

The unavoidable price of reliability is simplicity. -- C.A.R. Hoare

The ability to simplify means to eliminate the unnecessary so that the necessary may speak. -- Hans Hoffmann

First, solve the problem. Then, write the code. -- John Johnson

La fonction de développement a les connaissances et l'expérience pour le travail à effectuer sur xVote, étendue du travail qu'elle assume totalement, et qui comprend en principe les points ci-dessous :

1. La réalisation de l'ensemble des logiciels composant le système xVote (client et serveurs), selon les meilleurs principes du génie logiciel.
Les développements¹ ont lieu sous MS-Windows (Vista édition Intégrale/Ultimate x64, ou l'équivalent en Windows 7), dans le cadre de virtualisation dotNET (code CLI, norme ISO), avec A#² (norme ISO).
Les textes sources des programmes sont en anglais. L'écriture suit les règles stylistiques optimisant la lisibilité, la maintenabilité et l'adaptabilité.

Pour mémoire, le système, son architecture et les plateformes d'exploitation sont intégralement spécifiés, les outils, méthodes, chaîne de développement et bibliothèques totalement définis.
2. La définition et la documentation des configurations d'exploitation (client et serveurs).
3. La conception et l'implantation complète des interfaces utilisateurs riches, tant natives que déportées, pour les démonstrations, les tests, le pilote 0³ et (en collaboration ou en appui) pour les trois votes de la phase pilote.
En particulier, pour ces interfaces utilisateurs riches : la rédaction des textes, la composition des pages, la conception des graphiques et des illustrations insérées, etc. nécessaires comme référentiel amont.
4. La conception et la rédaction des scripts par défaut ou de référence, internes, d'interfaçage (client-interface utilisateur, et serveurs) et système⁴ (serveurs et client virtual appliance).
5. La rédaction et l'incorporation des documents (structurés) XML des objets (p.ex. bulletins de vote) manipulés durant les tests et la primo-exploitation, puis l'appui aux éventuels rédacteurs⁵ pour la phase pilote. De même pour les documents structurés XSLT, XQuery et XPath (p.ex. manipulation du/des bulletin/s de vote,

1 Les systèmes utilisés pour les tests et primo-exploitation sont toujours des versions à jour (patch, update et service pack).

2 Langage Ada 2005, normalisé, génération du code CLI, normalisé, développement avec la plate-forme dotNET, origine US Air Force Academy (Prof. Carlisle), repris par AdaCore ACT Gnat Pro for dotNET.

3 Essai public d'un vote non juridique dans les écoles secondaires supérieures. Un tel essai a une valeur médiatique au sein du canton, et de certification vis-à-vis de la Confédération.

4 En AdaScript/BUSH

5 Avec les indications pour les alternatives d'interface utilisateurs selon les capacités des ordinateurs, connectivité ou handicaps.

dépouillement).

6. La définition et l'implantation des Bases de Données internes (structures, contraintes et procédures), des prescriptions d'accès (scripts de référence) en Lecture/Écriture des BD externes, l'implantation des BD-externes (maquettes fonctionnelles) pour les tests; la participation à cette implantation pour le pilote 0 et -de même- l'appui pour la phase pilote.
7. La spécification, la mise en place et l'accomplissement des tests (de développement, fonctionnels, de charge).
Les tests sont internes⁶.
L'exploitation du système pour le pilote 0 -essai public de votation non juridique- est aussi possible en interne, car l'infrastructure matérielle et logicielle de développement le supporte intégralement.
L'exploitation du système pour les votes pilotes 1 à 3 -essais publics de votations juridiques- pourrait être possible en interne, dans le sens où l'infrastructure matérielle et logicielle de développement est parfaitement à même de le supporter⁷.
Les tests (et la primo-exploitation) des logiciels serveurs se font sous Linux⁸.
Les logiciels clients sont testés sous Windows (essentiellement Vista/7 x64 et subsidiairement -et si disponible¹⁴- sous WinXP x32), ainsi que sous Linux.
Les tests sous Linux sont effectués sous la distribution⁹ (parties serveur) Ubuntu¹⁰ Server x64 (guest¹¹), év. SuSE Server x64 (host¹¹) et (partie client) Ubuntu Desktop x64¹²(en partie au dessus de WinVista/7 -host).
Il sera étudié la possibilité de faire en interne aussi les tests (partie client) sous Apple Mac OSX¹³.
L'intérêt et la possibilité pour la fonction développement d'effectuer en interne des tests des logiciels clients sous d'autres systèmes¹⁴ ne sont pas certains; il en est de même pour les distributions¹⁵ Linux autres¹⁴ qu'Ubuntu.

