DIRECTION GENERALE DE LA DEMOCRATIE ET DES AFFAIRES POLITIQUES

DIRECTION DES INSTITUTIONS DÉMOCRATIQUES

PROJET « BONNE GOUVERNANCE DANS LA SOCIETE DE L'INFORMATION »

GGIS (2010) 3 F fin.

Strasbourg, le 16 février 2011

Certification des systèmes de vote électronique

Lignes directrices pour la conception de processus de confirmation du respect des exigences et normes recommandées

Document élaboré par le Secrétariat

Introduction

En 2004, le Comité des Ministres du Conseil de l'Europe a adopté la Recommandation (2004) 11 sur les normes juridiques, opérationnelles et techniques relatives au vote électronique. A la suite de l'adoption de ce texte, les Etats membres du Conseil de l'Europe sont convenus de tenir des réunions biennales en vue d'examiner régulièrement leurs politiques et expériences respectives en matière de vote électronique. La première de ces réunions s'est tenue à Strasbourg en novembre 2006 ; la deuxième a eu lieu à Madrid, en Espagne, en octobre 2008 et la troisième réunion en novembre 2010, à Strasbourg.

Lors de la Deuxième réunion biennale (en 2008), le Secrétariat a été invité à étudier la question du renforcement de l'application de cette recommandation. Il a été notamment proposé d'analyser de manière plus approfondie certains aspects de la Recommandation, tels que la question de la certification des systèmes de vote électronique, ou encore celle de la transparence des élections pour lesquelles le vote électronique est autorisé.

C'est dans cet esprit que des travaux ont été entrepris au sujet de la certification des systèmes de vote électronique, et que les présentes lignes directrices ont été définies – à la lumière des conclusions des ateliers ayant travaillé sur cette question (ateliers qui ont eu lieu au Conseil de l'Europe, à Strasbourg, les 26 et 27 novembre 2009, les 31 mai et 1er juin 2010, et, enfin, les 27 et 28 septembre 2010). Elles ont été examinées et endossées lors de la troisième réunion biennale intergouvernementale en vue d'examiner les évolutions intervenues dans le domaine du vote électronique et l'application de la Recommandation Rec(2004)11 du Comité des Ministres, qui s'est tenue à Strasbourg les 16-17 novembre. La présente version finale des Lignes directrices tient compte des commentaires émis lors de cette réunion.

Les présentes lignes directrices sont un instrument concret, visant à faciliter l'application de la Recommandation de 2004 – et notamment des paragraphes 111 et 112, qui recommandent aux Etats membres de mettre en place des processus de certification permettant le contrôle et la validation de tous les éléments électroniques en vue de certifier leur conformité avec les exigences techniques définies.

Dans le présent document, la notion de « certification » se réfère à un processus de confirmation de la conformité de tel ou tel système de vote électronique avec les exigences et les normes définies dans ce domaine, et du fait que le système en question propose au minimum des dispositions permettant de vérifier son bon fonctionnement. Le processus en question peut aller de simples tests et audits à l'établissement d'une certification officielle. Le résultat final en sera un rapport et/ou un certificat.

La valeur ajoutée du processus de certification n'est pas seulement d'établir si tel ou tel système de vote électronique est conforme aux exigences et normes définies ; il s'agit également d'un instrument important pour susciter la confiance. Le processus de certification peut être également utile dans le contexte des offres de marchés publics.

Les présentes lignes directrices doivent avoir leur utilité lors d'élections et de référendums politiques, à tous les niveaux de gouvernance. Elles ne visent pas à imposer une ligne de conduite précise à tel ou tel pays en matière de certification ; ces lignes directrices sont plutôt conçues comme un instrument au service des Etats membres, leur permettant d'évaluer les exigences liées à un processus global de certification. Le présent document vise à aider les Etats membres à améliorer leurs processus actuels, à l'échange des meilleures pratiques et à la mise en place progressive d'un cadre commun.

Le processus de certification peut prendre différentes formes. Tel ou tel Etat membre peut décider un processus national de certification d'un système unique de vote électronique ; il peut également opter pour la certification de plusieurs systèmes, accorder au système de vote électronique un certificat provisoire, ou encore tester une ou plusieurs composantes du système – ce que l'on pourrait appeler un test partiel. Un Etat membre pourra aussi choisir, dans les présentes lignes directrices, les dispositions correspondant le mieux à son propre système de vote – dans un souci de répondre à d'éventuels menaces ou risques particuliers, tout en respectant les engagements définis au niveau international.

