Kiezen op Afstand in het buitenland

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Inhoudsopgave

1. Inleiding

Op 8 april 2004 (BPR2004/U59272) heeft de Tweede Kamer een rapportage ontvangen over de wijze waarop in andere landen wordt omgegaan met elektronisch kiezen op afstand. Bijgaande rapportage geeft inzicht in de ontwikkelingen die het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) sinds april 2004 heeft geconstateerd.

De voorliggende rapportage heeft, om een vergelijking mogelijk te maken, dezelfde opzet als de voorgaande. Per land wordt, aan de hand van een vast stramien, geschetst of er voornemens zijn met betrekking tot elektronisch kiezen op afstand. Voorafgaand aan de beschrijvingen per land wordt specifiek ingegaan op ontwikkelingen die zich vanaf april 2004 hebben voorgedaan. In deze rapportage is dat met name de samenwerking binnen de Raad van Europa.

2. Belangrijkste ontwikkelingen

Raad van Europa

Op 30 september 2004 heeft het Comité van ministers van de Raad van Europa een aanbeveling aangenomen over de wijze waarop lidstaten elektronisch stemmen vorm zouden moeten geven. De aanbeveling bestrijkt zowel het elektronisch stemmen in een stemlokaal met stemmachines als nieuwe vormen van elektronisch stemmen op afstand met behulp van Internet of telefonie. De aanbeveling van de Raad van Europa ("Recommendation") en het toelichtende memorandum daarop ("Explanatory Memorandum") zijn als bijlagen 3 en 4 bij deze buitenlandrapportage gevoegd.

De aanbeveling is het resultaat van de werkzaamheden van de Raad van Europa van de "Multidisciplinary Ad Hoc Group of Specialists on legal, operational and technical standards for e-enabled voting (IP1-S-EE)", die eind 2002 door het Comité van ministers werd ingesteld. Deze expertgroep viel onder het Integrated Project 1 ("Making democratic institutions work") van het Secretariaat-Generaal van de Raad van Europa. In eerdere rapportages is de Tweede Kamer geïnformeerd over de wijze waarop, binnen de Raad van Europa, aan de ontwikkeling van de aanbeveling werd gewerkt.

Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) heeft actief geparticipeerd in de totstandkoming van de aanbeveling. Het beleid van Nederland op het gebied van ICT en de ervaringen met het project Kiezen op Afstand zijn ingebracht en zijn herkenbaar in de aanbeveling verwerkt. In het bijzonder betreft dit:

- het nastreven van het gebruik van open standaarden met het oog op de interoperabiliteit van de technische componenten van verkiezingssystemen. Daarbij gaat het bij verkiezingssystemen met name om een variant van de standaard XML;
- het nastreven van transparantie van de technische voorzieningen door evaluatie en/of certificatie voorafgaand aan het gebruik en auditing tijdens het gebruik. Op dit punt stelt de annex bij de aanbeveling dat openbaarheid van de broncode van de programmatuur of het beschikbaarstellen van de programmatuur als "open source" middelen kunnen zijn om vorm te geven aan de transparantie/evaluatie van elektronische stemsystemen.
- het belang van het uitvoeren van risico-analyses teneinde systematisch te verzekeren dat de juiste beveiligingsmaatregelen worden genomen.

In de aanbeveling staat centraal dat elektronisch stemmen de beginselen van democratische verkiezingen en referenda niet in gevaar mag brengen. Elektronisch stemmen moet derhalve net zo betrouwbaar en veilig zijn als stemvormen waarbij geen gebruik wordt gemaakt van elektronische hulpmiddelen. De vereisten op juridisch, operationeel en technisch gebied dienen in samenhang te samenhang met elkaar worden beschouwd.

Het is aan de lidstaten van de Raad van Europa om na te gaan of de nationale wetgeving in het licht van de aanbeveling aanpassing behoeft. Een tweede oproep aan de lidstaten betreft het monitoren van de ervaringen met betrekking tot elektronisch stemmen en de implementatie van de Aanbeveling. De resultaten van deze 'monitoring' zouden aan het secretariaat van de Raad van Europa en aan de lidstaten ter beschikking moetwen worden gesteld teneinde over twee jaar de aanbeveling te kunnen heroverwegen. Nederland zal aan deze oproepen gevolg geven.

Landenrapportage

Inhoudsopgave

Leeswijzer

Land	***betreffende naam van het land***
Kiesstelsel	De aard van het kiesstelsel zoals dat is ingedeeld volgens IDEA (bron: http://www.idea.int/). Bijlage 2 bevat een toelichting op de weergegeven kiesstelsels.
Toegestane vorm van stemmen	Hier wordt aangeduid welke vorm(en) van stemmen er in het betreffende land wordt (worden) gebruikt: • stemmen in een stemlokaal (al dan niet met papieren stembiljetten en/of stemmachines); • briefstemmen; • early voting: kiezers kunnen hun stem kunnen uitbrengen vóór de verkiezingsdag; • punch card: kaart op een klein klipbord waar de kiezer een gat in de kaart maakt bij de kandidaat van eigen keuze; • hefboommachine: de naam van elke kandidaat is in een rechthoekige rij voor de machine toegewezen aan een bepaald niveau. Een set van gedrukte strips identificeert voor de kiezer de hefboomaanwijzing voor elke kandidaat. De kiezer trekt aan de desbetreffende hefboom om op zijn kandidaat te stemmen.
Voornemens omtrent KOA	De voornemens van het desbetreffende land voor de (mogelijke) invoering van (elektronisch) kiezen op afstand. De aanduiding “geen” houdt in dat er geen voornemens zijn geuit.
Andere voornemens	Andere voornemens in het land die van belang kunnen zijn. Voorbeelden zijn: voornemens op het gebied van elektronisch stemmen in een stemlokaal, de ontwikkeling van een Public Key Infrastructure of de invoering van een elektronische identiteitskaart .
Status van de voornemens	Onder deze rubriek wordt bij landen die voornemens hebben, aangegeven hoe aan deze voornemens vorm wordt gegeven. Vormgeven kan door het houden van een pilot of een experiment. Als in de voorafgaande rubriek is aangegeven dat er geen voornemens zijn, dan wordt bij deze rubriek de aanduiding “niet van toepassing (nvt)” gebruikt.
Wet en regelgeving	De verandering van de wetgeving die nodig is om kiezen op afstand te introduceren of om daarmee te experimenteren.
Planning	De planning van bijvoorbeeld toekomstige pilots, publicaties van rapporten, het uitvoeren van studies en dergelijke.
Status van Proeven/experimenten	In hoeverre er proeven of experimenten zijn gehouden of zullen worden gehouden.
Ontwikkeling ten opzichte van de rapportage van april 2004	Weergave van de veranderingen ten opzichte van de rapportage in april 2004.

Hoofdstuk 3 Bevindingen EU-landen

In dit hoofdstuk worden de bevindingen over de lidstaten van de Europese Unie beschreven.

Land	***BELGIE***
Kiesstelsel	Evenredige vertegenwoordiging
Toegestane vorm van stemmen	Stemlokaal (papieren stembiljetten en stemmen met een computer)
Voornemens omtrent KOA	België onderzoekt de mogelijkheden om internetstemmen te kunnen invoeren.
Andere voornemens	Tijdens de federale verkiezingen van 2003 hadden de burgers de mogelijkheid de kiezerslijsten te raadplegen, stemmingsimulaties te maken en de resultaten te raadplegen zodra die bekend waren. De federale regering heeft tijdens de verkiezingen in 2004 deze informatie wederom op haar website geplaatst.
Status van de voornemens	Het streven van Federaal staatssecretaris Vanvelthoven (Informatisering) om bij de gemeenteraadsverkiezingen in 2006 stemmen via internet mogelijk te maken is van de baan. België heeft een stemplicht en stemmen via internet maakt het zeer lastig om te controleren of iedere kiezer zijn stem heeft uitgebracht zonder deze te koppelen aan de uitgebrachte stem. Een Belgische kiezer zou dan niet anoniem zijn stem kunnen uitbrengen. Het stemmen via internet staat wel nog steeds op de agenda. Het streven is om voor 2007 het project te concretiseren.
Wet en regelgeving	Er zijn wetwijzigingen doorgevoerd in verband met de herziening van het kiesstelsel.
Planning	Niet bekend.
Status van Proeven/experimenten	Bij de federale parlementsverkiezingen op 18 mei 2003 is in twee kiesdistricten geëxperimenteerd met het op papier afdrukken (in stemlokalen) van de stem die via een stemapparaat is uitgebracht. Deze “papieren” stemmen worden in een stembus gedeponeerd. De gedachte hierachter is dat “papieren” stemmen kunnen worden gebruikt bij een hertelling. Tijdens de federale verkiezingen in 2003 zijn de kiezerslijsten, stemmingsimulaties en de resultaten via internet beschikbaar gesteld. Dat is ook gebeur bij de verkiezing in juni 2004 voor de leden van het Europees Parlement.
Ontwikkeling ten opzichte van de rapportage van april 2004	België heeft de kiezerslijsten, stemmingsimulaties en de resultaten van de verkiezingen in juni 2004 via internet beschikbaar gesteld.

Land	***CYPRUS***
Kiesstelsel	Lijst evenredige vertegenwoordiging
Toegestane vorm van stemmen	Stemlokaal (papieren stembiljetten) en briefstemmen
Voornemens omtrent KOA	Geen. Hier zijn twee redenen voor: 1. Technische redenen: Cyprus is zelf niet in staat een elektronisch stemsysteem te ontwikkelen; 2. Juridische redenen: het risico van family voting.
Status van de voornemens	Geen
Wet en regelgeving	nvt
Planning	nvt
Status van Proeven/experimenten	nvt
Ontwikkeling ten opzichte van de rapportage van april 2004	Geen

Land	DENEMARKEN
Kiesstelsel	Lijst evenredige vertegenwoordiging
Toegestane vorm van stemmen	Stemlokaal (papieren stembiljetten)
Voornemens omtrent KOA	Geen
Status van de voornemens	Het voornemen bestaat om in november 2005 (parlementsverkiezingen) een proef in stemlokalen te houden met het controleren van de kiesgerechtigheid met behulp van een elektronisch kiezersbestand (in plaats van een papieren lijst). Bij elektronisch stemmen op afstand worden de nodige kanttekeningen geplaatst. Het belangrijkste tegenargument van Denemarken is dat het stemgeheim bij elektronisch stemmen op afstand niet gewaarborgd kan worden (“family voting”). Daarnaast hecht men aan de speciale betekenis en de tradities rond het stemmen in een stemlokaal. De ontwikkelingen in het buitenland worden wel nauwgezet gevolgd. Mocht een ander land succesvol elektronisch stemmen op afstand introduceren, dan zal Denemarken mogelijk experimenten gaan overwegen.
Wet en regelgeving	nvt
Planning	nvt
Status van Proeven/experimenten	Nvt
Ontwikkeling ten opzichte van de rapportage van april 2004	Geen.

Land	*DUITSLAND*
Kiesstelsel	Evenredige vertegenwoordiging en een meerderheidsstelsel
Toegestane vorm van stemmen	Stemlokaal (papieren stembiljetten; in Keulen met stemapparaten) en briefstemmen
Voornemens omtrent KOA	Stemmen per internet bij de nationale verkiezingen zal niet vóór 2010 worden toegepast. Het volgende stappenplan is voorzien: 1. Elektronisch stemmen in willekeurige (met elkaar verbonden) stemlokalen ; 2. Stap 1 en daarbij: stemmen in een kiosk 3. Stap 2 en daarbij: stemmen via internet vanuit elke locatie. Er is geen tijdplanning aan dit stappenplan gekoppeld.
Status van de voornemens	De ambtelijke werkgroep werkt nog steeds aan een analyse van de eisen en voorwaarden die voor internetstemmen zouden moeten gelden en aan een raming van de kosten.
Wet en regelgeving	De regelgeving moet aangepast worden om het stappenplan uit te voeren. Het proces om de regelgeving aan te passen is nog niet gestart.
Planning	Niet bekend.
Status van Proeven/experimenten	Er zijn en worden internetverkiezingen gehouden op scholen, bedrijven, universiteiten, met seniorraden en jeugdraden. Deze verkiezingen komen voort uit lokale initiatieven en samenwerking tussen het ministerie van Economische Zaken van de Bondsrepubliek en verschillende universiteiten.
Ontwikkeling ten opzichte van de rapportage van april 2004	Geen.

Land	*ESTLAND*
Kiesstelsel	Lijst evenredige vertegenwoordiging
Toegestane vorm van stemmen	Stemlokaal (papieren stembiljetten) en briefstemmen
Voornemens omtrent KOA	Invoeren van internetstemmen.
Status van de voornemens	Pilot met internetstemmen tijdens een raadplegend referendum in Tallinn in de herfst 2004. Het Nationale Kiescomité is verantwoordelijk voor de invoering van elektronisch stemmen. Er is een Task Force gevormd die belast is met de invoering van internetstemmen. Deze Task Force is in september 2003 met haar werkzaamheden begonnen.
Wet en regelgeving	De Kieswet van Estland is in 2002 aangepast zodat stemmen via internet na 2005 mogelijk is. Internetstemmen is mogelijk bij lokale, provinciale, nationale en Verkiezing van het Europees Parlement (na toetreding van Estland tot de Europese Unie).
Planning	Het doel is invoering van internetstemmen bij de lokale verkiezingen in oktober 2005.
Status van Proeven/experimenten	Tijdens een raadplegend referendum (in de herfst van 2004) in Tallinn zal een pilot met internetstemmen worden gehouden.
Ontwikkeling ten opzichte van de rapportage van april 2004	Geen.

Land	*FINLAND*
Kiesstelsel	Lijst evenredige vertegenwoordiging
Toegestane vorm van stemmen	Stemlokaal (papieren stembiljetten) en early voting
Voornemens omtrent KOA	Geen. Finland voorziet knelpunten bij het waarborgen van de stemvrijheid.
Andere voornemens	De regering heeft voornemens om te experimenteren met elektronisch stemmen in een stemlokaal. Er is nog geen concreet tijdpad hiervoor bekend.
Status van de voornemens	nvt
Wet en regelgeving	nvt
Planning	nvt
Status van Proeven/experimenten	Voorgenomen experimenten met elektronisch stemmen in een stemlokaal.
Ontwikkeling ten opzichte van de rapportage van april 2004	Geen

Land	*FRANKRIJK*
Kiesstelsel	Meerderheidsstelsel met twee ronden
Toegestane vorm van stemmen	Stemlokaal (papieren stembiljetten)
Voornemens omtrent KOA	Het mogelijk maken dat kiezers uit het buitenland bij de Presidentiële verkiezingen en referenda hun stem via internet kunnen uitbrengen.
Andere voornemens	Er is een programma van eisen opgesteld voor gemeenten die gebruik willen gaan maken van stemmachines of stemcomputers in stemlokalen. Er zullen bij verkiezingen experimenten met elektronische stemmachines in stemlokalen worden gehouden. Tijdens de verkiezing van het Europees Parlement in juni 2004 zijn er in 18 gemeenten proeven gehouden met stemmachines in stemlokalen. De resultaten waren in een aantal gemeenten bindend, waaronder Vandoeuvre-les-Nancy.
Status van de voornemens	Onbekend.
Wet en regelgeving	In 2003 is stemmen via internet mogelijk gemaakt voor kiezers in het buitenland aangaande verkiezingen van vertegenwoordigers van raadgevende instanties. Recentelijk is een wetsvoorstel ingediend dat het mogelijk zal moeten maken dat kiezers in het buitenland ook voor Presidentiële verkiezingen en referenda via internet hun stem kunnen uitbrengen.
Planning	Onbekend.
Status van Proeven/experimenten	In mei 2003 is een experiment gehouden waarbij kiezers in het buitenland (Washington en San Francisco), via internet hun stem konden uitbrengen voor het CSFE (Conseil Supérieur des Français de l'Etranger). Het CSFE heeft tot taak de belangen van de Fransen die in het buitenland wonen te behartigen. De leden van het CSFE kiezen 12 senatoren (van de 321 senatoren). Van de 61.058 kiesgerechtigden hebben 5354 kiezers uiteindelijk via internet gestemd. Het stemsysteem werd geleverd door Election.com. De kiezer kreeg toegang tot de stemdienst door gebruik te maken van een identificatiecode en een paswoord. Doel van het experiment is het faciliteren van de kiezer om zo de kiezer meer betrokken te krijgen bij de democratie. Het is op het ogenblik niet bekend of dit experiment herhaald zal worden. Ook is onbekend of het experiment wordt geëvalueerd.

	Tijdens regionale verkiezingen in maart 2004 heeft de gemeente Brest de, voor Frankrijk, eerste bindende verkiezing gehouden met elektronische stemapparaten. Tijdens de verkiezing van het Europees Parlement in juni 2004 zijn er in 18 gemeenten proeven gehouden met stemmachines. In een aantal gemeenten waren de resultaten bindend.
Ontwikkeling ten opzichte van de rapportage van april 2004	Tijdens de verkiezing van het Europees Parlement in juni 2004 zijn er in 18 gemeenten proeven gehouden met stemmachines. De uitkomsten van deze proeven zijn nog niet bekend.

Land	*GRIEKENLAND*
Kiesstelsel	Lijst evenredige vertegenwoordiging
Toegestane vorm van stemmen	Stemlokaal (papieren stembiljetten)
Voornemens omtrent KOA	Geen.
Andere voornemens	Griekenland overweegt stemmachines in stemlokalen te gaan gebruiken.
Status van de voornemens	nvt
Wet en regelgeving	nvt
Planning	nvt
Status van Proeven/experimenten	nvt
Ontwikkeling ten opzichte van de rapportage van april 2004	Geen

Land	*HONGARIJE*
Kiesstelsel	Evenredige vertegenwoordiging en een meerderheidsstelsel.
Toegestane vorm van stemmen	Stemlokaal (papieren stembiljetten)
Voornemens omtrent KOA	Geen
Andere voornemens	De wetswijziging van de Kieswet die in het Parlement aanhangig was is gedeeltelijk aangenomen. Het doel van de wetswijziging was om Hongaarse stemgerechtigden, die op de dag van de verkiezing van het Europees Parlement in het buitenland verblijven, de mogelijkheid te bieden om met behulp van stemmachines op ambassades te stemmen. De regering heeft er echter voor gekozen geen stemmachines in te zetten, maar de stemgerechtigden op de ambassades per stembiljet te laten stemmen.
Status van de voornemens	nvt
Wet en regelgeving	Er is een wetswijziging van de Kieswet aangenomen die het mogelijk maakt dat inwoners van Hongarije die op de dag van de verkiezing tijdelijk in het buitenland verblijven, op de Hongaarse ambassades mogen stemmen.
Planning	nvt
Status van Proeven/experimenten	Geen
Ontwikkeling ten opzichte van de rapportage van april 2004	Tijdens de verkiezing van het Europees Parlement hebben Hongaarse stemgerechtigden, die op de dag van de verkiezing tijdelijk in het buitenland verbleven, voor het eerst de mogelijkheid gekregen om hun stem op Hongaarse ambassades uit te brengen.

Land	*IERLAND*
Kiesstelsel	Een meerderheidsstelsel met preferente stemmen
Toegestane vorm van stemmen	Stemlokaal (papieren stembiljetten); briefstemmen
Voornemens omtrent KOA	Geen.
Andere voornemens	In mei 2002 is geëxperimenteerd met elektronische stemmachines in stemlokalen. In Ierland heeft een discussie plaatsgevonden over het gebruik van stemapparaten. De regering heeft in februari 2004 een commissie geïnstalleerd om de stemmachines te onderzoeken. De commissie heeft eind april 2004 de Ierse regering geadviseerd de elektronische stemmachines niet in te zetten bij de lokale verkiezingen en de verkiezing voor de leden van het Europees Parlement in 2004. De commissie is van mening dat nog onvoldoende is aangetoond dat de stemmachines accuraat en met behoud van het stemgeheim zouden functioneren. De Ierse regering heeft dit advies opgevolgd.
Status van de voornemens	nvt
Wet en regelgeving	nvt
Planning	nvt
Status van Proeven/experimenten	nvt
Ontwikkeling ten opzichte van de rapportage van april 2004	De Ierse regering heeft de inzet van stemmachines uitgesteld.

Land	*ITALIE*
Kiesstelsel	Evenredige vertegenwoordiging en een meerderheidsstelsel
Toegestane vorm van stemmen	Stemlokaal (papieren stembiljetten)
Voornemens omtrent KOA	Geen.
Andere voornemens	Er zijn lokale initiatieven waarvan enkele onderdeel uitmaken van projecten van de Europese Commissie. De Italiaanse regering heeft het voornemen over te gaan tot het elektronisch tellen van stembiljetten in de stemlokalen. Ook bestond het voornemen om bij de verkiezing van het Europees Parlement in juni 2004 een proef met stemmachines te houden.
Status van de voornemens	Niet van toepassing.
Wet en regelgeving	Niet aangepast voor hiervoor genoemde initiatieven.
Planning	Onbekend.
Status van Proeven/experimenten	Naast het Italiaanse ministerie van Binnenlandse Zaken zijn een aantal gemeenten, zoals Avellino en Cremona, betrokken bij projecten van de Europese Commissie. Verder zijn er enkele initiatieven op universiteiten. Bij de verkiezing van het Europees Parlement in juni 2004 is in ca 2.500 stemlokalen een proef gehouden met het elektronisch tellen van stembiljetten. De proef heeft naast het handmatig tellen plaatsgevonden en heeft derhalve geen juridische waarde. De proef wordt momenteel door een commissie geëvalueerd. De commissie zal in een evaluatierapport aanbevelingen doen voor eventuele volgende proeven met elektronisch tellen. Het is niet bekend wanneer de evaluatiegegevens zullen worden gepubliceerd.
Ontwikkeling ten opzichte van de rapportage van april 2004	Proeven met elektronisch stemmen en met elektronisch stemmen in stemlokalen.

Land	*LETLAND*
Kiesstelsel	Lijst evenredige vertegenwoordiging
Toegestane vorm van stemmen	Stemlokaal (papieren stembiljetten)
Voornemens omtrent KOA	Het houden van discussies en referenda via internet.
Status van de voornemens	onbekend.
Wet en regelgeving	
Planning	onbekend
Status van Proeven/experimenten	onbekend
Ontwikkeling ten opzichte van de rapportage van april 2004	Geen.

