Notes de spécifications[1] des plateformes des serveurs[2]

Le développement de la suite logicielle côté serveurs[3] est réalisé pour la plateforme **dotNET**[4] afin d'obtenir l'indépendance système/matériel et l'interopérabilité avec les composants logiciels écrits dans d'autres langages.

Les scripts systèmes sont en premier lieu en **AdaScript** (**BUSH**[5]), et ultérieurement pourront être en **Python**[6], soit reconnus comme très portables.

Le développement est réalisé sous Microsoft Windows x64 et testé sur la plateforme **GNU/ Linux**[7].

La distribution se fait en conditionnement de Virtual Appliance sous le système JeOS Ubuntu[8].

Toute autre plateforme[9] est néanmoins possible, si les logiciels utilisés y sont disponibles (ou portés) et les configurations nécessaires y sont réalisées.

Note : Les services d'identités numériques et de tiers de confiance, d'obtention des droits ou charges d'accès, etc. sont externes (et hors xVote).
Ils ne sont donc pas décrits ici.

Architecture :

Pour mémoire, il y a trois grappes : **Habilitation**, **Urne** et **Scrutation**; les deux premières sont exploitées pour le compte d'une autorité (l'Administration dans le cas public) et ne sont pas reliées entre elles, la dernière est située dans un site séparé des deux premières et exploitée pour une autre autorité (le contrôle politique dans le cas public) et elle est gérée/accédée par un autre personnel.

Les machines peuvent être physiquement distinctes, ou être virtuelles (sous un moniteur).

Si l'architecture High Availability (HA) est utilisée (cas standard, avec Hearthbeat[10] et

1 Sous réserve.

2 Le développement du serveur, tout comme le client, se fait sous et produit donc a priori pour Microsoft Windows x64 (Vista) et partiellement testé avec un serveur GNU/Linux (Ubuntu) avec Mono. Les versions et correctifs sont assumés à jour.
Les logithèques de haut niveau sont en grande partie les mêmes que pour le client.
Le programme et les logithèques utilisées sont totalement portables (dotNet ou AdaScript-BUSH/Python), donc pourraient être transférés sur d'autres plateformes, dont les configurations systèmes doivent alors être effectuées.

3 Le serveur est développé, comme le côté client, en Ada2005 avec l'environnement de l'US Air Force Academy (repris par AdaCore), donc sous Windows,.

4 Soit http://www.microsoft.com/net ou http://www.mono-project.com.
Aussi possible Portable dotNET (dotGNU) http://dotgnu.info/

5 Business Shell http://www.pegasoft.ca/bush.html , GPL et disponible sur Linux/Intel (x86 et 64b), et d'autres plateformes.

6 http://www.python.org/
Ce langage est reconnu pour fonctionner sans changement sur Unix, Windows, Macintosh, et d'autres plateformes.

7 Les deux systèmes sont sur architecture PC Intel EM64T (x64bits), donc compatible AMD64.
L'édition courante d'Ubuntu serveur est utilisé pour les tests et proto-exploitation.

8 Le format n'est pas totalement fixé, il sera soit KVM (i.e. QEMU I/O), soit VMware (Serveur)

9 Actuellement, MS-dotNET, Mono, Portable.GNU sont portés sur nombre de processeurs et sous un grand choix de systèmes. De plus, le code généré pourrait éventuellement être transcodé en ANSI C++ et recompilé vers n'importe quelles autres plates-formes avec crossNET http://www.codeplex.com/crossnet

10 Tenir compte dans les FreWall que Heartbeat communique par paquet sUDP

DRBD), certaines machines sont dupliquées (failover) localement et/ou distalement.

Chaque grappe est formée d'une machine (év. virtuelle) **Frontale** (très relatif pour l'Urne), une ou plusieurs de **Traitement** (sauf l'Urne) et d'une **Dorsale**.

Le frontal gère le dialogue en mini-sessions TCP, la sécurisation du canal de transport et un suivit d'efficience de la session virtuelle. Le traitement traite du dialogue de fond, de la sécurisation des requêtes/réponses, et est formé d'un rang extensible de serveur de transaction, chacun avec incarnation dynamique de services fugaces en son sein. Les dorsales contiennent les fonctions de rétention de données (sp. pour les sessions virtuelles), les clefs cryptographiques privées et les fonctions d'observation et d'alarme.

