



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Premier
ministre

Machines à voter pratiques et sécurisées

Les machines à voter de nouvelle génération

**Direction Centrale de la Sécurité des Systèmes
d'Information**

F. Chabaud,

4 décembre 2008

Plan

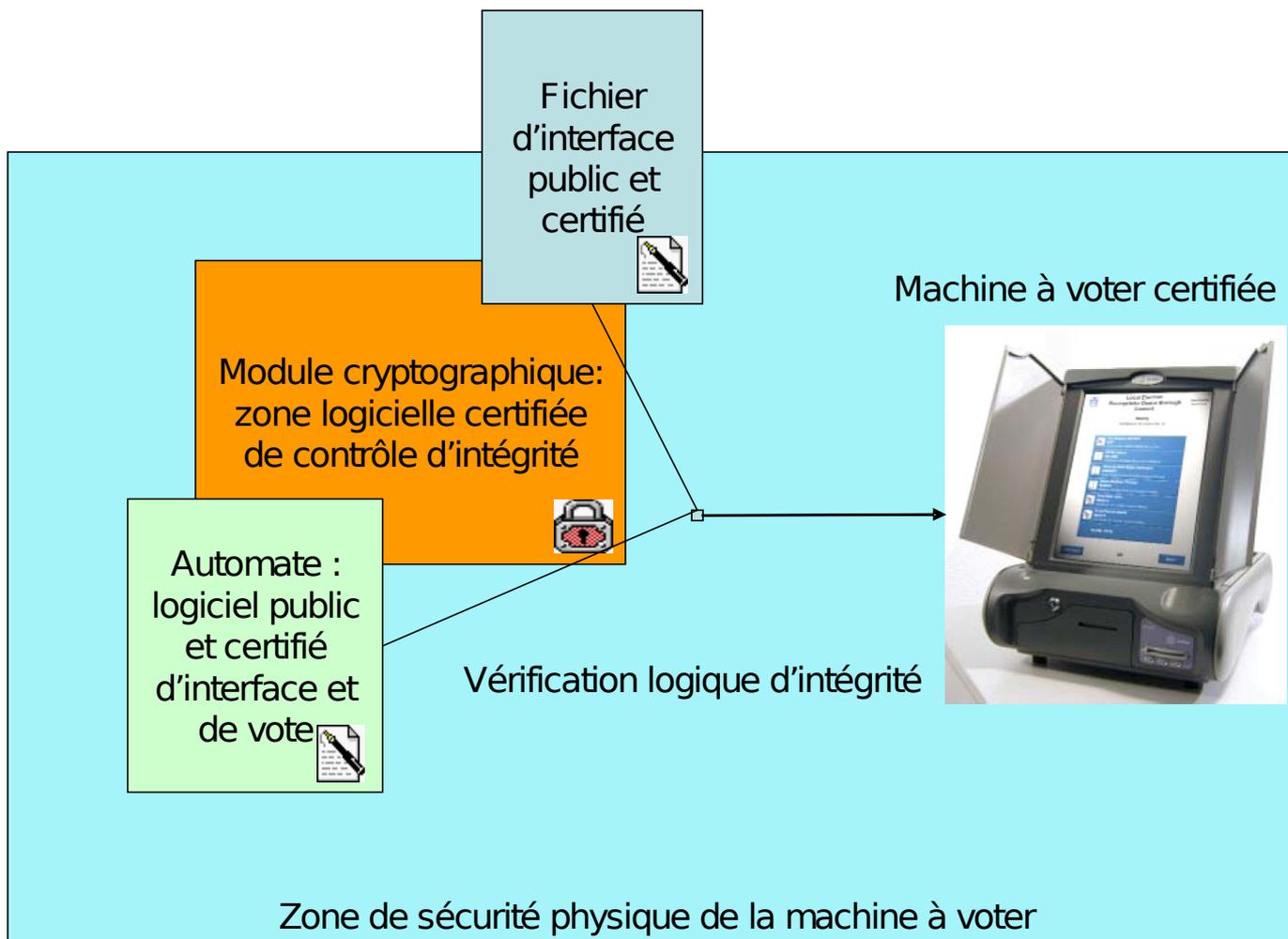
Cet exposé présente un travail conjoint avec E. Bresson, X. Chassagneux et M. Videau