Les présentes « Lignes directrices » abordent divers aspects pertinents des processus électoraux et référendaires – autrement dit, la phase préélectorale, l'élection même, puis la phase postélectorale, mais aussi les rôles et responsabilités des différents acteurs. Les Etats n'auront pas tous nécessairement recours aux techniques électroniques à tous les stades d'une élection ; par conséquent, les présentes lignes directrices concernent avant tout les phases électorales pour lesquelles tel ou tel Etat membre a décidé d'utiliser ces techniques.

Chaque ligne directrice se décline dans un ou plusieurs paragraphe(s) explicatif(s). Un glossaire des termes récurrents est également proposé à l'Annexe I, et des extraits pertinents de la Recommandation (2004) 11 figurent à l'Annexe II. Enfin, pour bien visualiser le processus de certification, un modèle théorique global – indiquant la forme éventuelle que peut prendre le processus – est proposé à l'Annexe III.

Réglementation et supervision

1. Les Etats membres sont responsables du fonctionnement de l'ensemble des systèmes de vote électronique utilisés sur leur territoire lors d'élections et référendums officiels

De nombreux acteurs ont un rôle à jouer et une certaine responsabilité dans les processus de conception, de test, de certification, de mise en place, d'application, d'observation et de contrôle des systèmes de vote électronique. Mais, au final, sur le plan électoral, seul l'Etat est globalement responsable du système de vote électronique et de sa certification.

2. Les Etats membres doivent définir les objectifs du processus de certification et les exigences en matière de procédures et de méthodes souhaitables dans ce domaine

En matière de certification d'un système de vote électronique – qu'il fonctionne ou non à distance -, la première étape consiste à définir clairement les objectifs et les exigences de la procédure de certification. Pour définir ces exigences, il importe de vérifier d'abord si elles sont conformes à la législation nationale et aux normes internationales – y compris les procédures d'appel ou de dépôt de plainte concernant la conduite des élections.

Si la définition d'un ensemble d'exigences très précises peut apparaître, a priori, comme une option satisfaisante pour garantir une bonne analyse dans le sens de la certification, un tel cadre juridique peut - du fait de son caractère rigide - avoir des effets pervers. Ainsi, alors que les contrôleurs des systèmes seraient soumis à des exigences très strictes, les concepteurs et vendeurs des systèmes en question pourraient simplement se contenter d'adapter le « produit » aux exigences particulières de telle ou telle

administration électorale. Dès lors, ces vendeurs pourraient ne pas rechercher une qualité optimale, et l'administration électorale concernée serait contrainte – du fait des règles juridiques qu'elle a elle-même fixées - d'accepter un « sous-produit ». L'utilisation d'un « contrat » où le critère de sélection serait la qualité et non le prix devrait aider à éviter ce piège.

Par conséquent, le fait de préciser très clairement les objectifs, le logiciel à utiliser, le mode opératoire, le matériel nécessaire et les exigences du processus de certification – ainsi que sa portée et les méthodes souhaitables – pourra contribuer à l'efficacité de ce processus, à son applicabilité parfaite et à une transparence globale des systèmes de vote électronique.

Le processus de certification des systèmes de vote électronique ne se limite pas à la certification initiale ; il recouvre également une démarche de « dé-certification » et de « re-certification » des logiciels, des modes opératoires, des matériels et de l'ensemble des processus.

D'autre part, un certain nombre de facteurs sociopolitiques peuvent influer sur la confiance du citoyen et créer des problèmes importants. Ce type de facteurs pouvant avoir également des effets sur les processus de certification, les Etats membres devraient promouvoir une recherche scientifique dans ce domaine – y compris des échanges, au niveau international, d'informations pertinentes. Sont nécessaires, dans ce contexte, une connaissance globale et néanmoins nuancée des attentes de la société et des responsables politiques, ainsi que des effets des nouveaux modes de vote sur le comportement électoral et les acteurs politiques.

