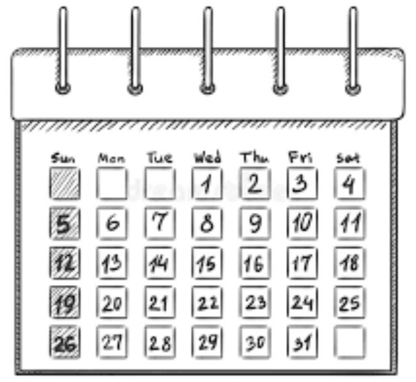
Reversing, Breaking, and Fixing the French Legislative Election E-Voting Protocol

Alexandre Debant *and Lucca Hirschi*

Université de Lorraine, CNRS, Inria, LORIA, Nancy, France

Cortier fest
January 31st 2023

Some numbers…



May 27th — June 1st first round of the election

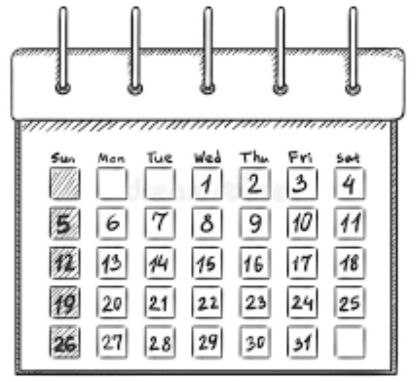
June 10th — June 15th second round of the election

> 1.5 millions number of eligible voters (French citizens abroad only)

11 number of deputies to elect, i.e. constituencies

~200 number of consulates

Some numbers…



May 27th — June 1st first round of the election

June 10th — June 15th second round of the election

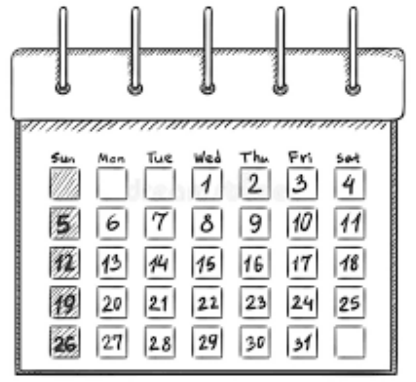
> 1.5 millions number of eligible voters (French citizens abroad only)

11 number of deputies to elect, i.e. constituencies

~200 number of consulates

⚠ **The results are published at the consulates level!**

Some numbers…



May 27th — June 1st first round of the election

June 10th — June 15th second round of the election

> 1.5 millions number of eligible voters (French citizens abroad only)

11 number of deputies to elect, i.e. constituencies

~200 number of consulates

⚠ **The results are published at the consulates level!**

~524 000 number of expressed votes (~251k first round and ~273k second round)

76,9% percentage of online voting (22,7% in person, 0,3% postal voting)

4 stakeholders

MINISTÈRE
DE L'EUROPE
ET DES AFFAIRES
ÉTRANGÈRES

1. **Organizer:** the French Ministry of Europe and Foreign Affairs *(the ministry)*

4 stakeholders

1. Organizer: the French Ministry of Europe and Foreign Affairs *(the ministry)*

2. Institutional security advisor: the French National Cybersecurity Agency *(ANSSI)*

4 stakeholders

1. Organizer: the French Ministry of Europe and Foreign Affairs *(the ministry)*

2. Institutional security advisor: the French National Cybersecurity Agency *(ANSSI)*

3. Vendor/service provider: Voxaly Docaposte *(Voxaly or the vendor)*

4 stakeholders

MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES

1. Organizer: the French Ministry of Europe and Foreign Affairs *(the ministry)*

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION · ANSSI

2. Institutional security advisor: the French National Cybersecurity Agency *(ANSSI)*

VOXALY UNE MARQUE DE DOCAPOSTE

3. Vendor/service provider: Voxaly Docaposte *(Voxaly or the vendor)*

Loria Laboratoire lorrain de recherche en informatique et ses applications

4. External third party: V. Cortier, P. Gaudry and S. Glondu *(the Loria)*

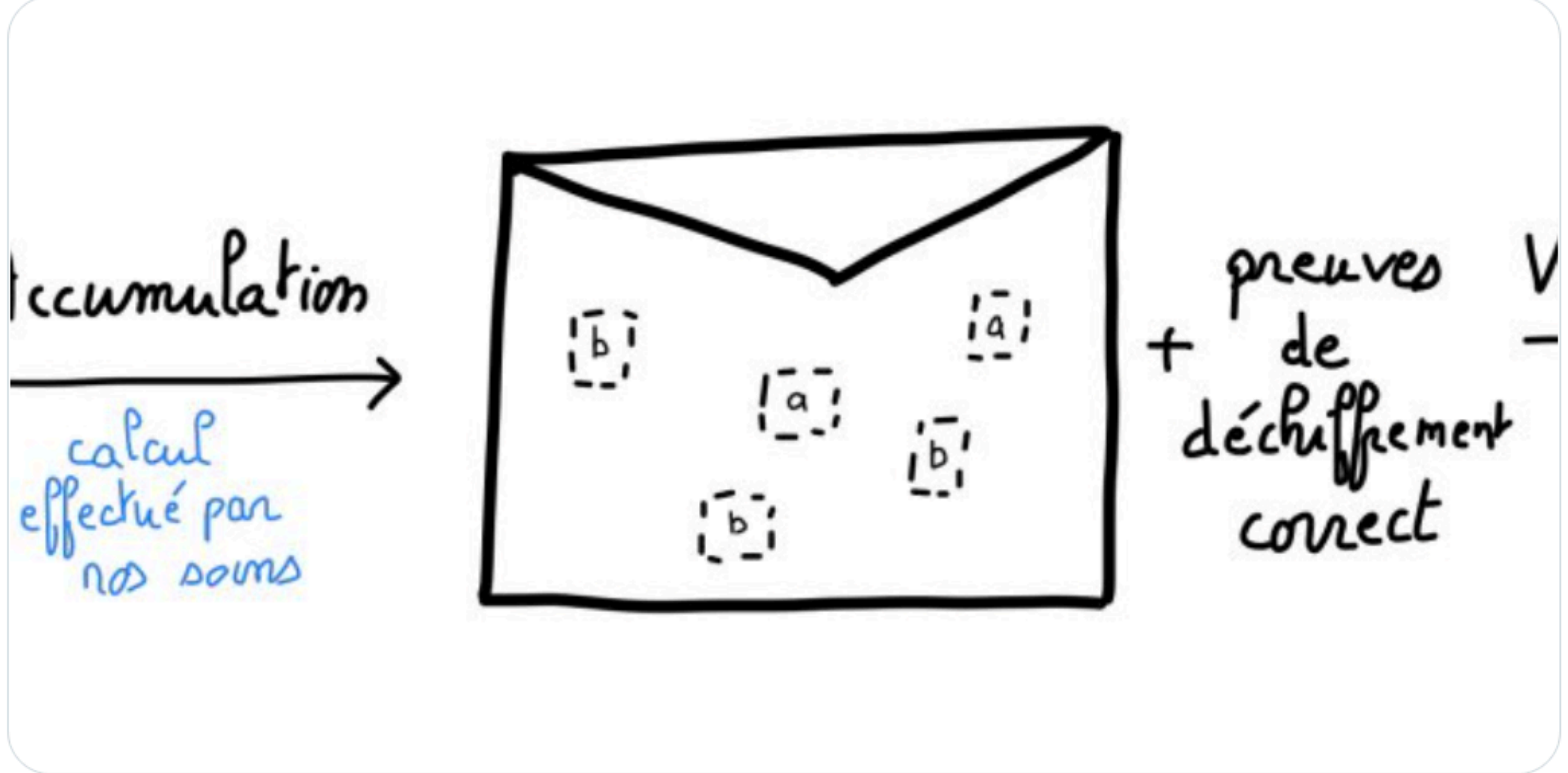
May 17th 2022….

Tweet

Inria Nancy - Grand Est
@Inria_Nancy

🗳 #Législatives2022 Être français, habiter à l'étranger & pouvoir vérifier son vote, ce sera possible ! Mandatés comme tiers de confiance par @francediplo & le @CNRS, des scientifiques @labo_Loria @Inria mettront en ligne un site sécurisé. 🔒
➕ d'infos : verifiabilite-legislatives2022.fr/informations.h...

Translate Tweet



Caramba, Nancy and 2 others

5:17 AM · May 17, 2022 · Twitter Web App

2 Retweets **1** Quote Tweet **14** Likes

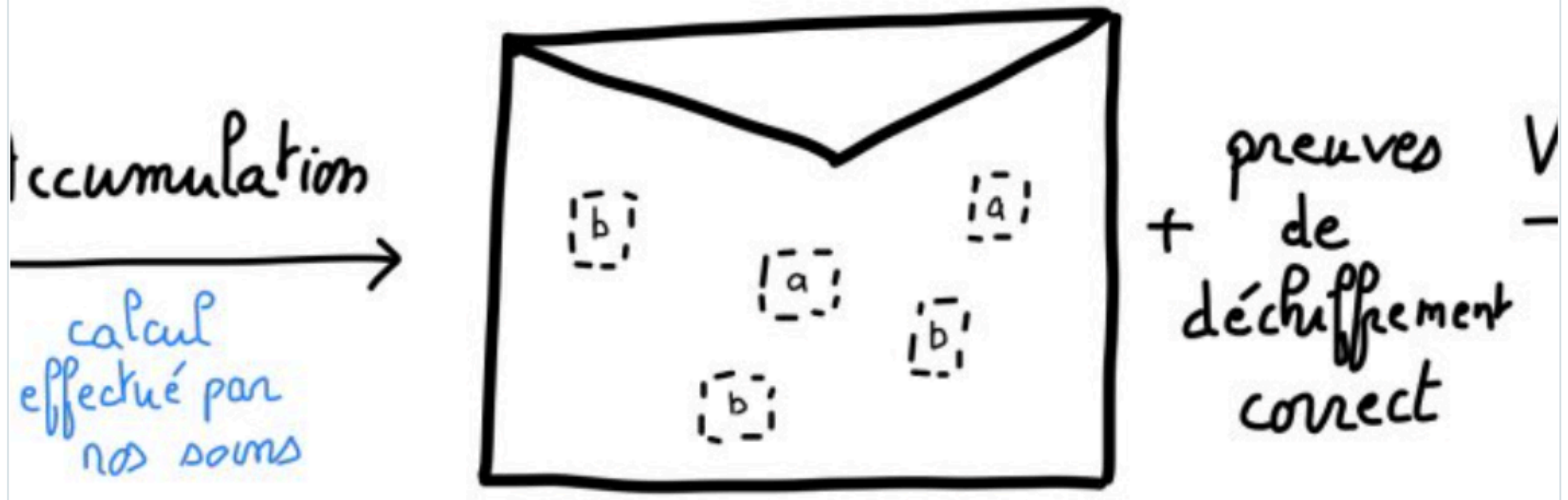
May 17th 2022….

← Tweet

Inria Nancy - Grand Est
@Inria_Nancy

🗳 #Législatives2022 Être français, habiter à l'étranger & pouvoir vérifier son vote, ce sera possible Mandatés comme tiers de confiance par @francedipl & le @CNRS, des scientifiques @labo_Loria @Inri mettront en ligne un site sécurisé. 🔒
➕ d'infos : verifiabilite-legislatives2022.fr/informations.h...

Translate Tweet



Caramba, Nancy and 2 others

5:17 AM · May 17, 2022 · Twitter Web App

2 Retweets **1** Quote Tweet **14** Likes

"Be French, live abroad, and be able to verify your vote, it will be possible. […] Acting as trusted third parties, researchers will launch a secure website."

May 17th 2022....

"Be French, live abroad, and be able to verify your vote, it will be possible. [...] Acting as trusted third parties, researchers will launch a secure website."

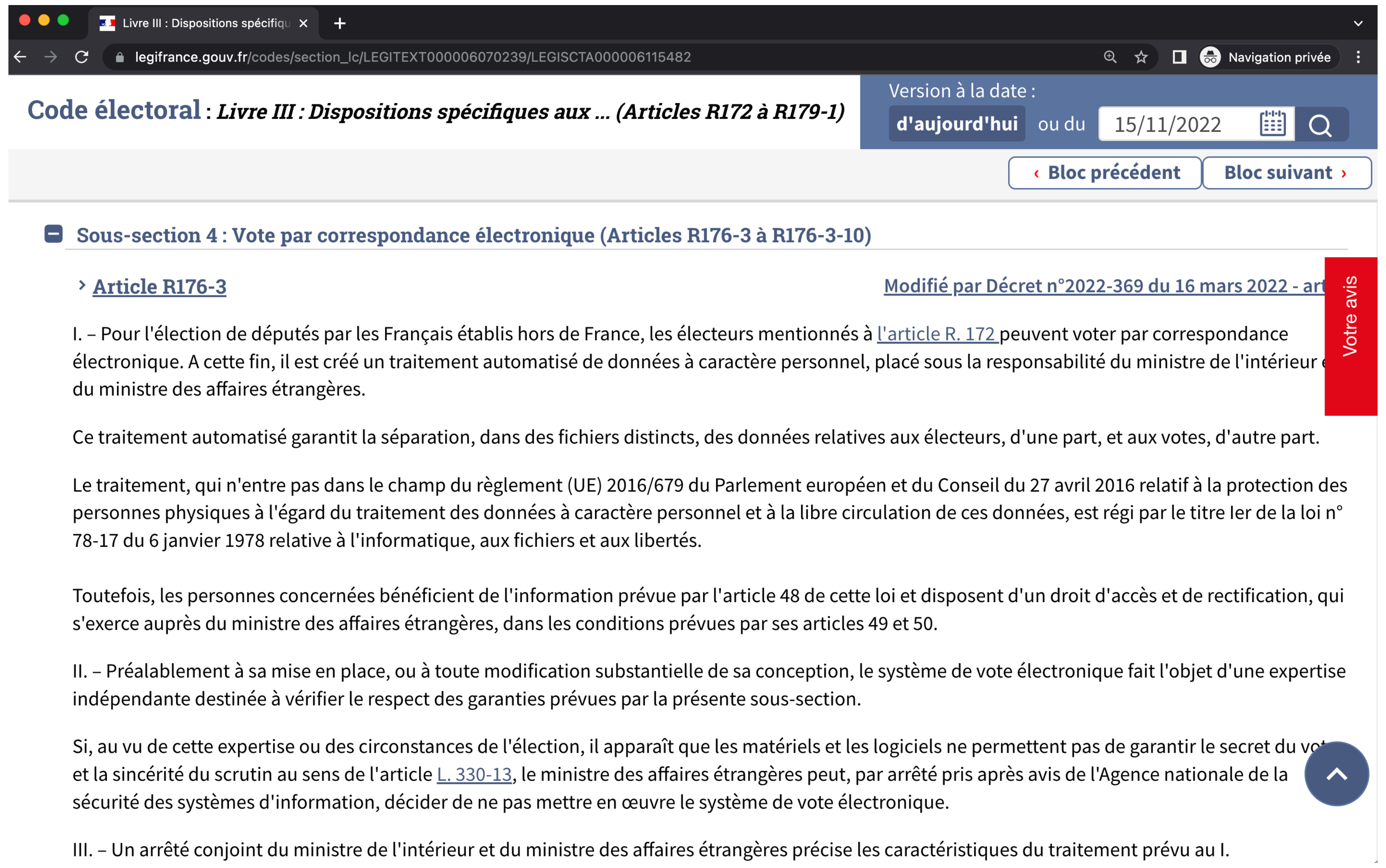
Outline

1. **Reverse the threat model and the protocol**

2. **Vulnerabilities, attacks, and fixes**
   - how to defeat verifiability?
   - how to defeat vote privacy?

3. **Other concerns and take away**

How to define the security targets?


Livre III : Dispositions spécifiq...

legifrance.gouv.fr/codes/section_lc/LEGITEXT000006070239/LEGISCTA000006115482

Navigation privée

Code électoral : *Livre III : Dispositions spécifiques aux ... (Articles R172 à R179-1)*

Version à la date : d'aujourd'hui ou du 15/11/2022

‹ Bloc précédent | Bloc suivant ›

Sous-section 4 : Vote par correspondance électronique (Articles R176-3 à R176-3-10)

› Article R176-3 — Modifié par Décret n°2022-369 du 16 mars 2022 - art

I. – Pour l'élection de députés par les Français établis hors de France, les électeurs mentionnés à l'article R. 172 peuvent voter par correspondance électronique. A cette fin, il est créé un traitement automatisé de données à caractère personnel, placé sous la responsabilité du ministre de l'intérieur et du ministre des affaires étrangères.

Ce traitement automatisé garantit la séparation, dans des fichiers distincts, des données relatives aux électeurs, d'une part, et aux votes, d'autre part.

Le traitement, qui n'entre pas dans le champ du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, est régi par le titre Ier de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Toutefois, les personnes concernées bénéficient de l'information prévue par l'article 48 de cette loi et disposent d'un droit d'accès et de rectification, qui s'exerce auprès du ministre des affaires étrangères, dans les conditions prévues par ses articles 49 et 50.

II. – Préalablement à sa mise en place, ou à toute modification substantielle de sa conception, le système de vote électronique fait l'objet d'une expertise indépendante destinée à vérifier le respect des garanties prévues par la présente sous-section.