La Scrutation possède plusieurs rôles (outre scrutation, la mémorisation et le postier) et est aussi complétée par une machine sécurisée scellée. Ce module matériel de sécurité (HSM), ou une machine pouvant approcher ce modèle (p.ex. PC industriel embarqué), contient et utilise les clefs des facteurs de masquage K_F^{dom} et qui est reliée ou fonctionne (réseau) avec le Dorsal de Scrutation.
Il y a une seconde machine similaire (i.e. conservée scellée) dans chaque canton pour la génération-authentification-scission de la clef de chiffrement des bulletins, puis sa recomposition et le déchiffrement de l'Urne.

Si nécessaire, pour absorber une plus grande charge, par exemple lors des périodes de crête[11], les machines peuvent être physiquement distinctes (migration des machines virtuelles vers des serveurs physiques disponibles), spécialement pour les machines de Traitement qui peuvent être extraites, voire multipliées à l'intérieur d'une grappe (distribution dynamique et équilibrage de charge).

Le trafic à l'intérieur d'une grappe (entre les machines -physiques ou virtuelles- la composant) doit être isolé des autres installations[12].

Il est souhaitable, mais pas nécessaire, que les machines serveur puissent avoir toutes la même architecture de données élémentaires du processeur[13] (boutianité/endianess et taille de registre).

Matériel:

Les spécifications matérielles sont celles requises par les systèmes originaux, et les composants additionnels.

Le logiciel est fortement parallélisé, et donc en mesure de tirer parti de processeurs multiples et à multiples cœurs. Les fonctions cryptographiques sont lourdes sur toutes les machines et donc les processeurs doivent être assez rapides pour les supporter.

Ceci est tout particulièrement vrai à la clôture du scrutin, lors de l'ouverture de l'Urne, le dépouillement des bulletins nécessitera un traitement massif très rapide, car sous l'oeil des politiciens : il est constitué du déchiffrage des bulletins, de la validation de leur

11 Le soir (entre 18 et 22h, surtout vers 20h) et les derniers jours en fin de session de votation (50% de votes la dernière semaine).

12 Séparé de facto par le moniteur de virtualisation si la grappe est entièrement et exclusivement sur une machine réelle, physiquement sur un segment de réseau local propre, strictement scindé par le firewall de tête/routeur filtrant, ou logiquement par une activation IPsec -mode transport crypté et authentifié- dans les noyaux des systèmes concernés et une gestion appropriée des clefs.

13 S'il s'agit des processeurs Intel actuels, ce sont des petits-boutiens (little-endian) de 64 bits, s'il s'agit de SPARC (Sun, etc.) ce sont des gros-boutiens (big-endian) de 64 bits (UltraSparc). Si le parc est hétérogène, c'est la norme network byte order (l'Internet Protocol définit comme standard "big-endian") qui sera activée.

signature, du contrôle des chainages avant-arrière, de la vérification du schéma XML, de l'extraction des choix et de l'examen de leur conformité (aux règles électives).

Outre l'espace système et le code du logiciel, les disques doivent supporter la journalisation système, de même pour la mémoire centrale qui doit maintenir les espaces des processus. En général[14], 1 Go de mémoire vive et 10 Go de capacité effective de stockage (disques) sont des paramètres de base envisageables par serveur élémentaire.