Il conviendrait de mettre en place un cadre pouvant garantir que toutes les parties concernées connaissent et comprennent bien le système utilisé. Dans ce domaine, tous les efforts déployés devraient concorder avec les méthodologies bien établies, telles que les tests de confirmation, les tests concernant les différentes composantes, les tests de performance et les tests de fonctionnement.

3. Les Etats membres doivent veiller à ce que l'ensemble des exigences techniques soit totalement conforme aux principes juridiques et démocratiques pertinents

Dans ce contexte, on doit prendre acte de deux réalités : d'une part, l'approche dite des « Critères communs », fondée sur le dialogue entre usagers et vendeurs des systèmes ; d'autre part, l'approche KORA (*Konkretisierung rechtlicher Anforderungen* – c'est-à-dire la « concrétisation des exigences juridiques »)[1], qui vise à améliorer et faciliter le rapport entre les points de vue juridique et technique. La loi ne devrait toutefois pas être changée seulement pour correspondre aux critères d'un concepteur de système.

[1] Pour de plus amples informations, veuillez consulter le site Internet http://www.uni-koblenz-landau.de/koblenz/fb4/institute/iwvi/aggrimm/projekte/modiwa (en langue allemande uniquement)

4. Les Etats membres doivent fixer et publier des règles très claires de communication du rapport final de certification et autres documents pertinents – sur la base du principe de transparence

Les Etats membres devront élaborer et rendre publiques des procédures déterminant qui a accès à quelles informations, et à quel moment. Il faudra accorder une attention toute particulière aux besoins des observateurs nationaux et internationaux, ainsi qu'à ceux des médias. Il faudra également établir des procédures en direction d'autres acteurs, tels que les citoyens, les partis politiques, les ONG et – cet élément n'étant pas des moindres – les responsables officiels des élections. Ces règles procédurales seront essentielles si l'on veut renforcer la confiance des populations dans des systèmes de vote électronique sécuritaires et fiables, ainsi que dans la fonction de contrôle qu'exercent les autorités électorales. Ce n'est que dans des circonstances exceptionnelles que l'on pourra envisager de ne pas divulguer le rapport de certification ou certains éléments du document en question.

Il faudra également accorder une attention particulière aux éléments du logiciel qui concernent la sécurité du système. Cela pourra se faire par des tests de sécurité dans le cadre de l'ensemble des tests à effectuer, afin de permettre à l'usager de bien comprendre la garantie de sécurité du système. On pourra également envisager un « étiquetage » de l'ensemble des documents, aussi bien par les Etats membres que par les « vendeurs ».

Il pourra y avoir désaccord entre les différents vendeurs des systèmes, voire entre les certificateurs eux-mêmes quant à la publication ou non de certains éléments du système en question – voire de la majeure partie des documents concernant ce système -, dans un souci de protection de la propriété intellectuelle. Mais, si l'on veut éviter un secret excessif au sujet des processus de certification, il conviendra de faire comprendre aux vendeurs et aux certificateurs potentiels – dans le cadre de l'appel d'offres – que tous les acteurs concernés doivent avoir accès à certains documents. Tout « accord de non-divulgation » permettant aux observateurs de ne pas rendre publics les évaluations et les éléments qui les fondent rendrait très difficile un processus de supervision pertinent.

Enfin, pour superviser le processus de certification ou compenser une publication partielle des informations concernées, les Etats membres pourront créer des comités spéciaux – composés d'experts, d'universitaires et/ou de responsables politiques Dans ce contexte, nous pouvons mentionner le « Collège d'experts » en Belgique, qui est chargé de superviser l'ensemble du processus électoral pour l'assemblée législative compétente.

5. Les observateurs électoraux accrédités doivent avoir accès à toutes les phases du processus de certification

Au cours des vingt dernières années, le processus d'observation des élections est apparu comme un excellent instrument de transparence électorale et d'accès aux processus électoraux. Mais, avec l'émergence du vote électronique, les méthodes traditionnelles d'observation des élections doivent être actualisées. Pour permettre aux observateurs de suivre les processus de certification des systèmes de vote électronique, il va falloir prolonger la durée des missions d'observation électorale. Il est essentiel qu'aucune procédure de certification du vote électronique n'ait lieu à huis clos – car une telle

pratique éveillerait forcément des soupçons. Les observateurs doivent avoir accès à l'ensemble des informations pertinentes pendant toute la durée du processus de certification, afin de pouvoir accomplir correctement leur mission.