Land	*LITOUWEN*
Kiesstelsel	Parallel meerderheidsstelsel met twee ronden
Toegestane vorm van stemmen	Stemlokaal (papieren stembiljetten)
Voornemens omtrent KOA	Geen. Litouwen vindt dat de waarborgen met betrekking tot stemgeheim, stemvrijheid en hertelling niet kunnen worden gerealiseerd bij elektronisch stemmen op afstand.
Status van de voornemens	nvt
Wet en regelgeving	nvt
Planning	nvt
Status van Proeven/experimenten	nvt
Ontwikkeling ten opzichte van de rapportage van april 2004	Geen

Land	*LUXEMBURG*
Kiesstelsel	Lijst evenredige vertegenwoordiging
Toegestane vorm van stemmen	Stemlokaal (papieren stembiljetten)
Voornemens omtrent KOA	Geen. De reden is dat internet nog in onvoldoende mate door de bevolking wordt gebruikt. Door elektronisch kiezen op afstand zou er een digitale tweedeling kunnen ontstaan.
Status van de voornemens	nvt
Wet en regelgeving	nvt
Planning	nvt
Status van Proeven/experimenten	nvt
Ontwikkeling ten opzichte van de rapportage van april 2004	Geen

Land	*MALTA*
Kiesstelsel	Lijst van evenredige vertegenwoordiging op basis van preferente stemmen
Toegestane vorm van stemmen	Stemlokaal (papieren stembiljetten)
Voornemens omtrent KOA	Geen.
Status van de voornemens	nvt
Wet en regelgeving	nvt
Planning	nvt
Status van Proeven/experimenten	nvt
Ontwikkeling ten opzichte van de rapportage van april 2004	Geen.

Land	*OOSTENRIJK*
Kiesstelsel	Lijst evenredige vertegenwoordiging
Toegestane vorm van stemmen	Stemlokaal (papieren stembiljetten)
Voornemens omtrent KOA	Het ministerie van Buitenlandse Zaken wil juridische en technische voorzieningen treffen zodat de kiezers die in het buitenland wonen makkelijker hun stem kunnen uitbrengen. Het ministerie wil de mogelijkheid van internetstemmen daarbij betrekken. De Oostenrijkse regering heeft in mei 2003 een e-government strategie bepaald. Elektronisch stemmen op afstand voor kiezers in het buitenland maakt deel uit van deze strategie.
Status van de voornemens	nvt
Wet en regelgeving	In mei 2004 heeft het ministerie van Binnenlandse Zaken een werkgroep e-voting opgericht. De werkgroep zal de wetgeving, de technologie en de internationale aspecten van e-voting bestuderen. De verwachting is dat de werkgroep in het najaar de uitkomsten van het onderzoek zal publiceren.
Planning	Onbekend.
Status van Proeven/experimenten	In mei 2003 is door de Universiteit van Wenen een schaduwverkiezing gehouden voor de Universiteitsraad. 355 studenten (van de 978 studenten) hebben via internet hun stem uitgebracht. Voor de identificatie van de kiezer is de nationale elektronische ID-kaart gebruikt (op het ogenblik nog beperkt uitgerold). Tijdens de presidentsverkiezingen in april 2004 is een schaduwverkiezing gehouden door de universiteit Wenen georganiseerd. Ca 20.000 studenten hebben een teststem via een internetsysteem kunnen uitbrengen. 961 studenten hebben dat gedaan.
Ontwikkeling ten opzichte van de rapportage van april 2004	Schaduwverkiezing met internetstemmen georganiseerd door de universiteit van Wenen. Instelling van een regeringswerkgroep e-voting.

Land	*POLEN*
Kiesstelsel	Lijst evenredige vertegenwoordiging en meerderheidsstelsel
Toegestane vorm van stemmen	Stemlokaal (papieren stembiljetten)
Voornemens omtrent KOA	Geen.
Status van de voornemens	nvt
Wet en regelgeving	nvt
Planning	nvt
Status van Proeven/experimenten	nvt
Ontwikkeling ten opzichte van de rapportage van april 2004	Geen.

Land	*PORTUGAL*
Kiesstelsel	Lijst evenredige vertegenwoordiging
Toegestane vorm van stemmen	Stemlokaal (papieren stembiljetten) en briefstemmen
Voornemens omtrent KOA	Geen.
Andere voornemens	De Portugese regering heeft elektronisch stemmen op de politieke agenda gezet.Het doel is de kiezer meer te betrekken bij het democratische proces.
Status van de voornemens	Niet bekend.
Wet en regelgeving	Niet aangepast voor hiervoor genoemde initiatieven.
Planning	Niet bekend.
Status van Proeven/experimenten	Bij de verkiezing van het Europees Parlement in juni 2004 zijn in 9 gemeenten proeven gehouden met elektronisch stemmen in een stemlokaal. Ca. 128.000 kiesgerechtigden konden één van drie verschillende elektronische stemsystemen testen. 9.390 kiezers hebben aan de proef meegedaan. Het is niet bekend wanneer de evaluatiegegevens zullen worden gepubliceerd.
Ontwikkeling ten opzichte van de rapportage van april 2004	Proef bij de verkiezing van de leden van het Europees parlement in juni 2004 met het elektronisch stemmen in een stemlokaal.

Land	*SLOVENIE*
Kiesstelsel	Lijst evenredige vertegenwoordiging
Toegestane vorm van stemmen	Stemlokaal (papieren stembiljetten)
Voornemens omtrent KOA	Er worden voorbereidingen getroffen om elektronisch stemmen op afstand in te voeren en er wordt gewerkt aan de ontwikkeling van Public Key Infrastructure.
Status van de voornemens	Onbekend
Wet en regelgeving	Het voorstel dat ingediend was om de Kieswet op een aantal punten aan te passen zodat elektronisch stemmen op afstand mogelijk is, is niet aangenomen.
Planning	Onbekend
Status van Proeven/experimenten	Onbekend
Ontwikkeling ten opzichte van de rapportage van april 2004	Geen.

Land	*SLOWAKIJE*
Kiesstelsel	Lijst evenredige vertegenwoordiging
Toegestane vorm van stemmen	Stemlokaal (papieren stembiljetten)
Voornemens omtrent KOA	Geen, omdat de financiële middelen ontbreken en de bestaande regelgeving het niet toe laat.
Status van de voornemens	Geen
Wet en regelgeving	Nvt
Planning	Nvt
Status van Proeven/experimenten	Nvt
Ontwikkeling ten opzichte van de rapportage van april 2004	Geen

	SPANJE
Kiesstelsel	Lijst evenredige vertegenwoordiging
Toegestane vorm van stemmen	Stemlokaal (papieren stembiljetten) en briefstemmen
Voornemens omtrent KOA	De Spaanse minister-president heeft op 10 augustus 2004 aangekondigd dat de Spaanse regering in september 2004 een wijziging van de Kieswet zal bespreken. Het doel van deze wetswijziging is het mogelijk maken dat tijdens het referendum inzake de Europese Grondwet (februari 2005) Spaanse kiesgerechtigden via internet hun stem kunnen uitbrengen.
Status van de voornemens	Onbekend
Wet en regelgeving	De wet staat elektronisch stemmen (op afstand) niet toe en zal pas worden aangepast als de pilots zijn geslaagd en de techniek goed is getest.
Planning	Niet bekend.
Status van Proeven/experimenten	Proef (16 maart 2003) in Hoyo de Pinares Avila (2.400 inwoners). Kiezers konden voor een lokaal raadgevend referendum via internet stemmen (vanuit huis of vanuit een stemlokaal) in combinatie met een smartcard. Pilot (november 2003) in Catalonië met Internetstemmen gehouden. 23234 stemmers in het buitenland konden met behulp van een user-ID en een paswoord via internet stemmen. 730 kiezers hebben dit gedaan. Pilot tijdens de Spaanse parlementsverkiezingen (maart 2004) met internetstemmen in de gemeente Jun. De evaluatie wordt uitgevoerd door de Universiteit van Madrid. Doel van de pilot is om te kijken of internetstemmen gewaardeerd wordt door de kiezer. Pilot (maart 2004) met internetstemmen in de provincies Zamora en Lugo. Hier konden 274 vrijwilligers hun stem uitbrengen met een digitaal certificaat. De gemeente Madrid heeft bij een lokaal referendum (juni 2004) een experiment met internet- en mobiel telefoonstemmen gehouden. Voorafgaand aan de verkiezing moesten de ca 136.000 kiesgerechtigden een digitaal certificaat aanvragen. 882 kiezers hebben hun stem uitgebracht.
Ontwikkeling ten opzichte van de rapportage van april 2004	Aankondiging dat de Spaanse regering internetstemmen mogelijk wil maken bij het referendum (in 2005) over de Europese Grondwet. Experiment in Madrid met internet- en mobiel telefoonstemmen.

Land	*TSJECHIE*
Kiesstelsel	Lijst evenredige vertegenwoordiging
Toegestane vorm van stemmen	Stemlokaal (papieren stembiljetten)
Voornemens omtrent KOA	geen.
Status van de voornemens	nvt
Wet en regelgeving	
Planning	nvt
Status van Proeven/experimenten	nvt
Ontwikkeling ten opzichte van de rapportage van april 2004	geen.

Land	*VERENIGD KONINKRIJK*
Kiesstelsel	First Past the Post systeem
Toegestane vorm van stemmen	Stemlokaal (papieren stembiljetten) en briefstemmen.
Voornemens omtrent KOA	De regering van het Verenigd Koninkrijk wil over de hele linie het stemproces moderniseren. Er wordt geëxperimenteerd met onder andere elektronisch tellen en stemmen in een stemlokaal, stemmen via internet, telefoonstemmen, SMS stemmen, stemmen via Digitale TV, (alleen) briefstemmen, andere openingstijden etc. De regering heeft het voornemen de kiezer na 2006 de mogelijkheid te bieden om, bij nationale verkiezingen, via internet te stemmen.
Status van de voornemens	Alle voor 2004 geplande experimenten met e-voting zijn afgelast op advies van de Electoral Commission. De Electoral Commission achtte de beschikbare tijd en de bereidheid van returning officers tot deelname onvoldoende om pilots met e-voting door te zetten. De regering van het Verenigd Koninkrijk heeft het advies overgenomen.
Wet en regelgeving	Om experimenten bij lokale verkiezingen in Engeland en Wales te kunnen houden in maart 2000 is een wetswijziging doorgevoerd.
Planning	De planning voor de komende twee jaar is nog niet bekend.
Status van Proeven/experimenten	In mei 2003 zijn in 14 gemeenten experimenten gehouden met elektronisch stemmen: • Internetstemmen (14 gemeenten)[1] • Touch tone telefoon stemmen (12 gemeenten) • SMS telefoonstemmen (4 gemeenten) • Stemmen via digitale televisie (5 gemeenten) • Stemmen vanuit een kiosk (1 gemeente) Daarnaast worden experimenten gehouden met elektronisch stemmen in een stemlokaal, elektronisch tellen, ‘all postal voting’ en variaties met openingstijden en andere stembiljetten. De Electoral Commission heeft naar aanleiding van deze experimenten aanbevolen “all postal voting” in te voeren voor de lokale verkiezingen. Onder ‘all postal voting’ wordt verstaan: De stembescheiden worden per post aan de kiezer toegezonden; de kiezer kan vervolgens naar eigen voorkeur ofwel het ingevulde stembiljet per post retourneren, ofwel de stembescheiden meenemen naar een stemlokaal en daar zijn stem uitbrengen. De Electoral Commission adviseerde verder door te gaan met experimenten met elektronisch stemmen (op afstand).

[1] Een groot aantal gemeenten experimenteert met verschillende stemmethoden.

	In juni 2004 is bij lokale verkiezingen en bij de verkiezing van de leden van het Europees Parlement in vier kiesdistricten (Yorkshire & the Humber, the North West, the North East en East Midlands) geëxperimenteerd met ‘all postal voting’. Er hebben zich bij deze verkiezingen veel problemen voorgedaan met het stemmen per post. Er zijn berichten dat er op grote schaal fraude heeft plaatsgevonden. De regering laat in een onderzoek nagaan wat er precies gebeurd is. hiernaar aangekondigd. Bij de verkiezingen in juni 2004 is ook een experiment met het elektronisch tellen van stembiljetten. Ca 6.000.000 stembiljetten zijn binnen enkele uren in de regio Londen elektronisch geteld.
Ontwikkeling ten opzichte van de rapportage van april 2004	Experimenten in juni 2004 met ‘all postal voting’ en met het elektronisch tellen van stembiljetten.

Land	*ZWEDEN*
Kiesstelsel	Lijst evenredige vertegenwoordiging
Toegestane vorm van stemmen	Stemlokaal (papieren stembiljetten); briefstemmen en early voting.
Voornemens omtrent KOA	Geen.
Andere voornemens	Een parlementaire commissie onderzoekt de mogelijkheden voor elektronisch stemmen in een stemlokaal. De conclusies zullen in november 2004 bekend worden gemaakt. Indien de commissie elektronisch stemmen in een stemlokaal aanbeveelt, zouden er in 2006 bij de nationale verkiezingen pilots kunnen worden gehouden.
Status van de voornemens	nvt
Wet en regelgeving	nvt
Planning	nvt
Status van Proeven/experimenten	De Universiteit van Umeå heeft op eigen initiatief in 2001 studenten per internet de Studentenraad laten kiezen.
Ontwikkeling ten opzichte van de rapportage van april 2004	Geen.

Hoofdstuk 4 Programma's van de Europese Commissie

Er zijn vier onderzoeks- en ontwikkelingsprogramma's die gefinancierd worden door de Europese Commissie: E-Poll, CyberVote, True Vote en E-Vote. De programma's hebben tot doel de stemsystemen te moderniseren, het onderzoek daarnaar te stimuleren en oplossingen uit te wissen.

EU	***E-POLL***
Doel van het project	Dit onderzoeksproject is gericht op de ontwikkeling van innovatieve systemen om het stemproces te ondersteunen. De achterliggende gedachte is dat kiezers hun stem via Internet moeten kunnen uitbrengen in elk stemlokaal in Europa.
Status van de voornemens	nvt
Wet en regelgeving	nvt
Planning	Het programma is beëindigd op 1 december 2002. In oktober 2002 is een evaluatie verschenen. De uitkomst van de evaluatie is dat het project E-poll goede resultaten heeft opgeleverd, welke zowel op technisch als commercieel gebied bruikbaar zijn.
Status van Proeven/experimenten	De volgende schaduwverkiezingen zijn afgerond: -Avellino (Italië): 2 oktober 2001 -Campo Basso (Italië): mei 2002 -Parma (Italië): mei 2002 -Vandoeuvre-les-Nancy (Frankrijk): 21 april en 5 mei 2002 -Merignac (Frankrijk): 9-16 juni 2002 -Polen: oktober 2002 -Cremona (Italië): november 2002
Ontwikkeling ten opzichte van de rapportage van april 2004	Geen.

EU	CYBERVOTE
Doel van het project	Het programma heeft tot doel de participatie van Europese burgers te vergroten door de inzet van moderne elektronische stemsystemen. Het programma richt zich in het bijzonder op jongeren, lichamelijk gehandicapten, immigranten en sociaal buitengesloten burgers. De burger zou moeten kunnen stemmen via internet en via mobiele telefoons met WAP. De Universiteit Eindhoven is partner in dit programma en is belast met de ontwikkeling van de cryptografische protocollen voor de elektronische stembus.
Status van de voornemens	De volgende pilots met internetstemmen zijn gehouden: -Issy-les-Moulineaux (Frankrijk): 11 december 2002; lokale stadswijk verkiezing (860 kiezers) -Hogeschool Bremen (Duitsland): 13-15 januari 2003; universiteitsraden (47 kiezers) -Kista (Zweden): 27- 31 januari 2003; lokale raadpleging (226 kiezers)
Wet en regelgeving	nvt
Planning	Eind september 2003 zijn tijdens een forum over e-democracy in Issy-les-Moulineaux de belangrijkste lessen van het project gepresenteerd. - Het voorbereiden van verkiezingen kost veel tijd. - Het gebruik van elektronische handtekeningen brengt veel administratieve procedures en technische problemen met zich mee. - Het gebruik van de programmeertaal Java op computers uitgerust zonder Java leverde veel problemen op. - De verkiezingsuitslagen en de tussenstanden zijn gemakkelijk op te vragen. Dit bevordert de efficiëntie. - Het vertrouwen in de veiligheid van de stemdienst is erg hoog (90%). Daarbij moet bedacht worden dat stembureauleden en kiezers geen veiligheidsexperts zijn. Enkele aanbevelingen - Breng een duidelijke scheidslijn aan (in tijd) tussen de registratieperiode en de stemperiode - Lever een ‘dual-speed’ stemsysteem. Eén voor kiezers met begeleiding of kiezers die voor het eerst stemmen en één voor ervaren gebruikers. - Laat kiezers van tevoren een simulatie of demo systeem gebruiken. - Publiceer foto’s van de kandidaten op het stemsysteem. Sta meer stemlocaties toe (indien mensen naar een buurthuis gaan om daar bijvoorbeeld vanaf een pc te stemmen). Het Cybervote project is beëindigd en het consortium zal in deze vorm niet verder gaan. De ontwikkelde software zal waarschijnlijk binnen de eigen organisaties ingezet worden.

Status van Proeven/experimenten	-Issy-les-Moulineaux (Frankrijk) : 860 kiezers hebben via internet gestemd, waarvan 20% van huis of werk uit en 80% in een stemlokaal. Een aantal kiezers kon niet stemmen omdat hun computer geen Java ondersteund. -Hogeschool Bremen (Duitsland): Studenten, professoren en medewerkers van de hogeschool konden hun stem uitbrengen via het intranet van de hogeschool. Er zijn 250 personen benaderd, uiteindelijk hebben 47 kiezers gestemd. Het kleine aantal deelnemers komt vanwege de bureaucratische procedure om de benodigde smartcard aan te vragen. De verkiezing is uitgesteld omdat de kandidatenlijst verkeerd was geïnstalleerd. Daarnaast waren er problemen met de smartcard. Er zijn geen Java problemen meer gesignaleerd omdat de gebruikte computers voorgeprogrammeerd waren. -Kista (Zweden): 226 (met name oudere) kiezers brachten hun stem uit via internet (via 3 zuilen of vanuit huis) voor een lokale volksraadpleging. Gemiddeld kostte het de kiezers 15 minuten om te stemmen. De relatief lange stemduur is veroorzaakt doordat veel van de kiezers niet vertrouwd waren met het gebruik van een computer cq internet. Ook hier waren de gebruikte computers voorgeprogrammeerd met Java.
Ontwikkeling ten opzichte van de rapportage van april 2004	Geen.

EU	E-VOTE
Doel van het project	Het programma heeft tot doel het ontwerpen, implementeren en valideren van een op internet gebaseerd elektronisch kiessysteem. Hierbij moet worden gedacht aan het uitreiken van het stembiljet, specificatie van de stemdistricten, registratie van de kiezers en het tellen van de stemmen. Er zal gebruik worden gemaakt van Web browsers en mobiele telefoons met WAP.
Status van de voornemens	In ontwikkeling
Wet en regelgeving	nvt
Planning	Er wordt gewerkt aan de oplevering van verscheidene documenten zoals systeemdocumentatie en resultaten van de demonstratie.
Status van Proeven/experimenten	Een tweede prototype is in april 2003 beproefd door studenten en medewerkers van de universiteit van Regensburg (Duitsland) en de universiteit van Aegean (Griekenland), door de bouwers van het systeem, juristen, studenten en burgers van de gemeente Amaroussion.
Ontwikkeling ten opzichte van de rapportage van april 2004	Geen.

EU	TRUE-VOTE
Doel van het project	Het programma beoogt onderzoek te doen naar stemmen via Internet (van huis uit of via een kiosk) met behulp van een smartcard met een elektronische handtekening. De pilots zijn voorzien in Italië, het Verenigd Koninkrijk en Frankrijk met elk maximaal 500 deelnemers. De deelnemers aan de pilots stemmen in totaal drie keer (november 2002, januari 2003 en februari 2003). Naast de normale evaluatie zal er ook gekeken worden naar de sociale aspecten. De Universiteit van Amsterdam is partner in dit programma en doet in dat kader onderzoek naar de sociologische aspecten van stemmen via Internet.
Status van de voornemens	nvt
Wet en regelgeving	nvt
Planning	Er wordt gewerkt aan een evaluatie.
Status van Proeven/experimenten	-December 2002: volksraadpleging in Milaan (Italië) waar 190 kiezers stemden vanuit huis; -December 2002: raadpleging van een Italiaanse vakbond in Lombardije (Italië) waar 326 kiezers via elektronische stemmachines hebben gestemd; -December 2002- Januari 2003: schaduwverkiezing in Upper North Karelia (Finland) waar 310 kiezers van huis uit hebben gestemd; -Januari 2003: lokaal referendum in Newham (VK) waar 83 kiezers hebben gestemd via elektronische stemmachines in stemlokalen. -Februari 2003: schaduwverkiezing in Upper North Karelia (Finland) waar 400 kiezers van huis uit hebben gestemd; -Februari 2003: volksraadpleging in Milaan (Italië) waar 3003 van huis uit hebben gestemd of via een kiosk; - Februari 2003: stemming in Orsay (Frankrijk) waar 926 kiezers hun stem via een kiosk konden uitbrengen; - Maart 2003: volksraadpleging in Milaan (Italië) waar 357 kiezers hun stem via een kiosk konden uitbrengen;
Ontwikkeling ten opzichte van de rapportage van april 2004	Geen.

H. 5 Lidstaten van de Raad van Europa (niet behorende tot de Europese Unie)

Land	*IJSLAND*
Kiesstelsel	Lijst evenredige vertegenwoordiging
Toegestane vorm van stemmen	Stemlokaal (papieren stembiljetten) en briefstemmen
Voornemens omtrent KOA	Invoeren van elektronisch stemmen, in eerste instantie door middel van PC's in stemlokalen. Na invoering hiervan zou stemmen via internet vanuit huis een optie kunnen zijn.
Status van de voornemens	Een ambtelijke projectgroep van het ministerie van Justitie heeft een experiment voor het voorjaar van 2002 voorbereid. Het experiment is echter niet uitgevoerd, omdat de voor het experiment noodzakelijke regelgeving niet door het parlement is aanvaard.
Wet en regelgeving	Wet- en regelgeving is niet aangepast.
Planning	De regering heeft de Kieswet nog niet aangepast.
Status van Proeven/experimenten	De ontwikkelde technieken van de ambtelijke projectgroep worden nu ingezet bij niet-bindende verkiezingen en opiniepeilingen.
Ontwikkeling ten opzichte van de rapportage van april 2004	Geen.