Les dimensionnements spécifiques des serveurs dépendent de la charge prévisible. Les sources des variations sont les suivantes :

Frontal	essentiellement selon le nombre de sessions TCP/HTTP(s) effectives simultanées et le premier niveau SOAP. Pour mémoire, il s'agit (pour le vote, pas l'administration) de *mini*-sessions de l'ordre de la seconde. Note : F est quasi inexistant pour l'Urne.
Traitement	selon la charge instantanée, soit le nombre de transactions en cours simultanées (de mini-sessions HTTP). Note : T n'existe pas pour l'Urne.
Dorsal	pour l'Habilitation il maintient un état transitoire, dépendant du nombre de sessions virtuelles[15] simultanées (requêtes de droits de vote en cours), en mémoire et en image de sauvegarde temporaire sur le disque. Pour l'Urne, il s'agit en mémoire (du tampon) de l'index (numéro d'ordre) des bulletins reçus et, sur le disque, des bulletins[16]. Pour la Scrutation, il s'agit essentiellement de l'espace (du tampon) de l'index des estampilles des récépissés des bulletins reçus (rôle postal), et sur le disque, de ces reçus[17] et surtout les liasses de votes en attente[18] (rôle mémorisation). Pour les trois grappes, outre les clefs déchiffrantes/signantes, de tailles négligeables, il s'agit surtout d'espace disque pour les journaux des fonctions d'observation.

Le sous-système de stockage de chaque machine doit être résistant aux défaillances d'un de ces disques élémentaires, y compris les défaillances partielles (de secteurs), et permettre la correction de la panne à chaud. La redondance des données est particulièrement critique pour l'Urne, qui ne peut perdre aucun bulletin.

La vitesse d'accès au stockage (disques) est sensible surtout pour le Dorsal de l'Habilitation, et dans une moindre mesure pour celui de Scrutation.

14 La configuration minimale pour un petit serveur Debian/Linux (ce qui est la base système suffisante ici) est de 64 Mo de MeV et 500 Mo de disque. L'exécutif de Mono peut être considéré comme inclus dans ces besoins.

15 Pour un cantons moyen, même si 1/16e de l'électorat votait en même temps le dernier jour, c'est à dire que le nombre maximal de sessions (virtuelles!) simultanées serait de 40'000, l'encombrement des données transitoires pour H.D serait en mémoire vive et sur disque, varierait entre 60 et 350 Mo (l'encombrement de l'objet individuel va de 1⅓ Ko à 2 Ko -env.-, et un court instant à 9 Ko).

16 Les bulletins sont stockés en deux parties, l'en-tête fixe (binaire) et le corps (texte) de taille variable. Pour un canton moyen, il s'agirait environ d'un espace (votations, 8 questions) d'environ 2 Go (si tous les électeurs inscrits votaient par Internet environ 8 Go). Ces valeurs sont pour des données textuelles XML, elles seraient bien moindre (-80% FstInf à -99% EFX) en cas de codage binaire d'XML (FastInfosec ou EFX/EXI).

17 Environ de l'ordre de 170 Mo pour un canton moyen; au maximum 700 Mo si tous les électeurs inscrits votaient par Internet.

18 Si tous les électeurs inscrits d'un canton moyen votaient et en utilisant le vote par internet, cela nécessiterait environ 10 Go (pour une votation de 8 questions).

Autres services nécessaires:

Les serveurs envoient des messages d'information ou d'alerte, pour ce faire ils utilisent tant le protocole SMTP que le protocole XMPP, et donc ont besoin d'accéder à un tel service.

Le serveur SMTP (Message Transfer Agents/MTA), mis à disposition des serveurs xVote, devrait implanter et être sous un DNS implantant le Sender ID – RFC 4406 ou (similaire) Sender Policy Framework /SPF – RFC 4408.

Le serveur SMTP et son DNS devrait, de plus, suivre le protocole DomainKeys Identified Mail (DKIM) selon la norme RFC 4871 (voir aussi Yahoo[19] et DKIM-WG[20] de l'IETF). Optionnellement, xVote peut marquer lui-même les courriels avec l'élément d'en-tête DKIM, dont alors la clef publique doit être servie par le DNS correspondant.

Pour l'envoi des cartes de votes dématérialisées (courriel sécurisé), c'est les serveurs SMTP des états (cantons) qui seront utilisés. Là aussi, il serait très souhaitable qu'ils appliquent les services Sender ID / SPF et DKIM.

Le serveur XMPP (eXtensible Messaging and Presence Protocole, Jabber) devrait être celui de Coversant[21] pour bénéficier de certaines extensions ad hoc optionnelles[22].