En 2005, « La Déclaration de principes pour l'observation internationale d'élections et le Code de conduite à l'usage des observateurs électoraux internationaux »[2] ont mis en place un cadre commun d'observation électorale – cadre approuvé par l'ensemble des organisations internationales opérant dans ce domaine. Parmi les principes en question figure celui de la divulgation des méthodes utilisées.

Sélection des organes de certification

6. Les Etats membres doivent concevoir un cadre précis de responsabilités institutionnelles, de critères et de procédures permettant de garantir la compétence et l'indépendance des organes de certification

Tout organe autorisé à participer au processus de certification d'un système de vote électronique – y compris les certificateurs, les évaluateurs et les contrôleurs – doit être indépendant et qualifié. Par conséquent, la législation des Etats doit mentionner explicitement les critères et les modes de sélection des organes de certification, ainsi que les institutions compétentes pour y procéder. Les Etats membres doivent assumer la définition des règles et lignes directrices concernant ce processus de sélection. L'ensemble des procédures doit être connu et rendu public assez longtemps avant la date des élections en question. Cela permettra de faciliter la tâche des vendeurs des systèmes et de contribuer à la confiance des électeurs dans les processus concernés. Le nombre d'organes de certification ne doit pas être restreint ; tout organe indépendant et qualifié devrait pouvoir se porter candidat au processus de certification. La préférence devrait être donnée à l'utilisation d'un appel d'offre ou d'une consultation européen/ne avec un ensemble de certificateurs potentiels pour la détermination de certificateurs qualifiés.

Les Etats membres devraient envisager de confier la sélection des organes de certification à des contrôleurs professionnels et certifiés au niveau international. Le « CISA » (« Certified Information System Auditors »/Auditeurs certifiés de systèmes d'information) en est un bon exemple, dans la mesure où cet organe a défini des normes de performance concernant l'ensemble des contrôleurs et évaluateurs de systèmes de technologies de l'information et de méthodologie commerciale de telle ou telle organisation. Il convient de prêter attention à de telles procédures. Un autre facteur important est que l'utilisation des certificats internationaux ne devrait pas devenir un obstacle empêchant les Etats membres d'utiliser un système de vote électronique spécifique ou même rendre impossible à certains pays l'utilisation d'un système de vote électronique valable.

7. Le mandat de l'organe de certification doit être confirmé à intervalles réguliers

Les Etats membres devront concevoir des méthodes concernant non seulement la procédure initiale de sélection, mais aussi les procédures de suivi telles que celles de

[2] cf. le site Internet http://www.venice.coe.int/site/dynamics/N_Opinion_ef.asp?L=E&OID=325

réexamen et de confirmation éventuelle du mandat en question, voire de non-reconduction de ce mandat. Tout mandat accordé à un organe de certification des systèmes de vote électronique doit être à durée limitée. De nouveaux appels d'offres doivent avoir lieu à intervalles réguliers et être rendus publics. On devra déterminer clairement si la décision de confier le processus de certification à tel ou tel organe relève du vendeur ou des autorités électorales compétentes.

Le processus de certification

8. Les organes chargés des processus de certification doivent respecter les règles et exigences officiellement définies et rendues publiques

Les procédures de certification doivent obéir à des règles et lignes directrices très claires – y compris les questions de responsabilité – et devant être rendues publiques assez longtemps avant la date des élections en question. Ce type de contrôle qualitatif est indispensable au processus. Comme nous l'avons déjà souligné, cela facilitera la tâche des vendeurs et renforcera la confiance de l'électorat.

Le processus de certification portera notamment sur les logiciels, les modes opératoires, les matériels, les procédures et le personnel – y compris la capacité effective d'utilisation, l'accessibilité, des éléments tels que les bulletins de vote, la publication des résultats du scrutin, les liens entre le système de vote électronique et d'autres logiciels, ou encore l'examen des documents pertinents. On devra également intégrer au processus de certification les éléments suivants : la phase préélectorale, le vote en soi, le comptage, le caractère adapté ou non du cadre juridique régissant le vote électronique, etc.

Parmi les responsabilités spécifiques des organes de certification, on citera la réunion de preuves objectives suffisantes pour décider ou non d'accorder le certificat, et l'engagement à sélectionner des contrôleurs compétents et dûment formés.