Land	*NOORWEGEN*
Kiesstelsel	Lijst evenredige vertegenwoordiging
Toegestane vorm van stemmen	Stemmen in een stemlokaal (papieren stembiljetten); briefstemmen en early voting.
Voornemens omtrent KOA	Geen.
Andere voornemens	Noorwegen overweegt om elektronisch stemmen in een stemlokaal in te voeren. Naar aanleiding van experimenten in 2003 en de uitkomsten van de evaluatie daarvan is een commissie ingesteld, die onderzoekt of elektronisch stemmen in een stemlokaal landelijk zou kunnen worden ingevoerd.
Status van de voornemens	De verwachting is dat de ingestelde commissie in december 2005 rapport zal uitbrengen. Tot die tijd zullen er geen verdere experimenten worden gehouden.
Wet en regelgeving	De Kieswet is recent aangepast en staat experimenten met elektronisch stemmen in een stemlokaal toe.
Planning	nvt
Status van Proeven/experimenten	Het ministerie van Justitie heeft drie experimenten gehouden met elektronisch stemmen in een stemlokaal. De kiezers in drie gemeenten, de gemeenten Bykle, Larvik en Oppdal, hadden tijdens de lokale verkiezingen van 15 september 2003 de keuze om te stemmen met een papieren stembiljet of via een stemcomputer. Het evaluatierapport is afgerond in februari 2004. Het rapport roept op tot verder onderzoek over de beveiligingsaspecten van elektronisch stemmen, de kosten en de benodigde administratie.
Ontwikkeling ten opzichte van de rapportage van april 2004	Geen

Land	*ROEMENIE*
Kiesstelsel	Lijst evenredige vertegenwoordiging
Toegestane vorm van stemmen	Stemlokaal (papieren stembiljetten)
Voornemens omtrent KOA	Stemmen via internet bij nationale en lokale referenda. De kiezer zal worden geïdentificeerd dmv een gebruikerscode, een paswoord en een elektronisch certificaat.
Status van de voornemens	Onbekend
Wet en regelgeving	De wetgeving is nog niet aangepast.
Planning	Onbekend.
Status van Proeven/experimenten	Tijdens een nationaal referendum (oktober 2003) is er een pilot gehouden met internetstemmen voor soldaten en politieagenten die buiten Roemenië gestationeerd waren. 1623 personen hebben deelgenomen aan de pilot.
Ontwikkeling ten opzichte van de rapportage van april 2004	Geen

Land	*ZWITSERLAND*
Kiesstelsel	Lijst evenredige vertegenwoordiging
Toegestane vorm van stemmen	Stemlokaal (papieren stembiljetten); briefstemmen
Voornemens omtrent KOA	Invoeren van internetstemmen met als doel de opkomst te verhogen.
Status van de voornemens	De regering zal in samenwerking met de Kantons Genève, Neuchâtel en Zürich een aantal pilots houden met elektronisch stemmen op afstand.
Wet en regelgeving	Er is een wetsvoorstel aangenomen zodat de kantons Genève, Zürich en Neuchâtel experimenten kunnen houden met elektronisch stemmen op afstand bij verkiezingen, referenda en volksinitiatieven. Deze wet is op 1 januari 2003 in werking getreden.
Planning	De verwachting is dat in 2005 de pilots met internetstemmen worden geëvalueerd. Aansluitend zou de Zwitserse regering in de periode 2006-2007 een parlementaire beslissing moeten nemen over de introductie van internetstemmen. Indien de regering positief beslist zal de wetgeving worden aangepast.
Status van Proeven/experimenten	**Genève** In januari 2003 werd in Anières (1200 stemgerechtigden) tijdens een lokaal referendum een experiment gehouden met stemmen via internet. In november 2003 werd in Cologny (2600 stemgerechtigden) tijdens een lokaal referendum een experiment gehouden met stemmen via internet. In april 2004 konden in Carouge ca 9.000 kiesgerechtigden tijdens een lokaal referendum hun stem via internet, in een stemlokaal of als briefstem uitbrengen. 3.978 mensen hebben hun stem uitgebracht, waarvan 1.024 via internet hebben gestemd. **Neuchâtel** In Neuchâtel is in het voorjaar van 2003 het kiezersregister van 62 gemeenten gecentraliseerd. Tussen juni en december 2003 werd de software getest en werd een audit uitgevoerd. In de zomer van 2004 zullen gebruikerstesten met elektronisch kiezen op afstand worden gehouden. **Zürich** In Zürich wordt een elektronisch kiezersregister gebouwd. In april 2003 is hiermee begonnen. De testfase is nog niet afgerond. Deze is eind 2003 begonnen.

	Op 26 september 2004 zal tijdens een nationaal referendum in vier gemeenten (Carouge, Cologny, Anières & Meyrin) een experiment met internetstemmen worden gehouden. Zwitserland wil hiermee een volgende stap maken met het landelijk invoeren van internetstemmen. Tot nu toe betroffen de experimenten lokale referenda. De verwachting is dat in 2005 de pilots met internetstemmen worden geëvalueerd. Aansluitend in de periode 2006-2007 een parlementaire beslissing genomen worden over de introductie van internetstemmen.
Ontwikkeling ten opzichte van de rapportage van april 2004	Experiment in Carouge (Genève). Voorgenomen proef in Carouge, Cologny, Anières & Meyrin.

Hoofdstuk 6 Overige landen

Land	*AUSTRALIE*
Kiesstelsel	Meervoudig meerderheidssysteem op basis van preferente stemmen
Toegestane vorm van stemmen	Stemlokaal (papieren stembiljetten); briefstemmen en early voting
Voornemens omtrent KOA	Er is een discussie gaande over het invoeren van internetstemmen. De Australische Electoral Commission (AEC) beveelt aan, mede naar aanleiding van de experimenten die in het Verenigd Koninkrijk zijn gehouden, dat er proeven gehouden worden. Het Comité van het Australische Parlement dat zich bezig houdt met de verkiezingen heeft (na onderzoek te doen naar de uitkomsten van de pilots die in 2001 in Australië zijn gehouden) besloten de mening van de AEC niet over te nemen. Het Comité vindt dat er een gedetailleerd implementatie-plan nodig is, voordat er wordt overgegaan tot het houden van pilots met elektronisch stemmen op afstand.
Status van de voornemens	Op het gebied van KOA worden er geen pilots voorzien. In 2001 zijn door de 'Australian Capital Authority' experimenten gehouden met het gebruik van stemcomputers in stemlokalen.
Wet en regelgeving	Twee staten (Australian Capital Territory en Victoria) hebben hun Kieswet gewijzigd zodat elektronisch stemmen in een stemlokaal is toegestaan.
Planning	Op het ogenblik wordt gewerkt aan de ontwikkeling van standaarden voor de evaluatie van elektronisch stemmen. De verwachting is dat dit medio 2004 zal zijn afgerond.
Status van Proeven/experimenten	Er worden nog geen pilots voorzien.
Ontwikkeling ten opzichte van de rapportage van april 2004	Geen.

Land	*NIEUW ZEELAND*
Kiesstelsel	Evenredige vertegenwoordiging en een meerderheidsstelsel
Toegestane vorm van stemmen	Stemlokaal (papieren stembiljetten) en briefstemmen
Voornemens omtrent KOA	1. Faciliteren via internet. 2. Stemmen via internet.
Status van de voornemens	1. Bij de verkiezing in juli 2002 konden de kiezers in het buitenland het stembiljet downloaden van het internet. Het ingevulde stembiljet kon per post of per fax teruggezonden worden. De opkomst van kiezers uit het buitenland is met 40% gestegen. 2. In 2003 is onderzoek gedaan naar het houden van een pilot met internetstemmen, telefoonstemmen en interactieve televisie bij de nationale verkiezing in 2005. Dit is niet haalbaar gebleken. In plaats daarvan wordt geprobeerd om een pilot op te zetten bij de verkiezingen in 2008.
Wet en regelgeving	Dit proces is nog niet in gang gezet.
Planning	Onbekend.
Status van Proeven/experimenten Ontwikkeling ten opzichte van de rapportage van april 2004	Geen.

Land	*CANADA*
Kiesstelsel	First past the Post system
Toegestane vorm van stemmen	Stemlokaal (papieren stembiljetten); briefstemmen en early voting.
Voornemens omtrent KOA	Geen
Andere voornemens	Er is een elektronisch Nationaal Kiezersbestand gevormd. Op nationaal niveau wordt in dit bestand bijgehouden wie kiesgerechtigd is. Gemeenten en provincies kunnen het bestand inzien, maar kunnen zelf niet in het bestand muteren. Gemeenten en provincies gebruiken het bestand veelal om hun eigen kiezersbestand actueel te houden. Er is een onderzoek gedaan naar de uitvoerbaarheid van de ontwikkeling en invoering van online kiezersregistratie. Dit wordt mogelijk geacht.
Status van de voornemens	Het Elections Committee is bezig met de voorbereidingen van een eenvoudige versie van een online kiezersregistratie. Dit zou gereed moeten zijn voor de volgende nationale verkiezing (uiterlijke datum, november 2005). Na deze verkiezing volgt een evaluatie.
Wet en regelgeving	Volgens de Kieswet is elektronisch stemmen niet mogelijk. De wet geeft wel ruimte om pilots te houden met alternatieve vormen van stemmen bij tussentijdse verkiezingen en nationale verkiezingen. Experimenten mogen echter alleen worden gehouden als de commissie van de House of Commons die belast is met verkiezingen, het betreffende experiment heeft goedgekeurd.
Planning	Voor de volgende nationale verkiezing (uiterlijk november 2005) dient er een online kiezersregister te zijn.
Status van Proeven/experimenten	Tijdens gemeenteverkiezingen is in de staat Ontario (november 2003) een pilot gehouden met internet- en telefoonstemmen.
Ontwikkeling ten opzichte van de rapportage van april 2004	Geen.

Land	*VERENIGDE STATEN*
Kiesstelsel	First past the Post systeem
Toegestane vorm van stemmen	Stemlokaal (papieren stembiljetten, punchcards, hefboom machines, elektronische machines); briefstemmen en early voting.
Voornemens omtrent KOA	Zowel op het niveau van de federale regering als op het niveau van de Staten zijn er voornemens voor elektronisch stemmen (al dan niet buiten stemlokalen).
Status van de voornemens	Bij de presidentsverkiezingen in november 2004 worden door verschillende Staten stemmachines (in stemlokalen) gebruikt. Gepoogd wordt hiermee de problemen van de verkiezing in 2000 te voorkomen. Het voornemen om kiezers die in het buitenland verblijven per internet te laten stemmen is ingetrokken.
Wet en regelgeving	Het wetsvoorstel van de Federale regering "Help America Vote Act of 2002" is eind 2002 aangenomen. De staten die deelnemen aan SERVE hebben zelf via hun eigen wetgeving de mogelijkheid geboden om te experimenteren met andere vormen van stemmen.
Planning	Op 1 januari 2007 moet de "Help America Vote Act of 2002" zijn uitgevoerd.
Status van Proeven/experimenten	In maart 2000 kon bij een voorverkiezing voor de Democratische presidentskandidaat in Arizona via internet worden gestemd. In november 2000 is er een experiment gehouden waar militairen via internet konden stemmen. 84 militairen hebben geparticipeerd. Het ministerie van Defensie heeft begin februari 2004 besloten om af te zien van een experiment (Secure Electronic Registration and Voting Experiment) met online registratie en internetstemmen voor kiezers in het buitenland. van een bij de presidentsverkiezingen in november 2004. Aanleiding voor dit besluit was een rapport van deskundigen waarin de betrouwbaarheid van het stemmen per internet in twijfel werd getrokken.
Ontwikkeling ten opzichte van de rapportage van april 2004	Geen.

Bijlage 1 Opzet van de inventarisatie

De landen zijn op dezelfde wijze geïnventariseerd als de vorige rapportages. Het gaat in de eerste plaats om de vergelijkbaarheid van de verschillende soorten verkiezingen in de onderzochte landen. Zo kan men bijvoorbeeld denken aan de vraag of een Zwitsers referendum vergelijkbaar is met een referendum in het Verenigd Koninkrijk. Het tweede referentiekader betreft een stramien waarmee de politiek-bestuurlijke status van KOA in een land geobjectiveerd in beeld kan worden gebracht. Daarbij gaat het om vragen over de vergelijkbaarheid van de status en betekenis van bijvoorbeeld beleidsnotities in verschillende landen. Het derde en laatste referentiekader betreft de wijze waarop in een land elektronisch kiezen op afstand als project wordt aangepakt. Daarbij gaat het bijvoorbeeld om de vraag in hoeverre plannen om te komen tot een bepaalde mogelijke bouwsteen zoals een landelijke raadpleegbaar kiezersregister, vergelijkbaar kunnen zijn.

De werkwijze om de landen te inventariseren is dezelfde als in de vorige rapportage. Er is gebruik gemaakt van berichten uit de media, schriftelijke correspondentie op ambtelijk niveau en er is informatie ingewonnen door werkbezoeken te brengen aan landen en aan congressen. Daarnaast zijn er vele (Internet-) publicaties geraadpleegd. Een andere bron wordt gevormd door de bijeenkomsten van de ad hoc werkgroep elektronisch stemmen van de Raad van Europa.

Bijlage 2 Kiesstelsels

- Lijst evenredige vertegenwoordiging:

Het aandeel van de stemmen van een partij bij nationale verkiezingen is ook het aandeel in de zetels die een partij krijgt.

- Evenredige vertegenwoordiging en een meerderheidsstelsel:

Er wordt één stem uitgebracht op een politieke partij en er wordt één stem uitgebracht op een kandidaat van het kiesdistrict waar de kiezer woont.

- Meerderheidsstelsel met twee ronden:

Verkiezingen waar de winnende kandidaat ernaar streeft om een absolute meerderheid van de stemmen te werven. Wordt dit niet in de eerste ronde behaald, dan wordt een tweede ronde gehouden.

- Een meerderheidsstelsel met preferente stemmen:

Kiezers worden gevraagd de kandidaten op het stembiljet te nummeren in de volgorde waarin zij aan hen de voorkeur geven. Als een kandidaat een absolute meerderheid van eerste voorkeuren verkrijgt, is hij verkozen.

- First Past the Post systeem:

De kandidaat die de meeste stemmen verwerft, wordt gekozen verklaard.

- Parallel meerderheidsstelsel met twee ronden:

Een semi-meerderheidssysteem waarin meervoudige representatie wordt gebruikt in combinatie met een districtensysteem. Vervolgens streeft de winnende kandidaat ernaar om een absolute meerderheid van de stemmen te werven. Wordt dit niet in de eerste ronde behaald, dan wordt een tweede ronde gehouden.

- Lijst van evenredige vertegenwoordiging op basis van preferente stemmen:

Personenstelsel met districten waar meerdere kandidaten gekozen kunnen worden en waar kiezers hun voorkeuren uitbrengen op kandidaten. Wil een kandidaat worden gekozen, dan dient hij een kiesdrempel (quotum van eerste voorkeur stemmen) te halen.

- Meervoudig meerderheidssysteem op basis van preferente stemmen:

Een meervoudig meerderheidssysteem met districten waar één kandidaat kan worden gekozen. Kiezers geven hun voorkeur van de kandidaten aan. Een kandidaat die 50% van de eerste voorkeuren ontvangt, is gekozen.

Bijlage 3: Tekst Recommendation Raad van Europa

COUNCIL OF EUROPE
COMMITTEE OF MINISTERS

Recommendation Rec(2004)11
of the Committee of Ministers to member states on legal, operational and technical standards for e-voting

(Adopted by the Committee of Ministers on 30 September 2004 at the 898th meeting of the Ministers' Deputies)

The Committee of Ministers, under the terms of Article 15.*b* of the Statute of the Council of Europe,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members for the purpose of safeguarding and promoting the ideals and principles, which are their common heritage;

Reaffirming its belief that representative and direct democracy are part of that common heritage and are the basis of the participation of citizens in political life at the level of the European Union and at national, regional and local levels;

Respecting the obligations and commitments as undertaken within existing international instruments and documents, such as:

– the Universal Declaration on Human Rights;
– the International Covenant on Civil and Political Rights;
– the United Nations Convention on the Elimination of All Forms of Racial Discrimination;
– the United Nations Convention on the Elimination of All Forms of Discrimination against Women;
– the Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 5), in particular its Protocol No. 1 (ETS No. 9);
– the European Charter of Local Self-Government (ETS No. 122);
– the Convention on Cybercrime (ETS No. 185);
– the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108);
– Committee of Ministers Recommendation No. R (99) 5 on the protection of privacy on the Internet;
– the document of the Copenhagen Meeting of the Conference on the Human Dimension of the OSCE;
– the Charter of Fundamental Rights of the European Union;
– the Code of Good Practice in Electoral Matters, adopted by the Council for democratic elections of the Council of Europe and the European Commission for Democracy through Law;

Bearing in mind that the right to vote is one of the primary foundations of democracy, and that, consequently, e-voting system procedures shall comply with the principles of democratic elections and referendums;

Recognising that as new information and communication technologies are increasingly being used in day-to-day life, member states need to take account of these developments in their democratic practice;

Noting that participation in elections and referendums at local, regional and national levels in some member states is characterised by low, and in some cases steadily decreasing, turnouts;

Noting that some member states are already using, or are considering using e-voting for a number of purposes, including:

– enabling voters to cast their votes from a place other than the polling station in their voting district;
– facilitating the casting of the vote by the voter;
– facilitating the participation in elections and referendums of all those who are entitled to vote, and particularly of citizens residing or staying abroad;
– widening access to the voting process for voters with disabilities or those having other difficulties in being physically present at a polling station and using the devices available there;
– increasing voter turnout by providing additional voting channels;
– bringing voting in line with new developments in society and the increasing use of new technologies as a medium for communication and civic engagement in pursuit of democracy;
– reducing, over time, the overall cost to the electoral authorities of conducting an election or referendum;
– delivering voting results reliably and more quickly; and
– providing the electorate with a better service, by offering a variety of voting channels;

Aware of concerns about certain security and reliability problems possibly inherent in specific e-voting systems;

Conscious, therefore, that only those e-voting systems which are secure, reliable, efficient, technically robust, open to independent verification and easily accessible to voters will build the public confidence which is a pre-requisite for holding e-voting,

Recommends that the governments of member states, where they are already using, or are considering using, e-voting comply, subject to paragraph iv. below, with paragraphs i. to iii. below, and the standards and requirements on the legal, operational and technical aspects of e-voting, as set out in the Appendices to the present Recommendation:

i. e-voting shall respect all the principles of democratic elections and referendums. E-voting shall be as reliable and secure as democratic elections and referendums which do not involve the use of electronic means. This general principle encompasses all electoral matters, whether mentioned or not in the Appendices;

ii. the interconnection between the legal, operational and technical aspects of e-voting, as set out in the Appendices, has to be taken into account when applying the Recommendation;

iii. member states should consider reviewing their relevant domestic legislation in the light of this Recommendation;

iv. the principles and provisions contained in the Appendices to this Recommendation do not, however, require individual member states to change their own domestic voting procedures which may exist at the time of the adoption of this Recommendation, and which can be maintained by those member states when e-voting is used, as long as these domestic voting procedures comply with all the principles of democratic elections and referendums;

v. in order to provide the Council of Europe with a basis for possible further action on e-voting within two years after the adoption of this Recommendation, the Committee of Ministers recommends that member states:

– keep under review their policy on, and experience of, e-voting, and in particular the implementation of the provisions of this Recommendation; and
– report to the Council of Europe Secretariat the results of their reviews, who will forward them to member states and follow up the issue of e-voting.

In this Recommendation the following terms are used with the following meanings:

– authentication: the provision of assurance of the claimed identity of a person or data;
– ballot: the legally recognised means by which the voter can express his or her choice of voting option;
– candidate: a voting option consisting of a person and/or a group of persons and/or a political party;
– casting of the vote: entering the vote in the ballot box;

– e-election or e-referendum: a political election or referendum in which electronic means are used in one or more stages;
– electronic ballot box: the electronic means by which the votes are stored pending being counted;
– e-voting: an e-election or e-referendum that involves the use of electronic means in at least the casting of the vote;
– remote e-voting: e-voting where the casting of the vote is done by a device not controlled by an election official;
– sealing: protecting information so that it cannot be used or interpreted without the help of other information or means available only to specific persons or authorities;
– vote: the expression of the choice of voting option;
– voter: a person who is entitled to cast a vote in a particular election or referendum;
– voting channel: the way by which the voter can cast a vote;
– voting options: the range of possibilities from which a choice can be made through the casting of the vote in an election or referendum;
– voters' register: a list of persons entitled to vote (electors).

Appendix I

Legal standards

A. Principles

I. Universal suffrage

1. The voter interface of an e-voting system shall be understandable and easily usable.

2. Possible registration requirements for e-voting shall not pose an impediment to the voter participating in e-voting.

3. E-voting systems shall be designed, as far as it is practicable, to maximise the opportunities that such systems can provide for persons with disabilities.

4. Unless channels of remote e-voting are universally accessible, they shall be only an additional and optional means of voting.

II. 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 authorised to vote only if it has been established that his/her ballot has not yet been inserted into the ballot box.

6. The e-voting system shall prevent any voter from casting a vote by more than one voting 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.

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.

III. Free suffrage

9. The organisation of e-voting shall secure the free formation and expression of the voter's opinion and, where required, the personal exercise of the right to vote.

10. The way in which voters are guided through the e-voting process shall be such as to prevent their voting precipitately or without reflection.

11. Voters shall be able to alter their choice at any point in the e-voting process before casting their vote, or to break off the procedure, without their previous choices being recorded or made available to any other person.

12. The e-voting system shall not permit any manipulative influence to be exercised over the voter during the voting.

13. The e-voting 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.

14. The e-voting system shall indicate clearly to the voter when the vote has been cast successfully and when the whole voting procedure has been completed.