Pour la distribution[23] du tunnelier(otv)/distributeur, le protocole BitTorrent est utilisé, il est nécessaire d'avoir un serveur gestionnaire (tracker). Pour la livraison initiale en cascade, il faut un/des serveurs à haut débit des fichiers (par tronçons BT).

Pour la gestion de la livraison JeJIT de la version VirtApp du client xVote, il est nécessaire d'avoir un serveur "G2WebCache", et pour l'établissement avec la méthode ICE^{LITE} des transferts P2P il faut un serveur STUN (et subsidiairement TURN). Pour la livraison initiale P2P distribué, il faut un/des serveurs à haut débit des blocs des fichiers "disques virtuels" (fonctionnant en "feeder" et comme des "hub/supernode").

Même sans être strictement nécessaire, des serveurs étendant les sur-réseaux d'intraçabilité TOR[24] et JonDo[25] seraient toujours le bien venu.

Virtual Appliance

La livraison des serveurs d'xVote se fait sous la forme de *Virtual Appliance*, soit d'une solution empaquetée dans un système complet et entièrement configuré[26].

L'avantage de ce conditionnement en Virtual Appliance est la simplicité de sa mise en oeuvre, l'exhaustivité de son environnement, la justesse de configuration et la standardisation de sa manipulation, ainsi que la souplesse d'exploitation.
Pour des raisons d'ouverture, l'édition de référence d'xVote est prévue pour le "standard du marché", soit l'architecture machine x86; il s'agit aussi de garantir la rapidité de développement et la capacité de mise en test/proto-exploitation de démonstration.

19 http://antispam.yahoo.com/domainkeys
20 http://tools.ietf.org/wg/dkim/
21 http://www.coversant.com/
22 Dont, optionnellement si le mode applicatif d'xVote client est utilisé, pour le service de gestion de relais.
23 Optionnellement, aussi des éventuels compléments du bulletin.
24 http://www.torproject.org/
25 https://www.jondos.de/en/
26 http://en.wikipedia.org/wiki/Virtual_appliance

L'édition de référence est conditionnée en machines virtuelles sous le système JeOS Ubuntu avec tous les logiciels et bibliothèques nécessaires (dont Mono).

Cette édition est prévue au format VMDK. Actuellement, elle est prévue créée et testée sous VMware Server; il sérieusement envisagé qu'il soit décidé de la créer, tester et conditionner à l'aide de KVM (actuellement I/O QEMU, donc aussi au format VMDK).

Il est bien sûr possible d'adapter l'édition de référence pour d'autres plates-formes et hyperviseurs; essentiellement en ayant un noyau Linux à jour, et d'obtenir ou compiler Mono (nécessitant éventuellement un portage du JIT postcompiler)[27] et les autres logiciels utilisés. L'application et les bibliothèques utilisées sont en code intermédiaire dotNET(ou CLI) et donc directement portables sur toutes plates-formes comprenant Mono ou dotNET.

Détails :

Remarque pour la suite : La livraison se faisant sous la forme d'une *Virtual Appliance*, soit d'une solution empaquetée dans un système complet et configuré, le reste de cette description n'est pas directement nécessaire pour la mise en exploitation, et est donc purement informative.

Logiciels:

L'environnement d'exécution Mono[28] (dotNET) se trouve couramment dans la distribution d'origine du système d'exploitation[29]. Il faut veiller seulement à ce qu'il soit installé et à jour sur toutes les machines.

Sur toutes les machines, à charger et installer le système de scripting AdaScript/BUSH[30]. Les scripts peuvent être aussi compilés (très légèrement modifiés) avec GNAT ou A#. Ultérieurement et optionnellement, sur toutes les machines, à charger et installer[31] : le système Python[32], l'accélérateur Psyco[33] et la bibliothèque PyYAML[34].

Sur toutes les machines, à charger et installer : les applications xVote et les bibliothèques tierces fournies avec les programmes d'xVote. Ces bibliothèques tierces sont libres ou couvertes par notre obtention des droits de distribution [35&36]. Optionnellement, aussi la

---

27 En cas d'absence d'un tel portage, il est possible de convertir (quasi intégralement) le code dotNET en ANSI/C++ avec CrossNET http://www.codeplex.com/crossnet

28 http://www.mono-project.com/Main_Page

29 Si les serveurs sont sous MS-Windows, le Framework dotNet est soit inclus (Vista ou WinS2003), soit à charger depuis le site Microsoft.pour systèmes x86 ou x64.