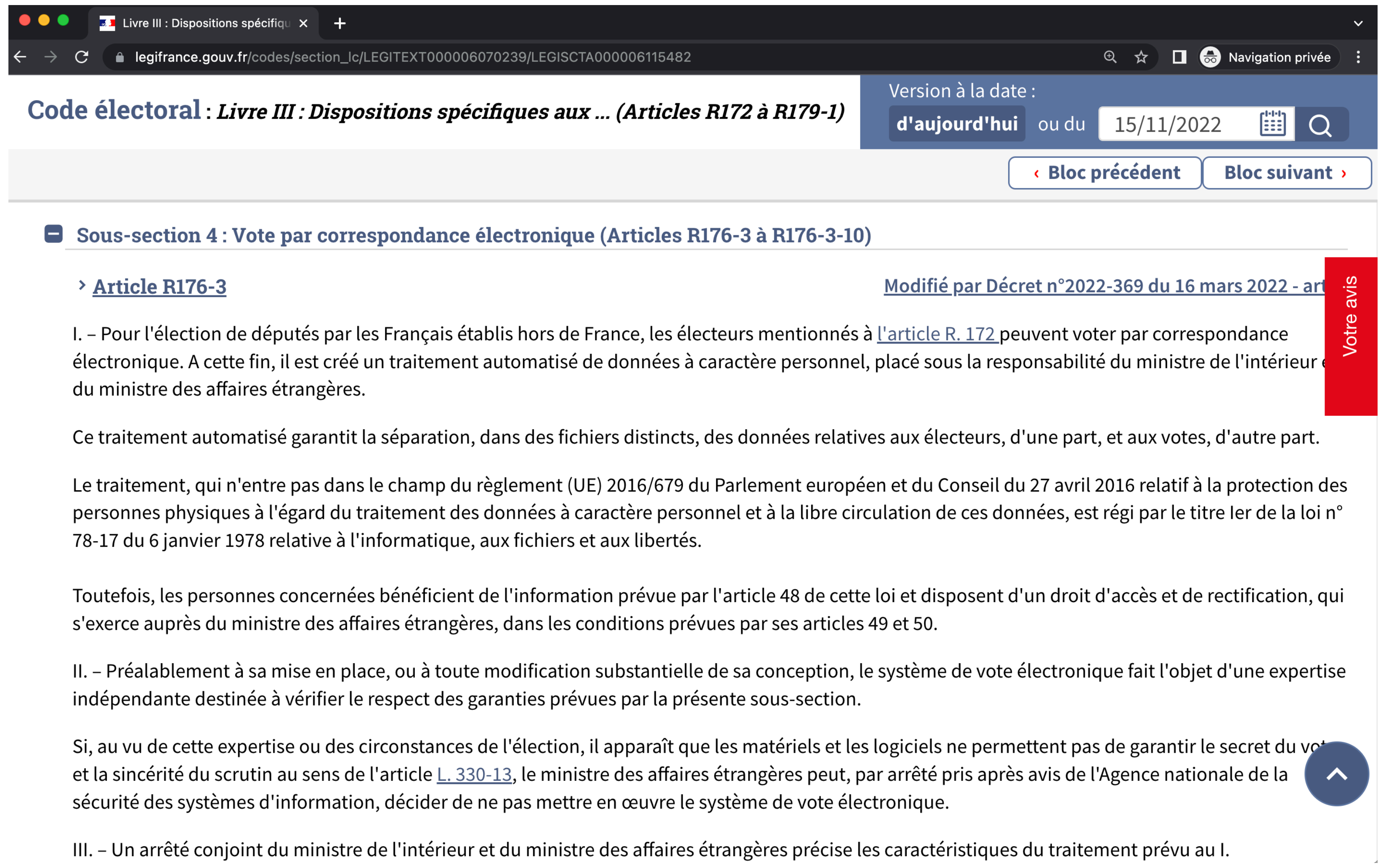
Si, au vu de cette expertise ou des circonstances de l'élection, il apparaît que les matériels et les logiciels ne permettent pas de garantir le secret du vo[te] et la sincérité du scrutin au sens de l'article L. 330-13, le ministre des affaires étrangères peut, par arrêté pris après avis de l'Agence nationale de la sécurité des systèmes d'information, décider de ne pas mettre en œuvre le système de vote électronique.

III. – Un arrêté conjoint du ministre de l'intérieur et du ministre des affaires étrangères précise les caractéristiques du traitement prévu au I.

1. The Code électoral

(the French law)

How to define the security targets?



Livre III : Dispositions spécifiq…

legifrance.gouv.fr/codes/section_lc/LEGITEXT000006070239/LEGISCTA000006115482

Code électoral : *Livre III : Dispositions spécifiques aux … (Articles R172 à R179-1)*

Version à la date : d'aujourd'hui ou du 15/11/2022

‹ Bloc précédent | Bloc suivant ›

Sous-section 4 : Vote par correspondance électronique (Articles R176-3 à R176-3-10)

› Article R176-3 — Modifié par Décret n°2022-369 du 16 mars 2022 - art

I. – Pour l'élection de députés par les Français établis hors de France, les électeurs mentionnés à l'article R. 172 peuvent voter par correspondance électronique. A cette fin, il est créé un traitement automatisé de données à caractère personnel, placé sous la responsabilité du ministre de l'intérieur et du ministre des affaires étrangères.

Ce traitement automatisé garantit la séparation, dans des fichiers distincts, des données relatives aux électeurs, d'une part, et aux votes, d'autre part.

Le traitement, qui n'entre pas dans le champ du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, est régi par le titre Ier de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Toutefois, les personnes concernées bénéficient de l'information prévue par l'article 48 de cette loi et disposent d'un droit d'accès et de rectification, qui s'exerce auprès du ministre des affaires étrangères, dans les conditions prévues par ses articles 49 et 50.

II. – Préalablement à sa mise en place, ou à toute modification substantielle de sa conception, le système de vote électronique fait l'objet d'une expertise indépendante destinée à vérifier le respect des garanties prévues par la présente sous-section.

Si, au vu de cette expertise ou des circonstances de l'élection, il apparaît que les matériels et les logiciels ne permettent pas de garantir le secret du vo[te] et la sincérité du scrutin au sens de l'article L. 330-13, le ministre des affaires étrangères peut, par arrêté pris après avis de l'Agence nationale de la sécurité des systèmes d'information, décider de ne pas mettre en œuvre le système de vote électronique.

III. – Un arrêté conjoint du ministre de l'intérieur et du ministre des affaires étrangères précise les caractéristiques du traitement prévu au I.

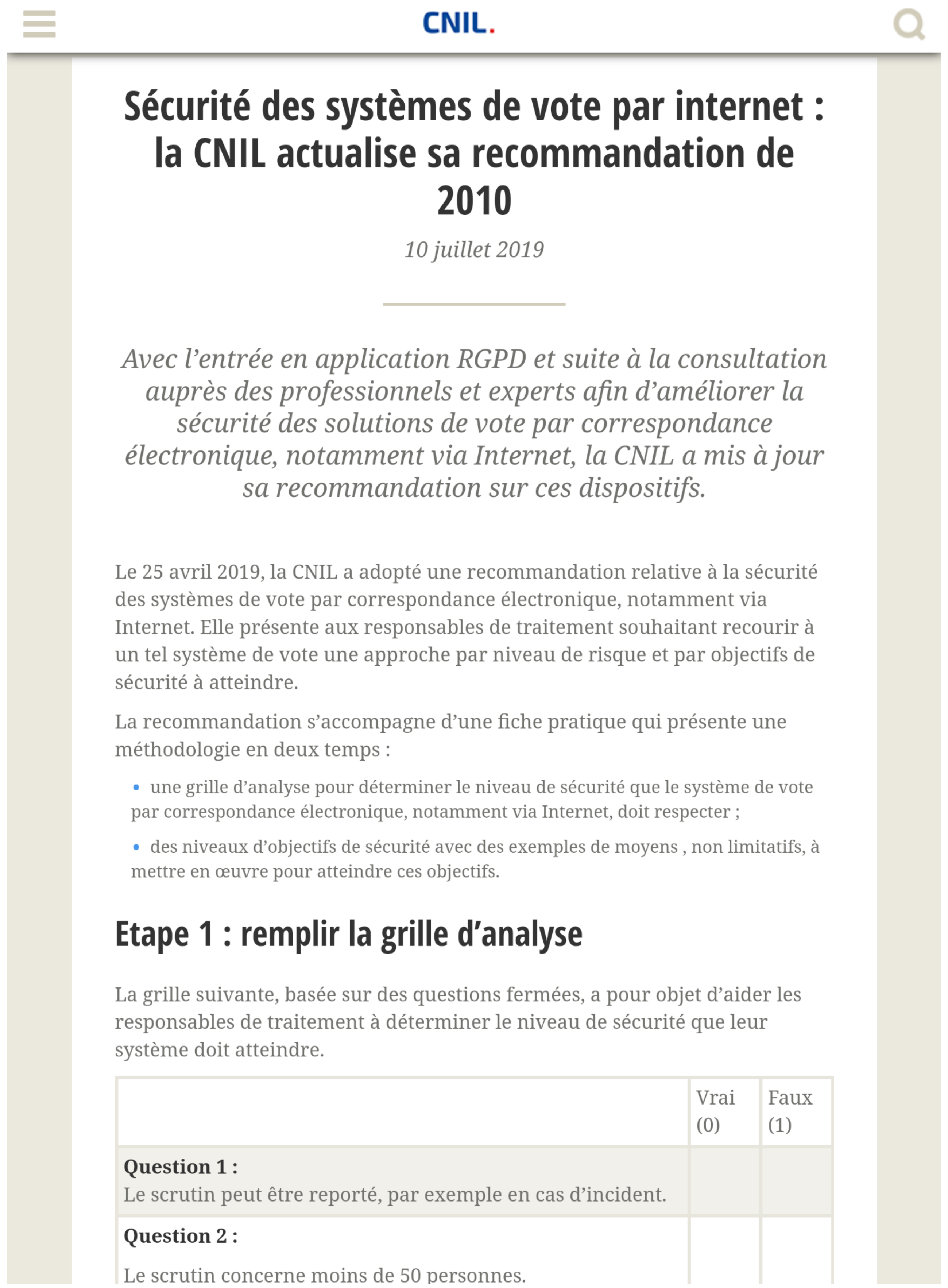
1. The Code électoral

(the French law)

2. The CNIL recommendations

(National Commission on Informatics and Liberty in English)

➡ level 3 is expected



CNIL.

Sécurité des systèmes de vote par internet : la CNIL actualise sa recommandation de 2010

10 juillet 2019

Avec l'entrée en application RGPD et suite à la consultation auprès des professionnels et experts afin d'améliorer la sécurité des solutions de vote par correspondance électronique, notamment via Internet, la CNIL a mis à jour sa recommandation sur ces dispositifs.

Le 25 avril 2019, la CNIL a adopté une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet. Elle présente aux responsables de traitement souhaitant recourir à un tel système de vote une approche par niveau de risque et par objectifs de sécurité à atteindre.

La recommandation s'accompagne d'une fiche pratique qui présente une méthodologie en deux temps :

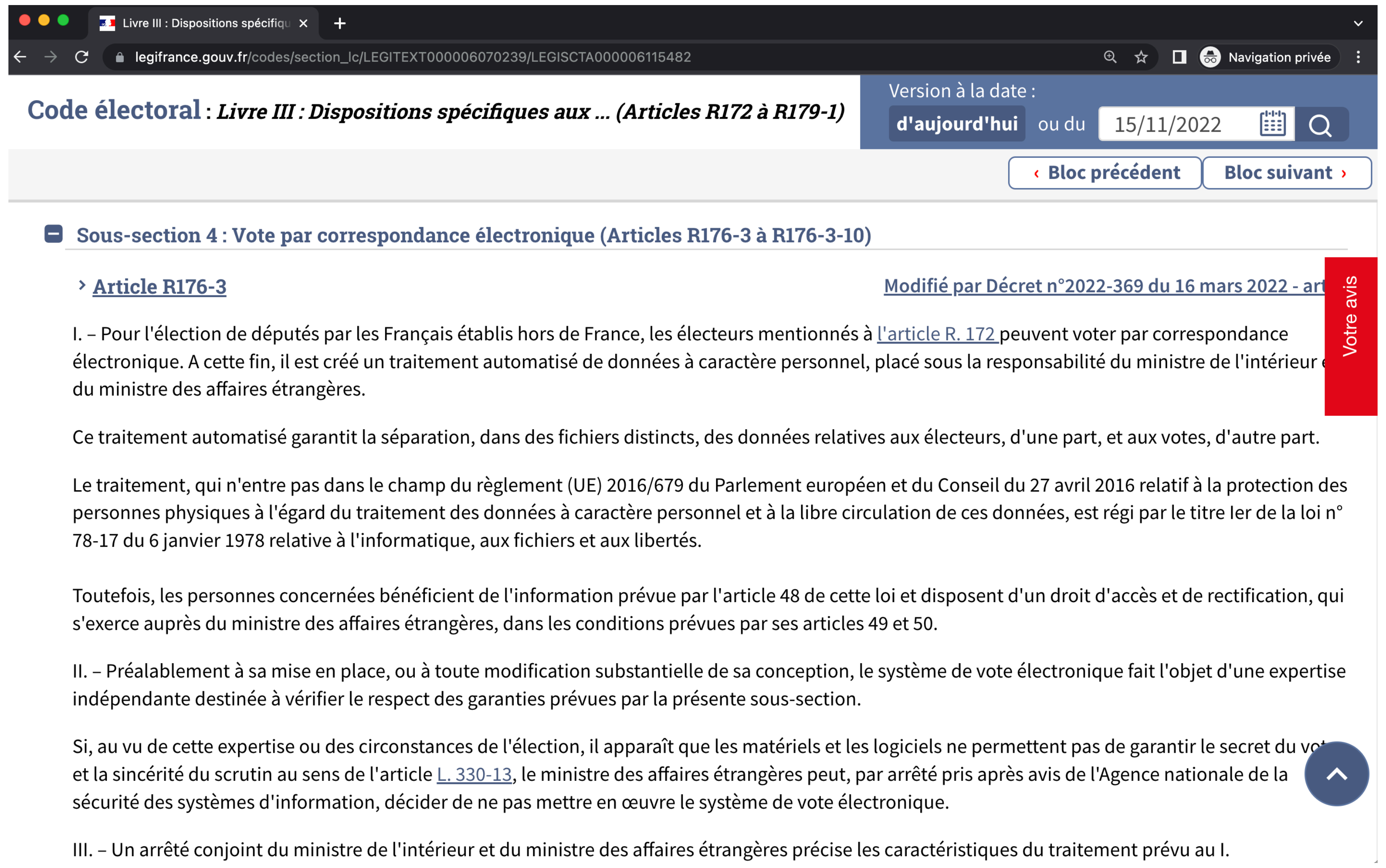
- une grille d'analyse pour déterminer le niveau de sécurité que le système de vote par correspondance électronique, notamment via Internet, doit respecter ;
- des niveaux d'objectifs de sécurité avec des exemples de moyens , non limitatifs, à mettre en œuvre pour atteindre ces objectifs.

Etape 1 : remplir la grille d'analyse

La grille suivante, basée sur des questions fermées, a pour objet d'aider les responsables de traitement à déterminer le niveau de sécurité que leur système doit atteindre.

	Vrai (0)	Faux (1)
Question 1 : Le scrutin peut être reporté, par exemple en cas d'incident.		
Question 2 : Le scrutin concerne moins de 50 personnes.		

How to define the security targets?



Livre III : Dispositions spécifiq... | legifrance.gouv.fr/codes/section_lc/LEGITEXT000006070239/LEGISCTA000006115482 | Navigation privée

Code électoral : *Livre III : Dispositions spécifiques aux ... (Articles R172 à R179-1)*

Version à la date : d'aujourd'hui ou du 15/11/2022

‹ Bloc précédent | Bloc suivant ›

Sous-section 4 : Vote par correspondance électronique (Articles R176-3 à R176-3-10)

› Article R176-3 — Modifié par Décret n°2022-369 du 16 mars 2022 - art

I. – Pour l'élection de députés par les Français établis hors de France, les électeurs mentionnés à l'article R. 172 peuvent voter par correspondance électronique. A cette fin, il est créé un traitement automatisé de données à caractère personnel, placé sous la responsabilité du ministre de l'intérieur et du ministre des affaires étrangères.

Ce traitement automatisé garantit la séparation, dans des fichiers distincts, des données relatives aux électeurs, d'une part, et aux votes, d'autre part.

Le traitement, qui n'entre pas dans le champ du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, est régi par le titre Ier de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Toutefois, les personnes concernées bénéficient de l'information prévue par l'article 48 de cette loi et disposent d'un droit d'accès et de rectification, qui s'exerce auprès du ministre des affaires étrangères, dans les conditions prévues par ses articles 49 et 50.

II. – Préalablement à sa mise en place, ou à toute modification substantielle de sa conception, le système de vote électronique fait l'objet d'une expertise indépendante destinée à vérifier le respect des garanties prévues par la présente sous-section.

Si, au vu de cette expertise ou des circonstances de l'élection, il apparaît que les matériels et les logiciels ne permettent pas de garantir le secret du vote et la sincérité du scrutin au sens de l'article L. 330-13, le ministre des affaires étrangères peut, par arrêté pris après avis de l'Agence nationale de la sécurité des systèmes d'information, décider de ne pas mettre en œuvre le système de vote électronique.

III. – Un arrêté conjoint du ministre de l'intérieur et du ministre des affaires étrangères précise les caractéristiques du traitement prévu au I.

