourteenth Name	74 Fourteenth Name	94 Fourteenth Name	114 Fourteenth Name	134 Fourteenth Name
15 Fifteenth Name	35. Fifteenth Name	55 Fifteenth Name	75 Fifteenth Name	95 Fifteenth Name	115. Fifteenth Name	135. Fifteenth Name
16 Sixteenth Name	36 Sixteenth Name	56 Sixteenth Name	76 Sixteenth Name	96 Sixteenth Name	116 Sixteenth Name	136 Sixteenth Name
17 Seventeenth Name	37 Seventeenth Name	57 Seventeenth Name	77 Seventeenth Name	97 Seventeenth Name	117 Seventeenth Name	137 Seventeenth Name
18 Eighteenth Name	38 Eighteenth Name	58 Eighteenth Name	78 Eighteenth Name	98 Eighteenth Name	118 Eighteenth Name	138 Eighteenth Name
19 Nineteenth Name	39 Nineteenth Name	59 Nineteenth Name	79 Nineteenth Name	99 Nineteenth Name	119 Nineteenth Name	139 Nineteenth Name
20 Twentieth Name	40 Twentieth Name	60 Twentieth Name	80 Twentieth Name	100 Twentieth Name	120 Twentieth Name	140 Twentieth Name

Figure 28: Voting ballot with 140 candidates, font size 6, 7 columns

Senate Election *Selected Party*	Chamber Election *Selected Party*	European Election *Selected Party*	Province Election *Selected Party*	Region Election *Selected Party*	Local Election *Selected Party*	Community Election *Selected Party*
1 First Name	27 First Name	53 First Name	79 First Name	105 First Name	131 First Name	157 First Name
2 Second Name	28 Second Name	54 Second Name	80 Second Name	106 Second Name	132 Second Name	158 Second Name
3 Third Name	29 Third Name	55 Third Name	81 Third Name	107 Third Name	133 Third Name	159 Third Name
4 Fourth Name	30 Fourth Name	56 Fourth Name	82 Fourth Name	108 Fourth Name	134 Fourth Name	160 Fourth Name
5 Fifth Name	31 Fifth Name	57 Fifth Name	83 Fifth Name	109 Fifth Name	135 Fifth Name	161 Fifth Name
6 Sixth Name	32 Sixth Name	58 Sixth Name	84 Sixth Name	110 Sixth Name	136 Sixth Name	162 Sixth Name
7 Seventh Name	33 Seventh Name	59 Seventh Name	85 Seventh Name	111 Seventh Name	137 Seventh Name	163 Seventh Name
8 Eighth Name	34 Eighth Name	60 Eighth Name	86 Eighth Name	112 Eighth Name	138 Eighth Name	164 Eighth Name
9 Nineth Name	35 Nineth Name	61 Nineth Name	87 Nineth Name	113 Nineth Name	139 Nineth Name	165 Nineth Name
10 Tenth Name	36 Tenth Name	62 Tenth Name	88 Tenth Name	114 Tenth Name	140 Tenth Name	166 Tenth Name
11 Eleventh Name	37 Eleventh Name	63 Eleventh Name	89 Eleventh Name	115 Eleventh Name	141 Eleventh Name	167 Eleventh Name
12 Twelfth Name	38 Twelfth Name	64 Twelfth Name	90 Twelfth Name	116 Twelfth Name	142 Twelfth Name	168 Twelfth Name
13 Thirteenth Name	39 Thirteenth Name	65 Thirteenth Name	91 Thirteenth Name	117 Thirteenth Name	143 Thirteenth Name	169 Thirteenth Name
14 Fourteenth Name	40 Fourteenth Name	66 Fourteenth Name	92 Fourteenth Name	118 Fourteenth Name	144 Fourteenth Name	170 Fourteenth Name
15 Fifteenth Name	41 Fifteenth Name	67 Fifteenth Name	93 Fifteenth Name	119 Fifteenth Name	145 Fifteenth Name	171 Fifteenth Name
16 Sixteenth Name	42 Sixteenth Name	68 Sixteenth Name	94 Sixteenth Name	120 Sixteenth Name	146 Sixteenth Name	172 Sixteenth Name
17 Seventeenth Name	43 Seventeenth Name	69 Seventeenth Name	95 Seventeenth Name	121 Seventeenth Name	147 Seventeenth Name	173 Seventeenth Name
18 Eighteenth Name	44 Eighteenth Name	70 Eighteenth Name	96 Eighteenth Name	122 Eighteenth Name	148 Eighteenth Name	174 Eighteenth Name
19 Nineteenth Name	45 Nineteenth Name	71 Nineteenth Name	97 Nineteenth Name	123 Nineteenth Name	149 Nineteenth Name	175 Nineteenth Name
20 Twentieth Name	46 Twentieth Name	72 Twentieth Name	98 Twentieth Name	124 Twentieth Name	150 Twentieth Name	176 Twentieth Name
21 Twenty first NameName	47 Twenty first NameName	73 Twenty first NameName	99 Twenty first NameName	125 Twenty first NameName	151 Twenty first NameName	177 Twenty first NameName
22 Twenty second Name	48 Twenty second Name	74 Twenty second Name	100 Twenty second Name	126 Twenty second Name	152 Twenty second Name	178 Twenty second Name
23 Twenty third NameName	49 Twenty third NameName	75 Twenty third NameName	101 Twenty third NameName	127 Twenty third NameName	153 Twenty third NameName	179 Twenty third NameName
24 Twenty fourth NameName	50 Twenty fourth NameName	76 Twenty fourth NameName	102 Twenty fourth NameName	128 Twenty fourth NameName	154 Twenty fourth NameName	180 Twenty fourth NameName
25 Twenty fifth NameName	51 Twenty fifth NameName	77 Twenty fifth NameName	103 Twenty fifth NameName	129 Twenty fifth NameName	155 Twenty fifth NameName	181 Twenty fifth NameName
26 Twenty sixth NameName	52 Twenty sixth NameName	78 Twenty sixth NameName	104 Twenty sixth NameName	130 Twenty sixth NameName	156 Twenty sixth NameName	182 Twenty sixth NameName

Figure 29: Voting ballot with 182 candidates, font size 5, 7 columns

13 Signatures

13.1 K.U.Leuven

This report was read and approved by:

Prof. dr. ir. Bart Preneel

Prof. dr. ir. Vincent Rijmen

Prof. dr. ir. Jan Engelen

Prof. dr. Jos Dumortier

13.2 Université catholique de Louvain

This report was read and approved by:

Prof. dr. ir. Jean-Jacques Quisquater

Prof. (em.) dr. ir. Elie Milgrom

Prof. dr. ir. Marc Lobelle

13.3 Vrije Universiteit Brussel

This report was read and approved by:

Prof. dr. Kris Deschouwer

Prof. dr. Jo Buelens

13.4 Universiteit Antwerpen

This report was read and approved by:

Prof. dr. Stefaan Walgrave

13.5 Universiteit Gent

This report was read and approved by:

Prof. dr. Carl Devos

13.6 Université libre de Bruxelles

This report was read and approved by:

Prof. dr. Pascal Delwit

13.7 Université de Liège

This report was read and approved by:

Prof. dr. Pierre Verjans