15. The e-voting system shall prevent the changing of a vote once that vote has been cast.

IV. Secret suffrage

16. E-voting shall be organised 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.

17. The e-voting 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.

18. The e-voting 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.

19. Measures shall be taken to ensure that the information needed during electronic processing cannot be used to breach the secrecy of the vote.

B. Procedural safeguards

I. Transparency

20. Member states shall take steps to ensure that voters understand and have confidence in the e-voting system in use.

21. Information on the functioning of an e-voting system shall be made publicly available.

22. Voters shall be provided with an opportunity to practise any new method of e-voting before, and separately from, the moment of casting an electronic vote.

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.

II. Verifiability and accountability

24. The components of the e-voting system shall be disclosed, at least to the competent electoral authorities, as required for verification and certification purposes.

25. Before any e-voting 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 e-voting system is working correctly and that all the necessary security measures have been taken.

26. There shall be the possibility for a recount. Other features of the e-voting system that may influence the correctness of the results shall be verifiable.

27. The e-voting system shall not prevent the partial or complete re-run of an election or a referendum.

III. Reliability and security

28. The member state's authorities shall ensure the reliability and security of the e-voting system.

29. All possible steps shall be taken to avoid the possibility of fraud or unauthorised intervention affecting the system during the whole voting process.

30. The e-voting system shall contain measures to preserve the availability of its services during the e-voting process. It shall resist, in particular, malfunction, breakdowns or denial of service attacks.

31. Before any e-election or e-referendum takes place, the competent electoral authority shall satisfy itself that the e-voting system is genuine and operates correctly.

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.

33. While an electronic ballot box is open, any authorised 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.

34. The e-voting 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.

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.

Appendix II

Operational standards

I. 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.

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 e-voting, the period shall be defined and made known to the public well in advance of the start of 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 e-voting will be organised, and any steps a voter may have to take in order to participate and vote.

II. 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/her on the register, and request corrections.

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 e-voting, shall be considered. If participation in e-voting requires a separate application by the voter and/or additional steps, an electronic, and, where possible, interactive procedure shall be considered.

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.

III. Candidates

42. The possibility of introducing online candidate nomination may be considered.

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

IV. Voting

44. It is particularly important, where remote e-voting takes place while polling stations are open, that the system shall be so designed that it prevents any voter from voting more than once.

45. Remote e-voting may start and/or end at an earlier time than the opening of any polling station. Remote e-voting shall not continue after the end of the voting period at polling stations.

46. For every e-voting channel, support and guidance arrangements on voting procedures shall be set up for, and be available to, the voter. In the case of remote e-voting, such arrangements shall also be available through a different, widely available communication channel.

47. There shall be equality in the manner of presentation of all voting options on the device used for casting an electronic vote.

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 e-voting system shall avoid the display of other messages that may influence the voters' choice.

49. If it is decided that information about voting options will be accessible from the e-voting site, this information shall be presented with equality.

50. Before casting a vote using a remote e-voting 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.

51. A remote e-voting system shall not enable the voter to be in possession of a proof of the content of the vote cast.

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.

V. Results

53. The e-voting 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.

54. The e-voting system shall prevent processing information on votes cast within deliberately chosen sub-units that could reveal individual voters' choices.

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.

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.

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.

58. In the event of any irregularity affecting the integrity of votes, the affected votes shall be recorded as such.

VI. Audit

59. The e-voting system shall be auditable.

60. The conclusions drawn from the audit process shall be applied in future elections and referendums.

Appendix III

Technical requirements

The design of an e-voting system shall be underpinned by a comprehensive assessment of the risks involved in the successful completion of the particular election or referendum. The e-voting system shall include the appropriate safeguards, based on this risk assessment, to manage the specific risks identified. Service failure or service degradation shall be kept within pre-defined limits.

A. 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 alternative ways of voting.

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.

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).

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.

65. The presentation of the voting options shall be optimised for the voter.

B. 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.

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 Council of Europe website.

68. In cases which imply specific election or referendum data requirements, a localisation 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.

C. Systems operation
(for the central infrastructure and clients in controlled environments)

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.

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.

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.

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.

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.

74. All technical operations shall be subject to a formal control procedure. Any substantial changes to key equipment shall be notified.

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.

76. Where incidents that could threaten the integrity of the system occur, those responsible for operating the 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.

D. Security

I. General requirements

(referring to pre-voting, voting, and post-voting stages)

77. Technical and organisational 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.

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.

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.

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.

81. The e-voting system shall protect authentication data so that unauthorised 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.

82. Identification of voters and candidates in a way that they can unmistakably be distinguished from other persons (unique identification) shall be ensured.

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.

84. The e-voting system shall maintain reliable synchronised 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 maintaining the time limits for registration, nomination, voting, or counting.

85. Electoral authorities have overall responsibility for compliance with these security requirements, which shall be assessed by independent bodies.

II. Requirements in pre-voting stages

(and for data communicated to the voting stage)

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.

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.

88. The fact that voter registration has happened within the prescribed time limits shall be ascertainable.

III. Requirements in the voting stage
(and for data communicated during post-election stages)

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.

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.

91. The fact that a vote has been cast within the prescribed time limits shall be ascertainable.

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.

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.

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.

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.

96. After the end of the e-voting period, no voter shall be allowed to gain access to the e-voting system. 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.

IV. Requirements in post-voting stages

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.

98. The counting process shall accurately count the votes. The counting of votes shall be reproducible.

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.

E. Audit

I. 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.

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.

II. Recording

102. The audit system shall be open and comprehensive, and actively report on potential issues and threats.

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.

III. 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.

105. Disclosure of the audit information to unauthorised persons shall be prevented.

106. The audit system shall maintain voter anonymity at all times.

IV. 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.

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.

V. Other

109. The audit system shall be protected against attacks which may corrupt, alter or lose records in the audit system.

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.

F. 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.

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 (EA), the International Laboratory Accreditation Cooperation (ILAC), the International Accreditation Forum (IAF) and other bodies of a similar nature.

Bijlage 4: Toelichtend Memorandum

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Integrated Project 1
Projet Intégré 1

MAKING DEMOCRATIC INSTITUTIONS WORK
LES INSTITUTIONS DEMOCRATIQUES EN ACTION

IP1 (2004)41 Strasbourg, 22 July 2004

Draft

Explanatory memorandum

Recommendation No. R(2004)x of the Committee of Ministers to member states on legal, operational and technical standards for e-voting

Background

1. Common standards on e-voting, reflecting and applying the principles of democratic elections and referendums to the specificities of e-voting, are key to guaranteeing the respect of all the principles of democratic elections and referendums when using e-voting, and thus building trust and confidence in domestic e-voting schemes.

2. Such common standards are also important to deliver the inter-operability of e-voting systems in order to ensure the development of secure and effective e-voting systems. While inter-operability across borders in Europe may not seem necessary from a purely legal and operational point of view - at the time of adoption of the Recommendation there were no cross-border common electoral procedures in place (notwithstanding data exchange procedures with respect to a limited group within the electorate for the European Parliament) - inter-operable and open technical standards within and across member states borders can both assure the combined and continued use of e-voting systems from different providers and reduce procurement costs for domestic authorities.

3. This set of standards consists of legal, operational (which principally include organisational and procedural matters) and core technical requirements for e-voting. The legal standards are intended to apply the principles of existing Council of Europe and other international instruments in the field of elections to the case of e-voting.

4. The Recommendation has been developed by the Multidisciplinary Ad Hoc Group of Specialists on legal, operational and technical standards for e-voting (IP1-S-EE). This inter-governmental group of all member states was set up by the Committee of Ministers and was charged with developing a set of standards for e-voting, that reflect Council of Europe member states' differing circumstances, and should be followed by the ICT industry.

Scope of the recommendation

5. The Recommendation covers political elections and referendums. Both of them belong to the European democratic heritage and the need for standards in both cases is the same. Elections and referendums are held at different levels; in some countries no referendums are being held; in some countries not all the levels mentioned in the Recommendation are affected.

Reasons for introducing or considering the introduction of e-voting

6. The reasons for introducing or considering the introduction of e-voting in one or more stages of a political election or referendum can differ from country to country. In each country, the reasons depend on the specific domestic context.

Relation to member states competence

7. The competence of the member states of the Council of Europe in electoral matters and regarding referendums is not affected by this Recommendation. Where reference is made to the European Union level, the purpose is to include reference to elections to the European Parliament.

Principles of democratic elections and referendums

8. Democracy is inconceivable without elections and referendums held in accordance with certain principles that lend them their democratic status. In 2002, the European Commission for Democracy through Law (Venice Commission) adopted a non-binding Code of Good Practice in Electoral Matters[2] in which five such principles are identified as fundamental: universal, equal, free, secret and direct suffrage. These five principles reflect Europe's democratic heritage[3] and are equally applicable to e-elections and e-referendums as to those without any electronic means.

9. Although no generally agreed definitions of these principles exist, their meaning can for the purposes of this Explanatory Memorandum, be summarised as follows:

- *Universal suffrage:* all human beings have the right to vote and to stand for election subject to certain conditions, e.g., age and nationality.
- *Equal suffrage:* each voter has the same number of votes.
- *Free suffrage:* the voter has the right to form and to express his or her opinion in a free manner, without any coercion or undue influence.
- *Secret suffrage:* the voter has the right to vote secretly as an individual, and the state has the duty to protect that right.
- ***Direct suffrage:*** **the ballots cast by the voters directly determine the person(s) elected.**

10. Although these principles are generally accepted, their implementation in the context of e-voting raises a number of questions that call for close scrutiny. However, specificities of e-voting do not give rise to such questions to the same extent in relation to all of the five principles. Whereas for the principles of universal, equal, free and secret suffrage special provisions with regard to e-voting are necessary, the principle of direct suffrage does not call for special attention and is therefore not addressed in the Recommendation.

---

[2] Code of good practice in electoral matters:

(Venice Commission - Opinion 190/2002_el*)*, endorsed by Parliamentary Assembly resolution 1320(2003*)* and CLRAE Resolution 148 (2003), subject of a Declaration by the Committee of Ministers (114th session, 13 May 2004))

[3] - Point 7 of the Document of the Copenhagen Meeting of the Conference on the Human Dimension of the OSCE of 29 June 1990 clearly speaks of free, universal, equal and secret suffrage - point 6 of direct suffrage, albeit in a qualified form
- Article 25(b) of the International Covenant on Civil and Political Rights expressly provides for all these principles except direct suffrage, although the latter is implied (Article 21 of the Universal Declaration of Human Rights).
- Article 3 of the Additional Protocol to the European Convention on Human Rights explicitly provides for the right to periodic elections by free and secret suffrage; the other principles have also been recognised in human rights case law (Universality: ECHR No. 9267 or81, judgment in Mathieu-Mohin and Clerfayt vs. Belgium, 2 March 1997, Series A vol. 113, p. 23; judgment in Gitonas and others vs. Greece, 1 July 1997, No. 18747 or91, 19376 or92; 19379 or92, 28208 or95 and 27755 or95, Collected Judgments and Decisions, 1997-IV, p. 1233; re. Equality: Aforementioned judgment in Mathieu-Mohin and Clerfayt, p. 23.) The right to direct elections has been admitted by the Strasbourg Court implicitly (ECHR No. 24833 or94, judgment in Matthews vs. The United Kingdom, 18 February 1999, Collected Judgments and Decisions 1999-I, para. 64.)

11. The standards in the Recommendation address only those matters that are of specific relevance to e-voting. The general principles of democratic elections and referendums are not repeated.

Legal, operational and technical standards

12. Appendices I to III of the Recommendation contain a set of legal, operational and technical standards. This set consists of minimum standards, which, if followed in an e-voting system, would facilitate compliance with the principles of democratic elections and referendums. However, compliance with these standards alone does not guarantee the democratic quality of the e-election or e-referendum. The e-election or e-referendum has to be judged as a whole and in detail, in the specific context. But compliance with the standards is an important element in enhancing the democratic quality of the e-voting system.

13. There is a close interconnection between the three categories of standards which need to be taken into account when applying the Recommendation:

- **The legal standards relate to the legal context in which e-voting is permitted.**
- **The operational standards relate to the manner in which e-voting hardware and software should be operated and maintained.**
- **The technical requirements relate to the construction and operation of e-voting hardware and software. The adoption of the technical requirements will ensure the technical security, accessibility and inter-operability of e-voting systems.**

- **The three categories of standards all include provisions relating to all stages of elections and referendums, (i.e. the pre-voting stage, the actual casting of the vote, and the post-voting stage). The interconnection, referred to in 13 above can relate to one, two, or all stages.**

i. Introductory statement ("E-voting shall respect... ")

14. This introductory statement covers a number of issues that are of general relevance in relation to e-elections and e-referendums.

15. Existing non-electronic voting systems have been developed in a way that ensures that the principles required for democratic elections and referendums are met. It is essential that these principles are not undermined by the introduction of new voting methods and, accordingly, e-voting systems must be so designed and operated as to ensure the reliability and security of the voting process, just as is the case with the non-electronic voting systems in the state concerned.

16. In order to ensure that an e-voting system delivers an election or referendum that satisfies the overall principles, it may be necessary to give more attention to the application of one principle than to the application of another. However, the result must still be to ensure that overall the principles are met.

17. The comparison with the non-electronic voting system in the state concerned does not imply that e-voting has to be as secure and reliable as all the non-electronic voting channels together. The underpinning principle of the Recommendation is that a remote e-voting channel has to be – overall – as secure as an un-supervised remote non-electronic voting channel and a non-remote e-voting channel has to be as secure as a non-remote non-electronic voting channel.

18. Furthermore the comparison with non-electronic voting channels is not intended to prevent a state changing its non-electronic voting system, as long as the changes are in compliance with all the principles of democratic elections and referendums.

19. Comparing levels of reliability and security or other parameters at the time when e-voting is introduced, with levels of non-electronic voting methods is not intended to freeze the latter levels, in particular when improvements in implementing the principles of democratic elections and referendums are possible and necessary.

ii. Review of domestic legislation

20. The Recommendation indicates that member states should consider reviewing their relevant domestic legislation when introducing e-voting. Careful thought needs to be given to aspects of law other than those relating simply to the electronic equipment needed and its use. The extent of the review advisable will depend upon the existing laws of the member state in question and it is not possible to set these out in a comprehensive manner here. Examples are, criminal laws relating to elections matters, specific data protection laws and laws relating to election observation.

iii. Localisation

21. The purpose of this Recommendation is to provide for common standards on e-voting. In some states holding elections and referendums involves certain procedures which are very specific to the state concerned. Where such specific procedures are applicable only in one or a very small number of member states, those procedures were identified as "localisms" and therefore not included in the Recommendation, but referred to in the explanatory memorandum. States concerned can retain their "localisms" and, if they so wish, adapt them in the future and are not expected to abandon or change their "localisms" as a consequence of the Recommendation, as long as these are in compliance with the principles of democratic elections and referendums and any obligations and commitments undertaken by member states.

iv. Sustainability

22. E-voting is a new and rapidly developing area of policy and technology. Standards and requirements need to keep abreast of, and where possible anticipate new developments. In recognition of this, paragraph v. recommends that each member state keeps its own position on e-voting under review and reports back to the Council of Europe the results of any review that it has conducted. The Council may look again at this issue two years after the adoption of this Recommendation and member states may bear this timing in mind when deciding whether, and if so when, a review is appropriate in their particular circumstances.

23. As part of the follow up, a review of the Recommendation may be considered as soon as member states have gained further experience with e-elections or e-referendums.

24. Technological developments, unforeseeable at the time of the adoption of the Recommendation, cannot exclude that any system valid at that time, including EML, may one day not be the most appropriate system for e-elections or e-referendums, and thus not be recommended by individual or groups of countries.

Interpretation

25. The interpretation paragraph contains definitions of terms used throughout the Recommendation including its Appendices. The definitions should also be consulted when the Recommendation or parts of it are translated into other languages. In

Appendix 3 there is a separate technical glossary which contains additional definitions of terms used in that Appendix.

Definition of remote e-voting

26. E-voting can be conducted in remote and non-remote ways. Many electoral systems already include both non-remote and remote voting. Remote voting can be conducted in both supervised (e.g. voting at embassies or consulates, voting at post offices or municipal offices) and un-supervised (i.e. un-supervised by officials) environments (e.g. voting by mail). Each member state has its own established practice concerning the types of voting channels available to voters.[4] For the purpose of this Recommendation, however, remote e-voting means exclusively e-voting where the casting of the vote is done by a device not controlled by election officials.

Appendix I

Legal standards

I. Universal suffrage

Standard No. 1. "The voter interface of an e-voting system ... "

27. No single voting system may ever be understandable and usable by every possible voter; e.g. people with visual impairments may not be able to use a visual-only system. In order to ensure democratic elections and referendums, member states have to try to ensure that the voter interfaces of e-voting systems are useable and understandable by as many people as possible.

Standard No. 2. "Possible registration requirements for e-voting..."

28. The purpose of this provision is to ensure that no voter is prevented from using e -voting because of difficult registration procedures.

Standard No. 3. "E-Voting systems shall be designed... "

29. E-voting systems should be made accessible in so far as is possible and used in conjunction with other voting channels that together with the e-voting system provide accessibility for as many voters as possible. Not all persons with disabilities may be able to use e-voting. The design of the e-voting systems should, however, aim to maximise the potential of accessibility that these voting channels provide for disabled persons.

Standard No. 4. "Unless channels of remote e-voting are... "

30. Adding additional electronic voting channels to traditional forms of voting may make elections and referendums more accessible, strengthening the principle of universality. However, using a single remote electronic voting channel in isolation restricts accessibility. This provision is to protect the voter from a situation where the only means offered for voting is one that is not effectively available to him or her.

31. In the case of non-remote e-voting it has to be left to member states to decide whether they want to offer other options of voting. As is the case with all non-remote voting, places where voting takes place and the e-voting system should comply with standards of accessibility.

[4] The European Commission for Democracy through Law (Venice Commission) has provided a Report on the compatibility of remote voting and electronic voting with the requirements of the documents of the Council of Europe (Adopted by the Venice Commission at its 58th Plenary Session (Venice, 12-13 March 2004. Study no. 260, 2003, Strasbourg, 18 March 2004, CDL-AD (2004)012 Or. Fr.). The conclusion by the Venice commission is that remote voting is compatible with the Council of Europe's standards, provided that certain preventative measures are observed in the procedures for either postal voting or electronic voting.

II. Equal suffrage

Standard No. 5 & 6. "In relation to any election or referendum... " & "The e-voting system…"

32. The whole voting system should prevent multiple votes being cast by any one person. This principle is consistent with voting systems that allow voters to choose more than one option, such as systems that allow preferential votes, or one vote for a national list and one vote for a regional list. The concept of multiple votes relates to the risk that there might be an attempt to cast more votes than a particular voter has a right to cast. This might arise if the voter tried to cast multiple votes him or herself or if another person tried to use the voter's identity in order to vote in the voter's name and the voter also voted.

33. In some member states practices are in force where it may appear that a voter is allowed to vote more than once. However, in these systems the voter may cast only one vote that is finally counted. Examples of this include:

a) In the case of *Denmark and Sweden*, the voting systems provide the legal opportunity for voters to submit an advance vote and change it later. In Denmark, several advance votes may be submitted. In Sweden, only one advance vote may be submitted. In both systems only the last vote is inserted into the ballot box and thus is the vote cast.

b) In the case of the *UK,* if a person enters a polling station to vote and finds that somebody else has already voted in that person's name, that person is entitled to cast a special vote - a tendered ballot. This ballot is sealed in an envelope, is not placed in the ballot box, and is only looked at in the case of an election petition and in accordance with a direction of a court. A similar provision applies where two postal votes are received for the same voter.

Standard No. 7. "Every vote deposited... "

34. It is important that all votes cast by either electronic or non-electronic voting channels are counted.

III. Free suffrage

Standard No. 9. "The organisation of e-voting... "

35. Personal suffrage - the personal exercise of the right to vote - is a fundamental principle in many member states. As it is particularly vulnerable in the context of remote e-voting, special attention is drawn to this fact in the Recommendation. However, this standard does not prevent remote e-voting.

36. There are some member states that allow for voting procedures where, in order to ensure accessibility, the principle of universality is given priority over the principle of personal suffrage and therefore, for example, proxy voting is allowed. This is also possible within the e-voting standards.

37. Where remote e-voting channels are provided, special attention has to be given to the provision of facilities that allow the voter to exercise the right to cast a vote in a supervised environment.

Standard No. 10. "The way in which voters... "

38. "Without reflection" means without having had enough time to think about it.

Standard No. 11. "Voters shall be able... "

39. Only the voter must have access to the vote. For example, the e-voting facilities should not enable 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.

Standard No. 12. "The e-voting system shall not permit... "

40. The e-voting system should be designed and operated in a way that ensures that all kinds of manipulative influence are excluded. For example, sounds which can be associated with a candidate or an option, pop-up screens promoting a particular choice and similar devices should be prevented, as far as is possible.

Standard No. 13. "The e-voting system shall provide the voter... "

41. In non-electronic voting systems voters are able to cast a blank vote, i.e. not to express a preference for the proposed choices. This standard provides that the possibility of leaving the ballot blank has to be maintained with e-voting.

42. It is a matter for each member state's domestic policy whether the intended spoiling of a ballot paper or intentional casting of a non-blank invalid vote has to be possible with e-voting as well.

Standard No. 14. "The e-voting system shall indicate clearly... "

43. Generally speaking, the voting procedure is completed successfully when the electronic vote is deposited in the electronic ballot box. In the context of remote e-voting this means that the voting procedure is completed successfully only when the vote has been sent from the voter's voting device (PC, telephone, etc.), over the internet or another network and has reached its destination, i.e. the ballot box server.

44. The message confirms to the voter that his or her vote is deposited in the ballot box and thus will be counted. The voter then knows that he or she has cast his or her vote, which is important from the point of view of trusting the system and because of the principle that every vote

cast has to be taken into account. Furthermore, the voter must be able to know at what moment the whole voting procedure is completed successfully and he or she can safely break the connection. Both messages (the successful casting of the ballot and the completion of the procedure) could be combined in one, if both events coincide.

IV. Secret suffrage

45. All international obligations and commitments pertaining to secret suffrage that bind a member state, need to be implemented with any e-voting system used by that state.

Standard No. 16. "E-voting shall be organised in such a way... "

46. Secrecy must apply to the entire procedure: in the pre-voting stage (e.g. transmitting of PINs, or electronic tokens to voters), during the completion of the ballot paper, the casting and transmission of the ballot and during counting and any recounting of the votes.