Votre avis

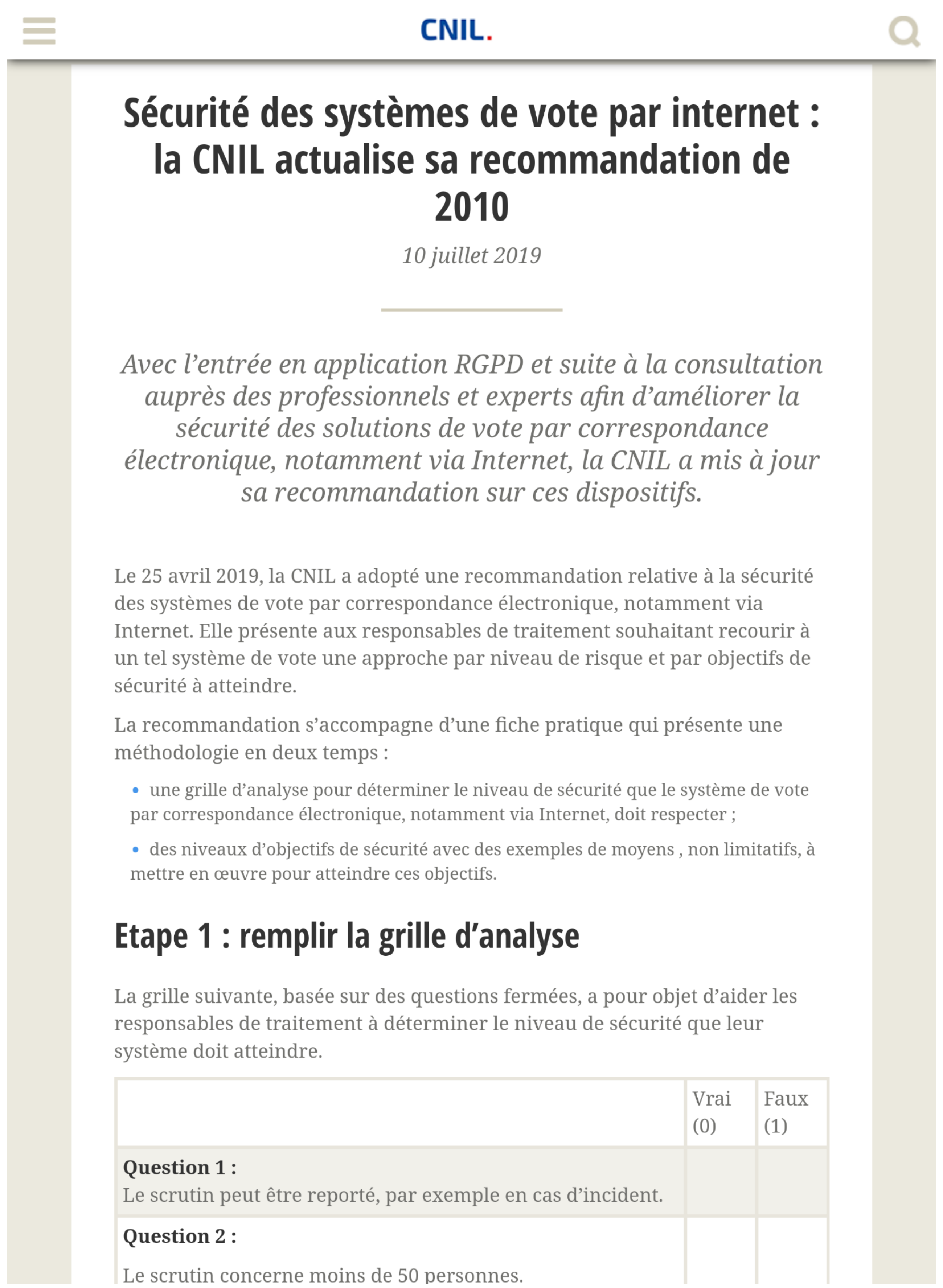
1. The Code électoral

(the French law)

2. The CNIL recommendations

(National Commission on Informatics and Liberty in English)

➡ level 3 is expected



CNIL.

Sécurité des systèmes de vote par internet : la CNIL actualise sa recommandation de 2010

10 juillet 2019

Avec l'entrée en application RGPD et suite à la consultation auprès des professionnels et experts afin d'améliorer la sécurité des solutions de vote par correspondance électronique, notamment via Internet, la CNIL a mis à jour sa recommandation sur ces dispositifs.

Le 25 avril 2019, la CNIL a adopté une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet. Elle présente aux responsables de traitement souhaitant recourir à un tel système de vote une approche par niveau de risque et par objectifs de sécurité à atteindre.

La recommandation s'accompagne d'une fiche pratique qui présente une méthodologie en deux temps :

- une grille d'analyse pour déterminer le niveau de sécurité que le système de vote par correspondance électronique, notamment via Internet, doit respecter ;
- des niveaux d'objectifs de sécurité avec des exemples de moyens , non limitatifs, à mettre en œuvre pour atteindre ces objectifs.

Etape 1 : remplir la grille d'analyse

La grille suivante, basée sur des questions fermées, a pour objet d'aider les responsables de traitement à déterminer le niveau de sécurité que leur système doit atteindre.

	Vrai (0)	Faux (1)
Question 1 : Le scrutin peut être reporté, par exemple en cas d'incident.		
Question 2 : Le scrutin concerne moins de 50 personnes.		

The CNIL recommendations are not legal requirements… but the protocol must meet them in practice any way!

Security properties

Vote secrecy

> “Votes must remain confidential”
>
> —Code électoral, Article R176-3-9

> "[the system must] ensure the strict confidentiality of the ballots as soon as created."
>
> —CNIL, Security objective n°1-04

> "[The system must] ensure that the identity of the voter and the expression of his choice can not be linked during the whole process"
>
> —CNIL, Security objective n°1-07

Verifiability

> "When a voter’s vote is registered, the voter is provided with a digital receipt allowing them to verify online that their vote has been taken into account."
>
> —Code électoral, Article R176-3-9

> "ensure the transparency of the ballot-box for all the voters [...] It must be possible for the voters to ensure that their ballot has been counted in the ballot-box."
>
> —CNIL, Security objective n°2-07

Security properties

Vote secrecy

"Votes must remain con[...]"

—Code élector[...]

"[the system must] ensure the strict [...]lots as soon as created."

[...] Security objective n°1-04

"[The sys[...]he expressio[...]rocess"

—CNIL, Security objective n°1-07

An attacker cannot learn the choice of a target voter

Verifiability

"When a voter's vote is registered, the voter is provided with a digital receipt allowing them to verify online that their vote has been taken into account."

—Code électoral, Article R176-3-9

"ensure the transparency of the ballot-box for all the voters [...] It must be possible for the voters to ensure that their ballot has been counted in the ballot-box."

—CNIL, Security objective n°2-07

Security properties

Vote secrecy

“Votes must remain con

—Code élector

"[the system must] ensure the strict
lots as soon as created."

Security objective n°1-04

An attacker cannot learn the choice of a target voter

"[The sys
expressio
he
rocess"

—CNIL, Security objective n°1-07

Verifiability

"When a voter’s v
verify online that

A voter must have the guarantee that their ballot appears in the ballot-box

"ensure the transparency of the ballot-box for all the voters [...] It must be possible for the voters to ensure that their ballot has been counted in the ballot-box."

—CNIL, Security objective n°2-07

Security properties

Vote secrecy

"Votes must remain con

—Code élector

"[the system must] ensure the strict

lots as soon as created."

Security objective n°1-04

"[The sys

expressio

he

rocess"

—CNIL, Security objective n°1-07

An attacker cannot learn the choice of a target voter

Verifiability

"When a voter's v

verify online that

A voter must have the guarantee that their ballot appears in the ballot-box

"ensure the transp

to ensure that their

The result must corresponds to the content of the ballot-box ✔

—CNIL, Security objective n°2-07

Ballots must be sent by legitimate voters only ?

Loria
Laboratoire lorrain de recherche en informatique et ses applications

Threat model

> "Security level 3: The threat actors include the voters, the election operators, outsiders, insiders within the provider or internal staff. They can be resourceful or highly motivated. "
>
> —CNIL, Security level 3

Threat model

> "Security level 3: The threat actors include the voters, the election operators, outsiders, insiders within the provider or internal staff. They can be resourceful or highly motivated. "
>
> —CNIL, Security level 3

Objective #3-02: The system must allow transparency of the ballot-box for all voters from **third-party tools**.

Threat model

> "Security level 3: The threat actors include the voters, the election operators, outsiders, insiders within the provider or internal staff. They can be resourceful or highly motivated. "
>
> —CNIL, Security level 3

Objective #3-02: The system must allow transparency of the ballot-box for all voters from **third-party tools**.

	Voter	Voting device	Com. channels	Voting server	Dec. auth.	3^{rd}-party
Verifiability	🙂	🙂	👹	👹	👹	🙂
Confidentiality	🙂	🙂	👹	👹	🙂	🙂

🙂 = trustworthy

👹 = compromised

Threat model

> "Security level 3: The threat actors include the voters, the election operators, outsiders, insiders within the provider or internal staff. They can be resourceful or highly motivated. "
>
> —CNIL, Security level 3

Objective #3-02: The system must allow transparency of the ballot-box for all voters from **third-party tools**.

Cast-as-intended is acknowledge as not satisfied

	Voter	Voting device	Com. channels	Voting server	Dec. auth.	3[rd]-party
Verifiability	trustworthy	trustworthy	compromised	compromised	compromised	trustworthy
Confidentiality	trustworthy	trustworthy	compromised	compromised	trustworthy	trustworthy

(smiley) = trustworthy

(devil) = compromised

Threat model

> "Security level 3: The threat actors include the voters, the election operators, outsiders, insiders within the provider or internal staff. They can be resourceful or highly motivated. "
>
> —CNIL, Security level 3

Objective #3-02: The system must allow transparency of the ballot-box for all voters from **third-party tools**.

Cast-as-intended is acknowledge as not satisfied

	Voter	Voting device	Com. channels	Voting server	Dec. auth.	3^{rd}-party
Verifiability	trustworthy	trustworthy	compromised	compromised	compromised	trustworthy
Confidentiality	trustworthy	trustworthy	compromised	compromised	trustworthy	trustworthy

= trustworthy

= compromised

TLS is broken
(e.g. middle-box TLS, corrupted network administrator, …)

Threat model

> "Security level 3: The threat actors include the voters, the election operators, outsiders, insiders within the provider or internal staff. They can be resourceful or highly motivated. "
>
> —CNIL, Security level 3

Objective #3-02: The system must allow transparency of the ballot-box for all voters from **third-party tools**.

Cast-as-intended is acknowledge as not satisfied

	Voter	Voting device	Com. channels	Voting server	Dec. auth.	3rd-party
Verifiability	trustworthy	trustworthy	compromised	~~compromised~~ trustworthy*	~~compromised~~ trustworthy	trustworthy
Confidentiality	trustworthy	trustworthy	compromised	~~compromised~~ trustworthy*	trustworthy	trustworthy

TLS is broken
(e.g. middle-box TLS, corrupted network administrator, …)

= trustworthy

= compromised

* = trustworthy (However, compromise decreases attacks complexity.)

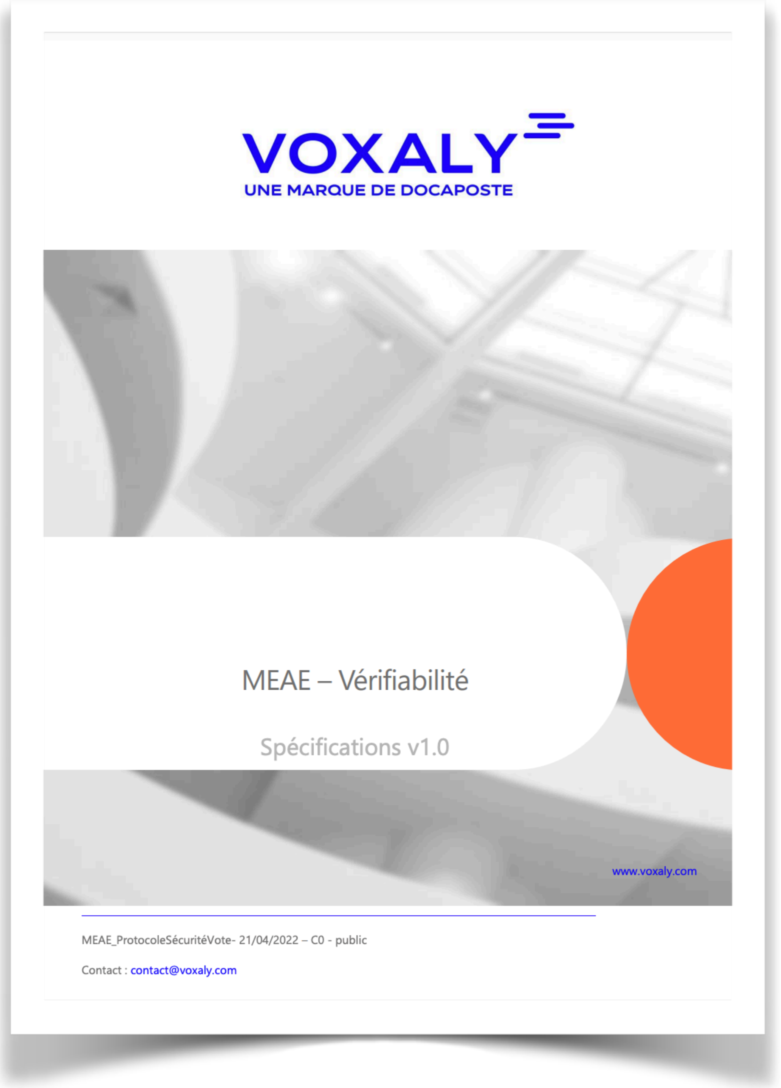
How to obtain a comprehensive description of the protocol?

A specification of the system

- published by Voxaly Docapost on April 21st 2022
- allowing one to develop a third party verifier

⚠ **This specification is incomplete… it does not describe the protocol itself!**

How to obtain a comprehensive description of the protocol?



A specification of the system

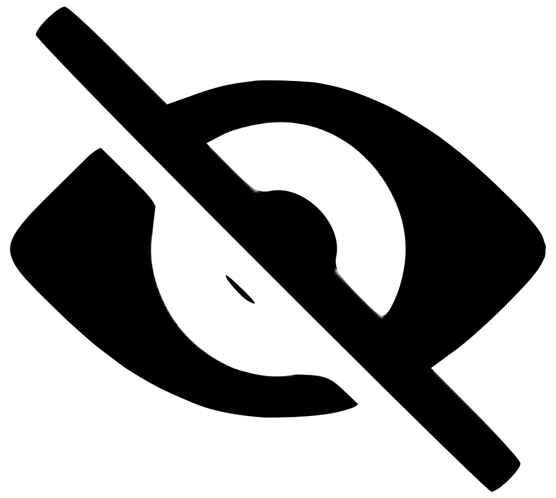
- published by Voxaly Docapost on April 21st 2022
- allowing one to develop a third party verifier

⚠ **This specification is incomplete… it does not describe the protocol itself!**

Some reverse engineering

- based on the voter’s journey (official tutorial and observation in-situ)
- based on HTML/JS/CSS data collected by different voters
- cross checking those data with data collected during a previous large-scale test

Security by obfuscation?



Standard obfuscation techniques:

- function and variable renaming
- control flow alteration (infinite for loop and breaks, switch case, nested functions, etc)

Security by obfuscation?

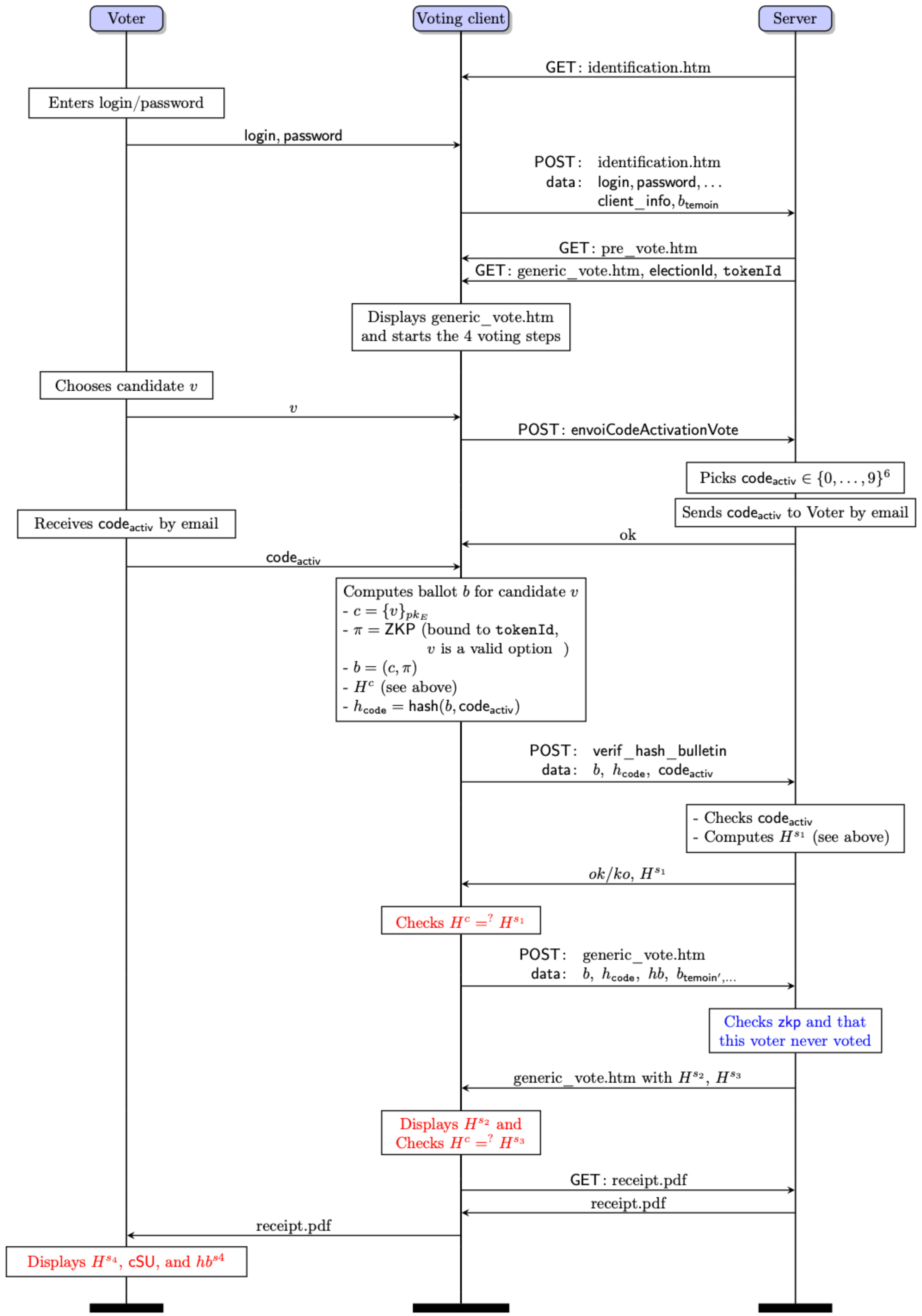
Standard obfuscation techniques:

- function and variable renaming
- control flow alteration (infinite for loop and breaks, switch case, nested functions, etc)

