

helios

*Bringing open audit elections into practice:
Real world uses of Helios*

Olivier Pereira – Université catholique de Louvain
Joint work with Ben Adida – Harvard and Olivier de Marneffe – UCL

Swiss E-Voting Workshop – September, 2010

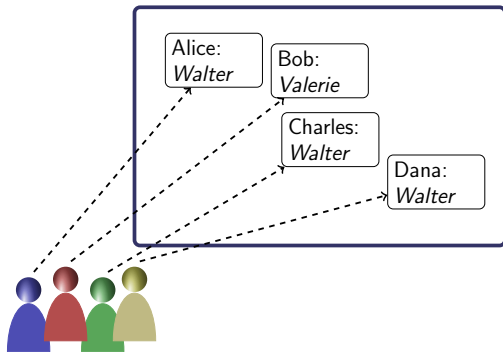


What is Helios?

- ▶ Open-audit elections from your browser
- ▶ Low-coercion elections
 - ▶ Impossible to fully prevent in a remote setting anyway
- ▶ More and more experience: > 25000 votes tallied



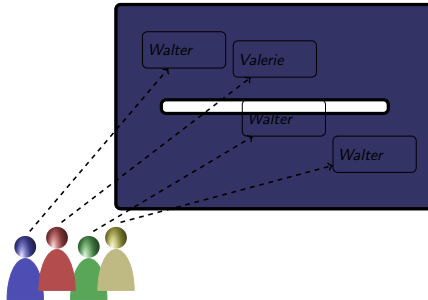
Open audit elections



- ▶ Each voter can verify that nobody tampered with his/her vote
- ▶ Each voter can compute the tally
- ▶ No privacy, no coercion-resistance, no fairness, ...



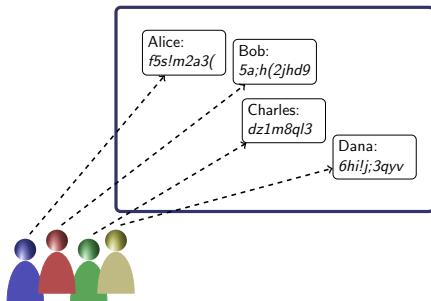
A traditional paper approach



- ▶ With voting booth: privacy, coercion-resistance, fairness, ...
- ▶ **If** a voter keeps an eye on the full urn content all day long, he can be convinced that:
 - ▶ his vote is untampered
 - ▶ the tally is correct
- ▶ A minute of inattention is enough to break this



A cryptographic approach




- ▶ Encryption enables making secret ballots public
 - ▶ I can check that my ballot is still there anytime!
 - ▶ Ballot stuffing becomes really dangerous
- ▶ Zero-knowledge proofs convince that the tally is correct



How does a Helios election work?

1. Organizers prepare and commit on election description: questions, public key, URL for casting vote, ...

helios

Swiss E-Voting Workshop edit
an election created by  **Olivier Pereira**
this election is not featured on the front page.

Swiss E-Voting Workshop demo election

[questions \(0\)](#) | [voters](#) | [trustees \(0\)](#)

Next Step: add questions, voters, and trustees.

voting is not yet open

You are *not eligible* to vote in this election, because registration is closed and you are not registered.

[Audit Info](#)

logged in as  Olivier Pereira [logout]
[About Helios](#)



How does a Helios election work?

2. Voter build/download a ballot preparation system (BPS):
 - ▶ single webpage provided by Helios
 - ▶ webpage provided by a candidate
 - ▶ own script

Université catholique de Louvain **UCL** services

Election du recteur 2009

Accueil ➔ Choix ➔ Confirmation ➔ Scellé ➔ Envoi ➔ Fin

Il vous reste 64 jours 8 heures 18 minutes et 28 secondes pour voter.

Bienvenue à l'élection de démonstration.

Pour voter, vous allez effectuer les étapes suivantes:

1. **Choix** d'un candidat et **Confirmation** de votre choix.
2. **Scellé** de votre bulletin de vote.
3. **Envoi** de votre bulletin de vote scellé.

[Démarrer la procédure de vote!](#)

Editeur responsable : Université catholique de Louvain | Informations sur l'élection | [Vie privée - élection](#)
Service Desk : +32 (0)10/47.82.82 | [Portail du système de vote](#) | Identifiant d'élection : MwUOQmE7U9wGz/zhLPQXK7K2yM



How does a Helios election work?