L'un des problèmes particuliers qui se posent en matière de certification est celui du vote électronique à distance, via Internet : en l'occurrence, les logiciels et matériels utilisés par l'usager peuvent être extérieurs à l'espace officiel de certification. Tous les acteurs concernés doivent être informés des risques potentiels d'un recours à des systèmes informatiques extérieurs à l'environnement électoral sous contrôle, ainsi que des solutions éventuelles à ce type de problème.

9. Les Etats membres pourront envisager le recours à des protocoles normalisés, notamment lors des processus officiels de certification

La ligne directrice que nous venons d'exposer a trait au processus de certification au sens le plus large et le plus officiel du terme.

Mais, au-delà des normes et recommandations reconnues en la matière – notamment les dispositions de la Constitution de tel ou tel pays, le Code de bonne conduite en matière électorale et le Code de bonne conduite en matière référendaire, établis par la Commission de Venise du Conseil de l'Europe, ou encore la Recommandation (2004) 11 du Comité des Ministres du Conseil de l'Europe sur les normes juridiques,

opérationnelles et techniques relatives au vote électronique -, il importe également de déterminer quels protocoles utiliser. Parmi les exemples de protocoles disponibles, il convient de citer ISO 9001, ISO 9000-3, IT Grundschutz[3] (qui concerne la protection de l'environnement opérationnel, y compris ISO 27001), ou encore les capacités de résistance k aux menaces internes[4], le « Content Management System » (Système de gestion des contenus) et les Critères communs (ISO 15408).

Si chacun de ces protocoles a son rôle à jouer dans le cadre du processus de certification, il sera préférable de les associer et de les utiliser ensemble. Pour prendre un exemple, le protocole ISO 27001 ne concerne que les questions procédurales et organisationnelles, et non pas le cœur du système – autrement dit le logiciel et autres éléments similaires. Par conséquent, il sera utile d'associer l'ISO 27001 et la méthode des Critères communs.

Si la certification par le protocole ISO peut être très utile, il faut noter que ce processus est également limité dans le temps. En d'autres termes, il pourra être nécessaire de reproduire l'ensemble du processus de certification ISO pour chaque élection, ce qui pourrait être une procédure très couteuse. Par ailleurs, cette procédure, qui est longue, pourra ne pas être valable dans le cas d'élections anticipées, qui pourraient soulever le problème de coûts exagérément élevés.

10. Les Etats membres pourront envisager d'autoriser les organes de certification à trouver des moyens adaptés d'analyser et de réutiliser éventuellement des matériels existants, déjà utilisés lors de précédents processus de certification

Les Etats membres pourront décider de réutiliser des certificats ou des rapports de certification délivrés ou publiés par d'autres organes ou d'autres pays. Cette réutilisation des données peut permettre des économies de temps, d'argent et de ressources, et contribuer ainsi à une efficacité accrue du processus. Toutefois, ce « recyclage » des informations devra au minimum respecter les normes de transparence du processus d'origine.

A défaut de réutiliser des certificats ou rapports de certification existants, les Etats membres pourront aussi envisager de faciliter des échanges, entre pays, de leurs expériences de certification respectives.

11. Les conclusions d'un rapport de certification devront être totalement vérifiables grâce aux informations mêmes contenues dans le rapport

Tout rapport de certification doit être auto-appréciable – autrement dit, ses conclusions doivent reposer exclusivement sur les données proposées par le rapport, et habilitant une tierce partie à ré-enquêter sur ces bases et à valider finalement les conclusions en question.

---

[3] cf. le site Internet https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

[4] Pour de plus amples informations sur cette notion de « résistance k » et les Critères communs, veuillez consulter le sitewww.coe.int/t/dgap/democracy/Source/EVoting/E-voting%202009/E-voting%20workshop/Volkamer_presentation.pdf

12. Les Etats membres devront déterminer les différents postes budgétaires du processus de certification, sur la base des principes d'intégrité, d'indépendance et de qualité

Les Etats membres devront désigner explicitement les organes chargés de la gestion financière des différentes étapes du processus de certification. Les Etats pourront décider que l'ensemble des coûts, y compris la certification officielle, soit à la charge des vendeurs de systèmes – ce qui, de toute évidence, serait synonyme d'un engagement plus important de la part de ces derniers. En revanche, le coût des opérations pourrait être exclusivement à la charge des Etats. Enfin, une troisième voie est possible : le partage des coûts entre vendeurs et Etats. Le coût du processus de certification ne doit en aucun cas porter atteinte aux principes d'indépendance, d'intégrité et de qualité du processus. Quelle que soit l'option financière, chaque Etat membre devra disposer de crédits suffisants pour le processus, et, dans ce contexte, les décisions devront être rendues publiques.