30 http://www.pegasoft.ca/bush.html Il est disponible en binaire pour Intel x86 ou AMD x86_64, sous Linux Red Hat , SuSE, Slackware, Xandros ou Debian (Ubuntu)

31 Pour les Unixes (plus rarement les Linux) ils sont généralement aussi à compiler.

32 http://www.python.org/

33 http://psyco.sourceforge.net/ right now only runs on Intel 386-compatible processors (under any OS)

34 http://pyyaml.org/wiki/PyYAML

35 Éventuellement, en cas de défaut du choix OSS, et seulement sur le serveur de l'Urne pour le dépouillement, la logithèque de Saxon http://www.saxonica.com/ la version avec vérification de l'XML-Schema (par sécurité) est de licence commerciale à environ 600.-/serveur (ici pour le contrôle de bonne forme des bulletins déchiffrés -au cas où le logiciel du poste du votant ne serait pas otiginal).

36 La licence de SecureBlackbox (de http://www.eldos.com/sbb/) est commerciale . Selon l'interprétation faite de ses termes, il *pourrait* être nécessaire de prendre un licence de serveur, *env*. 7500.- à titre unique pour un site d'entreprise)

bibliothèque d'IronPython en cas d'utilisation de scripts internes en Python[37].

Le(s) connecteur(s)[38] pour Mono aux divers logiciels de SGBD[39] des Registres des Électeurs des Administrations Publiques doivent être présents sur la machine de Traitement de l'Habilitation.

Complément sur les sauvegardes:

Dans toutes les grappes, le Frontal et le Traitement (inexistant(s) pour l'Urne) ne contiennent pas d'état[40], sauf transitoires à l'intérieur des mini-sessions, ce qui est sans importance (d'un ordre de la seconde). La fonction d'observation (confondue avec le Dorsal) contient les journaux qui peuvent être importants jusqu'à l'échéance du délai de contestation[41] et doivent être détruits ensuite (surtout pour les informations pouvant être reliées -uniquement indirectement- à une personne, bien que le bulletin personnel ne puisse s'y retrouver, ni même l'indication qu'elle a *effectivement* voté.

Le Dorsal de l'Habilitation contient les états des sessions virtuelles, et ces informations peuvent être momentanément sécurisées, mais pas maintenues au-delà de la fin de ces sessions (de 5 min normalement à 1 jour éventuellement) . Une sauvegarde ne s'impose pas avec un stockage à tolérance de pannes (p.ex. des disques redondants échangeables à chaud).

Le Dorsal de l'Urne contient les bulletins[42], qui doivent évidemment être sauvegardés régulièrement, de manière très sécurisée, localement et à distance, en plus de l'utilisation de disques redondants particulièrement fiables.

Le Dorsal de Scrutation contient les paquets[43] de votes mémorisés (fonction de mémorisation) et les récépissés (fonction postale), qui doivent être sauvegardés régulièrement.

37 http://www.codeplex.com/Wiki/View.aspx?ProjectName=IronPython

38 http://www.mono-project.com/Database_Access

39 "provider ADo.NET" au sens de Microsoft. PostgreSQL, MySQL, Firebird Interbase, SQLite, Oracle, Sybase, DB2, Microsoft SQL Server, Progress RDBMS, Mimer SQL; ainsi que le connecteuruniversel ODBC.

40 Pas d'état en absolu, strictement il contient une optimisation de reconnaissance *temporaire* des sessions virtuelles à l'aide d'un jeu de "cookies".

41 et, par là, l'obtention de la décharge de l'exploitant

42 Il s'agit de paires de fichiers à accès directs, la sauvegarde doit avoir lieu en synchronisation avec la libération du verrou d'accès par le processus Urne.

43 C'est un SGBD permettant la sauvegarde à chaud.