Standard No. 17. "The e-voting system shall secure that votes... "

47. This standard provides that it must never be possible to reconstruct the content of any voter's vote and link it to the voter who cast it.

48. In the context of (remote) e-voting special attention has to be given to the principles of free and secret suffrage. Only entitled voters are allowed to cast a vote; which means that every voter has to be authenticated and his/her right to vote has to be checked. Domestic legislation may vary on the extent of identification (indication of the voter's name, showing of an ID-Card etc.), but the basic principle remains the same: in order to prevent multiple votes being cast or other misuse, the voter has to be authenticated and a record must be made and checked in order to establish whether he or she has already cast a vote.

49. At a certain stage in the remote voting process the voter's identity and the voter's vote may be somehow connected. If the content of the vote were to be made known at that stage - or if the connection between voter and vote were to be kept and the content of the vote made known at a later stage, the secrecy of the vote would be breached. In traditional voting systems the separation of voter identification and vote is made by physical separation. This physical separation can easily be controlled by election officials and election observers. In non-remote e-voting processes the voter authentication and the vote could also be separated physically, as is the case if the e-voting system is used only for the casting of the vote. With a remote electronic voting system this separation has to be made electronically. The electronic separation requires specific technical solutions. This fact has to be taken into account when introducing e-voting.

50. In voting systems that provide a legal opportunity for the voters to submit an advance vote and change it later (e.g. Sweden), it must be possible to identify a specific person's sealed vote to be able to retract that specific vote. The identification and retraction of such a vote must be done without jeopardizing the secrecy of the vote, i.e. a vote must be completely sealed throughout the voting, storage and retraction processes. But the sealed vote must still be linked to a specific voter.

51. The moment of inserting a vote into the electronic ballot box is the latest point in time at which the vote has to be finally separated from the information on who has cast it – without any possibility of ever reconstructing this link.

52. In some cases domestic law requires a permanent link between the voter and the vote to exist and to be maintained during the election or referendum and for a specific

period thereafter (e.g. UK). In such cases, it has to be assured that the link between a voter and his or her ballot paper is sufficiently protected throughout the period in order to ensure the secrecy of the vote. This is only revealed pursuant to an order of a competent judicial authority and it must be ensured, that even where the link is so revealed, no voter is compelled to reveal how he or she has voted.

Standard No. 19. "Measures shall be taken to ensure..."

53. The necessary measures would include, for example, that the votes cast must be stored randomly in the electronic ballot box. The order in which they are stored must not make it possible to reconstruct the order in which they arrived.

Procedural safeguards

54. The procedural safeguards ensure that all principles of democratic elections and referendums are implemented and maintained in an e-voting context.

I. Transparency

Standard No. 20. "Member states shall take steps to ensure that... "

55. Confidence by voters and candidates in the voting system(s) used is essential, not only to participation but also to the democratic system of the member state. Full understanding of the e-voting system(s) in use is the basis for this confidence.

56. Traditional voting methods are simple and well tried and tested in member states. Voters are familiar with voting systems using ballot papers and ballot boxes and understand the general rules that govern how they should vote and how their vote is collected and counted unaltered. The introduction of e-voting produces a new situation in which voters will be less familiar with the electoral process and perhaps less able to understand the safeguards built into the e-voting system. Accordingly, as e-voting systems are introduced, it is likely that, in order to maintain voter understanding and confidence, steps will have to be taken to introduce the system to voters. Over time, it may be necessary to continue to take such steps in order to secure the understanding and confidence of voters who are unfamiliar with e-voting.

57. Confidence can be enhanced by providing voters with as much information as possible about the method of e-voting being used.

Standard No. 22. "Voters shall be provided with an opportunity to practise... "

58. Any (new) e-voting system may cause voters anxieties of different kinds. In order to promote understanding and confidence in any (new) e-voting system, including its transparency, opportunities to practice any (new) e-voting system should be provided before and separately from the moment of casting an electronic vote. Special attention should be paid to any voters who are not familiar with the (new) e-voting method, e.g. the elderly.

Standard No. 23. "Any observers, to the extent permitted by law... "

59. There are various international and domestic obligations on election observation: by representatives of candidates, as well as by independent domestic and/or international observers. All member states are bound to the commitments of the *Document of the Copenhagen Meeting of the Conference on the Human Dimension of the OSCE* of 29 June 1990 to "invite observers from any other OSCE participating state and any appropriate private institution and organisation who may wish to do so to observe the course of their national election proceedings [… and …] facilitate similar access for election proceedings held below the national level."

60. Observers should be able to verify that the e-voting system itself is designed and operated in a way which respects the fundamental principles of democratic elections and referendums. Therefore, member states should have clear legal provisions on observers' access to the e-voting system documentation and audit data.

61. E-elections/e-referendums pose special challenges to observers, inherent in the electronic conduct of the election or referendum. Observers will thus have to be provided with an opportunity, in particular, to have access to relevant software information, to see physical and electronic safety measures for servers, to inspect and test certified devices, to have access to and test, sites and information provided for remote e-voting, and to observe cast electronic votes entering the electronic ballot box and that votes are being counted. Security measures for telephone or 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.

II. Verifiability and accountability

Standard No. 24. "The components of the e-voting system…"

62. Assessment that e-voting systems function correctly and that security is maintained is essential. The means to achieve this is the independent evaluation or certification of the system as a whole or of its components, which requires disclosure of the critical system elements. The assessment can be accomplished by, e.g. the disclosure of the system design, inspection of detailed documentation, source code disclosure, inspection of component evaluation and certification reports, in-depth penetration testing, etc. The actual level of disclosure of the system elements needed to achieve appropriate assurance depends on the peculiarities of the system, its components and the services provided.

Standard No. 26. "There shall be the possibility for a recount."

63. The recount is a procedure that verifies election and referendum results that have already been established. There are different possibilities for recounts in the case of e-voting, these possibilities differ in their complexity and in their contribution to accountability. A very simple method of recounting can be produced by instructing the e-voting system to perform a second count. A second option is to transfer the electronic ballot box to a similar but distinct e-voting system and perform the second count on that system. A third option is to let the recount be carried out by a different system, which is inter-operable with the e-voting system. A fourth option is to produce, at some stage of the voting process, paper ballots and to use these for recounting.

64. To verify the result, it may not be sufficient only to conduct a recount. Depending on the architecture of the system used, there may be further elements that contribute to the correctness of the result. The confirmation that all votes cast have been considered is an example.

Standard No. 27. "The e-voting system shall…

65. If a re-run of an e-election or e-referendum becomes necessary, that re-run may not be possible without the support of the e-voting system that was used in the original election or referendum, even if that e-

voting system is not to be used in the re-run itself. This may be the case if the persons who are entitled to vote, can be identified only by using information that is available by means of that the original e-voting system.

III. Reliability and security

Standard No. 28. "The member state's authorities shall ensure... "

66. The new voting channels need to be as reliable and secure as traditional voting methods and it is the member state who has to guarantee that this is the case. The final responsibility can never be delegated to a voting system supplier.

Standard No. 29. "All possible steps shall be taken... "

67. Throughout the whole electronic voting process, there must be no intervention unconnected with the voting which is under way affecting either the ballot and election or referendum server or the electronic ballot box server. The recommendation is not intended to suggest that every possible method of protection available must be used in every case. In each case a judgement will have to be made as to the nature and extent of the protection measures to be applied. This judgement will require a proper balance to be struck between different factors. For example, in a particular case a balance may need to be struck between the all-important need for security and the advisability of having systems that are easily usable by voters. In such a case usability must not override the need for high levels of security but may be a factor in determining which security measures should be adopted. A similar position might apply were a very small additional security benefit to be achievable but only at an excessively high cost.

Standard No. 30. "The e-voting system shall contain measures to preserve…"

68. An e-voting system should be protected against malfunction and breakdown. However, the possibility of a breakdown can never be entirely excluded (cf. Appendix. III. Standard No. 77)

Standard No. 31. "Before any e-election…"

69. The standard requires that the correct functioning of an e-voting system is verified (cf. Standard No. 24). Furthermore, it has to be ensured that the verified e-voting system is actually being used during the e-election or e-referendum. Verification should prevent any e-voting system being installed where that system or any component of that system has been tampered with or might have been replaced. The authority needs to ensure that the correct system is put into service.

Standard No. 33. "While an electronic ballot box is open... "

70. "Any" indicates that, if election observers are allowed by domestic law, then they should have access. Security measures for telephone or internet voting may make it necessary not to allow the presence of observers in the computer room. In that case measures should be taken in order to give the observers the opportunity to monitor the intervention.

Standard No. 34. "The e-voting system shall maintain…"

71. From the moment the vote is cast, no one should be able to read or change it or relate the vote to the voter who cast it. This is achieved by the process of sealing the ballot box, and where the ballot box is remote from the voter by sealing the vote throughout its transmission from voter to ballot box. In some circumstances, sealing has to be done by using encryption.

72. To seal any ballot box, physical and organisational measures are needed. These

may include physically locking the box, and ensuring more than one person guards it. In the case of an electronic ballot box, additional measures may be necessary, such as access controls, authorisation structures and firewalls.

73. To seal an electronic vote for its transmission from voter to the ballot box (remote from the voter), encryption is required in addition to physical and organisational measures.

74. A vote is sealed when its content has been subject to the measures that ensure that it cannot be read, changed, or related to the voter who cast it.

Appendix II

Operational standards

I. Notification

Standard No. 36. " Domestic legal provisions governing... "

75. An e-election or e-referendum can differ from an election or referendum with regard to the procedures that have to be followed by voters. Examples of potential differences are the period of time during which votes can be cast, the steps a voter has to take in order to participate in the e-election or e-referendum and the way the e-voting actually takes place. These differences should be communicated to the voter in order to avoid any misunderstanding of the procedures and in order to give the voter all the information necessary to be able to make a well-founded decision on whether or not he or she wishes to use the available e-voting channels. Careful consideration should be given to deciding how much time the voter needs for this decision.

Standard No. 37. "The period in which an electronic vote can... "

76. Communicating the period of time for voting is especially important where this period of time differs in the case of an e-voting channel. This difference arises particularly in the case of remote e-voting in which the choice may be made to have a different period of time for voting using the electronic voting channels, due to the specific nature of those channels.

Standard No. 38. "The voters shall be informed... "

77. Communicating the procedures, and the steps the user has to take, is important because the use of electronic voting channels will (in most cases) mean that the voter has to have access to the means needed in order to use a particular electronic voting channel. For example, in the case of the internet as a channel, most personal computers that can connect to the internet will be able to use this facility but it is always possible that a small percentage of voters that use old computers or old software will not be able to use the internet channel. Thus, it should be made clear what equipment is necessary in order to use a particular channel. Consideration should also be given to offering the voter the opportunity to try the suitability of his or her equipment before he or she decides to use a specific electronic voting channel. Consideration should also be given to allowing the voter to change his or her preferred electronic voting channel in the case that he cannot use that specific channel. For example, the voter could choose to switch from the internet channel to the telephone channel, if both channels are being offered.

II. Voters

Standard No. 39. "There shall be a voters register... "

78. It is necessary to check whether or not a specific person has the right to vote and whether or not a specific voter has cast a vote. There are a variety of means to perform this check in non e-voting situations. Such checks can involve measures ranging from physically marking in a register the persons who have voted to registering by electronic means the fact that a person actually has cast his/her vote.

79. For these checks to be accurate, it is necessary that the registers in question contain up-to-date information as to those who have a right to vote at the election or referendum in question. Therefore these registers need to be updated before an election or referendum takes place. It should be noted that the use of the word ‘register’ in the singular

does not necessarily imply that there must be one single register that contains all the voters in a whole country or region.

80. In the case of remote e-voting, these checks are necessarily performed by using registers. Although it is feasible that in some cases paper-based registers could be used, in most remote e-voting schemes, the registers will have to be electronic. Where remote e-voting channels are available to a voter in parallel with voting in polling stations, the polling station officials should be able to verify whether that voter has already cast a vote.

81. The registers in question will in practice be created by different procedures. In some countries population registers exist which include almost all the voters (but may, for example, not include expatriate voters). Using these population registers it is possible to derive, often by electronic means, the registers that specifically contain the persons who are entitled to vote (the voters registers). In other countries where these population registers do not exist, the voters registers have to be prepared by a registration procedure that, among other things, involves persons applying to be registered as voters. These procedures will differ from country to country.

82. Persons claiming the right to vote should be able to check whether they are registered on the voters register and whether their personal information is correct. In some member states the voters register may be published (or accessible to the public). In other member states, personal data protection laws allow persons to check only their own registration.

Standard No. 40. "The possibility of creating an electronic register…"

83. It is conceivable that online registration will be offered to voters. This implies the existence of some means of electronic authentication through, for example, a digital signature and the existence of electronic registers. It is also conceivable that voters are enabled to apply for remote e-voting in an online or electronic way, for example after they have registered themselves. It should be noted that, for both possibilities, a very substantial effort will be necessary in order to solve the problems of identification and authentication in a remote electronic way. Therefore, the standard only provides for online registration to be considered.

III. Candidates

Standard No. 43. "A list of candidates that is generated…"

84. In order to offer the voters the voting options, complete lists of candidates must be created. These lists of candidates will be publicly presented in a variety of ways. Most common will be paper-based candidate lists. The use of new media, such as the internet for publicising this crucial information for the voter, is one of the ways in which more voters may be reached. Naturally, the internet should not be the only way of publicising the candidate lists. If the internet is used to create the candidate list (for example, by allowing online candidate nomination), it should be ensured that the lists of candidates generated are complete, accurate and authentic. This implies the use of digital signatures and certificating the website in an appropriate way.

85. In the case of non-remote e-voting, the voting machines in the polling station will probably contain all the information that is present on the ballot paper. With some types of voting machines, this information will be contained in a hardware display, for example, on

the physical buttons the voter has to press. In other situations, the information will be presented in digital form and one could speak of an electronic ballot.

IV. Voting

Standard No. 44. "It is particularly important, where remote e-voting takes place…"

86. The system for checking voters must be such that it is permanently updated with regard to those who have already cast a vote. However, if some voters are allowed to cast a vote only in the polling station and a separate register is being kept for those voters, the register of the remote e-voting system does not have to be updated with regard to those voters. In such a case, other methods may be required in order to prevent voters voting both in a polling station and by the other means available.

87. The introduction of remote e-voting brings with it the question of how the periods of time for voting in the polling station and remote e-voting are related. At first sight, it would seem logical that, for both methods of voting the same periods of time should apply, in order to avoid complications and distinctions. However, reasons that can lead to different periods of time being used include:

a) When casting a vote in a polling station is the fall-back option for voters who are within the national territory of the election or referendum in case the electronic voting channel breaks down, the closing time for the electronic voting channel may have to be before the closing time of the polling station.

b) When the system is designed and operated in such a way that voters can choose between channels without prior registration and the channels used do not have a common register in which is noted which voters have already cast their vote, the periods of time when these channels are available should in general not overlap.

88. Whatever the outcome of these architectural considerations, counting should only start after the closure of all the channels.

Standard No. 45. "Remote e-voting may start and/or end at an earlier …"

89. For various reasons, the period of remote e-voting may be longer than the period during which the polling stations are open. These reasons include providing a better service for citizens and enhancing accessibility.

90. However, remote e-voting should not continue after the end of the voting period at polling stations. In the case of the e-voting system being unavailable (e.g. a voter's PC is not working due to a power failure), the voter, resident or staying within the country where the election or referendum takes place, should still be able to go to the polling station to cast his or her vote. If e-voting continued after polling stations had closed, the voter would not have this possibility. Future developments may, however, demonstrate that this recommendation as to the time at which e-voting should end is unnecessary. This is a matter that it may be reviewed when the Council of Europe next considers the effects of this Recommendation and it will be beneficial if member states include any experiences they have of the issue in any reports they make to the Council on their consideration of e-voting or their e-voting experiences.

91. In order to accommodate possible delays in the transmission of electronic information, the acceptance of electronic votes cast before the end of the e-voting period,

should remain open for sufficient period of time after the closure of the e-voting period.(see Standard No. 96, Appendix III to the Recommendation).

Standard No. 46. "For every e-voting channel, support …"

92. Support and guidance arrangements on voting procedures should be in place regardless of the specific channel used. In the case of electronic voting channels, for each electronic voting channel these arrangements will be available using at least the same electronic voting channel. That is, a website with help information and e-mail facilities should be in place when the internet is the channel and a telephone hotline should be in place when voting by telephone is possible. Furthermore, fall-back arrangements on a different remote channel should be provided for situations in which one of the electronic voting channels is out of order. For example, a telephone hotline might be a suitable alternative in relation to remote e-voting over the internet.

93. These support and guidance arrangements should not endanger the secrecy of the vote.

Standard No. 47. "There shall be equality in the manner of presentation …"

94. Each voting option should be equally accessible to the voter within each channel. Equality of presentation may not be possible or appropriate between different channels. Mobile phone screens, digital TV screens, and PC screens display information in different ways.

95. It should be recognised that, although the arrangement of candidate names on screens might seem to be a purely technical matter, it is far more important than this and thus cannot be left to the (technical) designers of an e-voting system.

96. It is also necessary to provide, in order to ensure equality, protection measures to prevent the omission of information that should appear on the electronic ballot. In the absence of such measures there would be a risk that the result of the election or referendum would be affected because a possible choice for the voter had been omitted from some or all of the ballots cast by electronic means.

Standard No. 48. "The electronic ballot by which…"

97. During the casting of the vote, the voter's close environment should be free from objects and information that could influence the voter’s choice in a partisan way. In the case of the internet, this environment includes, in particular, the screens that are generated on a voter’s computer when accessing the e-voting website. These screens should not contain more information about the choices than paper ballots, such as pop-up screens that promote a specific candidate or audio elements that are associated with a particular candidate or point of view.

98. “Other messages” means partisan messages that may influence the voter, other than any allowed by domestic legal provisions. It does not prevent the display of, for example, official information on voting options.

Standard No. 49. "If it is decided that information about voting options will be …"

99. This standard does not conflict with the previous standard. It deals with the process of decision-making, whereas the previous standard deals with the process of casting a vote.

Standard No. 50. "Before casting a vote using a remote e-voting…"

100. Voting using the internet is not currently a common practice. Unless the attention of members of the public is specifically drawn to the fact that internet voting is real voting at a real election or referendum there is a risk that they may mistakenly imagine that they are taking part in a fake election or referendum or a test. On the other hand, if too little attention is drawn to the fact that people are participating in a demonstration or test version, they could get the impression that they have already voted. Also, an election or referendum might be confused with an opinion poll or vice- versa.

Standard No. 51 & 52. "A remote e-voting system…" and "In a supervised environment…"

101. In a supervised environment, the e-voting system should include provision for the disappearance of any information that could be used as a proof of the content of the vote cast. If the national electoral legislation requires that the e-voting system supplies the voter with a paper proof of his/her electronic vote, this proof should be subject to the same secrecy requirements as a paper ballot. The voter should not be able to show this proof to any other person, or take it out of the polling station. For instance, the voter could be required to deposit the paper proof in a box in the polling station, or in a device which destroys it.

102. In a remote e-voting system using the internet, the voter has to be able to delete information connected to his or her vote from the device used to cast the vote. One of the features of the most common way to use the internet, that is by means of a 'browser' on the voter's machine and a 'server' on the side of the election officials, is that the display and storage of information on the side of the voter can not entirely be controlled by the 'server'. This makes it necessary to pay specific attention to the way in which the anonymity and secrecy of the vote is realised in e-voting systems. There are at least three layers to be considered. The first one is the web application level. The second level is that of the browser. The third level is that of the utility software on the computer of the voter.

a) The web application should not allow the user to retain a copy of his or her vote. This means that the application should not offer the functionality of printing, saving or storing the vote or (part of) the screen on which the vote is visible.

b) The browser also should not offer the option of printing the screen on which the vote is visible. It should be noted that browsers can and do retain information in several ways. For example, by using the 'back' button on a browser, one or more previous screens can be displayed. As far as possible, this generic functionality of browsers should be disabled by the web application. At the very least, there should be no storing of information after the voter has finished casting the vote.

c) The third level that has to be accounted for is pieces of software that can record in some way what actions a specific user of a computer has performed. Three rather common examples are screen shot utilities, utilities that make films of the sequence of screens and utilities that record the key strokes a user makes. The e-voting system may not be able to prevent the use of such utilities.

Standard No. 55 "Any decoding required for the counting…"

103. The encryption of votes may be necessary to secure the anonymity of voting. In many cases the vote is encrypted before starting the transmission via networks, is held encrypted in the ballot box and is decoded before counting. The counting is carried out with decoded votes, which cannot be related to any voter.

104. However, there are encryption methods that do not require decoding before votes are counted (homomorphic encryption). Counting can then be performed without disclosing the content of encrypted votes. In some cases it may even be necessary for counting to be performed while votes are in the encrypted state, in order to secure anonymity.

Appendix III

Technical Requirements

Introduction to technical requirements

105. Electronic systems can be used to assist one or more of the different stages of an election or referendum. When considering the use of electronic systems for election or referendum purposes, it is necessary to confirm the complete and proper functioning of these systems. To this end, this document provides a set of technical requirements to help those who want to create such a system.

106. It may be that in a given election or referendum, not all stages will be conducted by electronics means. It is therefore important that functionalities are ordered in such a way that the main election or referendum stages are implemented as separate units.

107. Traditionally theses main stages are :
- announcement of election or referendum,
- voter registration,
- candidate nomination and registration, or determination of referendum options,
- voting,
- counting,
- declaration of the result,
- audit.

