

Pour la description du logiciel proprement dit, de son développement, voir le document similaire pour la version en "application à installer" :

"Notes sur les plateformes d'exécution client – application" fichier 20060904_2200.

Exploitation directe en machine virtuelle

Avec un PC sous Windows¹ 2000², Vista³ ou XP⁴, Mac OS X ou un Linux actuel (voir ci-dessous), il est possible d'utiliser xVote en "virtual appliance"⁵ (outil virtuel) avec un ensemble cohérent et idéalement configuré, sans installation⁶ et en parfaite sécurité.

Au lieu de s'exécuter directement sur le poste du votant, la votation a ainsi lieu dans une machine virtuelle saine, totalement isolée de la machine physique du citoyen, donc sans risque de contamination par des virus ou d'intrusion par des vers, sans crainte d'espionnage ou de piratage, et enfin sans laisser la moindre trace⁷ (données de vote) dans la machine du votant.

De plus, cette version effectue toutes les transactions concernant le bulletin (dépôt, reçu) via un sur-réseau d'intraçabilité⁸.

Le citoyen n'a aucune installation à faire, n'a pas de soucis d'incompatibilités, ne découvre pas que ses logiciels seraient obsolètes, incomplets ou inadaptés, que ses choix ou configurations de programmes ou du système iraient à l'encontre des besoins du vote, n'a pas la surprise que son poste serait modifié par la solution de votation. Enfin, il peut librement partager son ordinateur sans que son anonymat ou secret du bulletin soit compromis.

De plus, avec la solution de stockage transitoire adoptée (JeJiT), la livraison des logiciels est radicalement limitée et automatique : il suffit de télécharger l'installateur d'amorce depuis le site d'origine⁹, puis un rapide chargement en cascade¹⁰ et seulement de l'essentiel¹¹ est opéré.

Si la solution de vote a déjà été utilisée, ce petit installateur se mue en un gestionnaire de mise à jour¹².

Ensuite, le lancement¹³ a automatiquement lieu, et c'est lors de l'exécution que le solde nécessaire est chargé au vol¹⁴.

1 Les Windows supportés par Microsoft

2 Win2000 (ou 2003) y.c. Professional, Server ou Advanced Server, tous avec SP3 ou SP4. Le dotNET Framework doit être installé.

3 WinVista, toutes versions, en versions x86 (32bits) et x64 (environnement optimisé pour l'architecture 64 bits).

4 WinXP, avec tous les service pack SP1 ou SP2, en x86 uniquement. Le dotNET Framework doit être installé.

5 Application logicielle pré-configurée dans une machine virtuelle (avec son propre système d'exploitation) et prêtes à l'emploi.

6 Mise à part un logiciel complémentaire (hyperviseur), et un gestionnaire de liaisons (tunnelier-otv), qui sont pris en charge par un petit installateur/rafraîchisseur automatique.

7 Optionnellement, une éventuelle zone partagée avec la machine hôte [shared directory] est possible pour le transfert de données, p.ex. l'identité numérique, ceci en remplacement du stockage à distance proposé pour celle-ci.

8 Les connexions entre le poste du votant et les serveurs de la Scrutation se font en passant par une cascade de relais intermédiaires (Mix), avec un chiffrement en pelure d'oignon, où chaque relai ne connaît que le précédent et le successeur. Au final, l'adresse (IP) de la connexion est radicalement différente (et située ailleurs) de celle du poste du votant, empêchant de l'identifier et interdisant le un éventuel rapprochement avec l'adresse reçue par l'Habilitation.

Ceci ajoute une protection supplémentaire de l'anonymat, en rendant même toute collusion entre les exploitants de l'Habilitation et de la Scrutation inopérante.

9 Charge avec une connexion sécurisée HTTPS. Il est souhaitable de vérifier le certificat du site par sécurité supplémentaire, le site utilise les nouveaux certificats EV SSL.. Cet installateur est une applique exécutable dépendant de la plate-forme cible.

10 Avec le protocole BitTorrent, intégré dans l'installateur, permettant une haute vitesse de téléchargement (multiples sources dynamiques) sans risque de surcharge des serveurs (et donc de ralentissement).

11 Sont chargés uniquement un hyperviseur, un tunnelier(otv) et un serveur de sur-réseau de partage. Ces logiciels sont les seuls installés sur le poste, il le sont simultanément. Les accès à l'Internet de ces programmes doivent être autorisés par le système (personnal fire-wall).