3. Voter checks election description and picks candidate(s)



Élections étudiantes 2010



Etape 1 sur 3 : Sélection des candidats

Conseil de Faculté FASB

LICHTENSTEIN Sylvie FARM 11 [ADES]

Vote Blanc

Précédent

Suivant

Vous pouvez voter pour autant de personnes que vous le désirez. Les candidats sont présentés par ordre alphabétique.

[Pages d'aide](#) | [Informations élections](#) | [Contact : e-elections@aglouvain.be](#) | [Taux de participation](#) | [Valves de l'élection électronique](#)

Conception cryptographique: [UCL Crypto Group](#)

Éditeur responsable : Assemblée Générale des Étudiants de Louvain (AGL)

67 Rue des Wallons 1348 Louvain-la-Neuve - 010/45.08.88 - <http://www.aglouvain.be/>

Empreinte numérique de l'élection: RxYx7LKAG0mavVtBu6jXtIXQvcGmpIv3MyeZKwCxHdk



How does a Helios election work?

4. BPS commits on ballot (with Helios' BPS)

Université catholique de Louvain **UCL** 


Election du recteur 2009

Accueil → Choix → Confirmation → **Scellé** → Envoi → Fin

Il vous reste 64 jours 8 heures 18 minutes et 0 seconde pour voter.

Numéro de suivi du bulletin de vote scellé


Votre bulletin de vote a été scellé et est prêt à être envoyé.
Le numéro de suivi correspondant à ce bulletin est:

OJEiu3lhXvsArYwKzzYuHOH95S8 

[\[Imprimer\]](#)

Ce numéro de suivi vous permettra de vérifier que votre bulletin de vote est transmis sans erreur et correctement utilisé dans le décompte.

[Envoyer ce bulletin](#)

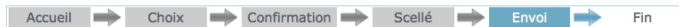
Editeur responsable : Université catholique de Louvain | [Informations sur l'élection](#) | [Vie privée - élection](#)
Service Desk : +32 (0)10/47.82.82 | [Portail du système de vote](#) | Identifiant d'élection : MwUOQmE7U9wGc/zhLPQxKr7K2yM 



How does a Helios election work?

5. Voter chooses to audit or cast (Benaloh challenge)

- ▶ Audit makes the BPS output the ballot and randomness
- ▶ Cast requires authentication for submission



Il vous reste 64 jours 8 heures 17 minutes et 32 secondes pour voter.

Identification pour l'envoi de votre bulletin de vote scellé

Votre bulletin de vote scellé est prêt à être envoyé.

Toutes les informations relatives à votre choix ont été effacées de votre ordinateur.

Seul le bulletin de vote scellé est désormais disponible.

Pour envoyer ce bulletin scellé, merci de compléter le formulaire ci-dessous en utilisant vos identifiants de vote, tels que repris dans [le cadre rose du document pdf](#) que vous avez obtenu lors de votre inscription.

Votre numéro d'électeur	<input type="text" value="ER"/>	Afficher le mot de passe
Votre mot de passe d'électeur	<input type="password"/>	
<input type="button" value="Identification et envoi du vote"/>		

Editeur responsable : Université catholique de Louvain | [Informations sur l'élection](#) |

[Vie privée - élection](#) |

Service Desk : +32 (0)10/47.82.82 | [Portail du système de vote](#) |

Identifiant d'élection : MwUOqmE7U9wGc/zhLPQXKr7K2yM



How does a Helios election work?

6. Voter checks correct reception from bulletin board



Bienvenue sur les valves de l'élection de démonstration

Il y a actuellement 6 bulletins de vote disponibles sur ces valves.

Ces valves vous permettent de vous assurer que votre bulletin de vote a bien été transmis et sera utilisé tel quel lors du décompte des votes. Si vous avez transmis plusieurs bulletins, seul le dernier est pris en compte et affiché ci-dessous.

Il vous est proposé d'indiquer votre numéro d'électeur dans le formulaire ci-dessous, de rechercher le numéro de suivi correspondant à votre bulletin de vote, et de vérifier que ce numéro de suivi est bien celui obtenu lorsque vous avez voté.