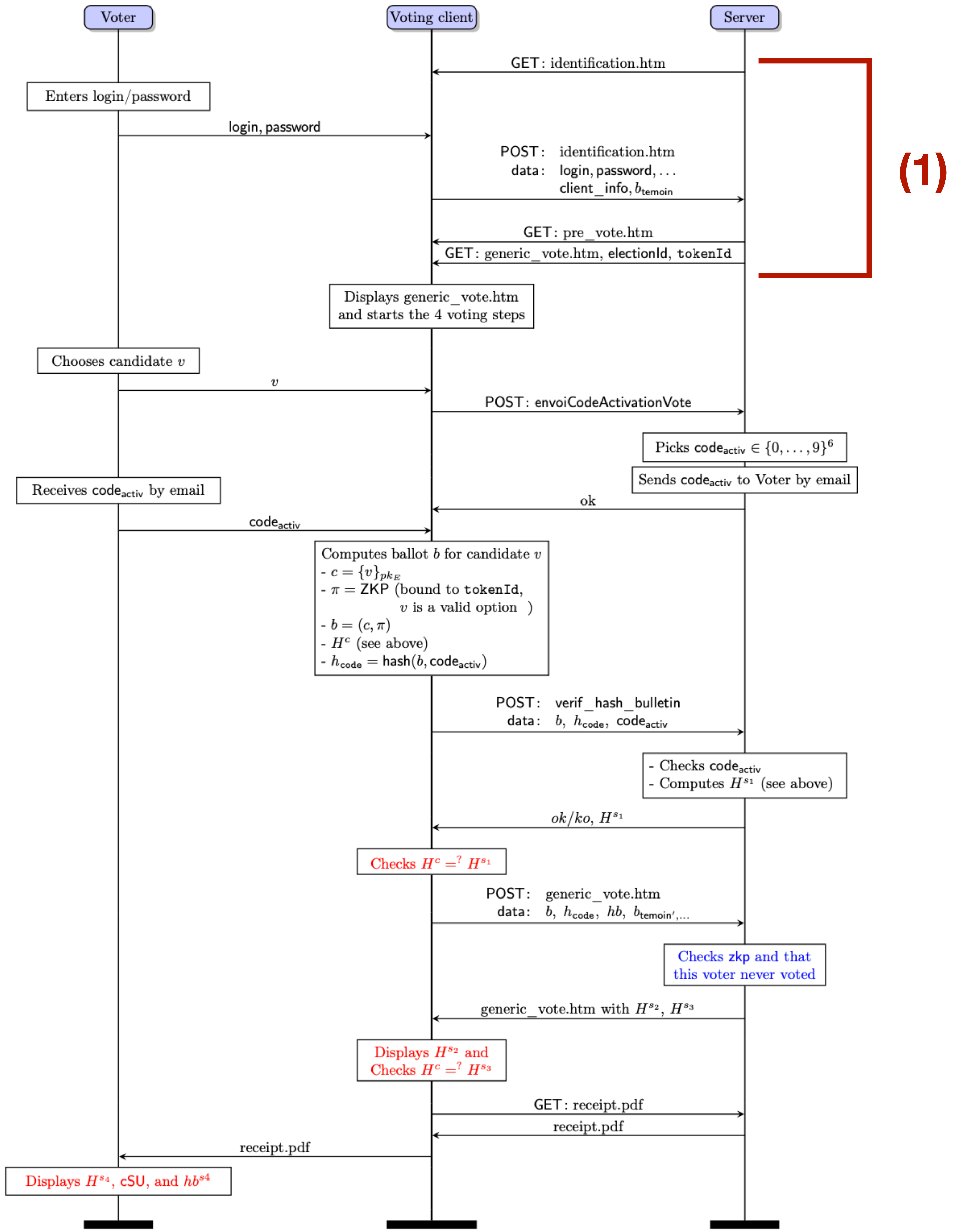
Few funny elements…

- it's mix of French and English: `bulletin`, `codeActivation`, `erreurHashVerification`, …
  `correctLength`, `chosenCandidates`, `updateVoteStatus`, …
- obfuscation "by-design", e.g, `o.voteSignature` is not a signature 🙈

A comprehensive description of the protocol

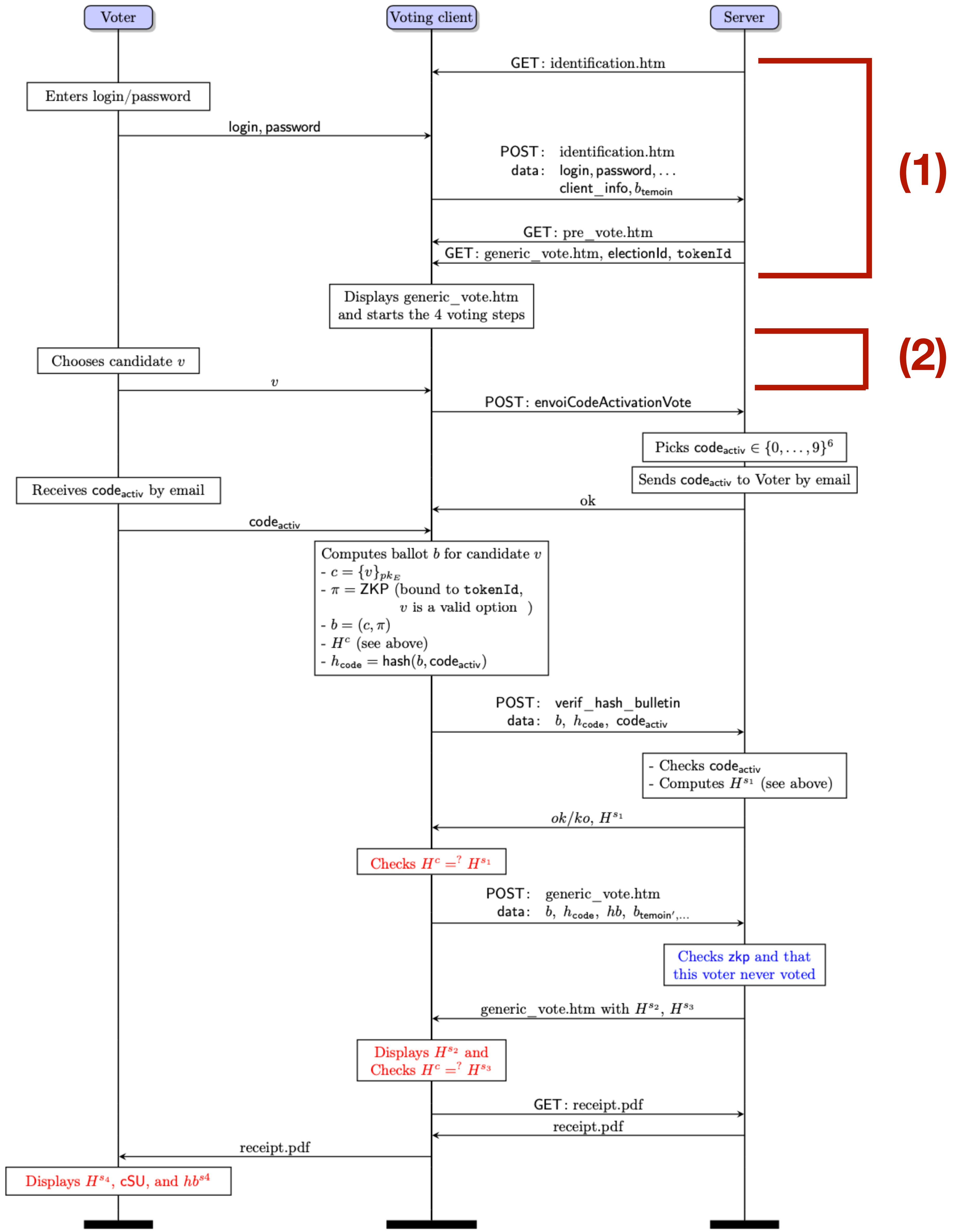


A comprehensive description of the protocol



1. **Authentication:** the voter sends their login/password to the server

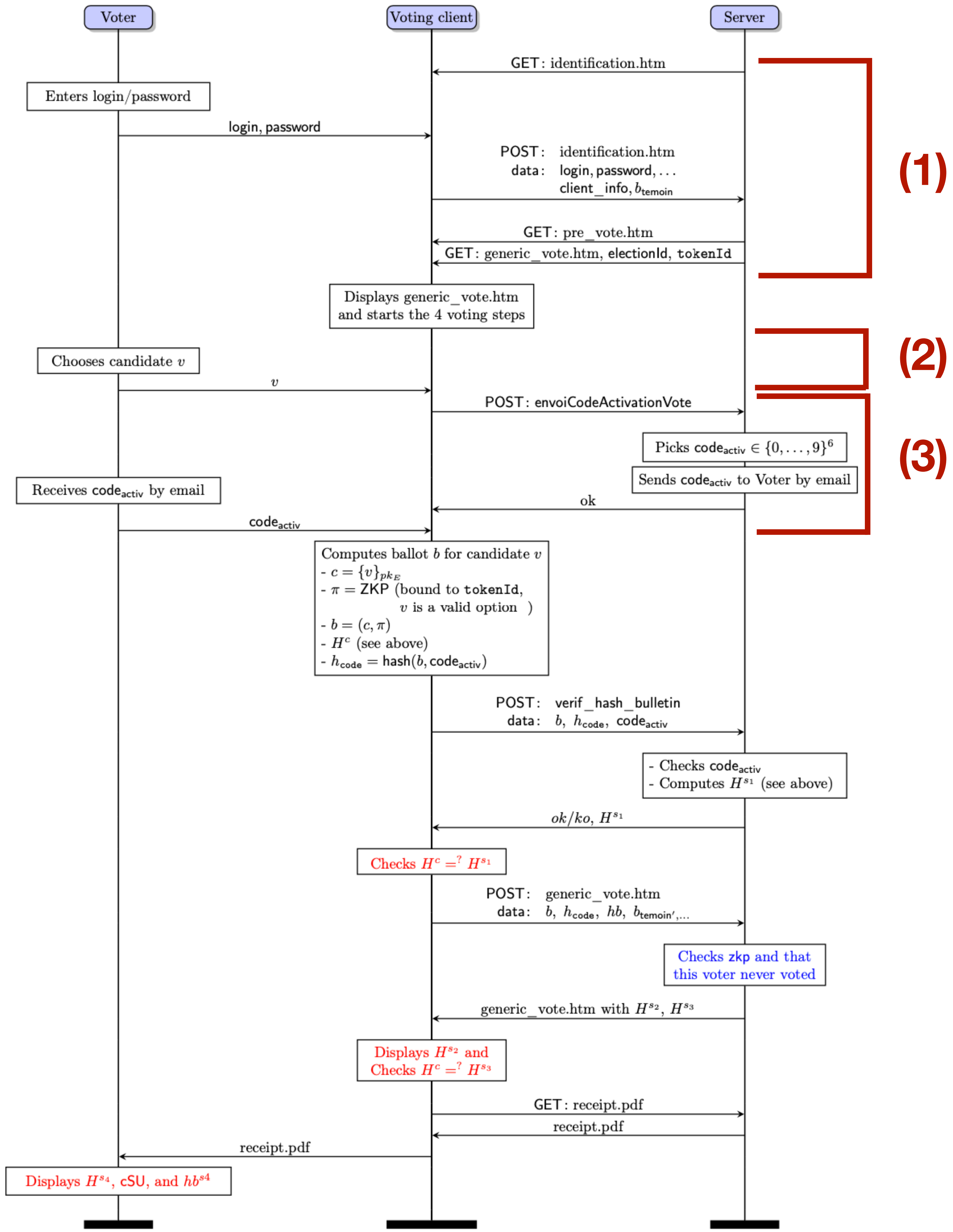
A comprehensive description of the protocol



1. **Authentication:** the voter sends their login/password to the server

2. **Vote section and confirmation**

A comprehensive description of the protocol

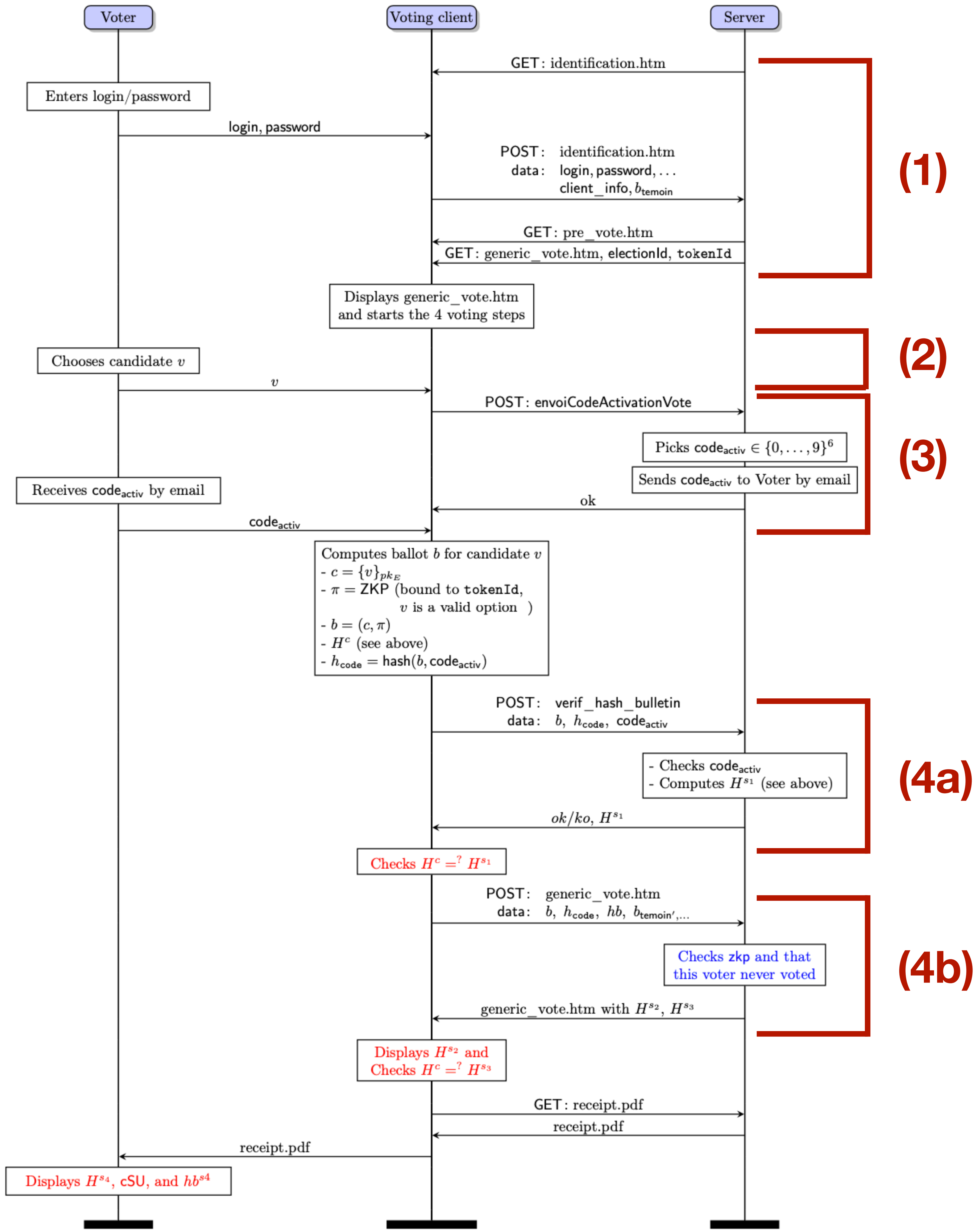


1. **Authentication:** the voter sends their login/password to the server

2. **Vote section and confirmation**

3. **Code activation:** once confirmed, the voter initiates the sending of the activation code by email

A comprehensive description of the protocol



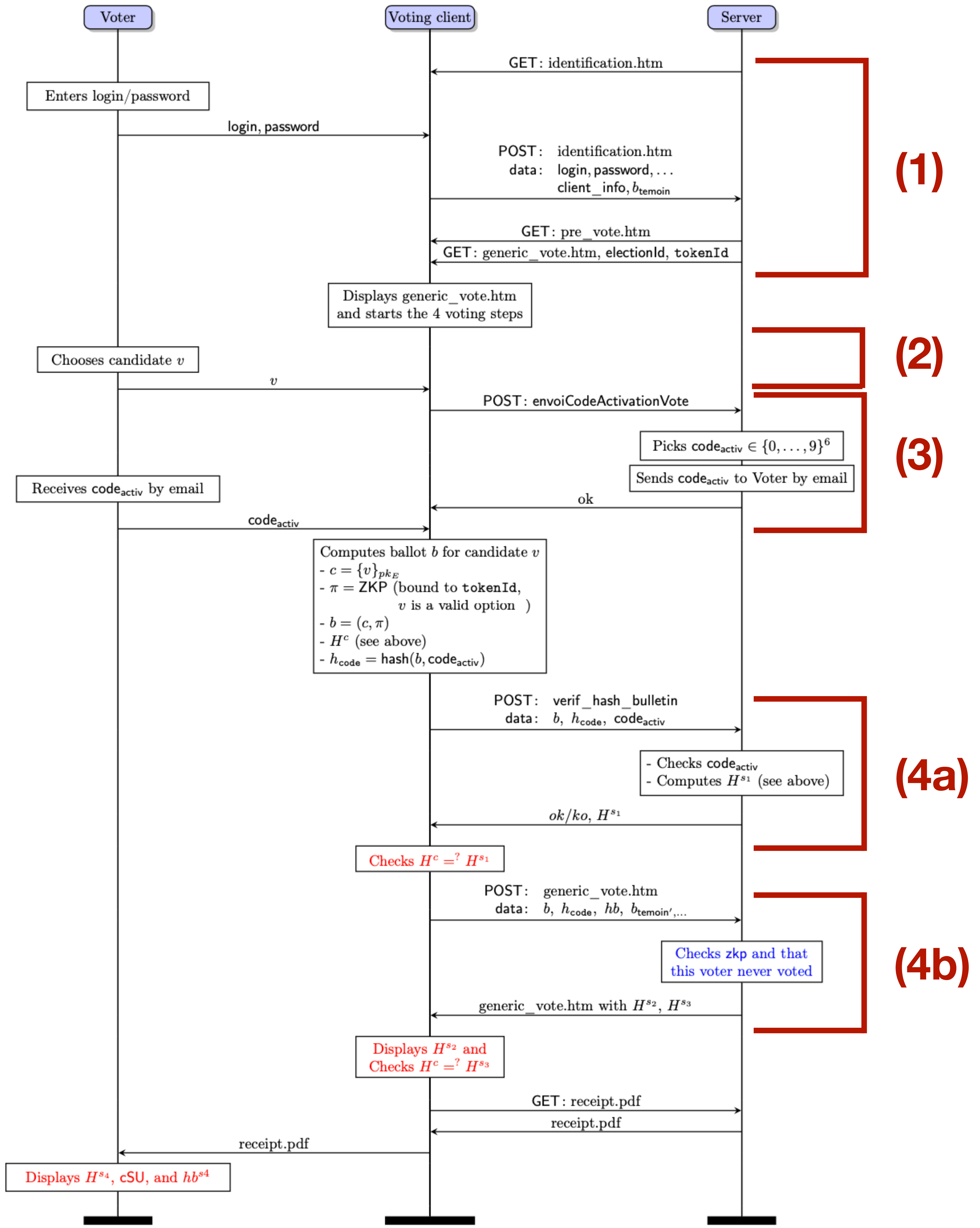
1. **Authentication:** the voter sends their login/password to the server