12 L'hyperviseur et le tunnelier/distributeur sont vérifiés pour leur fraîcheur et leur intégrité, et seulement à défaut (absence, corruption ou obsolescence), ils sont re-chargés

13 L'hyperviseur utilisé est un pur exécuteursans commandes de gestion.

14 Les lectures initiales se font à distance, à chaque fois soit depuis des unités de stockage déportées et adressés parallèlement à haut

En résumé, les avantages de ce conditionnement sont qu'aucune installation locale (hormis le très modéré chargement de l'essentiel) n'est nécessaire, et pratiquement aucun espace disque n'est utilisé définitivement (environ¹⁵ 30 Mo). Il n'y a aucun souci de complétude, de compatibilités ou de configurations. La votation est à l'abri de virus ou autres piratages. L'opération a lieu exactement dans les conditions indispensables. Les données manipulées durant l'exécution sont confinées et disparaissent lors de la sortie de l'outil virtuel.

Seulement le nécessaire et qu'au bon moment (*Just enough – just in time*) !

Les avantages de ce conditionnement hors pair viennent ainsi s'ajouter très naturellement aux avantages intrinsèques incomparables du système xVote.

☞ Caractéristiques^{16&17} minimales nécessaires du poste du votant :

- processeur Intel ou AMD x86 ou x86-64 (64 bits), raisonnablement puissant, ce qui est le cas de tous les récents, par exemple au moins 733 MHz ou 1500 MHz (1,5 GHz),
- avec une mémoire (RAM) de 512 Mo¹⁸ ou mieux (car c'est toujours préférable),
- avec une taille de l'espace disque libre¹⁹ d'environ une trentaine de Mo (pour la partie résidente), par ailleurs une part de l'espace libre supplémentaire est utilisé temporairement pour améliorer l'efficacité des chargements transitoires²⁰ et pour maintenir les données intermédiaires²¹,
- une connexion internet²².

☞ L'hyperviseur utilisé fonctionne et est disponible actuellement²³ pour les systèmes d'exploitation hôtes suivants :

Windows hosts:

- Windows XP, all service packs (32-bit)
- Windows Server 2003 (32-bit)
- Windows Vista (32-bit and 64-bit).

Apple Mac OS X hosts (Intel hardware only, all versions of Mac OS X supported)

Linux hosts (32-bit and 64-bit):

- Debian GNU/Linux 3.1 (“sarge”) and 4.0 (“etch”)
- Fedora Core 4 to 8

vitesse (il y en a une poignée déjà pour le prototype), soit -par la mise en cache locale implicite- depuis d'autres postes clients qui deviennent progressivement des serveurs supplémentaire (P2P/Pair-à-pair au moyen du standard Gnutella2).
Voir aussi les notes 20 et 21.

15 Hyperviseur env. 30 à 37 Mo (selon plateforme), Distributeur env. 4-5 Mo, Tunnelier de l'ordre de 3 Mo

16 Et bien sûr, des capacités graphiques d'une résolution d'au moins 1024x768 pixel, et de capacités sonores (optionnelles).

17 L'installation doit bénéficier des droits d'administrateur pour s'exécuter complètement. Par ailleurs, pour le chargement au vol à pleine vitesse, le poste doit pouvoir recevoir les datagrammes (UDP) d'une manière ou d'une autre.

19 Avec la solution purement transitoire (JeJIT), sinon bien plus.

S'il y avait une installation intégrale (ce qui est optionnellement possible), le transfert serait au total d'environ deux cents méga-octets[†] (compressé, à décompresser pour utiliser), et l'espace disque nécessaire d'environ 1 Go à 1 ½ Go avec les nécessaires zones libres.

(†) 200 Mo représentent un temps théorique de chargement de 2 mn avec une connexion (moyenne câble) de 15 Mb/s (=1,78 MiB/sec). En réalité, elle est souvent bien plus longue, couramment dix à trente fois plus.

20 Pour un cache des segments téléchargés et gardés à disposition (selon l'espace disponible). La zone est temporaire à la session. Optionnellement, cette zone peut être conservée pour une reprise proche, ou pour maintenir la mise à disposition dynamique.

21 Pour les segments modifiés localement, ceux-ci sont stockés chiffrés sous une clefs aléatoire à usage unique (donc illisibles pour des tiers) et de plus effacés à la fin de la session. La zone est temporaire à la session.

22 Une connexion internet *permanente*, qu'elle soit directe ou via le réseau local (LAN, WiFi, ADSL, câble, etc.); plus elle est rapide, mieux c'est (surtout descendante/downlink).

23 début mai 2008.

- Gentoo Linux
- Redhat Enterprise Linux 3, 4 and 5
- SUSE Linux 9 and 10, openSUSE 10.1, 10.2 and 10.3
- Ubuntu 5.10 (“Breezy Badger”), 6.06 (“Dapper Drake”), 6.10 (“Edgy Eft”), 7.04 (“Feisty Fawn”), 7.10 (“Gutsy Gibbon”)
- Mandriva 2007.1 and 2008.0

It should be possible to use VirtualBox on most systems based on Linux kernel 2.4 or 2.6 using either the VirtualBox installer or by doing a manual installation.

Solaris hosts (32-bit and 64-bit):

- OpenSolaris (“Nevada” build 81 and higher)
- Solaris 10 (u4 and higher, experimental support)