Numéro d'électeur:

Numéro d'électeur	Numéro de suivi
ER362268	OJEiu3lhXvsArYwKzzYuHOH95S8

| Editeur responsable : Université catholique de Louvain | [Informations sur l'élection](#) |

| [Vie privée - élection](#) |

| Service Desk : +32 (0)10/47.82.82 | [Portail du système de vote](#) |

| Identifiant d'élection : MwUOQmE7U9wGc/zhLPQXkr7K2yM |



How does a Helios election work?

7. Voter can see (and copy) other ballots from bulletin board

Bienvenue sur les valves des élections étudiantes 2010

Les bulletins de 4488 électeurs sont disponibles sur ces valves.

Ces valves vous permettent de vous assurer que votre bulletin de vote a bien été transmis et sera utilisé tel quel lors du décompte des votes. Si vous avez transmis plusieurs bulletins, seul le dernier est pris en compte et affiché ci-dessous.

Il vous est proposé d'indiquer votre nom et votre prénom dans le formulaire ci-dessous, de rechercher le numéro de suivi correspondant à votre bulletin de vote, et de vérifier que ce numéro de suivi est bien celui obtenu lorsque vous avez voté.

Nom
Prénom

Rechercher

Il y a 9 réponses

Nom	Sigle	Numéro de suivi
Mahieu Raphaël	HIST 13 BA/	45NsWkfBoI4PkA1annC+WktZCjoUjt9b+ACxAQlKiHE
Masquelier Robert	INGE 11 BA/	5+4IKZtx0JVZ0N1I7QDhsTRh3t03Tjg2oZcG2u5hs9Y
Mathot Richard	SINF 13 BA/	ghBQW4vHyoZYUpLWgq9eqYFZ6caJkMH0doQHv8HETGI
Maurice Rebecca	COMU 21 MS/RP	oAkVC+iYRDZVkjvlcpkV5WTlZF43ePFJJDWMf12btFvg



How does a Helios election work?

8. Trustees compute and publish tally, together with correctness proofs

<p>Should the IACR keep its current voting system, based on double envelopes sent via postal mail, or switch to electronic voting over the Internet?</p> <p><i>[select 0 or 1 answer]</i></p>	<p>32 - Keep current system 344 - Switch to electronic voting</p>
<p>Is the Helios voting system, used for these demo elections, appropriate for the purpose of holding future IACR elections?</p> <p><i>[select 0 or 1 answer]</i></p>	<p>293 - Yes 39 - No</p>
<p>Distributing hard copies of the Journal of Cryptology is rather costly. How do you prefer to access the journal?</p> <p><i>[select 0 or 1 answer]</i></p>	<p>153 - Both hard copy and web access, as is done today 224 - Electronic form only</p>
<p>In what format would you like to obtain your copy of the proceedings when you attend an IACR conference or workshop?</p> <p><i>[select 0 or 1 answer]</i></p>	<p>128 - A printed book, as done today 120 - Only on a USB stick (cheaper than a book) 56 - Both a printed book and a USB stick (more expensive than just a book) 74 - I don't need a copy at the conference. Web access to the proceedings is sufficient</p>



Implementations/Uses

Various uses/deployment modes:

- ▶ Current President of Université catholique de Louvain
Amazon WS, CGS crypto
- ▶ Student elections at Princeton, IACR test election, various boards
Google App Engine, CGS crypto
- ▶ Student elections at UCL
Local servers, Mixnet-based crypto



UCL President Election

- ▶ 1st significant-outcome, multi-thousand-voter open-audit election (March 2009)

Elections à l'UCL: un vote électronique vérifiable, "inédit" à grande échelle



L'élection ces 2 et 3 mars du nouveau recteur de l'université catholique de Louvain (UCL), au suffrage universel pondéré, se fait via un système de vote électronique d'une nouvelle génération qui permet à l'électeur de vérifier que le résultat de l'élection est correct, a indiqué l'UCL au premier jour du scrutin.

Bruno Delvaux élu recteur de l'UCL

Mis en ligne le 23/03/2009



Bruno Delvaux est né en 1964, il est marié et père de trois enfants. Il pratique le cyclisme et est passionné d'œnologie et d'histoire.