2. **Vote section and confirmation**

3. **Code activation:** once confirmed, the voter initiates the sending of the activation code by email

4. **Sending the ballot:** the voter sends their ballot together with the activation code

A comprehensive description of the protocol



1. **Authentication:** the voter sends their login/password to the server

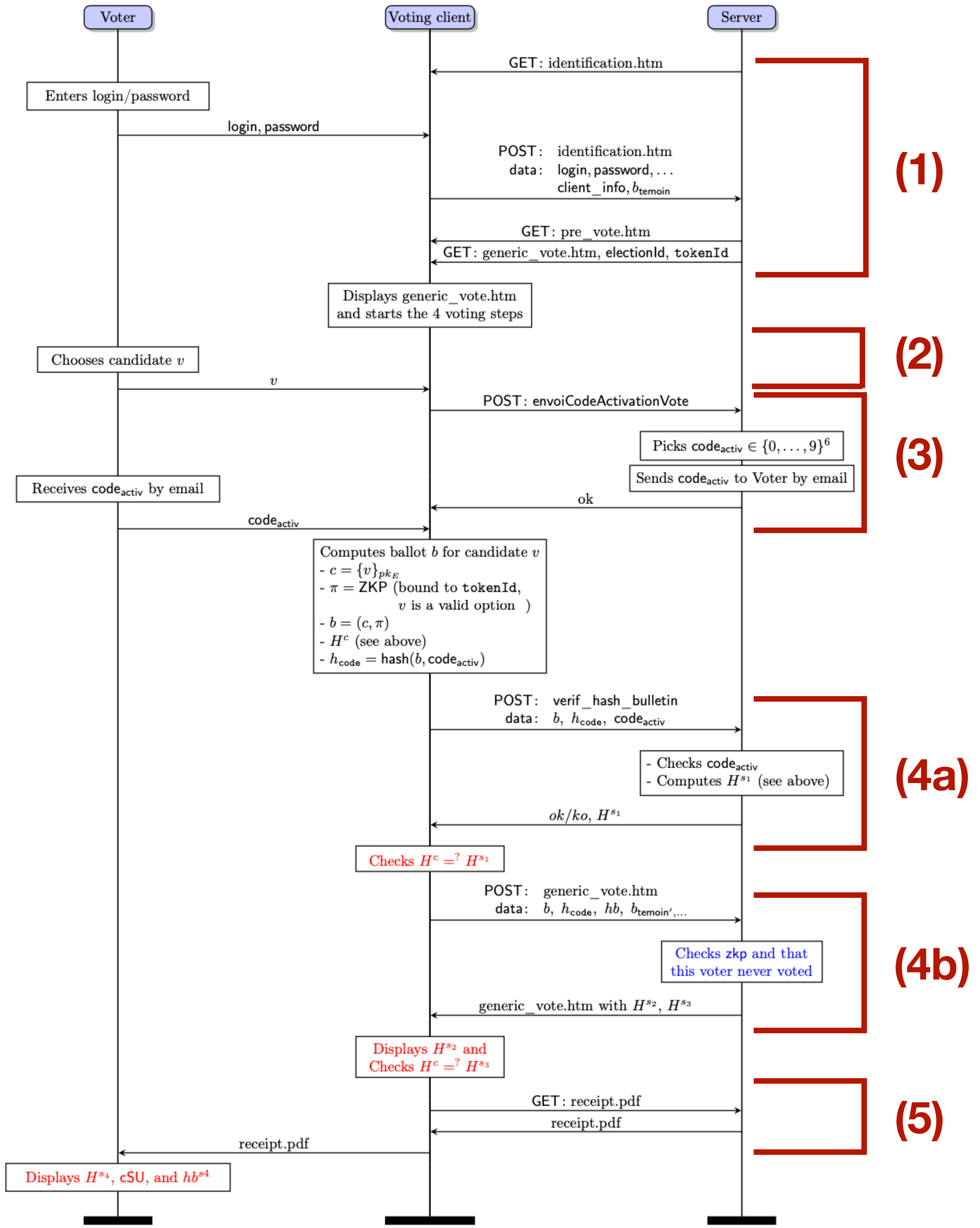
2. **Vote section and confirmation**

3. **Code activation:** once confirmed, the voter initiates the sending of the activation code by email

4. **Sending the ballot:** the voter sends their ballot together with the activation code

🤔 Why is the ballot sent twice… ?

A comprehensive description of the protocol



1. Authentication: the voter sends their login/password to the server

2. Vote section and confirmation

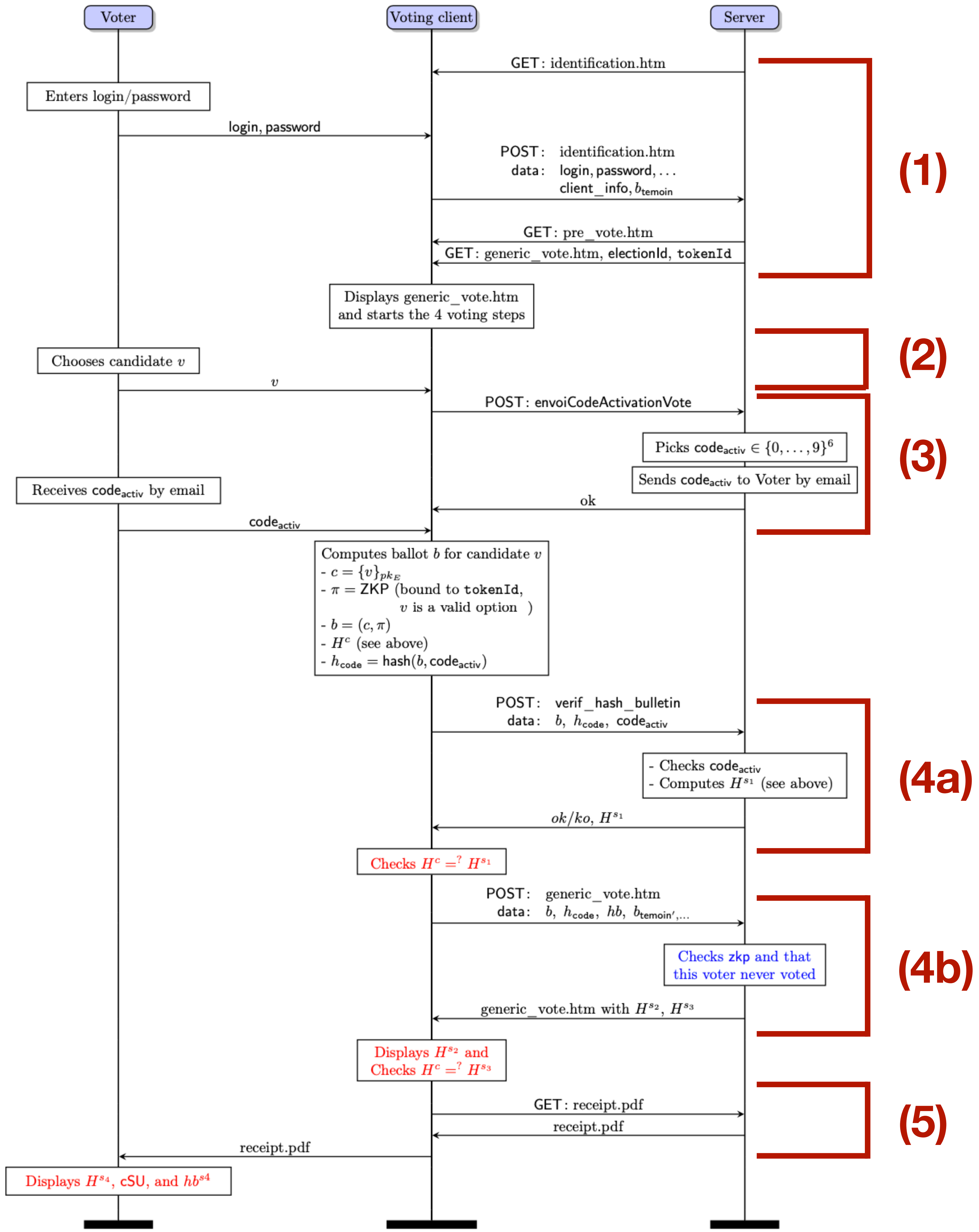
3. Code activation: once confirmed, the voter initiates the sending of the activation code by email

4. Sending the ballot: the voter sends their ballot together with the activation code

Why is the ballot sent twice… ?

5. Receiving the receipt: the server sends the PDF receipt to the voter

A comprehensive description of the protocol



1. Authentication: the voter sends their login/password to the server

2. Vote section and confirmation

3. Code activation: once confirmed, the voter initiates the sending of the activation code by email

4. Sending the ballot: the voter sends their ballot together with the activation code

🤔 Why is the ballot sent twice… ?

5. Receiving the receipt: the server sends the PDF receipt to the voter

This is the first public comprehensive description of the protocol.

Outline

1. Reverse the threat model and the protocol

2. **Vulnerabilities, attacks, and fixes**
   - how to defeat verifiability?
   - how to defeat vote privacy?

3. Other concerns and take away

More details about the receipt

MINISTÈRE
DE L'EUROPE
ET DES AFFAIRES
ÉTRANGÈRES
Liberté
Égalité
Fraternité

Elections législatives 2022 1er tour

Preuve de dépôt du bulletin de vote dans l'urne

Voici la preuve de dépôt de votre bulletin dans l'urne.

Votre bulletin de vote a bien été introduit dans l'urne électronique.

La référence ci-dessous vous permet de contrôler que votre bulletin est bien dans l'urne.

80011&1&3318f83ea80861c9Sdfsd7gd90f7g7896df87g598asd76f89689 65da78sd587as6 **(1)**

Pour contrôler la référence de votre bulletin : cliquez ici
https://votefae.diplomatie.gouv.fr/pages/verifierEmpreinte

Une fois le dépouillement effectué, vous pouvez vérifier que votre bulletin a bien été pris en compte dans le calcul des résultats, à l'aide d'un outil tiers développé par le CNRS, conformément aux exigences de la CNIL en matière de transparence de l'urne. Pour ce faire, vous devrez renseigner le cachet électronique ci-dessous.

Vous pouvez accédez à l'outil en cliquant ici.

Ce cachet électronique vous permet également de vérifier que votre preuve de vote a bien été produite par le système de vote homologué.

hjkHKLJHSAJLKhsnlkjahsJKLHAJKLHDY&Y786S8D7F6S87D6F87SDOYF89A7S6F87AS6D89AOIYIUASDGASDSDysu
hjkHKLJHSAJLKhsnlkjahsJKLHAJKLHDY&Y786S8D7F6S87D6F87SDOYF89A7S6F87AS6D89AOIYIUASDGASDSDysu
hjkHKLJHSAJLKhsnlkjahsJKLHAJKLHDY&Y786S8D7F6S87D6F87SDOYF89A7S6F87AS6D89AOIYIUASDGASDSDysu
hjkHKLJHSAJLKhsnlkjahsJKLHAJKLHDY&Y786S8D7F6S87D6F87SDOYF89A7S6F87AS6D89AOIYIUASDGASDSDysu
hjkHKLJHSAJLKhsnlkjahsJKLHAJKLHDY&Y786S8D7F6S87D6F87SDOYF89A7S6F87AS6D89AOIYIUASDGASDSDysu
hjkHKLJHSAJLKhsnlkjahsJKLHAJKLHDY&Y786S8D7F6S87D6F87SDOYF89A7S6F87AS6D89AOIYIUASDGASDSDysu
hjkHKLJHSAJLKhsnlkjahsJKLHAJKLHDY&Y786S8D7F6S87D6F87SDOYF89A7S6F87AS6D89AOIYIUASDGASDSDysu
sadjoklasd678a(DSadsd6

(2)

Pour contrôler le cachet électronique, cliquez ici
https://votefae.diplomatie.gouv.fr/pages/verificationCachetServeur

La valeur chiffrée de votre bulletin de vote ci-dessous vous permet de vérifier que le contenu de votre bulletin de vote est identique tout au long du scrutin. Cette valeur est à comparer avec celle obtenue en vérifiant la présence de votre bulletin dans l'urne.
asd68asd6a907df90s78fuopaf90ads7f87a6sda78s96da8s76f908sd7f68sif **(3)**

1. **Reference of the ballot:** $H = \mathtt{hash}(ballot \,\&\, context)$
2. **Seal of the ballot:** $cSU = sign_{skS}\,(ballot \,\&\, context')$
3. **Ballot fingerprint:** $hb = \mathtt{hash}(ballot)$

More details about the receipt

MINISTÈRE
DE L'EUROPE
ET DES AFFAIRES
ÉTRANGÈRES
Liberté
Égalité
Fraternité

Elections législatives 2022 1er tour

Preuve de dépôt du bulletin de vote dans l'urne

Voici la preuve de dépôt de votre bulletin dans l'urne.

Votre bulletin de vote a bien été introduit dans l'urne électronique.

La référence ci-dessous vous permet de contrôler que votre bulletin est bien dans l'urne.

80011&1&3318f83ea80861c9Sdfsd7gd90f7g7896df87g598asd76f89689
65da78sd587as6

(1)

Pour contrôler la référence de votre bulletin : cliquez ici
https://votefae.diplomatie.gouv.fr/pages/verifierEmpreinte

Une fois le dépouillement effectué, vous pouvez vérifier que votre bulletin a bien été pris en compte dans le calcul des résultats, à l'aide d'un outil tiers développé par le CNRS, conformément aux exigences de la CNIL en matière de transparence de l'urne. Pour ce faire, vous devrez renseigner le cachet électronique ci-dessous.

Vous pouvez accédez à l'outil en cliquant ici.

Ce cachet électronique vous permet également de vérifier que votre preuve de vote a bien été produite par le système de vote homologué.

hjkHKLJHSAJLKhsnlkjahsJKLHAJKLHDY&Y786S8D7F6S87D6F87SDOYF89A7S6F87AS6D89AOIYIUASDGASDSDysu
hjkHKLJHSAJLKhsnlkjahsJKLHAJKLHDY&Y786S8D7F6S87D6F87SDOYF89A7S6F87AS6D89AOIYIUASDGASDSDysu
hjkHKLJHSAJLKhsnlkjahsJKLHAJKLHDY&Y786S8D7F6S87D6F87SDOYF89A7S6F87AS6D89AOIYIUASDGASDSDysu
hjkHKLJHSAJLKhsnlkjahsJKLHAJKLHDY&Y786S8D7F6S87D6F87SDOYF89A7S6F87AS6D89AOIYIUASDGASDSDysu
hjkHKLJHSAJLKhsnlkjahsJKLHAJKLHDY&Y786S8D7F6S87D6F87SDOYF89A7S6F87AS6D89AOIYIUASDGASDSDysu
hjkHKLJHSAJLKhsnlkjahsJKLHAJKLHDY&Y786S8D7F6S87D6F87SDOYF89A7S6F87AS6D89AOIYIUASDGASDSDysu
hjkHKLJHSAJLKhsnlkjahsJKLHAJKLHDY&Y786S8D7F6S87D6F87SDOYF89A7S6F87AS6D89AOIYIUASDGASDSDysu
sadjoklasd678a(DSadsd6

(2)

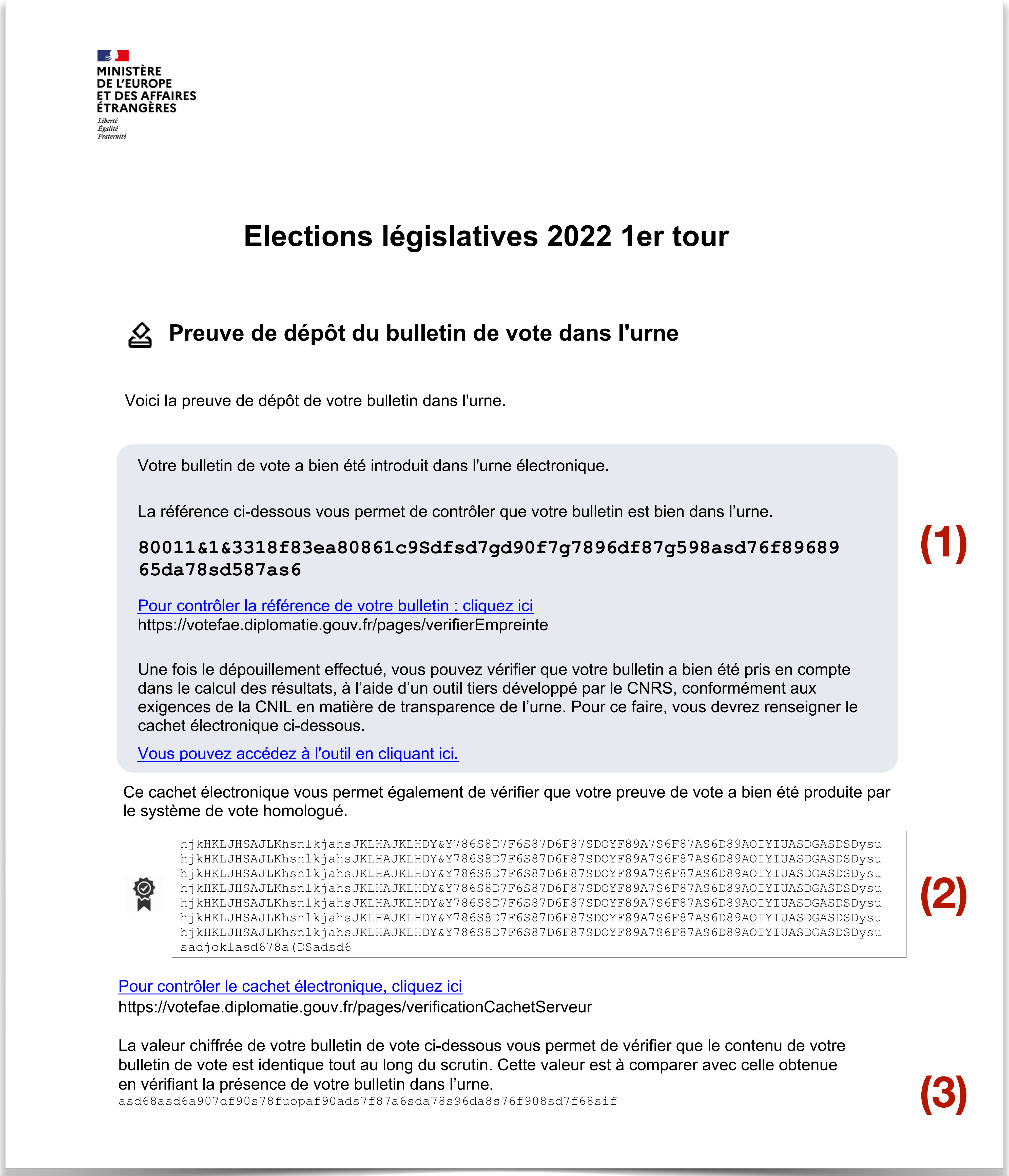
Pour contrôler le cachet électronique, cliquez ici
https://votefae.diplomatie.gouv.fr/pages/verificationCachetServeur

La valeur chiffrée de votre bulletin de vote ci-dessous vous permet de vérifier que le contenu de votre bulletin de vote est identique tout au long du scrutin. Cette valeur est à comparer avec celle obtenue en vérifiant la présence de votre bulletin dans l'urne.
asd68asd6a907df90s78fuopaf90ads7f87a6sda78s96da8s76f908sd7f68sif

(3)

1. **Reference of the ballot:** $H = \mathtt{hash}(ballot\ \&\ context)$
2. **Seal of the ballot:** $cSU = sign_{skS}\ (ballot\ \&\ context')$
3. **Ballot fingerprint:** $hb = \mathtt{hash}(ballot)$ 🤔 This is useless…

More details about the receipt



MINISTÈRE
DE L'EUROPE
ET DES AFFAIRES
ÉTRANGÈRES

Elections législatives 2022 1er tour

Preuve de dépôt du bulletin de vote dans l'urne

Voici la preuve de dépôt de votre bulletin dans l'urne.