6 Éventuellement. un complément de test de charge pourrait être fait avec des clients externalisés, automatiques ou non.

7 Serveurs centraux doublés multi-site, sauvegarde distante constante des données, serveurs répartis et distribués des services complémentaires, forte participation multi-localisée aux sur-réseaux d'intraçabilité.

8 L'importance de Linux n'est plus à relever, en particulier l'intérêt pour Ubuntu est très grand ("Ubuntu is a great server and desktop distribution for the GNU/Linux® operating system", 15 jan. 2008 IBM.com).

9 En Virtual Machine, sous hyperviseur KVM (alt.VMware Server) et serveur hôte SUSE Server x64.

10 Pour mémoire, Ubuntu est de la célèbre lignée Debian. "Since its launch in October 2004, Ubuntu has become one of the most highly regarded Linux distributions, with millions users around the world. Ubuntu aims at being the most widely used of all Linux systems and at the centre of a global open source software ecosystem." /IBM.com, portail DB2, oct 19, 2007
Numéro un de DistroWatch.

11 Guest/Host c'est-à-dire "guest" en machine virtuelle sur un "host" avec hyperviseur (KVM).

12 Le test du client en "Virtual Appliance" sous l'hyperviseur VirtualBox pourrait être fait (selon les disponibilités en cours au moment du test) pour un "guest" Ubuntu à 32 bits, minimalisé et avec une interface utilisateur allégée (i386 ou x86-32, et non AMD64 ou x86-64).

13 Apple et le Mac OSX détient environ 11% du marché Suisse, soit le double de sa pénétration moyenne dans le reste du monde. [Bilan, 21/05/2008]

14 La livraison principale étant en "virtual appliance" (voir infra page 4), au sein d'un Linux Ubuntu isolé par un hyperviseur du système hôte de l'utilisateur, la dépendance à ce dernier est minime.

15 Les tests (tout ou seulement certaines parties) des logiciels clients seront éventuellement effectués sur un mini-Linux ("UMPC" ou "Internet Appliance", "Mobile Internet Device" ou "Linux-phone", avec un port bien documenté de Mono, p.ex. Maemo, ou peut-être Ubuntu-Mobile, voire ultérieurement Android ou LiMo).

Il en est de même (tests partiels) des plates-formes mobiles : sur un "Smartphone" sous Symbian S60 et sous MS-

8. La définition générale des procédures opératoires (procédures politiques, administratives ou techniques des états, de leurs services ou sous-traitants).
9. La rédaction initiale des documentations générales ou descriptives (documents généraux, d'implantations, techniques).
La rédaction initiale des modes d'emploi (utilisateurs et exploitants).
La rédaction des documents techniques : l'architecture, les technologies mises en oeuvre, les principaux algorithmes, etc.
Les documents sont fournis au format standard ISO/IEC 26300:2006 - OASIS Opendocument¹⁶ (OpenOffice), ainsi qu'en PDF.
La préparation de ces documents à la publication (XHTML), leurs conditionnement et (primo-)publication, avec formatage sobre et illustrations¹⁷ adaptées : graphiques, images, photos, vidéos simples, "screencasts" et animations simples.
La maintenance et l'animation du "site" de la communication technique.
10. Est inclus¹⁸ tout le matériel (architecture de la chaîne) et les logiciels nécessaires : au développement, à la documentation/communication technique/collaboration, aux propres démonstrations, aux tests internes (de développement, de charge) et à la proto/primo-exploitation.
Sont prises en charge toutes les relations et négociations avec les fournisseurs des matériels, des logiciels et des services nécessaires aux tâches décrites ici..
Tous les services de supports techniques (des licences logicielles acquises) nécessaires pour ce travail, du développement jusqu'à la primo-exploitation, sont aussi intégralement pris en charge.
Les licences développeurs acquises couvrent intégralement les droits de redistribution du/des logiciel/s résultant/s¹⁹. Les autres licences utilisées sont soit propriétaires gratuites, soit (surtout) libres (OSS).
11. La spécification, la réception et la mise en place, la configuration et la mise en exploitation des divers serveurs complémentaires¹⁸ pour les tests et la proto/primo-exploitation.
Il en est de même de la mise en place, de la configuration et de l'exploitation des serveurs (en relation personnelle) pour les moyens de communication, de travail collaboratif et de promotion ou de publication durant le mandat.
Il en va de même pour la mise en oeuvre et pour la primo-exploitation des serveurs de publication durant le mandat de développement.

Windows Mobile.