13. Les organes de certification devraient avoir un accès total à l'ensemble des informations pertinentes et disposer de suffisamment de temps pour pouvoir accomplir le processus de certification avant l'élection concernée

Les organes chargés de la certification doivent avoir accès aux informations et données nécessaires et suffisantes pour l'accomplissement de leur mission – c'est-à-dire la formulation de conclusions sur le système de vote électronique examiné ; les organes en question doivent avoir suffisamment de temps pour passer en revue l'ensemble des informations et données. Les citoyens ont le droit de savoir quel type d'informations n'a pas été considéré comme nécessaire et suffisant pour la réalisation du processus de certification. En outre, les règles régissant la relation entre le vendeur et le certificateur – telles que les « Accords de non-divulgation » et autres textes similaires – doivent être rendues publiques.

Dans certains cas, notamment lors d'élections anticipées ou de l'introduction d'un nouveau système de vote, le processus de certification n'a pu être effectué que peu de temps avant la date des élections concernées. Cela entraîne un risque : celui de manquer de temps pour effectuer la procédure de certification, et, dès lors, de porter atteinte à la fiabilité même du scrutin. En d'autres termes, le processus de certification doit être achevé avant la date des élections, de manière à donner le temps d'en examiner les conclusions.

L'une des solutions à ce problème – en vue d'une économie de temps et d'argent, et dans la perspective des processus de certification à venir – est de certifier les modules et leur séquence tels qu'ils auront été modifiés à l'issue du processus de certification initial, et, notamment, de la certification du système de vote électronique.

14. En ce qui concerne les certifications officielles, le certificat délivré devra identifier clairement les éléments certifiés et intégrer des garanties contre toute modification imprévue

Le certificat en question devra indiquer en toute transparence l'ensemble du processus de certification et ses résultats ; les éléments ainsi certifiés devront être réutilisables par toute tierce partie ayant accès au système. C'est sur la base de ce certificat que l'on

pourra vérifier que tel ou tel système électoral est effectivement conforme aux éléments certifiés. Le certificat devra indiquer (au minimum) les données suivantes (ou indiquer de quelle manière s'y référer) :

- La personne ou le groupe ayant délivré le certificat ;
- La durée/les dates/les conditions de validation ;
- Un exposé des objectifs du certificat. De plus, des indications concernant l'accessibilité du système, sa sécurité, son applicabilité, son bon fonctionnement, et le degré de ces divers éléments ;
- Un exposé de la méthode de certification. Quelles normes ont été utilisées ? Quels sont les modes de contrôle et d'évaluation des systèmes ? Quel est le mode d'analyse du code source ? Quel est le mode de vérification des composants matériels ?;
- Une description du système certifié. Pour en permettre la reproductibilité par des tierces parties, cette description doit intégrer des empreintes digitales numériques liées aux composants du logiciel, des spécifications précises des versions logicielles intégrées, ou encore les composants matériels – entre autres éléments ;
- Les résultats du processus de certification ;
- Des observations concernant les exigences opérationnelles et autres conditions préalables ;
- Une empreinte digitale numérique liée au certificat ou système similaire.

Annexe I

Glossaire des termes employés dans les lignes directrices relatives à la certification des systèmes de vote électronique

Le présent document utilise les termes suivants, dans les acceptions suivantes :

- Evaluation : évaluation des personnes, des matériels, des logiciels et procédures de vérification de leur adaptation à l'accomplissement de certaines tâches.

- Contrôle (ou Audit) : évaluation indépendante, avant ou après une élection, des personnes, organisations, systèmes, processus, entités, projets ou produits, avec analyses quantitative et qualitative intégrées.

- Certificat : document publié à l'issue d'un processus officiel de certification – qui certifie ou approuve un certain nombre d'éléments.