- ❑ Fondements scientifiques
- ❑ Principes
 - ✓ Architecture
 - ✓ Certification de l'interface
 - ✓ Automate
 - ✓ Sécurité physique
- ❑ Le jour J
 - ✓ Vérification de la machine à voter
 - ✓ Déroulement du scrutin
- ❑ Le contrôle par le citoyen
- ❑ Usage de la cryptographie

Fondements scientifiques

- ❑ L'utilisation des machines à voter existantes a fait apparaître des anomalies qui jettent le doute sur ce mode de scrutin
- ❑ De fausses bonnes idées sont apparues en réaction
 - ✓ Ne pas recourir aux machines à voter
 - C'est une solution, mais peu constructive.
 - ✓ Utiliser des bulletins classiques que l'on scanne ou que l'on stocke pour permettre une vérification ultérieure
 - Problème juridique : quel résultat prévaut en cas de différence ?
 - Problème de fond : cela ne dissipe pas les doutes, au contraire.
 - ✓ Utiliser des protocoles cryptographiques de vote
 - Coût d'infrastructure élevé
 - Compréhension très (trop) difficile pour le citoyen
- ❑ Par contre, une idée semble intéressante :
 - ✓ Séparer le processus de configuration du scrutin de celui du vote
 - ✓ Publier et prouver formellement ce dernier processus