Nota : The personal computer is a machine you work *on*. Netbooks are essentially machines you work *through*, out into the Cloud (aka Internet).

16 IBM et Sun ont la majorité des voix du comité ayant normalisé OpenDocument; le format est utilisé par OpenOffice et par la nouvelle suite IBM Lotus Symphony.

17 Dans les formats standards et usuels du Web. "*Un petit dessin vaut mille mots, une petite animation cent-mille*"

18 Doubles jeux de capacités de traitement légères sous trois SE (et quatre à sept modules de consultation et communication additionnels), trois sites avec multiples serveurs massifs, plusieurs compagnons et chacun une station de traitements lourds, deux sites complémentaires avec chacun un serveur d'appoint, deux sites supplémentaires (donc au total sept) avec échangeurs pour intraçabilités et délocalisation de flux. Les services annexes novateurs sont distribués par minigrappes sur dix sites en supplément. Sécurisation générale et suffisamment de capacités de débits, de trafics, de redondance de connexion, de stockage et d'alimentation. Sauvegardes croisées, distantes ponctuelles et en "cloud computing". Certification des identités principales serveurs.

19 Il peut y avoir une ou deux exceptions très mineures et très limitées.

12. Le conditionnement (packaging) des fichiers binaires du logiciel client et de l'interface utilisateur²⁰ de référence (et des scripts internes), avec l'élaboration et la mise à disposition des scénarios automatiques de conditionnement. Trois modes, dont le principal en trois types de formats, seront proposés :

VA Principalement et prioritairement en "virtual appliance" dans un OS invité sous machine virtuelle (VM), donc garanti sain :

Le conditionnement intégralement constitué et prêt à être exécuté (virtual appliance³³) sous un système d'exploitation (invité) ajusté et minimalisé²¹, au sein d'une machine virtuelle, avec le démarrage²² adapté, les utilitaires nécessaires²³ inclus et configurés, des scripts système et les moyens d'assistance²⁴ à distance, le tout directement exploitable avec son hyperviseur²⁵ sur (hôte) Windows, Mac ou Linux. **VM^{live}** Alternativement, identique, mais pour distribution et exploitation comme "application virtuelle portable" sur disque "clef" USB²⁶.

VD Complémentairement, en utilisation confortable et universelle, par bureau virtuel (VD, multicanal), autrement dit déportée depuis une machine virtuelle dédiée basée sur un serveur distant (VdaaS); seul l'affichage est local. Avec adaptation de la MV, et l'élaboration de la structure et configuration du service de gestion et mise à disposition (réception demande, incarnation, destruction) des MV.

LD Secondairement, en image standard (.iso) avec le système d'exploitation pour « installation » généralisée²⁷, mais restreint aux services nécessaires, et gravable afin d'obtenir un LiveCD/LiveUSB permettant le démarrage direct (bootstrapping) et ne nécessitant aucun usage de disque dur.

VM^{P2P} Ultérieurement et optionnellement, en variation de l'installation en machine virtuelle locale²⁸, avec le développement des logiciels complémentaires (sp. tunnelier-distributeur)²⁹.

20 L'interface utilisateur effective -dépendant de l'État- n'est pas *dans* le paquet à installer/exécuter, mais automatiquement téléchargée au démarrage (avec les év. mises à jour) si elle est différente de celle enregistrée (p.ex. de référence).

21 A priori basé sur Xubuntu, très allégé : "official derivative of the Ubuntu Linux distribution, using the Xfce desktop environment -an highly efficient desktop environment, also based on GTK+-. Xubuntu is intended for users with less-powerful computers or those who seek a highly efficient desktop environment on faster systems".

Une alternative plus standard pourrait être de garder l'environnement de bureau GNOME, mais en remplaçant le gestionnaire de fenêtres Compiz Fusion par Metacity plus simple.

22 Dont un garde-barrière (firewall) local

23 En particulier Mono (exécution), Moonlight et Firefox (interface utilisateur); et certains pilotes optimisés.

24 Dont Psi (MsgInst), et -pour la version VMware- FreeNX (téléassistance). Le "serveur" est utilisé en mode sortant, par sécurité et pour contourner les routeurs filtrants/NAT (serveur NX en application sous le S.E. invité ou RDP en application hyperviseur sous le S.E. hôte).

25 Innotek Virtual Box; de préférence Open Source Edition, ou éventuellement la version propriétaire, dans ce dernier cas, il y a gratuité pour l'usage personnel. L'hyperviseur et l'image de la machine virtuelle seront obtenus par l'installateur.