- Certification : processus visant à confirmer la conformité d'un système de vote électronique avec les exigences et les normes prescrites, et prévoyant au minimum un certain nombre de dispositions en vue d'attester du bon fonctionnement du système en question. Ce processus peut aller d'un simple test ou contrôle jusqu'à une certification officielle globale. Il en résulte un rapport et/ou un certificat.

- Organe de certification (ou « Certificateur ») : organisme habilité à effectuer un processus de certification et à délivrer un certificat au terme de ce processus.

- Rapport de certification : document exposant les éléments approuvés dans le cadre du certificat, ainsi que le mode de certification.

- Test des composants et composantes : mode de contrôle de chaque élément du système, afin de déterminer sa validité.

- Vote électronique : élection ou référendum ayant recours à des instruments électroniques, notamment pour le déroulement du scrutin.

- Certification officielle : certification menée sous l'égide des autorités officielles, avant le jour du scrutin, et permettant de délivrer un certificat.

- Lignes directrices : tout document visant à rationaliser un ensemble de procédures très précises, selon des règles établies. Par définition, ces « lignes directrices » ne sont pas juridiquement contraignantes.

- Accord de non-divulgation : contrat juridique entre deux parties au moins, précisant les éléments confidentiels, les données ou informations que les différentes parties en question souhaitent partager à des fins très précises, mais en n'autorisant qu'un accès restreint aux parties extérieures au contrat.

- Exigence : exposé documenté et singulier de la nature et des objectifs de tel ou tel produit ou service.

- Acteurs : personnes, groupes, organisations ou systèmes susceptibles d'influer sur les actes d'un gouvernement ou d'une organisation, ou d'en subir l'influence. Les « acteurs » en question sont notamment les citoyens, les responsables officiels des élections, les partis politiques, les Etats, les observateurs nationaux et internationaux, ou encore les organes de certification des systèmes de vote électronique.

- Norme : toute norme établie, sous forme de document officiel définissant les critères techniques et de gestion, les méthodes, les processus et les pratiques qui doivent être communs à tous.

- Tests : vérification du bon fonctionnement des éléments étudiés.

- Transparence : exposé très clair des moyens et des objectifs de diffusion des informations.

Annexe II

Texte de la Recommandation Rec(2004)11 sur les normes juridiques, opérationnelles et techniques relatives au vote électronique

F. Homologation

111. Les Etats membres sont invités à mettre en place des procédures d'homologation permettant de tester tout élément informatique et de vérifier sa conformité aux exigences techniques décrites dans cette recommandation.

112. Soucieux d'améliorer la coopération internationale et d'éviter les doubles emplois, les Etats membres envisageront de faire adhérer leurs organismes respectifs qui ne l'auraient pas encore fait aux accords internationaux pertinents de reconnaissance mutuelle tels que la Coopération européenne pour l'accréditation (European Co-operation for Accreditation-EA), la Coopération internationale sur l'agrément des laboratoires d'essais (International Laboratory Accreditation Cooperation-ILAC), le Forum international de l'accréditation (International Accreditation Forum-IAF) et les autres organismes similaires.

Texte de l'exposé des motifs de la Recommandation Rec(2004)11 sur les normes juridiques, opérationnelles et techniques relatives au vote électronique

F. Homologation

Norme no 111. «Les Etats membres sont invités à mettre en place des procédures d'homologation…»