Votre bulletin de vote a bien été introduit dans l'urne électronique.

La référence ci-dessous vous permet de contrôler que votre bulletin est bien dans l'urne.

`80011&1&3318f83ea80861c9Sdfsd7gd90f7g7896df87g598asd76f89689 65da78sd587as6`

Pour contrôler la référence de votre bulletin : cliquez ici
https://votefae.diplomatie.gouv.fr/pages/verifierEmpreinte

Une fois le dépouillement effectué, vous pouvez vérifier que votre bulletin a bien été pris en compte dans le calcul des résultats, à l'aide d'un outil tiers développé par le CNRS, conformément aux exigences de la CNIL en matière de transparence de l'urne. Pour ce faire, vous devrez renseigner le cachet électronique ci-dessous.

Vous pouvez accédez à l'outil en cliquant ici.

(1)

Ce cachet électronique vous permet également de vérifier que votre preuve de vote a bien été produite par le système de vote homologué.

hjkHKLJHSAJLKhsnlkjahsJKLHAJKLHDY&Y786S8D7F6S87D6F87SDOYF89A7S6F87AS6D89AOIYIUASDGASDSDysu
hjkHKLJHSAJLKhsnlkjahsJKLHAJKLHDY&Y786S8D7F6S87D6F87SDOYF89A7S6F87AS6D89AOIYIUASDGASDSDysu
hjkHKLJHSAJLKhsnlkjahsJKLHAJKLHDY&Y786S8D7F6S87D6F87SDOYF89A7S6F87AS6D89AOIYIUASDGASDSDysu
hjkHKLJHSAJLKhsnlkjahsJKLHAJKLHDY&Y786S8D7F6S87D6F87SDOYF89A7S6F87AS6D89AOIYIUASDGASDSDysu
hjkHKLJHSAJLKhsnlkjahsJKLHAJKLHDY&Y786S8D7F6S87D6F87SDOYF89A7S6F87AS6D89AOIYIUASDGASDSDysu
hjkHKLJHSAJLKhsnlkjahsJKLHAJKLHDY&Y786S8D7F6S87D6F87SDOYF89A7S6F87AS6D89AOIYIUASDGASDSDysu
hjkHKLJHSAJLKhsnlkjahsJKLHAJKLHDY&Y786S8D7F6S87D6F87SDOYF89A7S6F87AS6D89AOIYIUASDGASDSDysu
sadjoklasd678a(DSadsd6

(2)

Pour contrôler le cachet électronique, cliquez ici
https://votefae.diplomatie.gouv.fr/pages/verificationCachetServeur

La valeur chiffrée de votre bulletin de vote ci-dessous vous permet de vérifier que le contenu de votre bulletin de vote est identique tout au long du scrutin. Cette valeur est à comparer avec celle obtenue en vérifiant la présence de votre bulletin dans l'urne.
`asd68asd6a907df90s78fuopaf90ads7f87a6sda78s96da8s76f908sd7f68sif`

(3)

1. **Reference of the ballot:** $H = \texttt{hash}(ballot \; \& \; context)$
2. **Seal of the ballot:** $cSU = sign_{skS} \; (ballot \; \& \; context')$
3. **Ballot fingerprint:** $hb = \texttt{hash}(ballot)$ 🤔 This is useless…

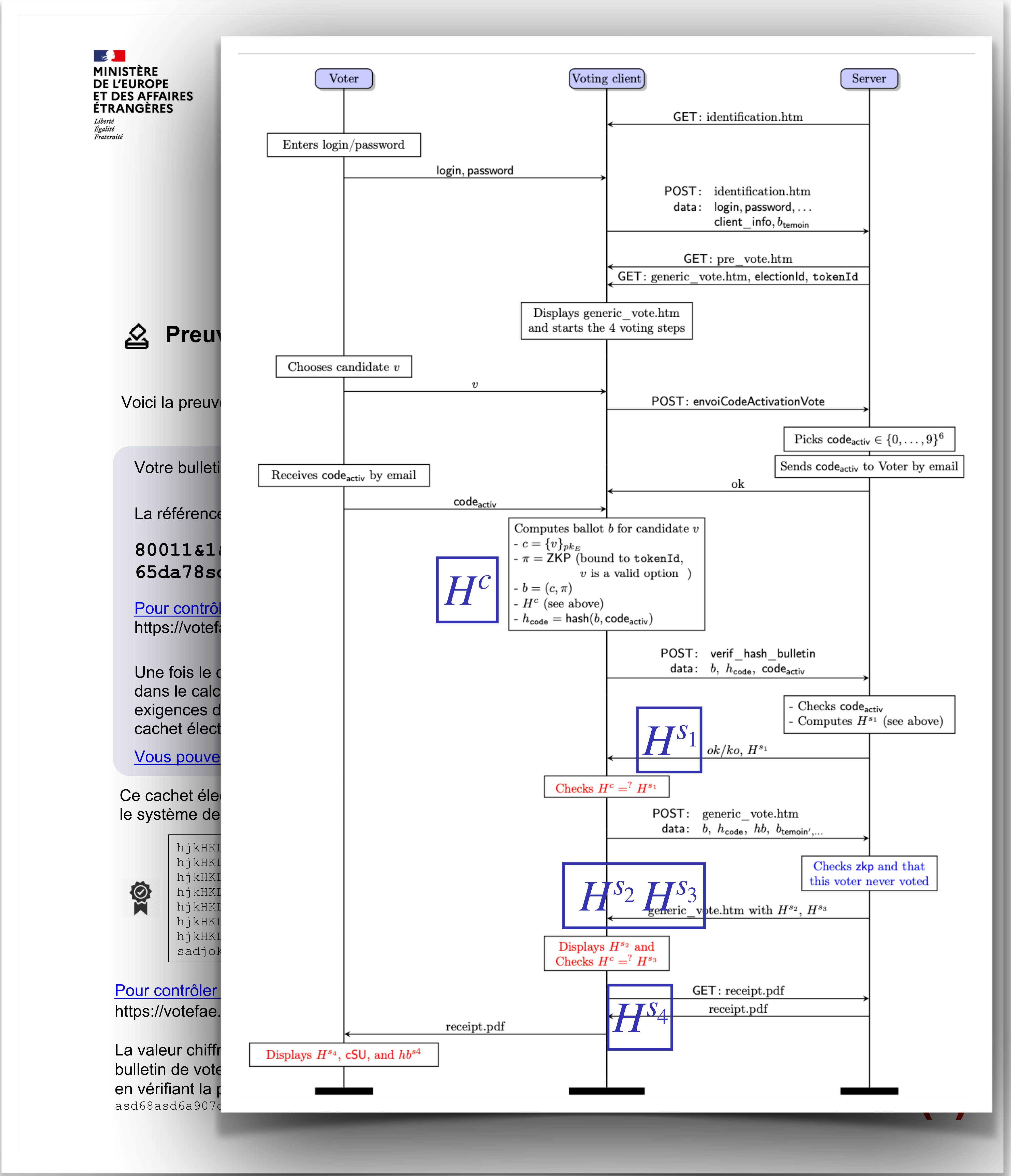
Vulnerability 1:

- The seal **is not checked** by the voting device
- H is computed by the voting device (H^c) and received from the server 4 times ($H^{S_1}, H^{S_2}, H^{S_3}, H^{S_4}$).

➡ the device ensures only: $H^c = H^{S_1} = H^{S_3}$

➡ the voter can only see H^{S_2} and H^{S_4}

More details about the receipt



1. Reference of the ballot: $H = \mathtt{hash}(ballot\ \&\ context)$

2. Seal of the ballot: $cSU = sign_{sk_S}\ (ballot\ \&\ context')$

3. Ballot fingerprint: $hb = \mathtt{hash}(ballot)$ 🤔 This is useless…

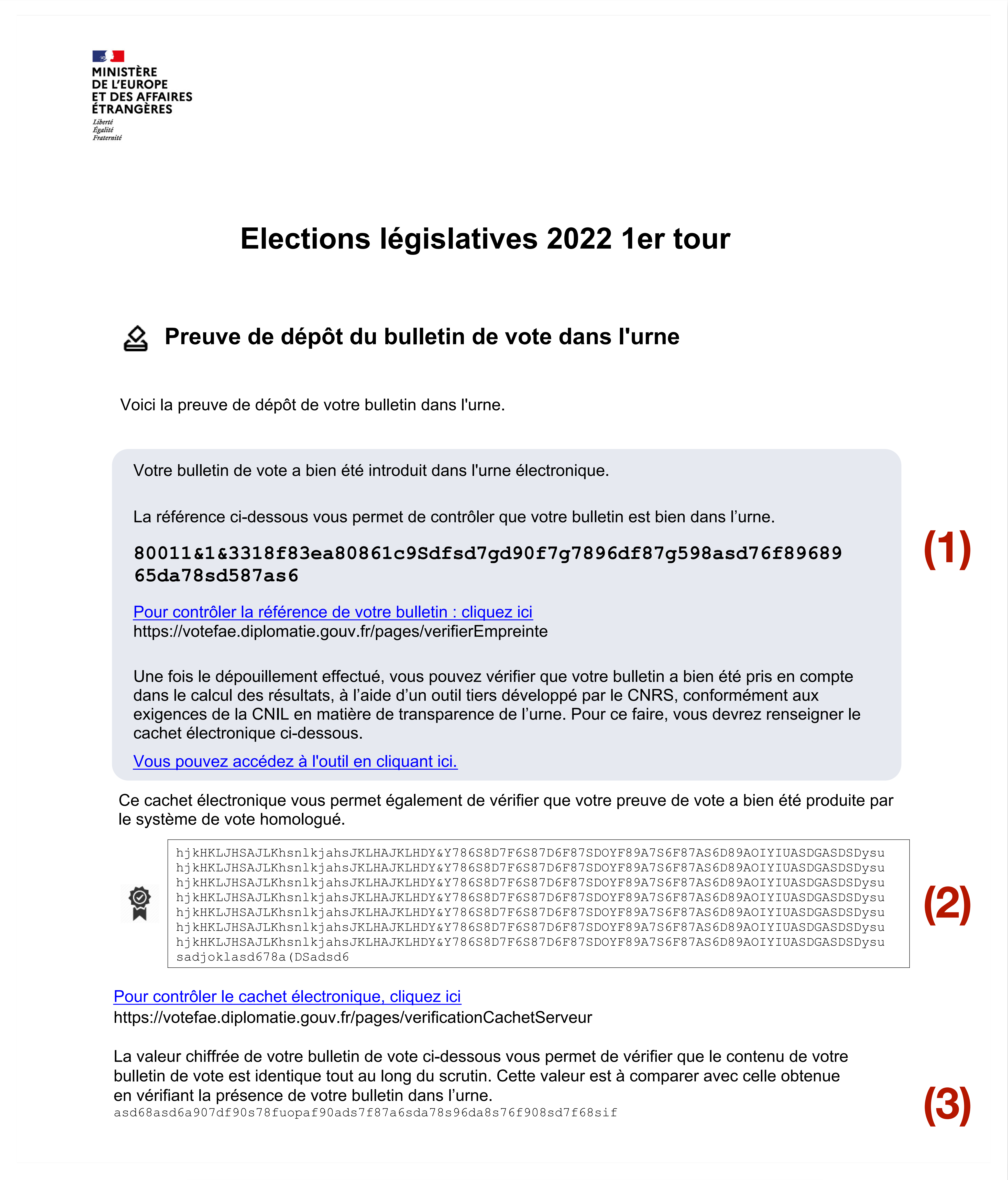
Vulnerability 1:

- The seal is not checked by the voting device
- H is computed by the voting device (H^c) and received from the server 4 times ($H^{S_1}, H^{S_2}, H^{S_3}, H^{S_4}$).

➡ the device ensures only: $H^c = H^{S_1} = H^{S_3}$

➡ the voter can only see H^{S_2} and H^{S_4}

More details about the receipt



MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES

Liberté Égalité Fraternité

Elections législatives 2022 1er tour

Preuve de dépôt du bulletin de vote dans l'urne

Voici la preuve de dépôt de votre bulletin dans l'urne.

Votre bulletin de vote a bien été introduit dans l'urne électronique.

La référence ci-dessous vous permet de contrôler que votre bulletin est bien dans l'urne.

80011&1&3318f83ea80861c9Sdfsd7gd90f7g7896df87g598asd76f89689 65da78sd587as6 **(1)**

Pour contrôler la référence de votre bulletin : cliquez ici
https://votefae.diplomatie.gouv.fr/pages/verifierEmpreinte

Une fois le dépouillement effectué, vous pouvez vérifier que votre bulletin a bien été pris en compte dans le calcul des résultats, à l'aide d'un outil tiers développé par le CNRS, conformément aux exigences de la CNIL en matière de transparence de l'urne. Pour ce faire, vous devrez renseigner le cachet électronique ci-dessous.

Vous pouvez accédez à l'outil en cliquant ici.

Ce cachet électronique vous permet également de vérifier que votre preuve de vote a bien été produite par le système de vote homologué.

hjkHKLJHSAJLKhsnlkjahsJKLHAJKLHDY&Y786S8D7F6S87D6F87SDOYF89A7S6F87AS6D89AOIYIUASDGASDSDysu
hjkHKLJHSAJLKhsnlkjahsJKLHAJKLHDY&Y786S8D7F6S87D6F87SDOYF89A7S6F87AS6D89AOIYIUASDGASDSDysu
hjkHKLJHSAJLKhsnlkjahsJKLHAJKLHDY&Y786S8D7F6S87D6F87SDOYF89A7S6F87AS6D89AOIYIUASDGASDSDysu
hjkHKLJHSAJLKhsnlkjahsJKLHAJKLHDY&Y786S8D7F6S87D6F87SDOYF89A7S6F87AS6D89AOIYIUASDGASDSDysu
hjkHKLJHSAJLKhsnlkjahsJKLHAJKLHDY&Y786S8D7F6S87D6F87SDOYF89A7S6F87AS6D89AOIYIUASDGASDSDysu
hjkHKLJHSAJLKhsnlkjahsJKLHAJKLHDY&Y786S8D7F6S87D6F87SDOYF89A7S6F87AS6D89AOIYIUASDGASDSDysu
hjkHKLJHSAJLKhsnlkjahsJKLHAJKLHDY&Y786S8D7F6S87D6F87SDOYF89A7S6F87AS6D89AOIYIUASDGASDSDysu
sadjoklasd678a(DSadsd6

(2)

Pour contrôler le cachet électronique, cliquez ici
https://votefae.diplomatie.gouv.fr/pages/verificationCachetServeur

La valeur chiffrée de votre bulletin de vote ci-dessous vous permet de vérifier que le contenu de votre bulletin de vote est identique tout au long du scrutin. Cette valeur est à comparer avec celle obtenue en vérifiant la présence de votre bulletin dans l'urne.
asd68asd6a907df90s78fuopaf90ads7f87a6sda78s96da8s76f908sd7f68sif **(3)**

1. Reference of the ballot: $H = \texttt{hash}(ballot \ \& \ context)$

2. Seal of the ballot: $cSU = sign_{skS}\ (ballot \ \& \ context')$

3. Ballot fingerprint: $hb = \texttt{hash}(ballot)$ 🤔 This is useless…

Vulnerability 1:

- The seal is not checked by the voting device
- H is computed by the voting device (H^c) and received from the server 4 times ($H^{S_1}, H^{S_2}, H^{S_3}, H^{S_4}$).