As shown in the next figure :

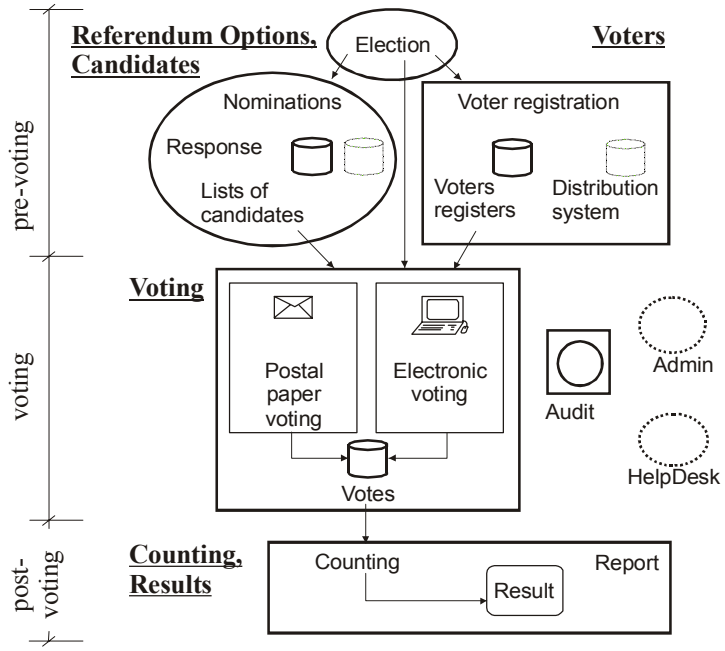

Figure 1: EML process model (simplified; from EML v4.0a, figure 2B)

108. The elements displayed above are the fundamental elements of an election or referendum system, which should be ordered in a way that makes associating them with their traditional counterparts easy. These elements are:
- the voters register,
- the candidates list or options list (which the voter may vote),

- the electronic ballot box,
- the counting of results.

109. The technical requirements cover six different areas: accessibility, interoperability, system operation, security, auditing and certification. Each area is detailed in a separate chapter both in the recommendation and in the explanatory memorandum. After the last one, certification, there is a description of a methodology for risk analysis.

A. Accessibility

Standard No. 61. "Measures shall be taken to ensure... "

110. In order to guarantee accessibility and ease of use of e-election or e-referendum systems, consideration must be given to different user-related constraints linked to age, language, disability and lifestyle.

111. For example, individuals with a visual impairment or with dyslexia may need screen reading devices, sharply contrasting text and backgrounds, as well as the possibility of adjusting the text size in their Web browsers or on voting machines. Users with communication impairments may prefer graphically presented information. Those with co-ordination impairments may prefer using a keyboard rather than a mouse. Kiosks need to be adapted to the needs of mobility impaired users.

112. Voters should be supplied with appropriate instructions, which are easy to understand and follow.

Standard No. 62. "Users shall be involved in the design of e-voting systems… "

113. The need for accessibility of e-voting systems means that systems should be designed in such a way that as many voters as possible, and ultimately all voters, can use them.

114. Products and services must be functional, suitably adapted to the age-range and needs of the public, yet without unnecessarily complicated or expensive features that only provide slight benefits.

115. Both these requirements might be achieved with a collaborative approach involving the development team and a users' panel.

Standard No. 63. "Users shall be supplied, …, with additional facilities… "

116. The World Wide Web Consortium was created in October 1994 to lead the World Wide Web to its full potential by developing common protocols that promote its evolution and ensure its interoperability. W3C has around 400 Member organisations from all over the world and has earned international recognition for its contributions to the growth of the Web. The W3C develops interoperable technologies (specifications, guidelines, software, and tools) and is a forum for information, commerce, communication, and collective understanding.

117. To promote a high degree of usability for people with disabilities, the W3C started the Web Accessibility Initiative (WAI). In coordination with organizations around the world, the WAI pursues WEB accessibility through five main areas of work: technology, guidelines, tools, education and outreach, and research and development. The WAI has already produced a set of standards and guidelines in support of accessibility (e.g.: Web contents accessibility guidelines, authoring tools accessibility guidelines, user agent

accessibility guidelines, XML accessibility guidelines, etc.). More information is available from the WAI web site: http://www.w3.org/WAI.

Standard No. 64. "Consideration shall be given, …, to their compatibility with existing… "

118. It is a constant in system development that a new version may be so different from the previous one that they are incompatible. To avoid such a situation, it might be helpful to create and maintain a list of compatible systems, products and specific equipments. International bodies like OASIS (see Interoperability) may be helpful in this respect.

Standard No. 65. "The presentation of the voting options shall be optimised for the voter."

119. Products and services must be adaptable to the users' functional restrictions and specific circumstances without infringing the equality principle. This can be achieved by offering different versions of the same product, changes to key parameters, modular design, ancillaries or other methods.

B. Interoperability

Standard No. 66. "Open standards shall be used… "

120. In order to be able to use e-voting systems or services from different suppliers, these must be interoperable. Interoperability means that the input and output conform to open standards and especially open standards for e-voting.

121. The main benefits of using open standards are:
- Greater choice of products and suppliers
- Less dependency on a single supplier
- Avoidance of proprietary lock-in
- Stability or reduction in costs
- Easier accomodation of future changes

Standard No. 67. "At present, the Election Mark-up Language (EML)… "

122. OASIS, the International e-Business interoperability consortium, formed the Election and Voter Services Technical Committee in the spring of 2001 to develop standards for election and voter services information using XML. Further information about the membership and work of the committee is available at http://www.oasis-open.org/committees/election.

123. The Election Markup Language (EML), the first XML specification of its kind, is at present the only standard for the structured interchange of data among hardware, software, and service providers who engage in any aspect of providing election or voter services. Its function is to ensure open, secure, standardised and interoperable interfaces between the components of election systems. EML is a set of data and message definitions described as XML schemas. It is continually evolving to meet the needs of different voting systems based on experience gained from successive e-elections and e-referendums. The newest available version at the time when the Recommendation is adopted is the version that is to serve as a reference to every member state that wants to use EML when implementing an e-voting system. The way this reference will be updated in the future should be defined.

124. Technological developments, unforeseeable at the time of the adoption of the Recommendation, may mean that any system valid at that time, including EML, may one day not be the most appropriate system for e-elections or e-referendums, and thus not be used by individual or groups of countries.

Standard No. 68. "In cases which imply specific election or referendum data requirements… "

125. As electoral provisions differ between member states, it must be possible to adapt the standard to local needs. EML, being XML based, provides for a localisation procedure that allows, for instance, additional data or a particular structure. There are several methods of localising XML schemas, eg. Schematron. It should be borne in mind that any localisation should not prevent an equivalent module from another supplier from working in the localised environment.

C. Systems Operation

126. This section refers to equipment, infrastructure and software running in a controlled environment. These include servers, communication devices, kiosk machines and their related operating systems and other pieces of software. This excludes voters' personal devices like PCs, organisers, mobile phones and their related software as well as public network equipment, devices and software.

Standard No. 69. "The competent electoral authorities shall publish… "

127. Constant development in information and communication technologies makes it necessary for those in charge of the infrastructure to keep up to date with hardware and software. This calls for recurrent adaptations to central systems and voting facilities used in a controlled environment (for example, voting machines). Any adaptation will need to be certified according to the rules in force in each state before it can be brought into operation.

128. It is essential that electronic voting systems remain as transparent as possible for authorities and citizens alike. Exact, full, up-to-date descriptions of the hardware and software components should be published, thus enabling interested groups to verify for themselves that the systems in use correspond to the ones certified by the competent authorities. The results of certification should be made available to the authorities, political parties and, depending on legal provisions, citizens.

Standard No. 70. "Those responsible for operating the equipment shall draw up a contingency procedure…"

Standard No. 71. "Sufficient back-up arrangements shall be in place… "

Standard No. 72. "Those responsible for the equipment shall have procedures to ensure… "

129. An electronic voting system, more so than any other electronic system in public use, must possess reliability to the highest degree - hence the need to formalise the procedures for dealing with special cases and problems and to provide adequate resources for troubleshooting the infrastructure.

130. The electoral authorities must define a specific service level before running the system. Based on the desired service level, a risk analysis should be made and scenarios should be established. These will imply procedures, back-up arrangements, resources reservation and so on.

Standard No. 73. "Before each election or referendum, the equipment shall be checked and approved… "

131. As it is not possible for every member of the electorate to exercise his/her right to transparency of the ballot personally, the competent authorities, the candidates and any observers (where relevant), should be able to have the whole or part of the system inspected by a specialist entity.

132. A clear distinction should be made between checking done on a regular basis after each election or referendum, and the checking done whenever the system is

modified in any respect. In the first case, employees of the entity running the election or referendum system might do the checking. However in the second case an external body should do the checking, as the check is closer to being a certification procedure. See the certification section below for more information.

Standard No. 74. "Any technical operations shall be subject to a formal change control procedure…"

133. All work done on hardware or software carries intrinsic technical and human risks, which should be kept to a minimum while an operation is in progress. That is why automatic controls are to be preferred and limits placed on remote manipulations without official supervision. If there is a necessity to intervene, these risks (of intrusion, human error, sabotage, etc.) are to be reduced as far as possible. This should be done by establishing a working procedure to be followed and validated, which restricts the number of persons authorised to do the work to a small supervised group and requires the verification of each act through the physical presence of two or more qualified persons. Those persons should comply with the security rules laid down by the competent authority.

134. The electoral authorities must be made aware of all critical changes made on the system in order to anticipate any consequences and choose the appropriate policy to communicate such changes.

Standard No. 75. "Key e-election or e-referendum equipment shall be located…"

135. For their safekeeping, it is highly desirable that the central systems be installed in secure, controlled locations. Physical access should be restricted. To be able to react after a physical disaster, an alternative location solution should also be planned, with the appropriate equipment pre-reserved.

136. All election or referendum data that has to be stored should be stored in a secure manner. This means several copies of data will be needed on several types of information support (hard disk, tapes, USB memory key, and printout) and they should be stored in different locations.

Standard No. 76. "Where incidents that could threaten the integrity of the system occur…"

137. It is important that any incident be reported to the competent authorities, who are entrusted with the duty to specify communication rules in keeping with the applicable legislation and to ensure that the political parties and voters are properly informed.

D. Security

Introduction

138. Appropriate security measures are indispensable preconditions for e-voting. As with any technical system, an e-voting system may be exposed to errors and deliberate or unintended attempts to circumvent security measures. Attacks need to be prevented and the cardinal principles of *universal*, *equal*, *free*, *secret* and *direct suffrage* need to be maintained. Particular attention is to be paid to possible systematic attacks, as these can particularly affect results. In general, e-elections and e-referendums involving the use of e-voting should be as reliable and secure as elections or referendums which do not involve the use of electronic means (cf. the Recommendation, indent (i.)).

139. Technical security requirements of the Recommendation follow accepted IT security practices and are based on a risk analysis (cf. section VII). The requirements are based on the following criteria:

1. *Technology neutrality*: The purpose is to develop the technical security recommendations in a technology neutral approach, and not to restrict solutions to a limited set of technologies or voting channels (e.g. solely concentrating on the Internet)
2. *Sustainability*: The security requirements are to outlast rapid technological changes. This is closely related to technology neutrality.
3. *Methodology*: Accepted practices and standards are to be followed to develop the security requirements in order to provide confidence in the result.
4. *Versatility*: The requirements are applicable to all forms of e-elections and e-referendums, i.e. voting machines at polling stations, kiosk voting in controlled environments, and remote e-voting in uncontrolled environments.
5. *EML*: The technical security requirements have been based on the Election Markup Language (EML) process model that is a basis of work carried out in the subgroup on core technical standards.

IT Security Terms

140. The following IT security terms are frequently used in this section. The definitions have mainly been taken from relevant ISO standards.

Access Control	The prevention of unauthorised use of a resource (ISO 7498-2:1989)
Authentication	The provision of assurance of the claimed identity of an entity (ISO/IEC 10181-2:1996)
Availability	The property of being accessible and usable upon demand (TR 13335-1:1996)
Confidentiality	The property that information is not made available or disclosed to unauthorised individuals, entities, or processes (ISO 7498-2:1989) (TR 13335-1:1996)
Protection profile	An implementation-independent set of security requirements for a category of products that meet specific consumer needs. (ISO 15408)
User or actor	An entity that is authorised to interact with the e-voting system as a whole or with its components. This includes, *inter alia,* voters, candidates, auditors, etc.

I. General Requirements

Standard No. 77. "Technical and organisational measures shall be taken… "

141. Service level agreements (SLAs) usually lay down availability and failure rates. A certain level of service degradation may be acceptable during failure periods, e.g. when a server in a cluster breaks. In registration processes even short periods of service disruptions or maintenance periods may be tolerable. The system developers, however, need to consider deliberate denial of service attacks and shall document the contingency

reserve in system performance that has been designated. Independent penetration tests can reduce the probability of successful deliberate service disruption.

142. The services to be preserved in availability depend on the stage – Pre-Voting, Voting, Post-Voting. In the Pre-Voting Stage, nominations, the registration processes and its services are to be available, in the Voting Stage the voting processes and its services, and in the Post-Voting Stage the counting and reporting processes and its services. Auditing processes need to be available in all stages. The pre-defined limits for SLAs, tolerable failure rates, or service degradation may however be different for the various stages or services.

Standard No. 78. "The e-voting system shall maintain the privacy of individuals… "

143. Depending on national practices there may be further confidentiality requirements with respect to the candidate's decision. In that case those requirements must be met.

Standard No. 79. "The e-voting system shall perform regular checks…"
Standard No. 80. "The e-voting system shall restrict access… "
Standard No. 81. "The e-voting system shall protect authentication data "

144. The objective refers to all subjects. Services, such as information services for the voter prior to entering the voting process, which clearly do not need authentication, are outside the scope of this document.

Standard No. 82. "Identification of voters and candidates in a way that they can unmistakably be distinguished… "

145. Unique identification refers to validating the identity of a specific person by means of one or more features so that the person can unmistakably be distinguished from all other persons. The voters registers therefore need to provide means to avoid digital twins – i.e. persons holding the same identification data. In cases where central voters' registers are used, unique identification may implicitly be given by the entry of the person in the database, with interconnected voters registers additional means may be necessary.

146. As someone may be both a voter and a candidate or both an administrator and a voter, it is important to prevent the same person having the same identification in the system for all his or her roles. Authentication can be identity-based or role-based. While identity-based authentication is advisable for voters registering or casting a vote, or candidate nomination, it might be sufficient to have role-based authentication for administrators, auditors, etc.

Standard No. 83. "E-voting systems shall generate reliable and sufficiently detailed observation data… "
Standard No. 84. "The e-voting system shall maintain reliable synchronised time sources… "

147. There may be different accuracy requirements for different consumers of the time source, such as different tolerances for the registration event and casting a vote. This may lead to multiple time sources or a single time source that provides the highest accuracy. The term "time mark" has been used as an indication for marking the data. There are several means depending on the situation: Secure time stamps might be needed for critical events, whereas e.g. continuous sequence numbers or preserving the sequence may be sufficient for log entries. Note, that time stamps on votes may jeopardise the confidentiality of the vote. And thus careful consideration should be given as to how and if they should be used in relation to ballots or votes.

Standard No. 85. " Electoral authorities have overall responsibility… "

148. The electoral authorities have the responsibility for ensuring that the e-voting system is in compliance with the security standards. The notion of an independent body to assess compliance with the security standards covers both independence from the system manufacturer or service provider, and independence from political interference. The former shall provide assurance that the technical security measures are effective and correctly implemented. The latter shall provide confidence that there is no inappropriate political influence in the evaluation of the e-voting system. The independent body may be a governmental organisation, such as an agency in charge of national IT security certification, or the electoral authority itself; a private or international organisation such as evaluation laboratories or certification bodies, for instance those that are accredited for the national or international evaluation schemes such as BS7799/ISO17799, Common Criteria, or ITSEC. Designation of an independent body shall be transparent.

149. In case evaluated and certified Common Criteria / ISO 15408 Protection Profiles are developed based on these security recommendations, independent assessment is given under the Common Criteria scheme.

II. Requirements in Pre-Voting Stages

Standard No. 86. "The authenticity, availability and integrity of the voters registers … "

150. Data-origin authentication can e.g. be provided by electronic signatures in fully electronic processes. In semi-electronic processes, data-origin authentication may employ also conventional security measures, such as manual signatures, seals, couriers, etc.

Standard No. 87. "The fact that candidate nomination and, … "

151. This can, e.g., be provided by time marks or by a confirmation of a trustworthy system.

Standard No. 88. "The fact that voter registration… "

152. This can e.g. be provided by time marks or a confirmation of a trustworthy system.

III. Requirements in the Voting Stage

Standard No. 89. "Data communicated from the pre-voting stage… "

153. Depending on the approach followed, the data actually needed in the voting stage may vary. For example, lists of candidates are required in the voting stage if the ballot is dynamically generated in that stage, whereas an alternative is to generate ballots in the pre-voting stage and to communicate the ballots to the voting stage. Therefore, standard no. 89 does not list the data that shall be kept in integrity and authenticity but generally refers to “data communicated”.

154. The voters register may not be required if in two-phase models an anonymous voting token is used to establish the right to vote. Note that voters’ registers in the polling station might be needed to prevent multiple votes (electronically and on paper-ballot) or where voting is compulsory and thus a list of those who have voted is essential.

Standard No. 90. "It shall be ensured that the e-voting system presents … "

155. Aspects to be considered are that fraudulent servers may be introduced, for example faking an official server by tampering with the domain name system (DNS), using a similar domain name to that of the official server, by man-in-the-middle attacks, or Trojan horses in the voter’s system replacing the original ballot or fading in counterfeit

ballots. Electronic signatures applied to the ballot by the electoral authority allow for verification of the ballot. This shall, however, not violate the confidentiality of the vote.

Standard No. 91. "The fact that a vote has been cast … "

156. This can e.g. be provided by time marks or a confirmation of a trustworthy system. A time-mark attached to the vote may not, however, leave data trails that can reveal the vote.

Standard No. 92. "Sufficient means should shall be provided to ensure … "

157. In remote voting environments, such as Internet voting, usually the voter or third parties control the environment. There are limited means by which the e-voting system can control whether a secure environment exists. Provision should be made to enable voters to have confidence in the system should be provided, such as measures to ensure that genuine software is used, or recommendations on how to protect the system environment.

Standard No. 93. "Residual information holding the voter's decision … "

158. During the process of casting a vote, information carrying the voter's decision may be kept in various locations for technical reasons. E.g. in internet voting scenarios using a PC, data carrying the voter's decision may be kept in the PC's memory, the browser cache, the video memory, swap files, temporary files, etc. Depending on the system, other storage locations may need to be considered. The term residual information refers to information that remains accessible at the various locations after the vote has been cast and which may reveal the voter's decision. The standard advises the system developers or service providers to design the e-voting system in such a way that this information may be deleted after the vote has been cast. However, technically there may be limited means to ensure this in a remote voting environment. Nevertheless, every measure possible shall be taken to delete such residual information when the vote has been cast.

Standard No. 94. "The e-voting system shall at first… "

159. In cases where anonymous voting tokens prove that a voter is eligible to vote, identification of the voter may not be required. Multiple votes under anonymous authentication need to be prevented.

Standard No. 96. "After the end of the e-voting period, … "

160. In remote voting scenarios, a higher load on the services might occur in the short period just before close of the poll. This may lead to increased load and delays before a cast vote enters the electronic ballot box. Votes that have been cast in time, however, shall not be discarded as a result of such delays. Thus, a period of grace shall be given to overcome overloaded periods right before the close of the poll. E.g., the processing of the votes must not be shut down immediately with the closing time of the service, if such increased delays are to be expected.

IV. Requirements in Post-Voting Stages

Standard No. 97. "The integrity of data communicated from the voting stage… "

161. Data-origin authentication can e.g. be provided by electronic signatures in fully electronic processes. In semi-electronic processes, data-origin authentication may employ also conventional security measures, such as manual signatures, couriers, etc. Cast votes and any results derived from those votes are the most valuable assets in an election or referendum. Thus, technical measures are preferable in order to protect these assets in transfer.

Standard No. 98. "The counting process shall accurately count the votes… "

162. To gain confidence, it is most important that the counting process can be reproduced and that this can be done with a different system from a different source.

Standard No. 99. "The e-voting system shall maintain the availability and integrity of the electronic ballot box… "

163. The information kept in the electronic ballot box must be securely saved for as long as this is necessary to permit any recount or legal challenge or for the period after the election required by the electoral process in the member state in question.

E. Audit

I. General Requirements

Standard No. 100. "An audit system shall be designed and implemented… "
Standard No. 101. "End-to-end auditing of an e-voting system… "

164. Auditing of the election or referendum processes is the means by which in particular the processes used to collect and count the vote can be examined, in order to confirm the authenticity of the result.

165. Auditing of the system operation, resources and communication infrastructure is the means by which trust and confidence can be established in operation of the ICT system(s) used for e-voting. This requires integrity and authenticity of the audit information and trust in the deployed auditing systems.

166. The greatest danger to e-voting systems is if attacks on systems are not detected and the attack affects the result of the vote. This is why independent and extensive security monitoring, auditing, cross checking and reporting are a critical part of e-voting systems.

167. E-voting systems should therefore have audit facilities for each of the main components (vote, count, etc.). Audit facilities should be present on different levels of the system: logical, application, technical.

168. Audit facilities on the logical level should report upon the use that is being made of the system.

169. Audit facilities on the application level should give information on the activities that the system supports in order to enable reconstruction of the system's operation.

170. Audit facilities on the technical level should provide information on the activities that the infrastructure that is being used supports. This varies from routine information on, for example, specific load information and system malfunction, to specific information on the signals an intrusion detection system (IDS) gives with regard to possible attacks.

II. Recording

Standard No. 102. "An audit system shall be open, comprehensive… "

171. Audit trails are critical for e-voting systems, so they must be as comprehensive as possible and open to scrutiny by authorised third parties. Audited data shall be provided at various points and levels within an electronic voting system, for example data can be audited at the EML, IT system or communications infrastructure levels.

172. At the EML level there are many standardised open interface points, data flows at these interface points can be easily observed and monitored. Audit systems shall also

cover non EML interfaces, for example interfaces within the communications infrastructure, databases and system management functions.

173. There should be procedural requirements specified for the use of audit systems while running election or referendum systems and predetermined procedures for rapid response scenarios.

Standard No. 103. "An audit system shall record times, events and actions… "

174. Automated tools and system procedures shall enable the data to be analysed and reported on in a fast and accurate manner, thus enabling rapid corrective action.

175. The audit system shall provide verifiable reports on:
- Cross-checks of data, including EML based data,
- System or network attacks,
- Intrusion detection and reporting,
- Data manipulation,
- Fraud and fraud attempts.

176. The audit system shall maintain records of any attacks on the operation of the election or referendum system or its communications infrastructure. The system shall include functionality that detects and reports attempts at hacking, intrusion or manipulation. Detection of attacks on the voting system shall be logged, reported and acted on immediately.