Il entrera en fonction le 1er septembre 2009. La commission électorale annonce, ce lundi 23 mars, les résultats du 2e tour de l'élection du recteur de l'UCL. 3 758 électeurs ont voté sur un total de 5 143 électeurs inscrits sur les listes électorales. Les résultats enregistrés au 2e tour sont les suivants : Bruno Delvaux : 53,83 %, Vincent Blondel : 42,45 %, Votes blancs : 3,72 %

- ▶ Helios with:
 - ▶ CGS cryptography [CGS97]
 - ▶ Custom server software (on Amazon EC2 + UCL)
 - ▶ Custom tallying rules (weighting system, ...)
 - ▶ Conflict resolution procedure (mixing browser and paper)



From election days

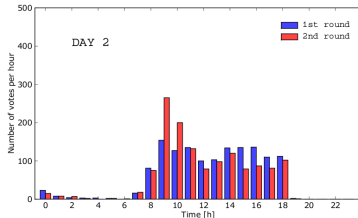
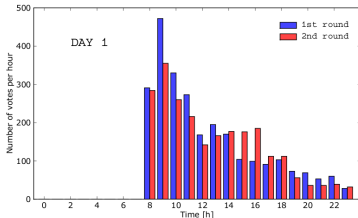
Participation

- ▶ 5142 registered voters

Very useful for credential negotiation

Very useful for 1st bound on number of voters

- ▶ 10644 votes tallied
 - ▶ ≈ 3000 votes for test election
 - ▶ ≈ 4000 votes for each of 2 rounds
- ▶ max. 17 votes/minute, emails trigger vote



From election days

Voter behavior

- ▶ 1% vote more than once

Quite controversial, no strong impact

- ▶ 3% use voting offices

*Mostly people unfamiliar with PC
Quite over-dimensioned on our side*

- ▶ 30% check their vote on WBB

*Quite high!
Decreases on 2nd round*

- ▶ 120 tickets raised by UCL support

1. Loss of Credentials
2. JVM missing, use of Win95, IE4.0, ...
3. Did I do everything correctly?

Importance of testing with non-CS people...



From election days

WBB Audit days

- ▶ 7 complaints issued during 2 rounds

Reasons (after investigation):

1. "I am just trying to vote after the deadline"
2. "I want to test the procedure"
3. "I switched my receipt with someone else in the printer"

Convenience of voting server with public data only

Tally

- ▶ 1st round leader was < 2 electoral votes from majority

no objection, clear majority on 2nd round



IACR election

- ▶ Test election: Winter 2010
- ▶ Adoption: CRYPTO 2010

- ▶ Helios with:
 - ▶ CGS cryptography
 - ▶ Google App Engine hosting



Monitoring Helios elections

Helios offers a bulletin board, but . . .

- ▶ What if the Helios server is getting hacked?
Audit will detect it, but are we stuck?
- ▶ Audit is technical. . .
Can I share my audit results?

Observation:

The Helios server only stores public data!



Monitoring Helios elections

Helios Election Monitor

<https://www.uclouvain.be/crypto/electionmonitor/>



Helios Election Monitor

This website monitors Helios elections: it uses the Helios API, which is also used to collect ballots at tallying time, and examines the votes that have been submitted:

- the election parameters (identifier, questions and proposed answers, ...) are extracted and recomputed,
- a new version of the bulletin board is built, with all hashes recomputed from original data,
- the bulletin board also displays the validity of the ballots (all proofs of well-formedness are valid),
- a timeline showing the evolution of vote submissions is built (all date and time displayed on this website are UTC).

You can also audit a ballot with our [ballot auditor](#).

Elections previously monitored

Election name	UUID
IACR Helios demo election	3a40d55c-1396-11df-bd14-19dba45a8649

[click on election name to view monitoring data]

Quick links: [UCL](#) | [EPL](#) | [ELEC](#) | [DICE](#) | [CRYPTO GROUP](#)

Webmaster: Olivier de Marnette



IACR Helios demo election

[[view our bulletin board](#) | [view voting statistics](#)]

monitoring of this election is finished

Votes information

- **1542** registered voters
- **379** voters cast a vote
- **396** votes were cast (including re-votes)