26 Prête à l'emploi sans installation* avec le logiciel de virtualisation "portabilisé", les disques de la machine virtuelle (dont un choix d'IU), un lanceur/vérifieur/nettoyeur et mise à jour automatique en ligne (et si *nécessaire Mono Win/Mc/Lx), etc.

27 Sur les PC x86. Utilisation directe en cas de connectivité par Ethernet, ou WiFi ouvert. Nécessite l'entrée des codes en cas de WiFi fermé (no-SSID, WEP, WAP, etc.) ou autre accès sans fils sur abonnement.

28 Dont d'éventuel(s) post-chargement(s) avec flux sécurisé(s).

29 Le tunnelier-distributeur capture les lectures/écritures sur les disques virtuels (VDI) et les redirige comme blocs vers

IS Accessoirement (év.) en installation d'un système dédié (DS) sur un³⁰ fichier au sein de l'hôte, avec démarrage alternatif de la machine vers ce système complémentaire contenant l'application de vote³¹.

AS Accessoirement (év.) en chargement d'un appliquette avec transaction sécurisée vers l'application en MV (VmaaS); toute l'interface utilisateur est locale, seul le traitement est déporté. Avec adaptation de la MV, de la liaison entre l'application et l'appliquette, et l'élaboration de la structure et configuration du service de gestion et mise à disposition (réception demande, incarnation, destruction) des MV.

IA Subsidièrement (év.) en installation d'application (IA) au sein de l'hôte : Le conditionnement d'installation avec l'élaboration et la mise à disposition des scénarios automatiques d'installation :

- pour Windows, il s'agit d'un installateur automatique (élaboré avec NSIS);
- pour Linux, il s'agit d'un paquet d'installation pour le "package management system" (dpkg(.deb)/apt/Synaptic pour la distribution³² Debian/Ubuntu).

Les formats VA (simple) et VD ont la priorité, puis le LD.

Pour l'assistance durant l'installation (de tous les formats), ou l'utilisation du format en application, nous suggérons l'emploi d'UltraVNC SingleClick, bien sécurisé.

13. Le conditionnement (packaging) d'installation en "virtual appliance"³³ des divers progiciels serveurs, avec leur mise en place³⁴, le noyau et les seuls utilitaires du système nécessaires, les logiciels et bibliothèques complémentaires, les configurations³⁵ standards et les scripts système de référence; sous la forme d'une image³⁶ prête à être chargée. Ceci comprend aussi la fourniture de la description détaillée de l'opération, éventuellement les scénarios automatisant celle-là.

Ceci sous Ubuntu Server Edition JeOS (Just enough OS), testé³⁷ avec l'hyperviseur

les zones tampons de lecture ou d'écriture. En cas de défaut de bloc dans la zone tampon* de lecture, il génère une requête au réseau. Les blocs d'écriture transférés dans la zone tampon sur disque sont chiffrés. Les flux des blocs (lecture) requis sont gérés dynamiquement entre les serveurs sources, les clients en disponibilités et ceux en relais intermédiaires. Les divers cas d'accessibilités des clients derrière un NAT sont traités.

(*) dont la taille peut être limitée et le contenu géré alors en cache avec remplacement.

Le Tunnelier-Distributeur ne fait pas partie d'xVote, mais sera mis à disposition librement, sous une licence Open Source.

30 En fait deux fichiers, un second est créé pour l'espace d'échange (Swap).

31 Il s'agit du système Ubuntu, comme le client de la VM (mais non spécifiques), et installé à l'aide de WUBI.

32 La structure portable OpenPKG sera considérée en temps utile. A défaut de son emploi, la possibilité d'élaborer, en interne de la fonction de développement, des paquets d'installation pour les distributions autres que Debian/Ubuntu n'est cependant pas acquise.

Il est à noter que la distribution en format d'application, en opposition à celle au format de "Virtual Appliance", est secondaire et non prioritaire; La version en "VA" ne souffre pas -par définition- de la multiplicité des formats de conditionnement.

33 "Virtual appliance" = application logicielle pré-configurée dans une machine virtuelle (avec son propre système d'exploitation) et prêtes à l'emploi.

34 Y compris les mises à jour automatiques.

35 Avec postconfiguration automatique personnalisée, tant selon OVF que depuis un registre (p.ex. les scripts adaptés).

36 Il se pourrait que ce conditionnement suive alors l'OVF (Open Virtual Machine Format) du DMTF (IBM, HP, Dell, Microsoft, VMware, Xen, etc.). Proposed standard, october 2007.

37 Ubuntu-JeOS est actuellement optimisé/dédié pour les produits VMware et pour KVM.

KVM³⁸.