177. The audit system shall log all counts and recounts, including all decisions made, actions taken, or exceptions made during the counting process.

III. Monitoring

Standard No. 104. "An audit system shall provide the ability to oversee the election … "

178. The audit system should provide the ability for any observer to monitor the real time progress of the election or referendum without revealing the potential end count/result. For example, observers should be able to see the total number of ballots being cast in real time, so that independent cross checks can be preformed.

Standard No. 105. "Disclosure of the audit information to unauthorised persons shall be prevented."
Standard No. 106. "An audit system shall maintain voter anonymity all times."

179. Audit systems by their very nature gather a lot of information. However, if too much information is kept, the confidentiality of the vote may be compromised. Clearly, an audit system should maintain voter anonymity at all times, except when specifically required otherwise under domestic legal provisions. In all cases the information gathered by the audit system has to be protected against unauthorised access.

IV. Verifiability

Standard No. 107. "An audit system shall provide ability to cross check and verify… "

180. The audit system shall be able to detect voter fraud and provide proof that all counted votes are authentic. All occurrence of attempted voter fraud shall be logged; the audit system logs shall contain data that provides the ability to cross check credentials giving the right to vote and shall ensure that all counted votes were cast by a voter with a right to do so and that all authentic votes have been counted as such.

181. The audit system shall include all election or referendum data required by electoral officials to cross reference and account for all cast ballots, thereby verifying the correct operations of the voting system and the legitimacy of the result. A count of ballots is required to match the total votes cast, including valid and invalid votes. The audit system shall give information to facilitate an independent cross check and verify the correct operation of the e-election or e-referendum system and the accuracy of the result. The audit system shall be able to ensure that no authentic votes are lost and that there are no votes that are unaccounted for.

182. Cross checking of independent audit information increases the likelihood of detection of hidden attacks on e-voting systems, as the attack has to be hidden in a consistent way on both the e-voting system and the independent audit information.

Standard No. 108. "An audit system shall provide the ability to verify that an e-election…"

183. The audit system shall provide the ability for any observer to be able to directly or indirectly observe the election or referendum and verify that the number of votes cast is accurate. This, therefore, requires the system to provide open, standard interfaces with comprehensive observation facilities subject to the needs of confidentiality of the vote.

184. The audit system shall be publicly verifiable. It may be necessary to prove to the public that the principles of democratic elections and referendums have been upheld and that the results are correct.

185. This requires the ability to prove to third parties that the results are a true and accurate representation of the authentic votes cast and meet the legal requirements under which the election or referendum was held.

V. Other

Standard No. 109. "An audit system shall be protected against attacks… "

186. The audit system shall meet the same security requirements specified for the implementation of the e-voting system itself.

187. The audit system shall itself be protected against attacks intended or likely to corrupt, alter or lose records. Detection of any insider or outsider attacks on the audit system shall be reported and acted on immediately.

Standard No. 110. "Member states shall take adequate steps to ensure that… "

188. It is not enough simply to protect the information gathered by the audit system against unauthorised access. It is also necessary to take legal and organisational measures to control the persons in charge or having access to the audit system. Accordingly, anyone having access to the audit system should be subject to an accreditation process.

F. Certification

Standard No. 111. "Member states shall introduce certification processes… "

189. Election officials should consider the use of techniques ranging from testing to formal certification in order to ensure before the election or referendum takes place, that the system does exactly what it is supposed to do.

190. In the future there may be a number of e-voting systems available as well as individual components. It might become very hard for any electoral authority to make sure a particular product is ready to be used, will operate correctly and will produce the right results. A certification process will be very useful in this respect as it should provide evidence as to the effectiveness of the components and thus may reduce the testing required when building a complete system.

Standard No. 112. "In order to enhance international co-operation… "

191. Where agencies participate in international organisations that provide mutual recognition arrangements, member states can benefit from their work and hence reduce their costs of testing and certification.

Risk analysis - methodology

The technical security recommendations have been developed along the Common Criteria / ISO 15408. This offers a methodical approach to defining the security objectives in the same way that CC Protection Profiles (PPs) are a means to describe security requirements in a technology neutral manner. Moreover, CC is an IT security products evaluation scheme that is internationally accepted[5] and thus following this standard will enable the security recommendations to be developed into PPs that can be taken up by the industry.

The document however does not represent an actual complete PP, rather it "borrows" from CC by using that methodology to develop the requirements. This serves to demonstrate the completeness and effectiveness of the principles underpinning technical security recommendations. This methodology is explained in the following paragraphs.

The following figure 2 illustrates the CC basics. This shall introduce the ideas that have been used in developing the technical security recommendations to the reader that is unfamiliar with schemes like CC. Those elements that actually have been used in this document are shaded grey in figure 2.

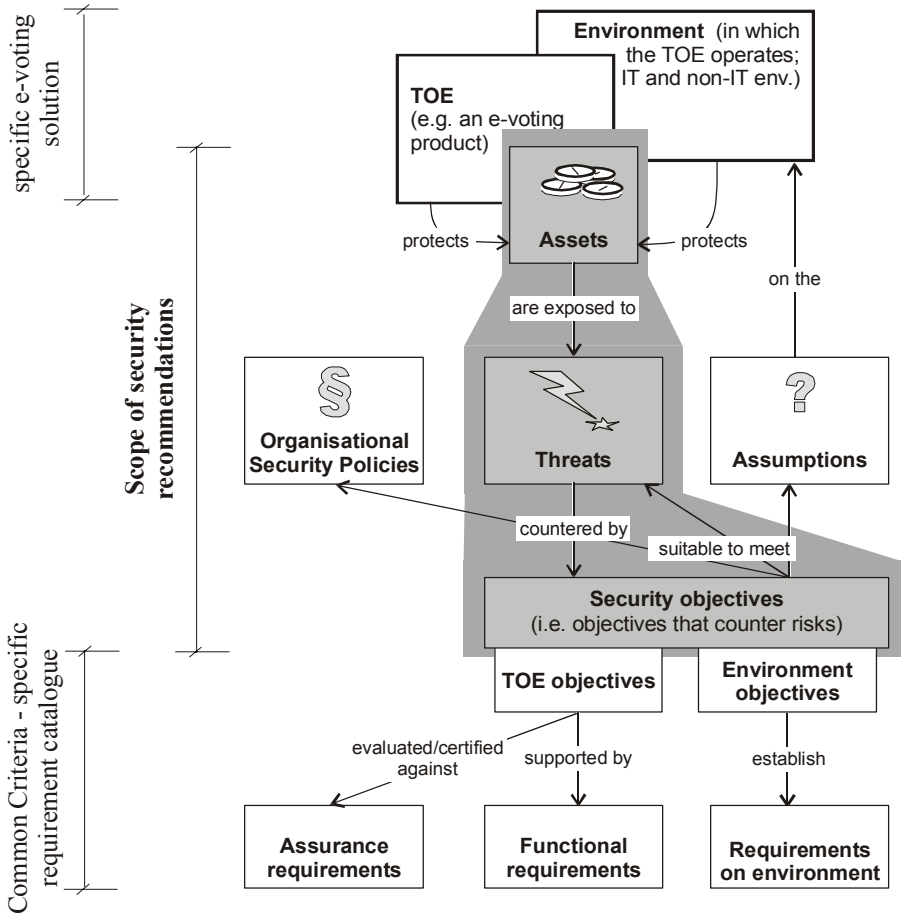

Figure 2: Common Criteria methodology overview and scope of draft security recommendations (shaded grey)

The CC defines a security product (e.g. an e-election system as a whole or a component of it) to be assessed as a target of evaluation (TOE). The TOE together with its environment protects the “assets”. By clearly defining the assets the elements needing protection are identified. This forms the basis for a comprehensive threat analysis by examining the assets that are stored or communicated. From these threats, security objectives can be derived and an analysis can be

[5] The CC Mutual Recognition Agreement (MRA) has been signed by several Council of Europe Member States. As of June 2004, the MRA signatory nations are Austria, Australia, Canada, Finland, France, Germany, Greece, Hungary, Israel, Italy, Japan, The Netherlands, New Zealand, Norway, Spain, Sweden, Turkey, United Kingdom, and the United States of America.

made whether the objectives are complete and effectively counter the threats (this approach has been used for developing the technical security recommendations for e-voting).

No organisational policies and related objectives have been defined in the current stage.

The distinction between a product and its environment has not been followed, as this is assumed to be too prescriptive for the purpose of the CoE recommendations and is rather related to the evaluation of actual products. However, it is worth noticing, that usually not all threats can be countered by technical means – leading to assumptions in CC terms. For example, it seems virtually impossible to avoid family voting in unattended remote voting scenarios by technical means.

Moreover, further elaboration of the security objectives by mapping functional requirements and assurance requirements using the CC catalogues has been omitted.

In summary, the methodology that has been "borrowed" from CC will generate a complete set of security objectives that lead to security recommendations. This document adopts some formal constraints from CC, even though only some underlying basics of CC have been used. This will assist developers to develop actual CC Protection Profiles or Security Targets and thus encourages independent evaluations of products.

Assets

Given the process model shown in Figure 1 the following assets can be identified:

General (all stages)

1. *Authentication data:* Information used to verify the claimed identity of a user (authentication data must be maintained in confidentiality).

2. *System integrity:* The authenticity of the e-election system or its components that carry out the intended functions (integrity of the e-election system or its components must be maintained)

3. *Verifiability and observability:* The information used to audit the correct functioning of the e-election or e-referendum system or components of it and information to carry out observation of the election or referendum event (availability and integrity of audit logs and observation information must be maintained)

Pre-Voting Stage:

1. *Candidate decision:* The decision to accept/decline a nomination, if provided by domestic law. (there might be privacy requirements with respect to the nominee's decision)

2. *List of candidates*: see Glossary for the definition of candidate (availability and integrity of the list of candidates must be maintained, there might be confidentiality requirements until accept/decline of nominations)

3. *Voters register:* The list of those eligible to vote at an election or referendum. (integrity of the voters register must be maintained, depending on the domestic legislation there may be confidentiality requirements for privacy reasons)

4. *Nomination process:* The process of nominating candidates, recording the candidate decision, if provided by domestic law, and establishing the lists of candidates (availability of the nomination process must be maintained)

5. *Privacy, data-protection:* The e-election system holds personal data, such as the voters register or the candidates' decisions. This data may not be disclosed to unauthorised third parties (different domestic legislation may vary between member states as to publication/disclosure of voters registers):
Application note: One aspect to be considered is the legal requirement whether e.g. the voters register has to be public (e.g. UK) or not (e.g. DK). However, even if the voters register is public information, granting unrestricted electronic access has privacy implications (e.g. being a national register of citizens and residences which can be misused). Thus, the means how public access is granted should be considered.

6. .*Registration process:* The process for registration of voters or to establish voters registers. (availability of the registration process must be maintained)

7. .*Right to Vote*: The voter's right to vote—including any provision preventing multiple voting by one voter. (the right to vote must be maintained)

8. *Nomination period:* The period during which nomination can take place (the fact that a nomination has become effective within the eligible timeframe shall be ascertainable)

9. *Registration period:* The period during which registration can take place (the fact that a registration has been performed within the eligible timeframe shall be ascertainable)

Voting Stage:

1. *Ballot:* see Glossary for the definition (the correct ballot must be presented to the voter, the integrity of the ballot must be maintained)

2. *List of candidates (if required, e.g. for generating the ballot):* Communicated from the pre-voting stage (cf. Pre-Voting Stage above, see Glossary for the definition) (availability and integrity of the list of candidates must be maintained)

3. *Vote*: see Glossary for the definition (availability, integrity and confidentiality of the votes must be maintained until the counting process and beyond for recounting purposes)

4. *Voters registers:* Communicated from the pre-voting stage. (cf. Pre-Voting Stage above) The list of those eligible to vote at an election or referendum. (integrity of the voters register must be maintained, depending on the domestic legislation there may be confidentiality requirements for privacy / data-protection reasons) Application note: The voters register may not be required if in two phase models an anonymous voting token establishes the right to vote. Note that voters registers in the polling station might be needed to prevent multiple votes (electronically and on paper-ballot) or where voters are required to vote.

5. *Right to Vote*: The voter's right to vote – including any provision preventing multiple voting by one voter. (the right to vote must be maintained)

6. *Voting period:* The timeframe in which voting is permitted (the fact that a vote has been cast in the voting period must be ascertainable)

7. *Voter's decision to vote:* The vote entered to the e-election system. (the voter's decision must remain an secret when examining a vote or residual data at the election-system, confidentiality and integrity of the voter's choice must be maintained).
Application note: The data to be protected is at least the vote. However, further data may be present while making the choice or after the vote has been cast.

8. *Voter's privacy, data- protection:* The e-election system holds voter's personal data, such as the voters register. This data may not be disclosed to unauthorised third parties (confidentiality of the voters register, different domestic legislation on publication/disclosure of voters registers may exist)
Application note: One aspect to be considered are the legal requirement whether e.g. the voters register has to be public (e.g. UK) or not (e.g. DK). However, even if the voters

register is public information, granting unrestricted electronic access has privacy implications (e.g. being a national register of citizens and residences which can be misused). Thus, the means how public access is granted should be considered.

9. *Casting of a vote:* The process by which an individual casts a vote (availability of the voting process must be maintained).

Post-Voting Stage:

1. *List of candidates* (if required, e.g. for generating the election result or the election report): Communicated from the pre-voting stage (cf. Pre-Voting Stage above) see Glossary for the definition (availability and integrity of the list of candidates must be maintained)

2. *Vote:* Communicated from the voting stage. see Glossary for the definition (cf. Voting Stage above) The main assets are the votes (availability, integrity and confidentiality of the votes must be maintained until the counting process and beyond for recounting purposes)

3. *Counting process*: The process of turning votes into the results of a election/referendum (availability of the counting process must be maintained)

4. *Election report:* The report generated by the e-election system (integrity of the report needs to be maintained)

5. *Counting result:* The result of counting votes and the prevention of premature partial results (counting needs to be correct, timely, and integrity of the result must be maintained)

6. *Reporting process*: The process generating an election or referendum report (availability of the reporting process must be maintained)

Subject	*Definition*
Administrator	A person that performs initialisation, operation or other administrative e-election system functions.
Auditor	A person, internal or external, responsible for assessing the condition, reliability, and security of the e-election system (authenticates as person eligible to access audit logs).
Authority	An entity, both a person or process, authorised by the electoral authority (authenticates to initiate election or referendum related events, such as initiating an event, generating voters registers, generating results, etc.)
Candidate	A voting option consisting of a person and/or a group of persons and/or a political party
Observer	A person authorised to observe an election or a referendum (authenticates as observer)
Proposer	A user – an individual, a group, entities such as political parties or an authority – nominating a candidate or candidates (authenticates as user eligible to nominate)
Voter	A person who is entitled to cast a vote in a particular election or referendum
Threat agent	*Definition*
Attacker	A human or process, both internal or external, mounting an attack to the

	e-election system or to parts of it. Also a subject authenticated as such but acting outside its role (internal attack, e.g. an administrator aiming to gain access to the voter's decision) acting outside its role. The main goal of an attacker is to access, modify or insert sensitive information or to disrupt services.
Malfunction	An external event that disrupts services or internal failure or breakdown of the e-election system or its services.

Threats

This section describes the threats to the assets. The threats are elaborated for each stage "Pre-Voting", "Voting" and "Post-Voting", as defined in the EML process model, illustrated in figure 1, respectively. This gives a certain level of modularity which allows investigation of the threat analysis for each process stage. General threats that are common to all process stages are given in a separate section. Threats that are common to two process stages are indicated as such.

General (all stages)

T.Audit_Forgery *Forgery of Audit Data*

An attacker generates, modifies, inserts or deletes audit data. This affects verifiability and observability.
Application note: Audit is addressed in Annex III in a specific audit section, a specific audit section in this explanatory memorandum, respectively.

T.Auth_Disclose *Disclosure of Authentication Data*

An attacker gains access to authentication data, thus the attacker can impersonate a legitimate user (Administrator, Auditor, Authority, Candidate, Observer, Proposer, or Voter) of the e-election system.

T.Hack *Hacking of the e-election or e-referendum system*

An attacker, both internal or external, interacts with the e-election or e-referendum system, its interfaces or parts of it to exploit vulnerabilities. This may result in arbitrary security compromise and addresses all assets.
Application note: Hacking usually refers to external attackers trying to break the system. However, an attacker has been defined as internal and external, as an authenticated user such as an Administrator acting beyond its legitimate role may also exploit vulnerabilities.

T.Observ_Forgery *Forgery of Observation Data*

An attacker generates, modifies, inserts or deletes observation information. This affects verifiability and observability.

T.System_Forgery *Forgery of System components*

An attacker replaces the e-election system or parts of it with counterfeit elements or presents feigned components as genuine system parts. This threatens system integrity, but may also result in arbitrary compromise of assets.
Application note: The threat is also vital, if in remote e-voting scenarios the attacker redirects the voter to counterfeit systems, such as Internet voting servers that look similar to the original official servers. An example is given, if the attacker controls the domain name service (DNS) and redirects connections to an official server – e.g. *www.voting.official.at* – to a different Internet address. Comparable situations are given, if the attacker owns a domain name that is spelled similarly – e.g. *www.voting.oficial.at* (note the typo).

Pre-Voting Stage:

T.CandList_Disclose *Disclosure of list of candidates information*

An attacker prematurely gains knowledge of the list of candidates or parts of it or the candidate's decision.

Application note: There may be different domestic requirements as to whether a candidate's decision may be disclosed.

T.CandList_Modify *Impersonating during candidate nominations*

An attacker impersonates a proposer nominating a candidate. An attacker impersonates a candidate accepting/declining a nomination. An attacker modifies or deletes the list of candidates.

T.Malfunction_pre *Malfunction of systems or services in pre-voting stage*

A malfunction irrecoverably destroys the list of candidates, or the voters register or the services provided by the nomination process or the registration process. Destruction of the voters register also affects the right to vote.

T.Nomin_DOS *Denial-of-Service against the nomination process*

An attacker disrupts the nomination process or its services, thus the availability of the process during the nomination period is not ensured. An attacker prevents generation of a list of candidates. Disruption of the service also affects the candidate's ability to make a candidate decision.

T.Nomin_Time *Manipulation of nomination period / time*

An attacker compromises the time source of the nomination process or alters the recorded time when a nomination occurred in such a way that, either persons nominated outside the nomination periods are accepted or those nominated within this eligible timeframe are disqualified. This addresses the nomination period, the list of candidates or can affect the timeliness of the candidate's decision.

T.Privacy *Disclosure of personal data*

An attacker reveals voter's or candidate's personal data.
Application note: Different domestic legislation on publication/disclosure of voters registers or candidate's decisions may exist.

T.Registr_DOS *Denial-of-Service against the registration process*

An attacker disrupts the registration process or its services, and thus the availability of the process during the registration period is not ensured. An attacker prevents generation of voters registers. This also affects the right to vote.

T.Registr_Time *Manipulation of registration period / time*

An attacker compromises the time source of the registration process or alters the recorded time when a registration occurred in such a way that either those registering outside the registration period are accepted or registrations within this eligible timeframe are disqualified. This affects the time period, the voters register, and the right to vote.

T.VotReg_Disclose: *Disclosure of voters register information*

An attacker gains knowledge of the voters register or parts of it.
Application note: There may be different domestic requirements on which entities may have access to the voters register or whether the voters register is confidential at all.

T.VotReg_Modify: *Impersonating during voter registration*

An attacker impersonates an entity eligible to be registered for voting and registers/deregisters voters. An attacker modifies or deletes the voters register. This also affects the right to vote.

Voting Stage:

T.Ballot_Forgery *Forgery of the Ballot or the Vote*

An attacker forges the vote carrying the voter's decision or presents a forged ballot to the voter. This also affects the vote, as an unintended decision is represented in the vote.

T.CandList_Modify (see Pre-Voting Stage)

The threat arises if the list of candidates is required in the voting stage, e.g. to generate the ballot. If the ballot is generated from a forged or modified list of candidates, the vote and the voter's decision are affected, as a forged ballot is generated (cf. T.Ballot_Forgery).

T.CommD_Avail_pre *Availability / Integrity of data from pre-voting stage*

An attacker modifies or disrupts data communicated from the pre-voting stages. This results in incorrect or missing lists of candidates or voters registers in the election or referendum stage. A modified voters register affects the voter's right to vote.
Refinement: The threat arises, if the list of candidates or option list are required in the voting stage, e.g. to generate the ballot.
Refinement: The threat arises, if the ballot is generated from a forged or modified list of candidates, the vote and the voter's decision are affected, as a forged ballot is generated (cf. T.Ballot_Forgery).

Application note: The voters register may not be required if in two phase models an anonymous voting token establishes the right to vote. Note that voters registers in the polling station may be needed to prevent multiple votes being cast by the same voter (electronically and on paper-ballot) or in case of a requirement that voters must vote.

T.CommD_Sec_pre *Confidentiality of communicated data*

An attacker gains knowledge of communicated voters registers.
Application note: There may be different domestic requirements on which entities may have access to the voters register or whether a voters register is confidential at all.
Application note: The voters register may not be required if in two phase models an anonymous voting token establishes the right to vote. Note that voters registers in the polling station might be needed to prevent multiple votes being cast (electronically and on paper-ballot) or in case of of a requirement that voters must vote.

T.Malfunction_elect *Malfunction of systems or services in voting stage*

A malfunction irrecoverably destroys the list of candidates, the voters register, votes, or the services provided by the voting process. This also affects the voter's right to vote. If the ballot is generated from the modified voters register, the vote and the voter's decision are affected, as a forged ballot is generated. A malfunction prevents a vote entering the electronic ballot box without the voter being aware or notified of the fact.
Refinement: The threat is given, if the list of candidates or option list is required in the voting stage, e.g. to generate the ballot.
Application note: The voters register may not be required if in two phase models an anonymous voting token establishes the right to vote. Note that voters registers in the polling station might be needed to prevent multiple votes being cast (electronically and on paper-ballot) or in case of a requirement that voters must vote.

T.Vote_Confidentiality *Confidentiality of the voter's decision*

An attacker gains knowledge of a vote. An attacker discovers the identity of the voter from the vote.