➡ the device ensures only: $H^c = H^{S_1} = H^{S_3}$

➡ the voter can only see H^{S_2} and H^{S_4}

Vulnerability 2: The ballot b is not cryptographically bound to the consulate, i.e. $ballotBoxId$

Attack against verifiability

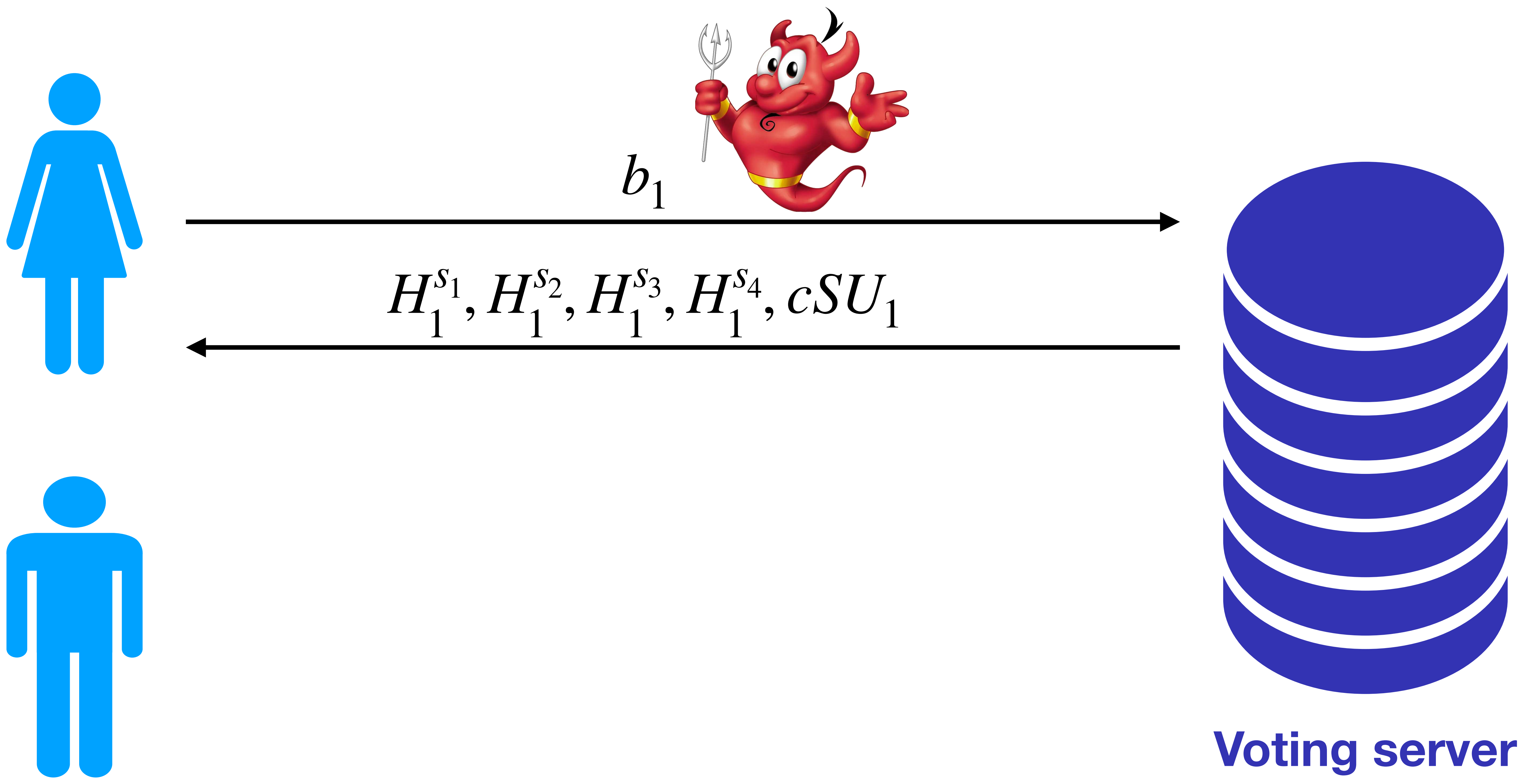
The references seen by the voter may not correspond to their ballot.

Attack against verifiability

The references seen by the voter may not correspond to their ballot.

Attack against verifiability

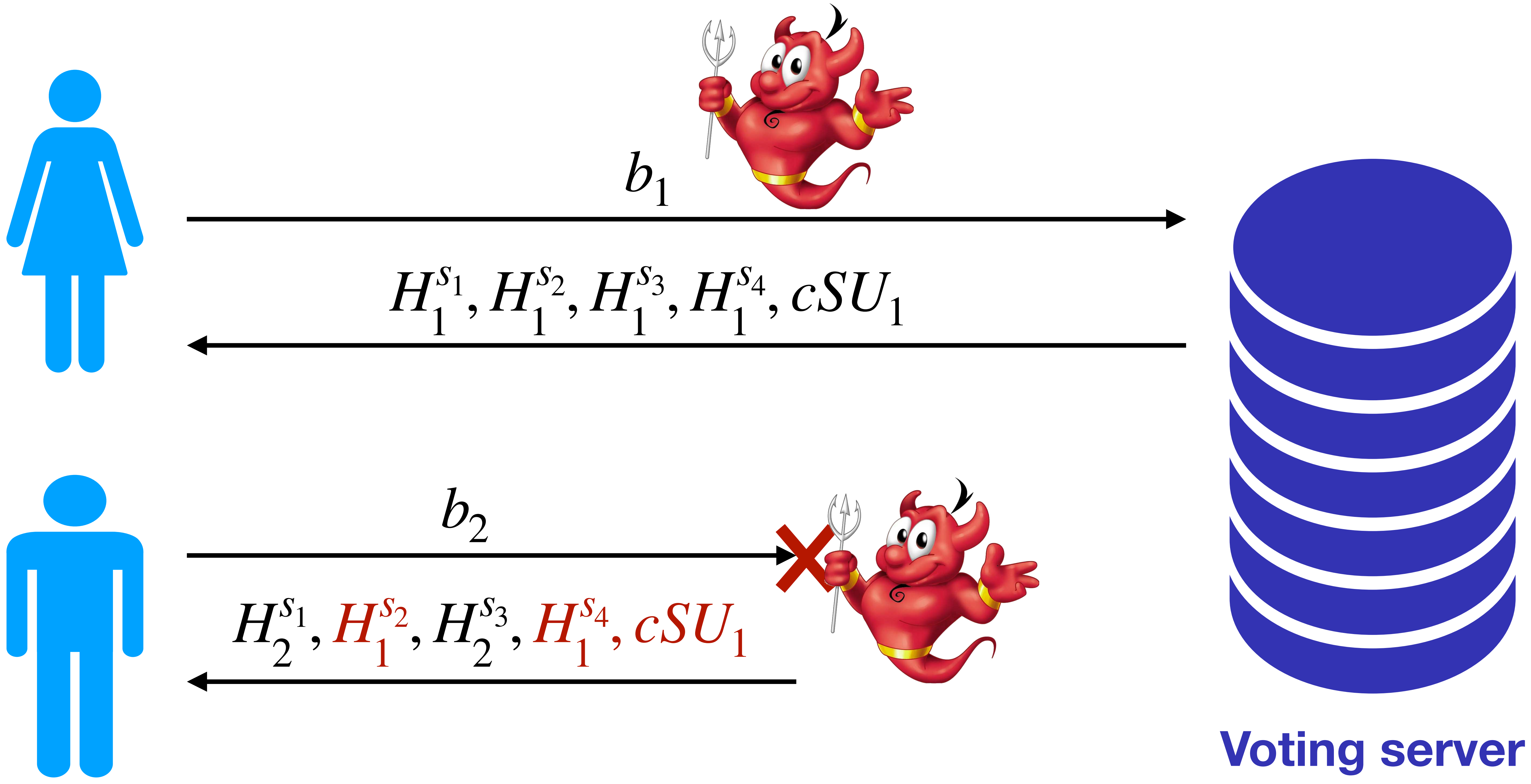
The references seen by the voter may not correspond to their ballot.



Step 1: Alice votes as expected

Attack against verifiability

The references seen by the voter may not correspond to their ballot.



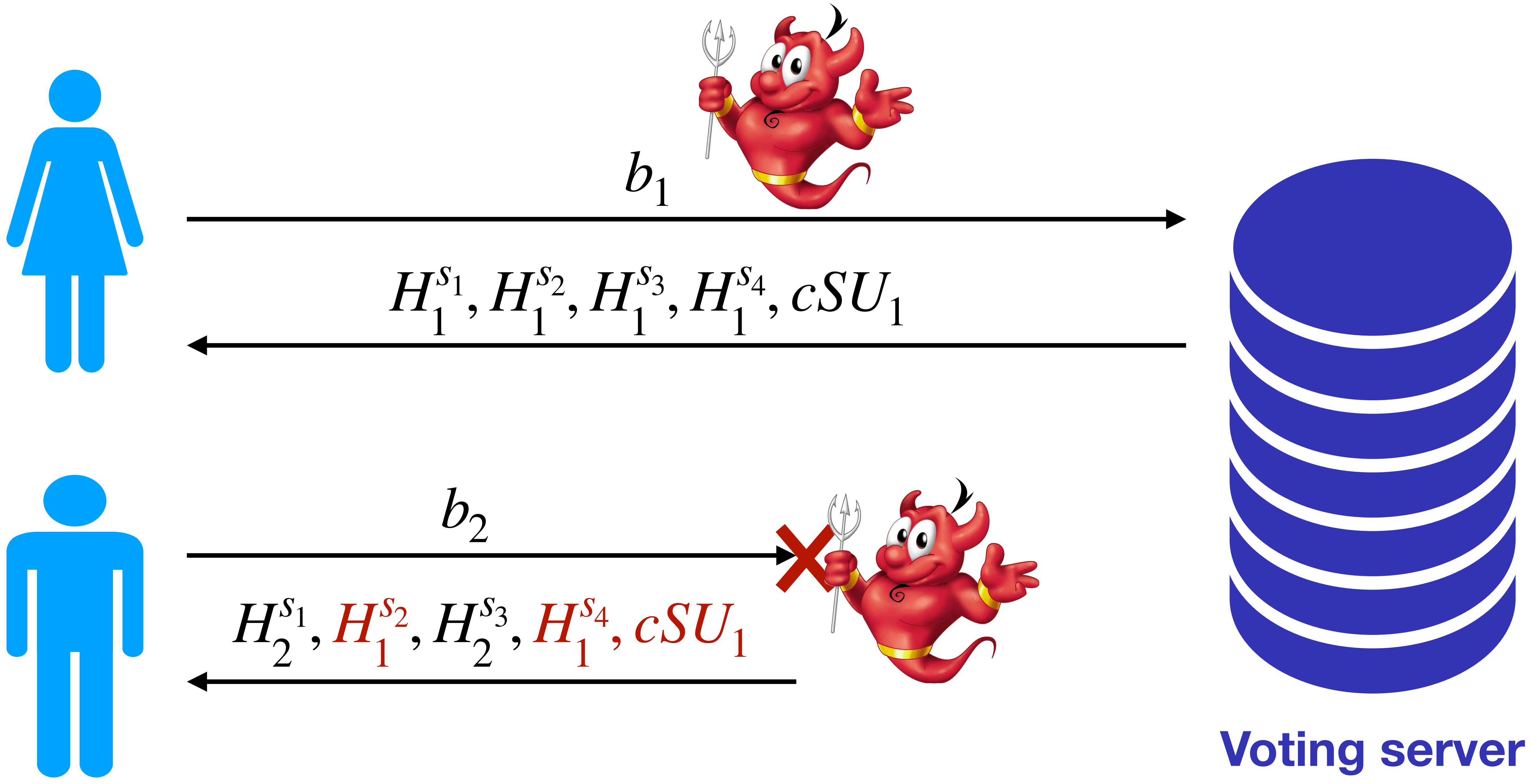
Step 1: Alice votes as expected

Step 2: the attacker intercepts Bob's request

- computes $H_2^{s_1}$ and $H_2^{s_3}$ as expected
- replays Alice's data otherwise

Attack against verifiability

The references seen by the voter may not correspond to their ballot.



Step 1: Alice votes as expected

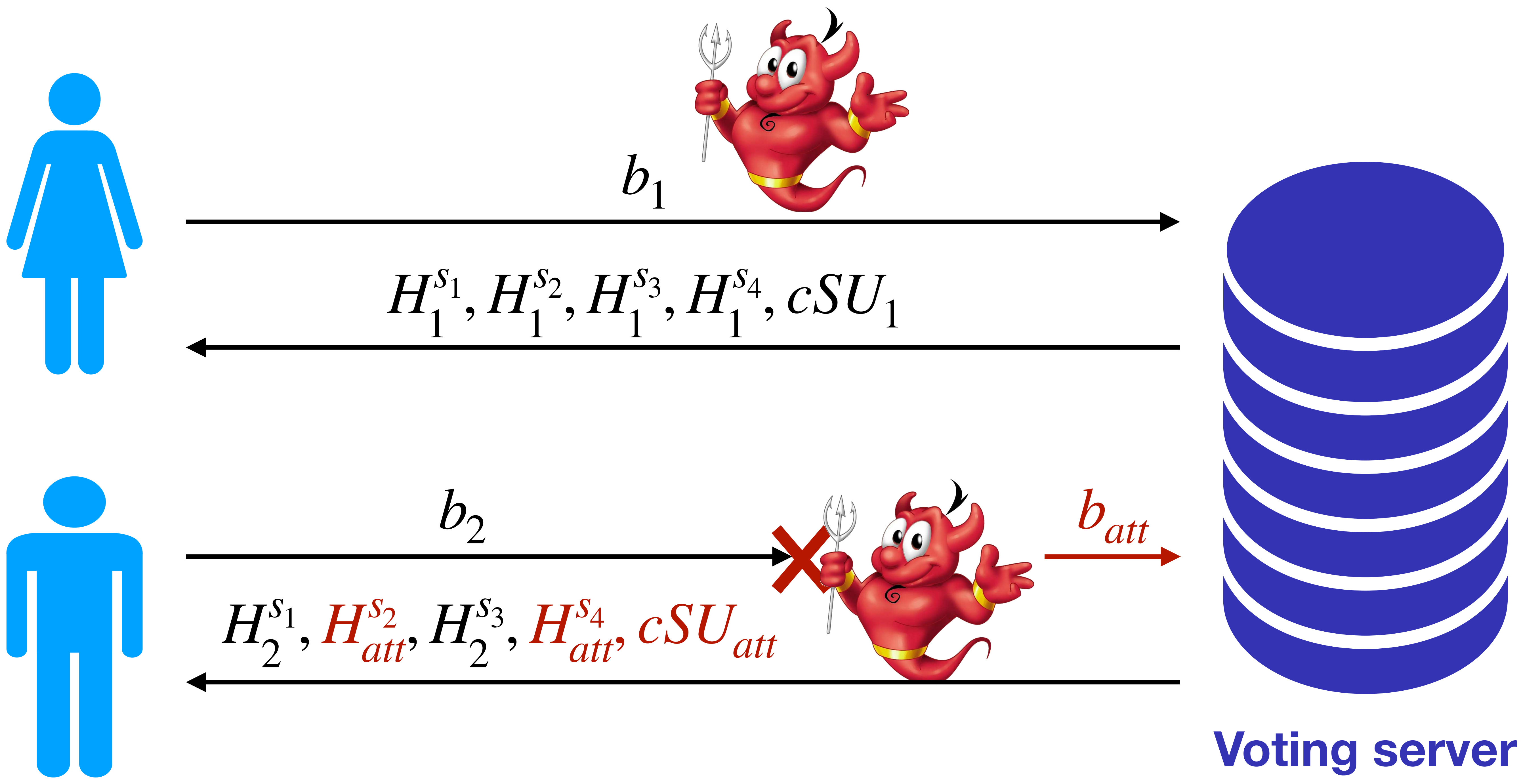
Step 2: the attacker intercepts Bob's request

- computes $H_2^{s_1}$ and $H_2^{s_3}$ as expected
- replays Alice's data otherwise

Result: Bob's ballot is dropped… but nothing went wrong in Bob's process

Attack against verifiability

The references seen by the voter may not correspond to their ballot.



Step 1: Alice votes as expected

Step 2: the attacker intercepts Bob's request

- computes $H_2^{s_1}$ and $H_2^{s_3}$ as expected
- replays Alice's data otherwise

Result: Bob's ballot is dropped… but nothing went wrong in Bob's process

Improvement: the attacker can completely modify Bob's ballot

An almost undetectable attack

1. No error detected during the voting process: $H_2^c = H_2^{s_1} = H_2^{s_3} \neq H_1^{s_2} = H_1^{s_4}$

but this check is never done….

2. Bob receives a valid receipt: Bob's receipt correspond to Alice's ballot or the attacker's ballot…

both are included in the ballot-box ⇒ verifications succeed

An almost undetectable attack

1. No error detected during the voting process: $H_2^c = H_2^{s_1} = H_2^{s_3} \neq H_1^{s_2} = H_1^{s_4}$
but this check is never done….

2. Bob receives a valid receipt: Bob's receipt correspond to Alice's ballot or the attacker's ballot…
both are included in the ballot-box ⇒ verifications succeed

The Loria's verifier is useless to guarantee individual verifiability…

An almost undetectable attack

1. No error detected during the voting process: $H_2^c = H_2^{s_1} = H_2^{s_3} \neq H_1^{s_2} = H_1^{s_4}$

but this check is never done….

2. Bob receives a valid receipt: Bob's receipt correspond to Alice's ballot or the attacker's ballot…

both are included in the ballot-box ⇒ verifications succeed

The Loria's verifier is useless to guarantee individual verifiability…

In rare cases, detection is possible…

- **Attack 1 (drop only):** Bob can see on the signing sheet that he is considered as absentee

➡ requires Bob goes to the polling station… it seems unlikely…

An almost undetectable attack

1. No error detected during the voting process: $H_2^c = H_2^{s_1} = H_2^{s_3} \neq H_1^{s_2} = H_1^{s_4}$

but this check is never done….