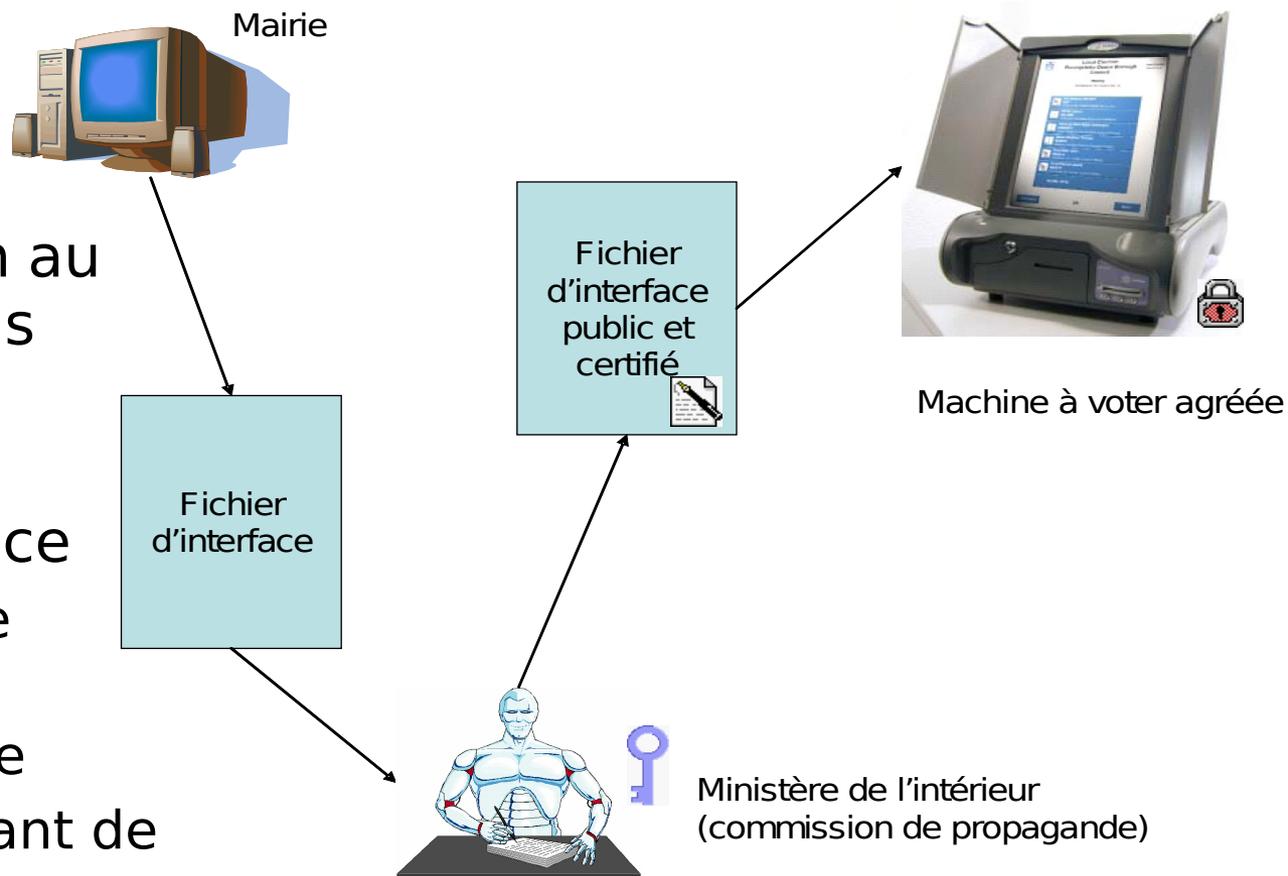
Principe d'architecture



- ❑ Automate minimal exécutant l'interface
- ❑ Fichier d'interface homme-machine
- ❑ Module cryptographique
- ❑ Logiciel de décompte
- ❑ Sécurité physique

Principe de certification de l'interface

- ❑ Application au cas français
- ❑ Principe : assurer la transparence
 - ✓ Interface publiée
 - ✓ Vérifiable
 - ✓ Permettant de s'entraîner au vote



Principe de l'automate

- ❑ Issu des travaux de Ka-Ping Yee, David Wagner, Marti Hearst et Steven Bellovin <http://zesty.ca/voting>
- ❑ L'automate doit être uniquement capable
 - ✓ d'afficher des images issues du fichier d'interface
 - ✓ d'affecter à certaines portions des liens selon une structure définie dans le fichier d'interface
 - ✓ de passer d'une page à une autre selon les liens choisis par l'utilisateur
 - ✓ de comptabiliser certaines transitions, qui constituent le vote proprement dit
- ❑ Le code de l'automate doit être
 - ✓ Public (source et binaire)
 - ✓ Prouvé et certifié cryptographiquement (binaire)
 - ✓ Vérifié par le module cryptographique de la M à V