Election information

- **Election Description:** The goal of this demo election is to solicit feedback from IACR members about moving to electronic elections, and also to help us evaluate the suitability of Helios for IACR elections. In addition to this goal, we would like to take this opportunity to conduct a straw poll about several issues currently under discussion by the board. The results of this demo election are **NOT** binding. The election will close on March-15 2010 at 11:59pm UTC. See More information at <http://www.iacr.org/elections/eVoting/ballot-questions.html>
- **Election UUID:** 3a40d55c-1396-11df-bd14-19dba45a8649
- **Election public key** *verified*
- **Election frozen at:** 2010-02-09 00:06:02
- **Election Fingerprint:** z1oRqXUyfvmsMH5s5VEd0gaa/wiwX5GG3t+RhzkfwGc
- **Election url:** <https://iacr-helios.appspot.com/helios/elections/3a40d55c-1396-11df-bd14-19dba45a8649/view>
- **Questions:** *election outcome audited - 2010-03-17 09:32:35 UTC*



IACR Helios demo election - Bulletin Board

[[view election information](#) | [view voting statistics](#)]

monitoring of this election is finished

1542 registered voters

Search

Look For:

In Field:

Voter ID ▾

Submit

only the first 2000 voters are displayed - hashes are recomputed - time is UTC

Voter ID	Status	Vote Fingerprint	Validity	Last Vote Cast at
V24	REVOTED	Uza64HFuZrIuygHdwuEv6W3X9rK37XdUV8ycHpmPGmA	✓	Feb 22, 2010 7:00:23 PM
V240	VOTED	TFz9hZH2sY060+ks9tYn0sWZ/BEHKVxG66tio38L4x8	✓	Mar 12, 2010 2:54:10 PM
V241	NO VOTE			

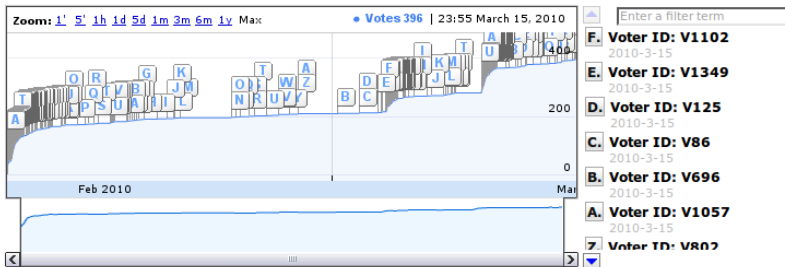


IACR Helios demo election - Voting Statistics

[[view election information](#) | [view our bulletin board](#)]

monitoring of this election is finished

379 voters cast 396 votes in this election



Audit of the tally

Should the IACR keep its current voting system, based on double envelopes sent via postal mail, or switch to electronic voting over the Internet?

[select 0 or 1 answer]

32 - *Keep current system*
344 - *Switch to electronic voting*

Is the Helios voting system, used for these demo elections, appropriate for the purpose of holding future IACR elections?

[select 0 or 1 answer]

293 - *Yes*
39 - *No*

Distributing hard copies of the Journal of Cryptology is rather costly. How do you prefer to access the journal?

[select 0 or 1 answer]

153 - *Both hard copy and web access, as is done today*
224 - *Electronic form only*

In what format would you like to obtain your copy of the proceedings when you attend an IACR conference or workshop?

[select 0 or 1 answer]

128 - *A printed book, as done today*
120 - *Only on a USB stick (cheaper than a book)*
56 - *Both a printed book and a USB stick (more expensive than just a book)*
74 - *I don't need a copy at the conference. Web access to the proceedings is sufficient*



UCL Student elections

AGL (the UCL student association), Sep. 2009:

“Could we also have verifiable elections on the Internet?”

- “Well, how do your elections work?”



UCL student elections

“Our ballots are a bit large, here is a typical list:



Élections étudiantes 2010



Etape 1 sur 3 : Sélection des candidats

Conseil de Faculté ESPO

- BEASSE Clément SPOL 12 [ADES]
- BORJA Andrés SPED 21 [ADES]
- CALLENS Fanny IAG 1 PM [CESEC]
- COLLINGE Marie-Lucie COMU 13 [Tous ensemble]
- DE DECKER Maité COMU 11 [CESEC]
- DEKEYZER Sébastien SPRI 21 [CESEC]
- DELHAYE Laurence ECGE 12 [CESEC]
- DEMBOUR Noémie SPRI 21 [ADES]
- DESPLANQUE Simon SPOL 11 [Tous ensemble]
- DESSY Gaspard INGE 13 [CESEC]
- DEWAELE Guillaume (Cubitus) ECGE 11 [CESEC]
- DINIER Julien SPOL 11 [ADES]

Vous pouvez voter pour autant de personnes que vous le désirez.
Les candidats sont présentés par ordre alphabétique.