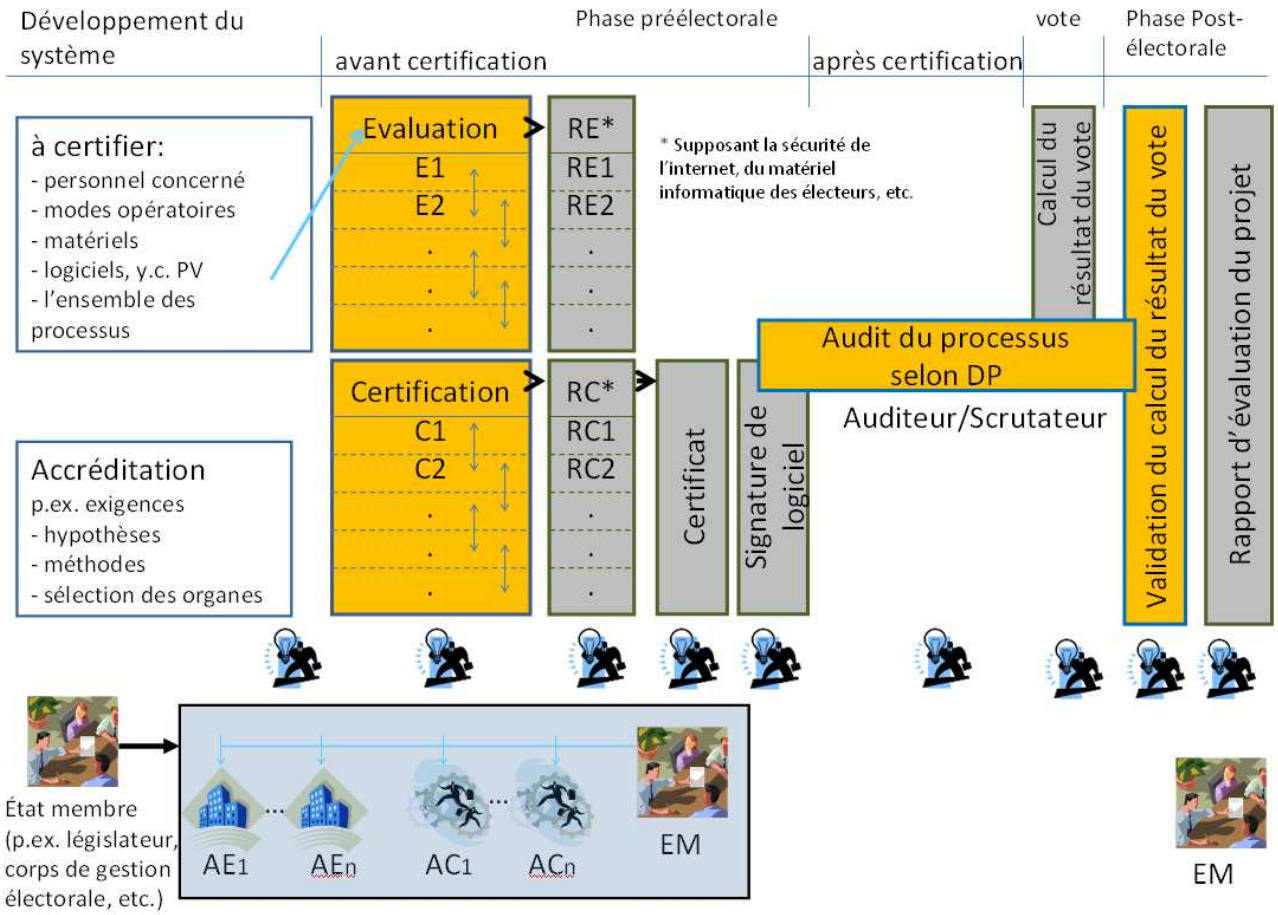
189. Les responsables des élections devraient envisager le recours à des techniques allant des simples tests à une homologation formelle, afin de garantir avant le déroulement d'une élection ou d'un référendum que le système fonctionne exactement comme prévu.

190. A l'avenir, il est possible que l'on se trouve en présence de divers systèmes de vote électronique et d'une multitude d'éléments individuels. Il pourrait alors devenir très difficile pour une instance électorale de déterminer si un produit donné est prêt à l'emploi, s'il fonctionnera correctement et fournira les bons résultats. Une procédure d'homologation s'avérera précieuse dans ce domaine, car elle pourra attester l'efficacité des éléments et limitera par conséquent les vérifications nécessaires dans l'élaboration d'un système complet.

Norme no 112. «Soucieux d'améliorer la coopération internationale…»

191. Quand leurs organismes participent aux travaux des organisations internationales qui prévoient des dispositifs de reconnaissance mutuelle, les Etats membres peuvent bénéficier de leur travail et donc réduire leurs coûts de tests et d'homologation.

Annexe III – Modèle théorique global du processus de certification



AC – Autorité de certification
AE – Autorité d'évaluation
AEx- N^{ième} Autorité d'évaluation
DP – Description du processus
E – Evaluation
Ex- N^{ième} évaluation si différent types d'évaluations sont requises
EM – Etat membre (e.g. législateur, corps de gestion électorale, etc.)
PV – Protocole du vote
RC – Rapport de certification
RE – Rapport d'évaluation