Ce conditionnement³⁹ standard est très utile soit comme moyen simple et robuste de livraison au client, soit surtout comme moyen efficace de mise en œuvre strictement itérative en vue du concept "Software as a service"⁴⁰.

14. La mise sur pied et la mise en production des moyens de traitement des systèmes ou services annexes nécessaires à xVote (en particulier, mais pas exclusivement, de services novateurs hors de ce mandat) sont intégralement pris en charge, de même que leur exploitation durant les tests [le cas échéant, durant les pilotes] et (pour les services novateurs) durant toute la phase pilote.

En conséquence, préalablement aura eu lieu l'implantation des parties des services novateurs utilisés par xVote, et ultérieurement la mise sur pied des structures d'établissement pérennes.

L'exploitation des services novateurs utilise, afin d'assurer la capacité et la fiabilité, une grille informatique spécialisée et disséminée, et des serveurs de soutien à ces services de base additionnels.

15. L'ensemble des moyens propres à assurer la qualité, l'efficacité, la continuité, la fiabilité et la sécurité du travail est pris en charge :

- redondance des connexions Internet et télécom⁴¹;
- surveillance et filtrage des connexions Internet;
- moyens de repli immédiats en cas de panne matérielle;
- alimentations filtrées et ininterrompibles par onduleurs et génératrices;
- alarmes et surveillance vidéo;
- sauvegardes locales, distantes et externes;
- chiffrement et contrôle d'intégrité des liaisons et sauvegardes externes;
- répartition de données critiques et basculement de serveurs si haute-disponibilité.
- distribution sécurisée et redondante de certains services critiques.

Il sera pris, pour les personnes réalisant le projet xVote, les précautions personnelles d'usage et les protections adéquates.

16. La préparation du code source pour publication, son conditionnement et sa (primo-)publication en ligne.

17. L'appui technique à l'obtention d'un ou -au plus- deux⁴² utilisateurs pilotes (cantons).

38 Le moniteur KVM utilise actuellement les I/O QEMU, donc -outre le format natif qcow2- divers formats de disques virtuels sont disponibles.

39 Il sera particulièrement étudié, et le cas échéant mis en œuvre, l'outil rBuidier de rPath, (ou/dont l'outil Coronary) pour la gestion de mise paquetage VA et des mises à jours.

40 En cas d'exploitation interne des pilotes, il s'agit bel et bien immédiatement un cas de SaaS.

Ainsi, la dépense passera dans les charges de fonctionnement du canton contrairement à une acquisition traditionnelle de licence, comprenant la mise en œuvre d'infrastructure matérielle, la formation de personnel et la création de postes, qui nécessitent d'être passés en ouverture de nouveau budget, généralement devant le parlement. Ainsi, le passage en mode SaaS peut être une stratégie pour réduire les dépenses d'investissement et passer le coût en charge opérationnelle. Cela peut permettre d'obtenir rapidement le service supplémentaire, alors que les dépenses nécessiteraient une phase de validation budgétaire longue.

41 Multi-opérateurs Internet, téléphonie fixe et mobile.

42 En cas de deux utilisateurs pilotes, ils seraient décalés : vote pilote 1 avec un seul canton, votes pilotes 2 et 3 avec deux cantons. La tâche de développement ne s'étend donc pas au troisième vote pilote pour le second canton.

18. La formation technique du partenaire pilote (un ou deux⁴² cantons) et un appui pour les activités de conseil et de formation auprès de celui-ci.
19. La facilitation des travaux d'audit (nous recommandons un audit du système xVote par une Haute École).
20. L'appui technique aux relations avec les partenaires (commerciaux, exploitants) et les acteurs du pilote (direction ou gouvernement, administration) ainsi qu'aux tâches de communication (hautes écoles, associations, politiciens et hauts fonctionnaires), et de promotion (auprès des média et leaders d'opinion).
21. Des moyens de déplacement optimaux adaptés à chaque phase du travail et à la situation de chaque cas seront mis en oeuvre.
Durant les dix-huit premiers mois environ, l'aire optimale est surtout la Suisse. Par ailleurs, tous les déplacements d'une journée sont intégralement pris en charge.
22. La mise en oeuvre (et la prise en charge) des moyens de télécommunication, de communication continue et de collaboration adaptés et performants, autant que possible assurant une connectivité permanente ou -par défaut- l'enregistrement et la notification des messages vocaux ou écrits.
23. L'appui, en tant qu'expert technique du domaine, pour l'élaboration de la politique commerciale et sa communication.

La langue de travail et des documents est le français.