T.Vote_DOS *Denial-of-Service against the voting process*

An attacker disrupts the voting process or its services, thus the availability of the process during the voting period is not ensured. An attacker prevents a voter casting a vote using the e-election system, which affects the voter's right to vote. Denial of Service attacks or system overload delay the transmission of the vote and prevent the vote entering the electronic ballot box before the end of the voting period.

T.Vote_Modify *Availability and integrity of votes*

An attacker modifies votes, which results in a vote that does not reflect the voter's decision or an attacker irrecoverably destroys votes.

T.Vote_Multiple *Impersonating an eligible voter*

An attacker or a voter casts multiple votes via a particular voting channel or by using multiple voting channels. This affects the right to vote, which also covers the provision preventing multiple votes being cast.

T.Vote_Time *Manipulation of voting time /period*

An attacker compromises the time source of the voting process or alters the recorded time when a vote has been cast, such that either a vote cast outside the voting period is accepted or a vote cast within the voting period is disqualified. This affects the right to vote.

T.Vote_Trail *Compromising data trails*

An attacker gains access to data trails that establish a link between a vote and the voter's identity. This compromises the voter's decision.

T.Voter_Impers *Impersonating an eligible voter*

An attacker impersonates an eligible voter. This affects the right to vote, as well as the voter's decision and the vote, as a vote which is different from the intention of the legitimate voter is cast.

T.Voter_Privacy *Disclosure of personal data*

An attacker reveals voter's personal data.
Application note: Different domestic legislation on publication/disclosure of voters registers may exist.

T.VotReg_Disclose (see Pre-Voting Stage)

Application note: The voters register may not be required if in two phase models an anonymous voting token establishes the right to vote. Note that voters registers in the polling station might be needed to prevent multiple votes being cast (electronically and on paper-ballot) or in case of a requirement that voters must vote.

T.VotReg_Modify (see Pre-Voting Stage)

Application note: The voters register may not be required if in two phase models an anonymous voting token establishes the right to vote. Note that voters registers in the polling station might be needed to prevent multiple votes being cast (electronically and on paper-ballot) or in case of a requirement that voters must vote.

Post-Voting Stage:

T.CommD_Avail_elec *Availability / Integrity of data from voting stage*

An attacker modifies or disrupts data communicated from the voting stages. This results in incorrect or missing votes – thus an incorrect result – or incorrect or missing lists of candidates.
Application note: The list of candidates or options may be required to generate the result or the election or referendum report.

T.CommD_Sec_elec *Confidentiality of communicated data from voting stage*

An attacker gains knowledge of communicated votes.

T.Count_DOS *Denial-of-Service against the counting process*

An attacker disrupts the counting process or its services, thus the availability of the counting result is not ensured.

T.Malfunction_post *Malfunction of systems or services in post-voting stage*

A malfunction irrecoverably destroys votes, disrupts the counting process or leads to errors in the counting process which affects the result. A malfunction disrupts the ability to generate an election or referendum report or irrecoverably destroys the report.

T.MisCount *Incorrect counting*

An attacker interferes with the counting process, which leads to incorrect results.

T.Partial_Count *Partial counting*

An attacker initiates counting of disaggregated sub-sets of the votes which may reveal the vote from data trails.

T.Premature_Count *Premature counting or disclosure of partial results*

An attacker initiates counting before the desired time and gains access to partial or premature results. Partial results also affect votes confidentiality out of data trails.

T.Report_DOS *Denial-of-Service against the reporting process*

An attacker disrupts the reporting process or its services, thus the availability of the election or referendum report is not ensured.

T.Report_Modify *Modification of the Election or referendum Report*

An attacker modifies the election or referendum report

T.Result_Modify *Modification of the Result*

An attacker modifies the result.

T.Vote_Confidentiality (see Voting Stage)

T.Vote_Duplicates *Modification of the Result*

An attacker or a malfunction generates duplicates of votes that can not be detected as such, which affects the result.

T.Vote_Modify (see Voting Stage)

T.Vote_Trail (see Voting Stage)

The following tables 1 to 3 gives an overview of which threat affects which asset in each of the process stages. Assets and threats that appear in several process stages (besides the general assets/threats) are marked with a *).

Table 1: Assets and threats to it in Pre-Voting Stage

	Assets / Threats	General			Pre-Voting Stage								
		Authentication Data	**Verifiabi./Observab.**	**System integrity**	**Candidate decision**	**List of candidates** *)	**Voters register** *)	**Nomination process**	**Nomination period**	**Privacy** *)	**Registration process**	**Registration period**	**Right to vote** *)
General	**T.Audit_Forgery**		X										
	T.Auth_Disclose	X											
	T.Hack	X	X	X	X	X	X	X	X	X	X	X	X
	T.Observ_Forgery		X										
	T.System_Forgery	X	X	X	X	X	X	X	X	X	X	X	X
Pre-Voting Stage	**T.CandList_Disclose**				X	X				X			
	T.CandList_Modify *)				X	X							
	T.Malfunction_pre					X	X	X			X		X
	T.Nomin_DOS				X	X		X					
	T.Nomin_Time				X	X			X				
	T.Privacy				X	X	X			X			
	T.Registr_DOS						X				X		X
	T.Registr_Time						X					X	
	T.VotReg_Disclose *)						X			X			
	T.VotReg_Modify *)						X						X

Table 2: Assets and threats to it in Voting Stage

Assets / Threats		General			Voting Stage								
		Authentication Data	**Verifiab./Observab.**	**System integrity**	**Ballot**	**List of candidates** *)	**Voters register** *)	**Right to vote** *)	**Vote** *)	**Voter's decision** *)	**Voter's privacy**	**Voting period**	**Casting of a vote**
General	**T.Audit_Forgery**		X										
	T.Auth_Disclose	X											
	T.Hack	X	X	X	X	X	X	X	X	X	X	X	X
	T.Observ_Forgery		X										
	T.System_Forgery	X	X	X	X	X	X	X	X	X	X	X	X
Voting Stage	**T.Ballot_Forgery**				X				X	X			
	T.CandList_Modify *)				X	X			X	X			
	T-CommD_Avail_pre					X	X	X					
	T-CommD_Sec_pre						X						
	T.Malfunction_elect				X	X	X	X	X	X			X
	T.Vote_Confidentiality *								X	X			
	T.Vote_DOS							X					X
	T.Vote_Modify *)								X	X			
	T.Vote_Multiple							X					
	T.Vote_Time							X				X	
	T.Vote_Trail *)									X			
	T.Voter_Impers							X	X	X			
	T.Voter_Privacy						X				X		
	T.VotReg_Disclose *)						X				X		
	T.VotReg_Modify *)						X	X					

Table 3: Assets and threats to it in Post-Voting Stage

Assets / Threats		General			Post-Voting Stage					
		Authentication Data	**Verifiab./Observab.**	**System integrity**	**List of candidates** *)	**Counting process**	**Counting result**	**Election report**	**Vote**	**Reporting process**
General	**T.Audit_Forgery**		X							
	T.Auth_Disclose	X								
	T.Hack	X	X	X	X	X	X	X	X	X
	T.Observ_Forgery		X							
	T.System_Forgery	X	X	X	X	X	X	X	X	X
Post-Voting Stage	**T.CommD_Avail_elec**				X		X		X	
	T.CommD_Sec_elec								X	
	T.Count_DOS					X	X			
	T.Malfunction_Post					X	X	X	X	
	T.MisCount						X			
	T.Partial_Count								X	X
	T.Premature_Count						X		X	X
	T.Report_DOS							X		
	T.Report_Modify							X		
	T.Result_Modify						X			
	T.Vote_Confidentiality *)								X	X
	T.Vote_Duplicates						X		X	
	T.Vote_Modify *)						X		X	
	T.Vote_Trail *)								X	X

Security Objectives

This section identifies and defines the security objectives for e-voting. The objectives reflect the stated intent and counter the identified threats. The security objectives given in this section represent the security requirements that are given as *Security Requirements* in *Appendix III*.

General objectives:

O.Access_Cntrl *Access control*

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.

O.Assessment *Independent assessment*

Election authorities have overall responsibility for compliance with these security requirements which shall be assessed by independent bodies.
Application note: In case evaluated and certified CC / ISO 15408 Protection Profiles are developed based on this security recommendations, independent assessment is given under the CC scheme.

O.Auth_User *User authentication*

The e-voting system shall protect authentication data so that unauthorized entities can not misuse, intercept, modify, or otherwise gain knowledge of authentication data or part of it. In uncontrolled environments, authentication based on cryptographic mechanisms is advisable.
Application note: The objective refers to all subjects. Services such as information services for the voter prior to entering the voting process, which (clearly do not need authentication) are outside the scope of this document.

O.Avail *Availability of the e-election processes*

Technical and organisational 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. The e-voting system shall contain measures to preserve the availability of its services during the e-voting process. It shall resist, in particular, malfunction, breakdowns or denial of service attacks.
Application note: Service level agreements (SLAs) usually lay down availability and failure rates. A certain level of service degradation may be acceptable during failure periods, e.g. when a server in a cluster breaks. In registration processes short periods of service disruptions or maintenance periods may be tolerable. The system developer however needs to consider deliberate denial of service attacks and shall document the contingency reserve in system performance that has been designated. Independent penetration tests can reduce the probability of successful deliberate service disruption.
Refinement: The services to be preserved in availability depend on the stage – Pre-Voting,. Voting, Post-Voting. In the Pre-Voting Stage, the nomination and the registration processes and its services are to be available, in the Voting Stage the voting processes and its services, and in the Post-Voting Stage the counting and reporting processes and its services. Auditing processes need to be available in all stages. The pre-defined limits for SLAs, tolerable failure rates, or service degradation may however be different for the various stages or services.

O.Ident_User *Identity-based user authentication*

Identification of voters and candidates in a way that they can unmistakably be distinguished from other persons (unique identification) shall be ensured.
Application note: Authentication can be identity based or role-based. While identity-based authentication is advisable for voters registering or casting a vote, or candidates accepting / declining a nomination, it might be sufficient to have role-based authentication for administrators, Auditors, etc.

O.Observation_Data *Observation data*

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.

O.Privacy *Privacy of voters and candidates*

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.

Refinement: When stored in or communicated to uncontrolled environments, the voters registers should be sealed.

Application note: Depending on domestic practices there might be further confidentiality requirements with respect to the candidate's decision. In that case confidentiality is required.

O.Reliable_Time *Reliable time source*

The e-voting system shall maintain reliable synchronised time sources. The accuracy of the time source shall be sufficient to maintain time marks for audit trails and observation data, as well as for maintaining the time limits for registration, nomination, voting, or counting.

Application note: There may be different accuracy requirements for different consumers of the time source, such as different tolerances for the registration event and casting a vote. This may lead to multiple time sources or a single time source that provides the highest accuracy. The term "time mark" has been used as an indication for marking the data. There are several means depending on the situation: Secure time stamps might be needed for critical events, whereas e.g. continuous sequence numbers or preserving the sequence may be sufficient for log entries. Note, that exact time stamps on votes may also jeopardise the confidentiality of the voter's decision.

O.Secure_Oper *Secure operation and system integrity*

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.

Pre-Voting-Stage:

O.Data_Sec *Availability and Integrity of the election or referendum, options, lists of candidates*

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 taken into account.

Refinement: Depending on domestic requirements, practice with respect to confidentiality/publication of candidate's decision or the voters register may differ.

Application note: Data-origin authentication can, e.g., be provided by electronic signatures in fully electronic processes. In semi-electronic processes, data-origin authentication may employ also conventional security measures, such as manual signatures, seals, couriers, etc.

O.Time_Nominate *Timely nomination*

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.

Application note: This can e.g. be provided by time marks or a confirmation of a trustworthy system.

O.Time_Register *Timely registration*

The fact that voter registration has happened within the prescribed time limits shall be ascertainable.

Application note: This can e.g. be provided by time marks or a confirmation of a trustworthy system.

Voting-Stage:

O.Authentic_Vote *Ensure authentic vote*

The e-voting system shall ensure that the voter's choice is correctly represented in the vote and that the sealed vote enters the electronic ballot box.

O.Ballot_Correct *Present an authentic ballot*

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 the authentic ballot been presented.
Application note: Aspects to be considered are that counterfeit servers may be given, such as faking an official server by tampering the domain name system (DNS), using a similar domain name to that of official server, man.in.the-middle attacks, or Trojan horses at the voter's system replacing the original ballot or fading in counterfeit ballots. Electronic signatures applied to the ballot by the electoral authority allow for verifying the ballot. This must, however, not violate the confidentiality of the voter's decision. Therefore the data to prove a authentic ballot shall either not lead to uniquely identifiable ballots, or such unique data shall be removed when the voter casts the vote.

O.Delayed_Vote *Accept delayed votes*

After the end of the e-voting period, no voters shall be allowed to gain access to the e-voting system. 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.
Application note: In remote voting scenarios, a higher load of the services might occur in the short period right before closing the poll. This may lead to increased load and increased delays until a cast vote enters the electronic ballot box. Votes that have been cast in time however shall be accepted. Thus, server shall not be shut down immediately with the closing time of the service, if such increased delays are to be expected.

O.Sec_Transfer_pre *Secure transfer of communicated data*

Data communicated from the pre-voting stage (e.g. voters registers and lists of candidates) shall be maintained in integrity. Data-origin authentication shall be carried out.
Refinement: Lists of candidates are required in the voting stage, if the ballot is generated in the election stage.
Refinement: The voters register may not be required if in two phase models an anonymous voting token establishes the right to vote. Note that voters registers in the polling station might be needed to prevent multiple votes being cast (electronically and on paper-ballot) or in case of a requirement that voters must vote.
Application note: Data-origin authentication can e.g. be provided by electronic signatures in fully electronic processes. In semi-electronic processes, data-origin authentication may employ also conventional security measures, such as manual signatures, seals, couriers, etc.

O.System_Secure *Secure Voting System*

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 can modify the vote.
Refinement: In unattended remote voting environments, such as Internet voting, usually the voter or third parties control the environment. There are limited means by which the election or referendum system can control whether a secure environment exists. Means that allow the voters to gain confidence in the system must be provided, such as means to ensure that genuine software is used, or recommendations on how to protect the system environment.

O.Residual_Info *Destroy residual information*

Residual information holding the voter's decision or the display of the voter's choice shall be destroyed when 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, from the device used to cast the vote.

Application note: Residual information may be given in the cache of Internet browsers, data swapped to disks, temporary files, etc. There are some means to, e.g., develop Internet applications in such a way that certain types of residual information can be avoided. However, the effectiveness of such measures is dependent on the voter's application and its configuration. In remote voting environments, such as Internet voting, usually the voter or third parties control the environment. There are limited means by which the e-election system can control whether a secure environment exists. Means that allow the voters to gain confidence in the system may be provided, such as means to ensure that genuine software is used, or recommendations on how to protect the system environment.

O.Time_Vote *Timely casting of a vote*

The fact that a vote has been cast within the prescribed time limits shall be ascertainable.
Application note: This can, e.g., be provided by time stamps or a confirmation of a trustworthy system. A time-stamp attached to the cast vote however may not leave data trails that can reveal the voter's decision (cf. O.Vote_Confidentiality).

O.Vote_Confidentiality *Confidentiality of a voter*

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.
Note: This objective gives technical requirements. It is, however, represented in the legal standards "Reliability and Security", standard 35.

O.Vote_Secure *Availability, Confidentiality and Integrity of cast votes*

The e-voting 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.
Note: This objective involves technical requirements. It, however, is also represented in the legal standards "Reliability and Seucurity", standard 34.
Application note: Encryption is a technology of choice to seal a vote, particularly in remote voting scenarios or when cast votes are transmitted via public channels. For voting machines in polling stations physical protection may also serve to seal a vote. The explanation for sealing (see Glossary) distinguishes between encryption and e.g. closed channels. In uncontrolled environments, the votes, as the primary asset of an e-elections and the confidentiality of the voter's choice, as being the primary concern of voters, require the highest level of security measures. Accordingly, the requirement explicitly refers to encryption when outside controlled environments.

O.Voter_Eligible *Authentication of a voter eligible to cast a vote*

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.
Refinement: In cases where anonymous voting tokens are used to prove that a voter is eligible to vote, authentication of the voter may not be required. However, even in such cases it is still necessary to ensure that the casting of multiple votes is prevented.

Post-Voting-Stage:

O.Count_Correct *Correctness and reproducibility of the counting result*

The counting process shall accurately count the votes. The counting of votes shall be reproducible.

O.Result_Secure *Availability and Integrity of ballot box and result*

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.

O.Sec_Transfer_vote *Secure transmission of communicated data*

The integrity of data communicated from the voting stage (e.g. votes, voters registers, lists of candidates) shall be maintained. Data-origin authentication shall be carried out.
Application note: Data-origin authentication can e.g. be provided by electronic signatures in fully electronic processes. In semi-electronic processes, data-origin authentication may also employ conventional security measures, such as manual signatures, couriers, etc. Cast votes or partially counted results are, however, the most valuable asset in an election or referendum. Thus, it is preferable to provide technical measures to protect these assets during the transmmission.

O.Vote_Confidentiality see Voting Stage

O.Vote_Secure see Voting Stage

The following tables 4 to 7 map the objectives to the threats that are countered. Threats that appear in several process stages (besides the general assets/threats) are marked with a *).

Table 4: Objectives to threats mapping, General Objectives - all stages

Objectives / Threats		General Objectives								
		O.Access_Cntrl	O.Assessment	O.Auth_User	O.Avail	O.Ident_User	O.Observation_Data	O.Privacy	O.Reliable_Time	O,Secure_Oper
General	T.Audit_Forgery	X	Independent assessment does not directly counter threats, but provides confidence in the correctness. i.e., threats are indirectly countered.	X					X	
	T.Auth_Disclose	X		X						
	T.Hack	X		X	X					X
	T.Observ_Forgery	X		X			X		X	
	T.System_Forgery	X		X			X			X
Pre-Voting Stage	T.CandList_Disclose	X		X			Observation assists in correct operation of the election event, i.e. indirectly counters threats.	X		
	T.CandList_Modify *)	X		X	X					
	T.Malfunction_pre				X					X
	T.Nomin_DOS				X					X
	T.Nomin_Time	X		X					X	
	T.Privacy	X		X		X		X		
	T.Registr_DOS				X					X
	T.Registr_Time	X		X					X	
	T.VotReg_Disclose *)	X		X				X		
	T.VotReg_Modify *)	X		X	X	X				
Voting Stage	T.Ballot_Forgery									X
	T.CandList_Modify *)	X		X						
	T-CommD_Avail_pre	X		X	X					
	T-CommD_Sec_pre	X		X				X		
	T.Malfunction_elect				X					X
	T.Vote_Confidentiality *)									
	T.Vote_DOS				X					X
	T.Vote_Modify *)	X		X						
	T.Vote_Multiple					X				
	T.Vote_Time	X		X					X	
	T.Vote_Trail *)									
	T.Voter_Impers	X		X		X				
	T.Voter_Privacy	X		X				X		
	T.VotReg_Disclose *)	X		X				X		
	T.VotReg_Modify *)	X		X						
Post-Voting Stage	T.CommD_Avail_elec	X		X						
	T.CommD_Sec_elec	X		X						
	T.Count_DOS				X					X
	T.Malfunction_Post				X					X
	T.MisCount									
	T.Partial_Count	X		X						
	T.Premature_Count	X		X					X	
	T.Report_DOS				X					X
	T.Report_Modify	X		X						
	T.Result_Modify	X		X						
	T.Vote_Confidentiality *)									
	T.Vote_Duplicates									
	T.Vote_Modify *)	X		X						
	T.Vote_Trail *)									

Table 5: Objectives to threats mapping, Pre-Voting Stage

Objectives / Threats		General	Pre-Voting Stage		
			O.Data_Sec *)	**O.Time_Nominate**	**O.Time_Register**
General	**T.Audit_Forgery**	see table 4			
	T.Auth_Disclose				
	T.Hack				
	T.Observ_Forgery				
	T.System_Forgery				
Pre-Voting Stage	**T.CandList_Disclose**	see table 4	X		
	T.CandList_Modify *)		X		X
	T.Malfunction_pre				
	T.Nomin_DOS				
	T.Nomin_Time			X	
	T.Privacy		X		
	T.Registr_DOS				
	T.Registr_Time				X
	T.VotReg_Disclose *)		X		
	T.VotReg_Modify *)		X	X	

Table 6: Objectives to threats mapping, Voting Stage

Objectives / Threats		General	Voting Stage									
			O.Authentic_Vote	O.Ballot_Correct	O.Delayed_Vote *)	O.Residual	O.Sec_Transfer_pre	O.System_Secure	O.Time_Vote	O.Vote_Confidentiality	O.Vote_Secure	O.Voter_Eligible
General	T.Audit_Forgery	see table 4										
	T.Auth_Disclose							X				
	T.Hack							X				
	T.Observ_Forgery											
	T.System_Forgery							X				
Voting Stage	T.Ballot_Forgery	see table 4	X	X			X	X				
	T.CandList_Modify *)						X					
	T-CommD_Avail_pre						X					
	T-CommD_Sec_pre						X					
	T.Malfunction_elect		X					X				
	T.Vote_Confidentiality *)		X			X		X		X	X	
	T.Vote_DOS		X		X				X			
	T.Vote_Modify *)		X	X				X	X		X	
	T.Vote_Multiple											X
	T.Vote_Time								X			
	T.Vote_Trail *)					X			X	X		
	T.Voter_Impers							X				X
	T.Voter_Privacy									X	X	
	T.VotReg_Disclose *)						X					
	T.VotReg_Modify *)						X					

Table 7: Objectives to threats mapping, Post-Voting Stage

Objectives / Threats		General	Post-Voting Stage				
			O.Count_Correct	O.Result_Secure	O.Sec_Transfer_vote	O.Vote_Confidentiality	O.Vote_Secure
General	T.Audit_Forgery	see table 4					
	T.Auth_Disclose						
	T.Hack						
	T.Observ_Forgery						
	T.System_Forgery						
Post-Voting Stage	T.CommD_Avail_elec	see table 4			X		
	T.CommD_Sec_elec				X		
	T.Count_DOS						
	T.Malfunction_Post						
	T.MisCount		X				
	T.Partial_Count			X		X	
	T.Premature_Count						
	T.Report_DOS						
	T.Report_Modify				X		
	T.Result_Modify			X	X		
	T.Vote_Confidentiality *)					X	X
	T.Vote_Duplicates		X				
	T.Vote_Modify *)						X
	T.Vote_Trail *)					X	