Principe du module cryptographique

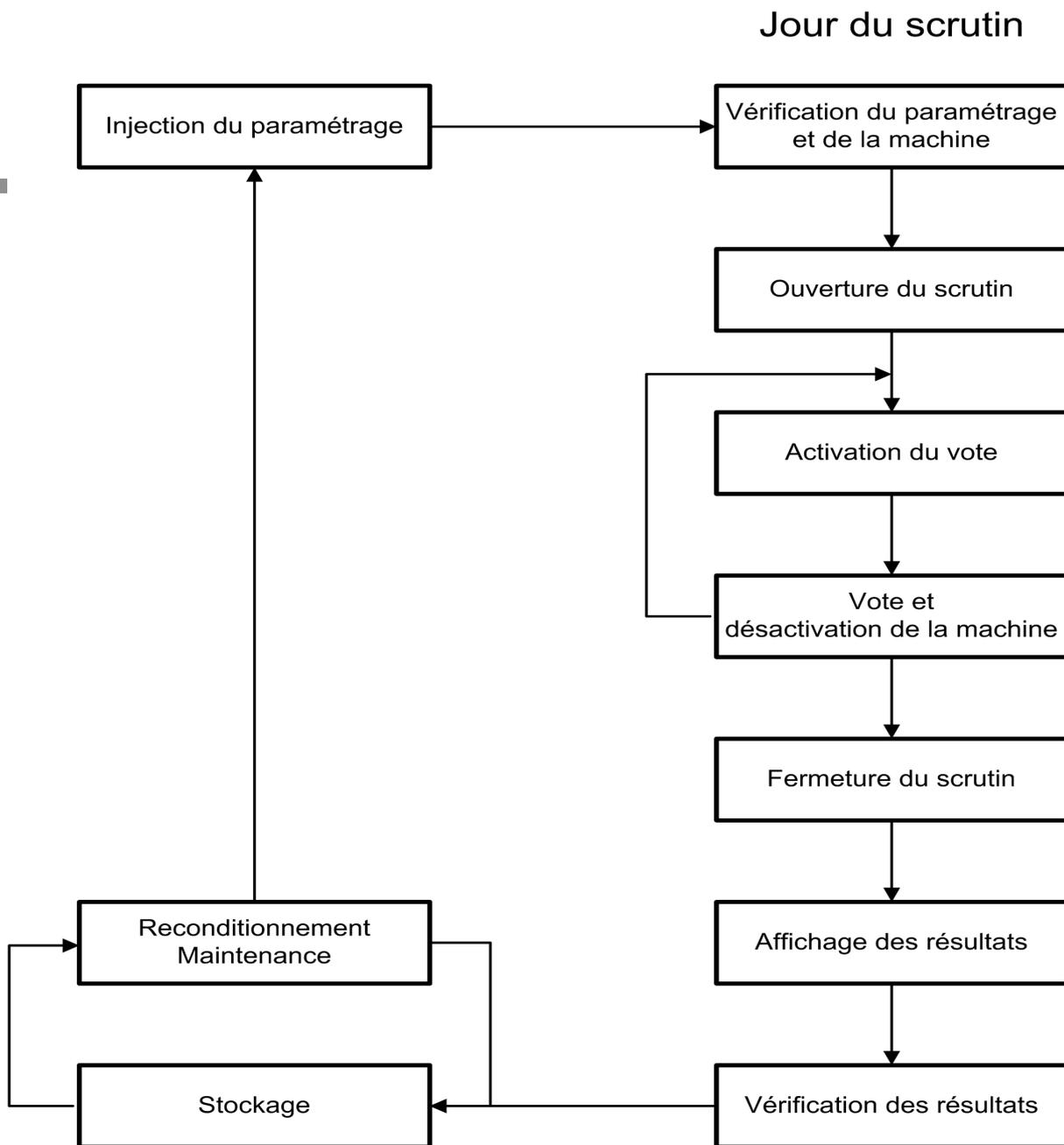
- ❑ Ne participe pas au décompte des voix
 - ✓ Aucun chiffrement dans le dépouillement du scrutin
- ❑ Sert à vérifier les certifications cryptographiques
 - ✓ De l'automate
 - ✓ Du fichier d'interface homme-machine
- ❑ Dispose pour cela d'un affichage autonome et indépendant de l'interface de vote
 - ✓ Une simple diode verte suffit !
 - ✓ L'idée est que le module doit pouvoir afficher que tout va bien
- ❑ Ce module est sécurisé.
- ❑ Ses fonctions sont publiques.
 - ✓ Mais son code interne n'a pas besoin de l'être
 - ✓ Ses dispositifs de sécurité physique ne sont pas publics
- ❑ Il est évalué et certifié, avec le reste de la MÀV
 - ✓ Selon un processus qui préserve le savoir-faire des fabricants

Sécurité physique

- ❑ La protection logique est assurée par le module cryptographique
- ❑ Elle est complétée par des mesures de sécurité physique
 - ✓ Scellé externe numéroté inspectable visuellement
 - Protège contre l'ouverture de la MÀV et l'accès aux mémoires
 - ✓ Capot interne transparent
 - Protège l'accès aux composants électroniques assurant la sécurité logique de la machine (notamment le module cryptographique)
 - Protège les connecteurs des interfaces de la machine (écran, clavier, console déportée du président du bureau de vote)
 - ✓ Scellé interne numéroté
 - Protège contre l'ouverture du capot transparent
 - ✓ Deux clés physiques distinctes
 - Permettent au président et à l'un de ses assesseurs d'activer les opérations sensibles de la machine.