UCL student elections

“and:

- DONNET Constantin ANTR 21 [CESEC]
- DUGAUTHIER Morgane COMU 13 [CESEC]
- EVRARD Johanne ECGE 13 [CESEC]
- FIXELLES Caroline (Josette) COMU 13 [CESEC]
- GAUTIER Stéphanie SPOL 13 [CESEC]
- GONZALES-MOHINO François (Number One) SPRI 21 [CESEC]
- HATERTE Alexandre (Penne) INGE 11 [CESEC]
- HENRY DE FRAHAN Philip INGE 11 [Tous ensemble]
- HOREMANS Mélissa COMU 12 [CESEC]
- IMPELLIZZERI Nicolas ECGE 13 [CESEC]
- JANUS Marie-Anaëlle ECGE 11 [CESEC]
- LÉ Olivier INGE 12 [ADES]
- LEMAIRE Joseph COMU 12 [ADES]
- LUTZ Fanny SPRI 21 [Tous ensemble]
- MAGNERY Marc (Marco) POLS 21 [ADES]
- MALAY Olivier SPOL 12 [Tous ensemble]
- MANSOR SAFAIAN Parham (Le Perse-Cesec) COMU 12 [CESEC]
- MARSILY Hugues ECGE 13 [CESEC]
- MENDEZ YEPEZ David Manuel ECON 21 [ADES]
- MERTENS François INGE 12 [CESEC]
- MOREAU Thomas SPRI 21 [CESEC]
- MOREAU Simon ECGE 11 [Tous ensemble]
- MOUTON Arnaud (Rouge) ECGE 11 [CESEC]
- NSANZIMANA Jérôme SPRI 21 [CESEC]



UCL student elections

“and:

- PELTIER Benjamin SPOL 21 [ADES]
- PERDAENS Alizée SPOL 13 [CESEC]
- PIERRE LOUIS Luné Roc COMU 3 D [ADES]
- POTIE Olivier ECGE 13 [CESEC]
- SCHAMPS Claire INGE 13 [ADES]
- STAS Bruno SPED 21 [ADES]
- THOMAS Vanessa ANTR 21 [Tous ensemble]
- ULUC Timur SPOL 11 [CESEC]
- VAN BINSBERGEN Laura SOCA 12 [ADES]
- VAN HIRTUM Erwin ECON 22 [Tous ensemble]
- VAN RUYCHEVELT Jérôme (Van Spring) SPRI 21 [ADES]
- VERHOEVEN Johan (Yan) SOCA 21 [ADES]
- VERMEIRE Jean-Gabriel SPRI 21 [ADES]
- WALLEMACQ Alexandre IAG 1 PH [Tous ensemble]

- Vote Blanc

Suivant

[Pages d'aide](#) | [Informations élections](#) | [Contact : e-elections@aglouvain.be](#) | [Taux de participation](#) | [Valves de l'élection électronique](#)

“and we typically have 3 such lists + a few smaller ones”



Helios ballot encoding

CGS ballot preparation: 6 modexp/*candidate*

- ▶ one ciphertext per candidate: 2 modexp/candidate
- ▶ one 0/1 ZKPOK/ciphertext: + 4 modexp/candidate
- ▶ one global proof: more modexp

≈ 250 candidates: minutes on an old browser



Move to something else...

Move to completely different cryptography:

- ▶ Mixnet-based tallying
- ▶ one ciphertext per *ballot*
- ▶ use augmented cryptosystems [Wik08] to ensure ballot independence: Cramer-Shoup encryption

$$\leq 5 \text{ modexp/ballot}$$

- ▶ 4488 votes tallied in March 2010
- ▶ Much more burden than homomorphic tallying:
 - ▶ checking ballot independence,
 - ▶ mixing,
 - ▶ decryption and counting + proof verifications
- ▶ Still much more comfortable than paper tallying...



Conclusions

- ▶ More and more experiences!
- ▶ Each election is a project on its own
- ▶ Open audit seems to come with a lot of side advantages:
 - ▶ Read all server data without any risk (complaints, ...)
 - ▶ Lower deployment costs (public replication, cloud computing, ...)
- ▶ Try Helios 3.0!

<http://heliosvoting.org>

