



## Point de Contact

Pour plus d'information, vous pouvez contacter le Directeur du Projet CyberVote :

EADS Systems & Defence Electronics  
Mr **Stephan BRUNESSAUX**  
Tel : +33 2 32 63 40 55  
Fax : +33 2 32 63 42 00  
Mail : [contact@eucybervote.org](mailto:contact@eucybervote.org)  
Web : <http://www.eucybervote.org>



# CYBERVOTE

## Voter en toute confiance via internet !

### Le consortium :

#### > PARTENAIRES INDUSTRIELS

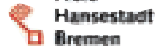
- EADS Systems & Defence Electronics,  
<http://www.eads.net>
- le centre de recherche de Nokia en Finlande,  
<http://www.nokia.com>
- BTexact Technologies au Royaume Uni,  
<http://www.bt.com>

#### > PARTENAIRES UNIVERSITAIRES

- l'Université de Leuven en Belgique,  
<http://www.kuleuven.ac.be/kuleuven/>
- l'Université de Eindhoven aux Pays-Bas,  
<http://www.tue.nl>

#### > PARTENAIRES UTILISATEURS

- la ville de Brême en Allemagne,  
<http://www.bremen.de>
- la Mairie d'Issy-les-Moulineaux en France,  
<http://www.issy.com>
- l'arrondissement de Kista/Stockholm en Suède,  
<http://www.kista.com>





CyberVote, un système innovant de vote en ligne à partir de terminaux Internet fixes ou mobiles, est un projet de recherche et développement (RDT) co-financé par la Commission Européenne et les industriels et organisations participants. Il s'inscrit dans le cadre du programme 1999 des Technologies de l'Information (IST) pour la recherche, le développement et la démonstration de technologies du 5ème programme cadre (5ème PCRD). Il est rattaché à l'action clé « Systèmes et services pour les citoyens ». Le projet a démarré le 1 septembre 2000. Il se terminera le 31 mars 2003. Le budget total du projet est de 3 243 629 Euros et représente un effort total de 27.4 hommes-années.

## > Description du projet

L'objectif du projet CyberVote est de réaliser et faire la démonstration d'un prototype de système de vote en ligne intégrant un protocole de vote par Internet hautement sécurisé et vérifiable, et conçu pour être utilisé dans des élections de différents types.

Ce prototype permet aux électeurs d'exprimer leur vote par le biais de l'utilisation de terminaux Internet tels que PCs, ordinateurs de poche et téléphones mobiles. Il repose sur un protocole innovant de vote, qui assure l'authentification des électeurs, l'intégrité et la confidentialité de leur vote lors de son envoi par Internet mais également lors du dépouillement et de la phase de vérification des votes.

## > Objectifs sociaux

Le projet CyberVote a pour objectif de contribuer à la mise en place d'une démocratie plus participative. CyberVote facilite la procédure de vote de tous les électeurs et en particulier des personnes à mobilité réduite (handicapés, personnes souffrantes, personnes hospitalisées, personnes âgées, etc.), des personnes en déplacement au moment des élections, des expatriés. Il répond ainsi aux contraintes des citoyens, en leur permettant de s'exprimer sans être obligés de se rendre dans les bureaux de vote habituels ou de faire une procuration. Il offre également une alternative sécurisée au vote par correspondance quand celui-ci est autorisé.

# Voter en toute confiance via internet !

## > Principales caractéristiques techniques

1. Utilisation d'un algorithme de cryptographie homomorphe qui assure un secret total du vote envoyé par le votant : le vote est crypté avant son envoi vers l'urne virtuelle et n'est jamais décrypté même lors du dépouillement du scrutin.
2. Confiance distribuée et robustesse : le calcul du résultat du scrutin repose sur la présence de  $p$  scrutateurs parmi les  $n$  scrutateurs autorisés. Les bulletins de votes cryptés sont multipliés entre eux pour obtenir le résultat crypté du scrutin. Ce résultat est décrypté avec les morceaux de la clé privée partagée par les scrutateurs.
3. Approche vérifiable permettant à chaque votant de vérifier que son vote a été pris en compte pour établir le résultat final du scrutin.
4. Support de différents terminaux Internet pour l'envoi du vote. Les terminaux actuellement supportés incluent les Pocket PC (testé sur iPAQ Pocket PC), les téléphones mobiles Java (testé sur Nokia 9210 et 9210i) et les PC (testé sur W98/W2000/WXP - IE 6.0).
5. Support de différents types d'authentification (cartes à puce ou codes PIN).



## > Elections menées avec le prototype CyberVote

- Brême, Allemagne, du 20 novembre au 4 décembre 2002, élection des conseils de l'Université de l'Administration Publique, résultat à valeur légale
- Issy-les-Moulineaux, France, le 11 décembre 2002, élection prud'homale, élection test
- Kista/Stockholm, Suède, janvier 2003, référendum, élection test.