Le jour J

- ❑ Vérification du paramétrage
- ❑ Déroulement du scrutin
- ❑ Fermeture du scrutin
- ❑ Affichage des résultats
- ❑ Vérification des résultats



Jour du scrutin

9/16

Vérification de la machine à voter

- ❑ Les modes de vérification actuels n'étaient pas satisfaisants
- ❑ Le nouveau mode de vérification s'appuie sur :
 - ✓ La preuve formelle *a priori* des logiciels
 - ✓ La certification cryptographique de ces logiciels
 - ✓ La vérification de cette certification le jour J
 - ✓ Le contrôle *a posteriori* de l'intégrité physique de la machine
 - ✓ L'existence d'un cahier de suivi de chaque machine
- ❑ Juste avant le scrutin, on vérifie :
 - ✓ Scellé physique externe, autotest du module cryptographique, empreintes cryptographiques des logiciels certifiés et nombre nul de votants
- ❑ Juste après le scrutin, on vérifie :
 - ✓ Preuve cryptographique d'origine du résultat du vote, scellé interne, contrôle visuel de la zone de sécurité (par référence au cahier de suivi)

Déroulement du scrutin

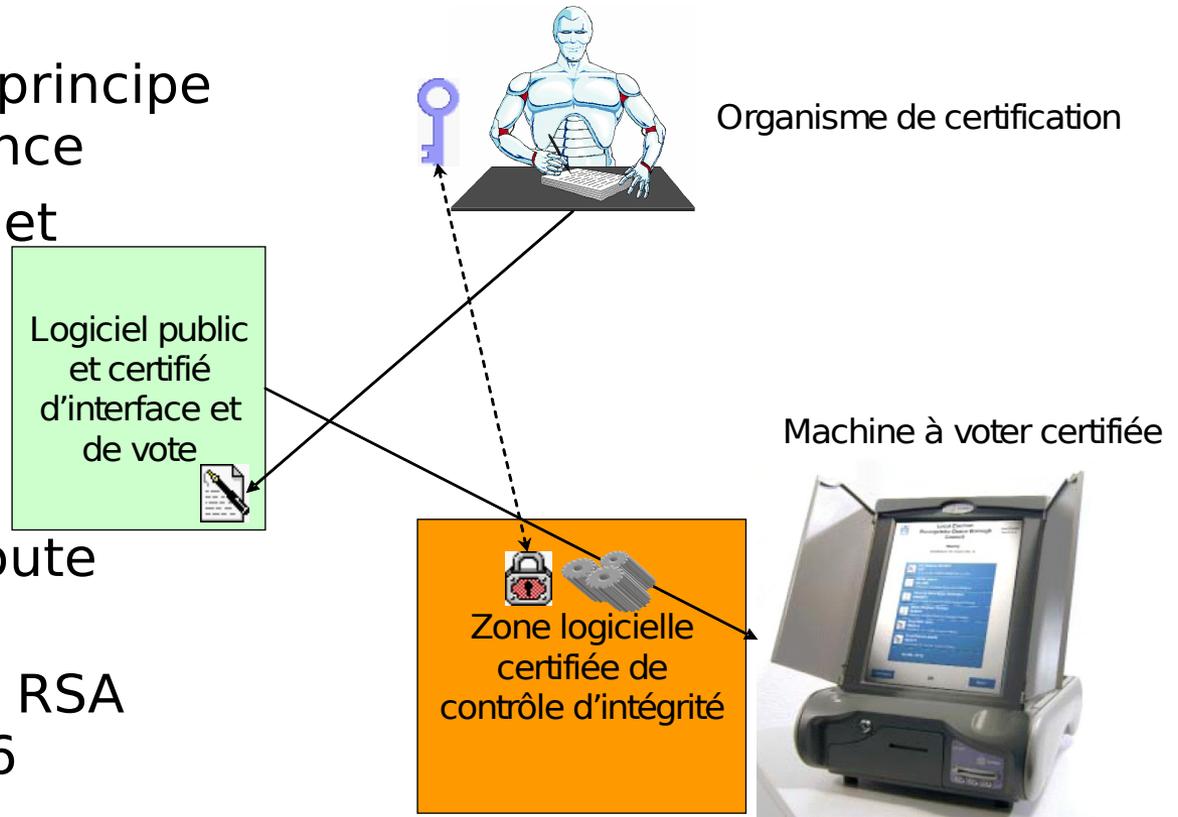
- ❑ Déroulement d'un processus de vote :
 - ✓ Le président active un droit de vote après vérification de l'identité
 - ✓ La confirmation du vote désactive automatiquement la MÀV
 - ✓ Si un votant ne valide pas son vote
 - On essaie de le rattraper :-)
 - Sinon, le président et son assesseur, à distance de la MÀV, activent la fonction « vote nul » ; ce point est porté au PV.
- ❑ Cas de panne
 - ✓ On met en place une machine de secours
 - ✓ En fin de scrutin :
 - après vérification de l'intégrité physique des deux MÀV.
 - les mémoires de la machine défaillante sont insérées dans la machine de secours.
 - La machine de secours affiche (si possible) le contenu des mémoires et la signature cryptographique de la machine défaillante.
- ❑ Principe : toute anomalie est consignée au procès-verbal

Le contrôle par le citoyen

- ❑ L'agrément des machines suppose une certification de sécurité dont le résultat est public, même s'il n'est pas détaillé.
- ❑ En fonction de ses compétences, le citoyen peut vérifier :
 - ✓ Les signatures de l'automate et du fichier d'interface employés
 - Calcul mathématique
 - Concordance avec les valeurs publiées par l'administration
 - ✓ Le logiciel d'interface
 - Tant son contenu...
 - Que la preuve formelle de son bon fonctionnement
 - ✓ Les résultats affichés
 - Vérification de la signature de la MÀV, même en cas de panne
 - Contrôle de l'intégrité physique de la machine
 - Concordance des scellés
 - Aspect visuel interne

Usage de la cryptographie

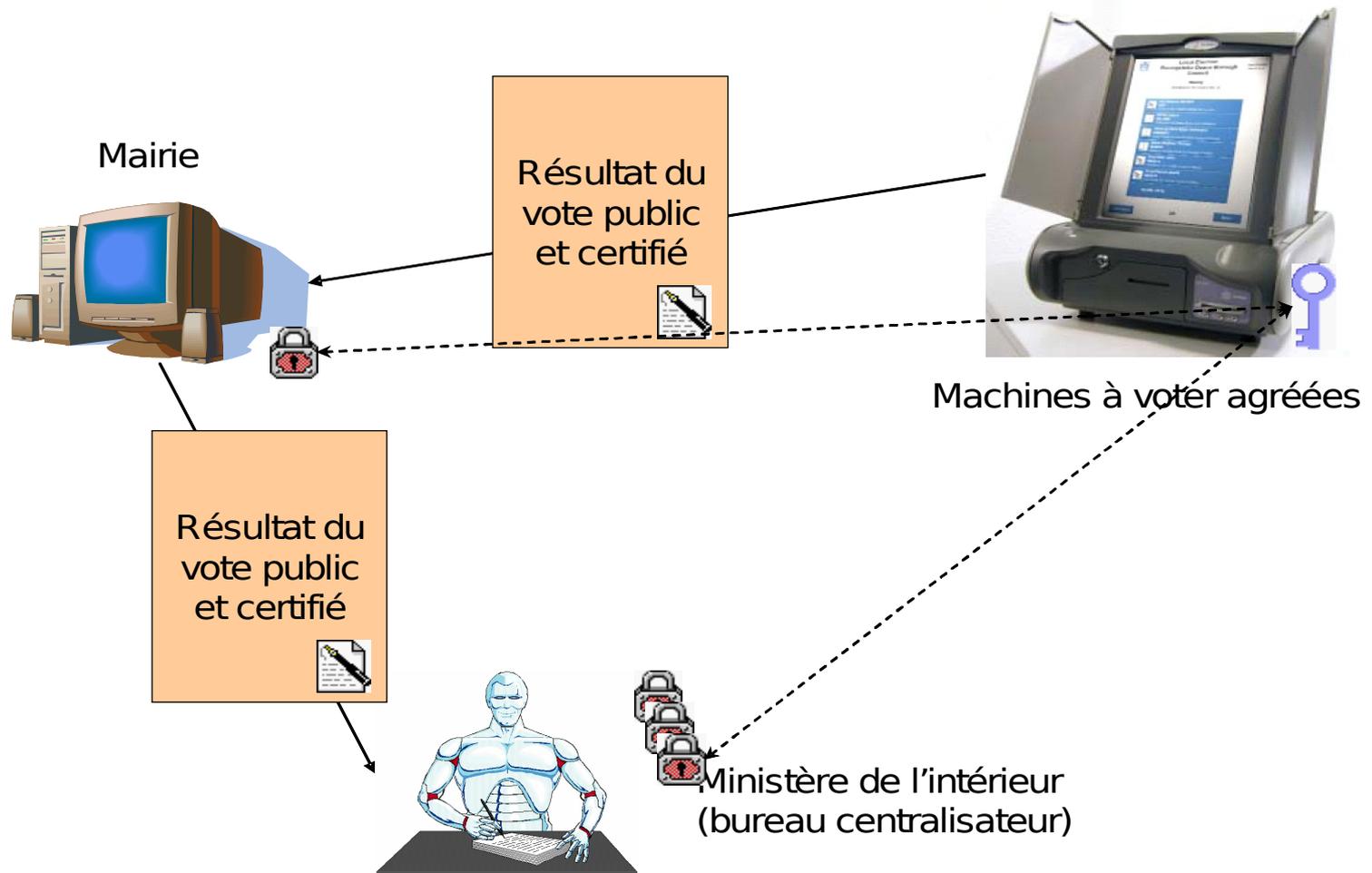
- ❑ Pas d'usage en confidentialité
 - ✓ Contraire au principe de transparence
- ❑ Assure intégrité et preuve d'origine
- ❑ Cryptographie asymétrique « classique »
 - ✓ Pour éviter toute suspicion
 - ✓ Typiquement RSA 2048 ou 4096



Gestion des clés

- ❑ Nécessité d'une IGC « minimaliste »
 - ✓ Publication d'un certificat d'autorité racine
 - ✓ Intégré au module cryptographique
 - ✓ Attestant de la vérification « officielle » du logiciel de l'automate
 - Par exemple, publication au JORF
 - ✓ Protège contre l'introduction d'un logiciel d'interface et de vote non certifié
- ❑ Pour le reste, la simple publication des certificats est suffisante pour assurer la possibilité de contrôle
 - ✓ Il suffit que le module cryptographique affiche les éléments pertinents des vérifications de signature.
 - Empreinte cryptographique de la clé publique
 - Valeur de la signature
 - Empreinte cryptographique de la donnée signée

Certification des résultats du dépouillement



Conclusion

- ❑ L'architecture de machine à voter proposée permet :
 - ✓ D'améliorer la transparence des opérations de vote sur une urne électronique.
 - ✓ D'améliorer la sécurité des machines à voter par des fonctions élaborées de contrôle d'intégrité et de preuve d'origine.
 - ✓ D'assurer une meilleure traçabilité des incidents de vote :
 - Vote nul
 - Panne
- ❑ La sécurité obtenue n'est pas absolue
 - ✓ On peut imaginer des scénarios d'attaque
 - ✓ Mais le coût en est important
 - Chaque machine dispose de sa propre clé cryptographique
 - Le cahier de suivi assure une traçabilité de la maintenance
 - ✓ Et surtout, une attaque sur le système global paraît improbable