2. Bob receives a valid receipt: Bob's receipt correspond to Alice's ballot or the attacker's ballot…

both are included in the ballot-box ⇒ verifications succeed

The Loria's verifier is useless to guarantee individual verifiability…

In rare cases, detection is possible…

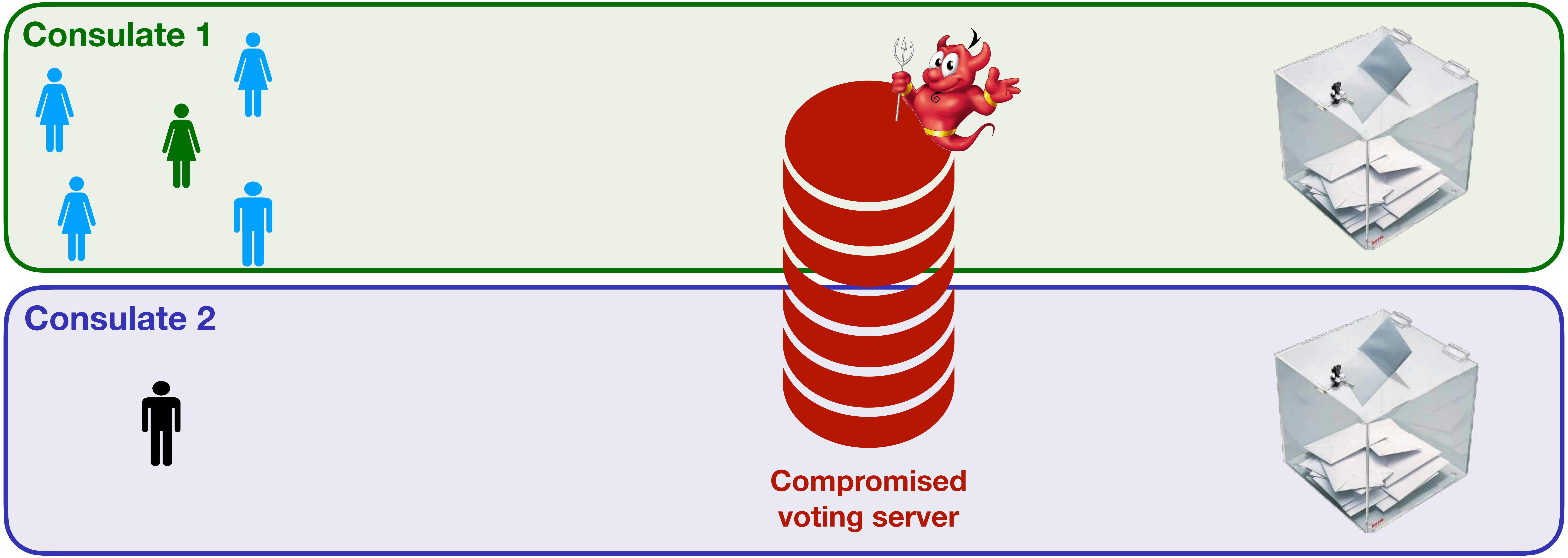
- **Attack 1 (drop only):** Bob can see on the signing sheet that he is considered as absentee
  ➡ requires Bob goes to the polling station… it seems unlikely…
- **Attack 2 (drop and replace):** detectable if no-one else voted for Bob's candidate
  ➡ unlikely in large consulates…

Attack against vote secrecy

The ballot b are not cryptographically bound to the consulate

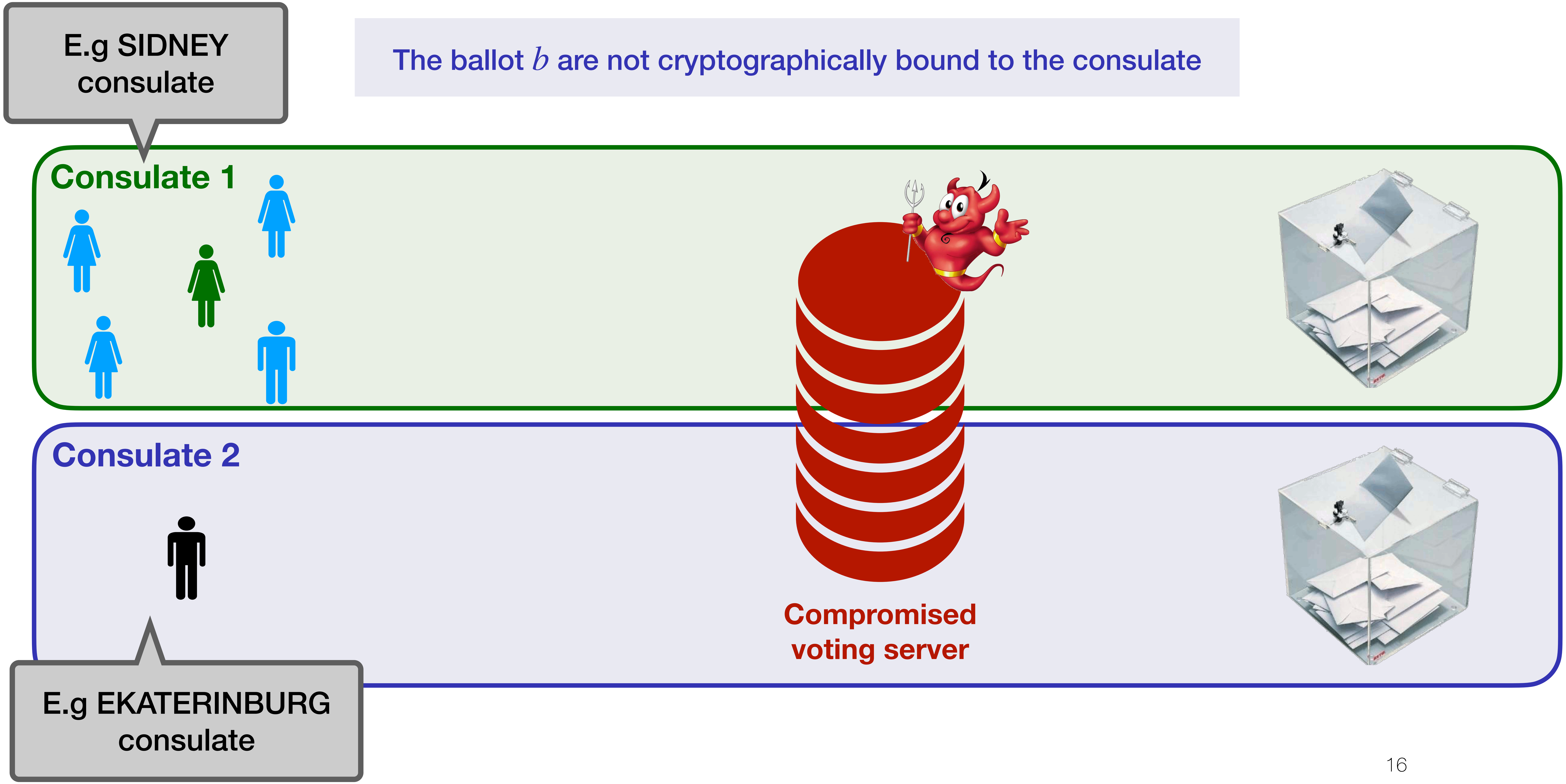
Attack against vote secrecy

The ballot b are not cryptographically bound to the consulate



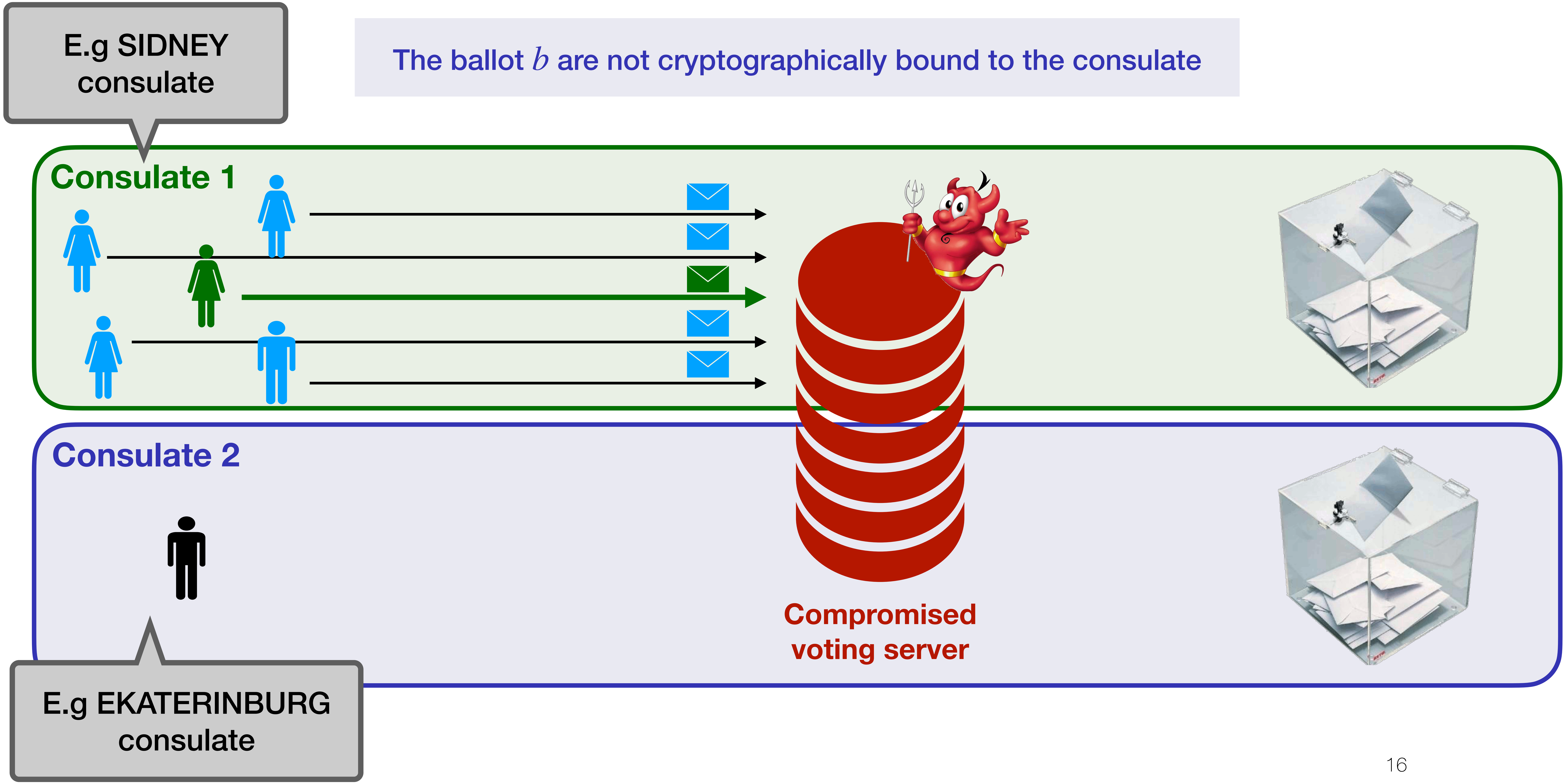
Attack against vote secrecy

The ballot b are not cryptographically bound to the consulate



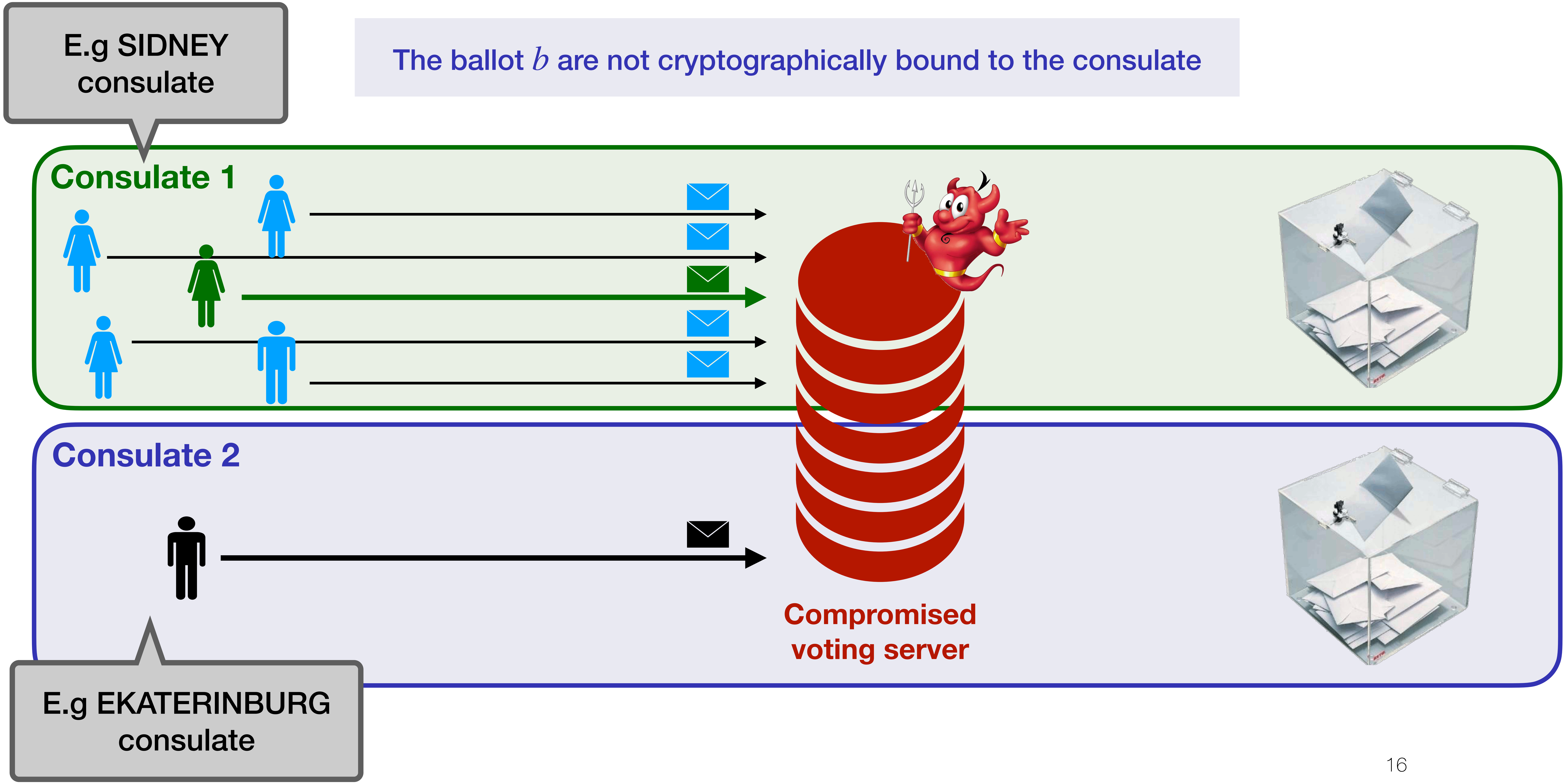
Attack against vote secrecy

The ballot b are not cryptographically bound to the consulate



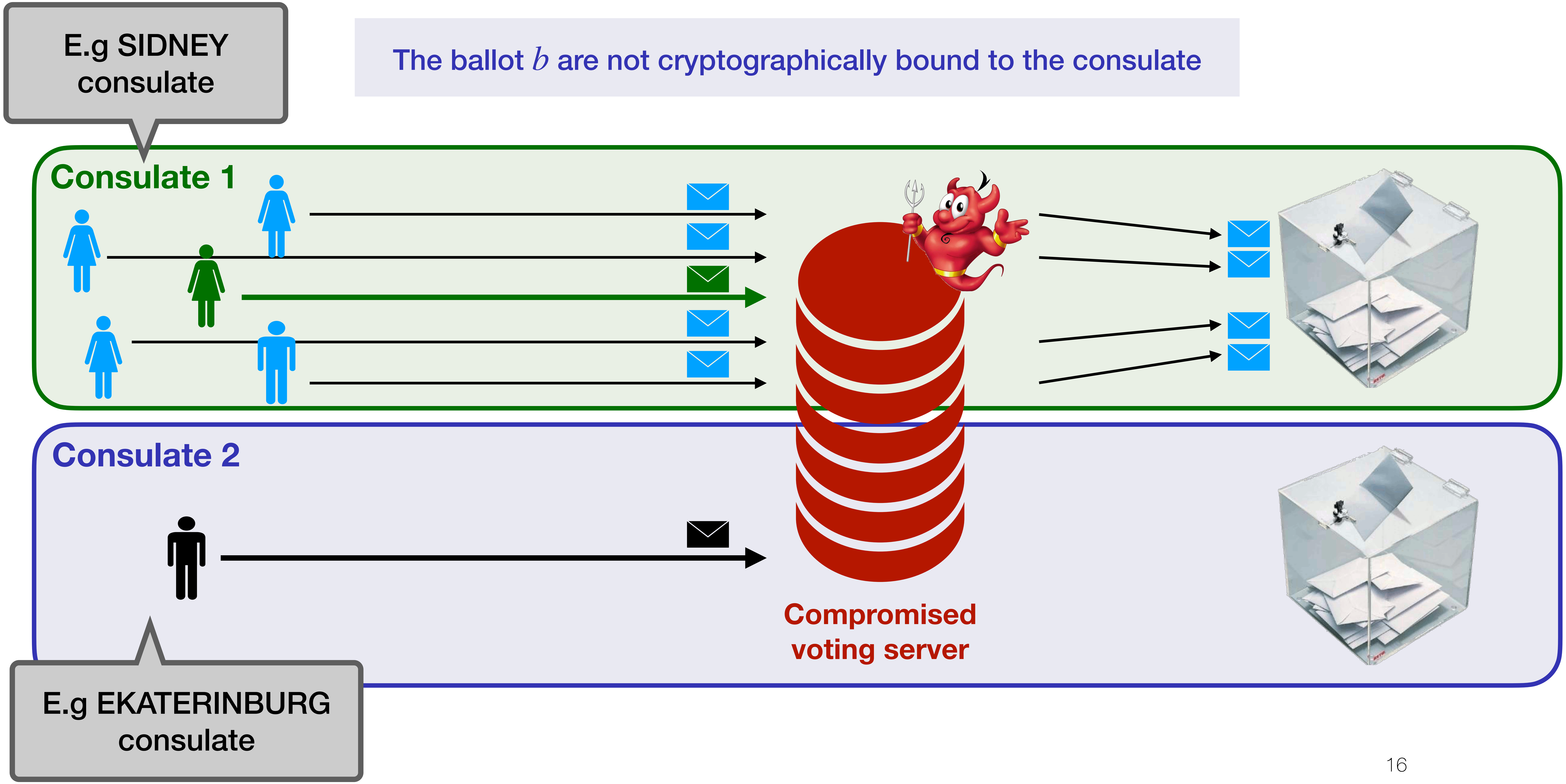
Attack against vote secrecy

The ballot b are not cryptographically bound to the consulate



Attack against vote secrecy

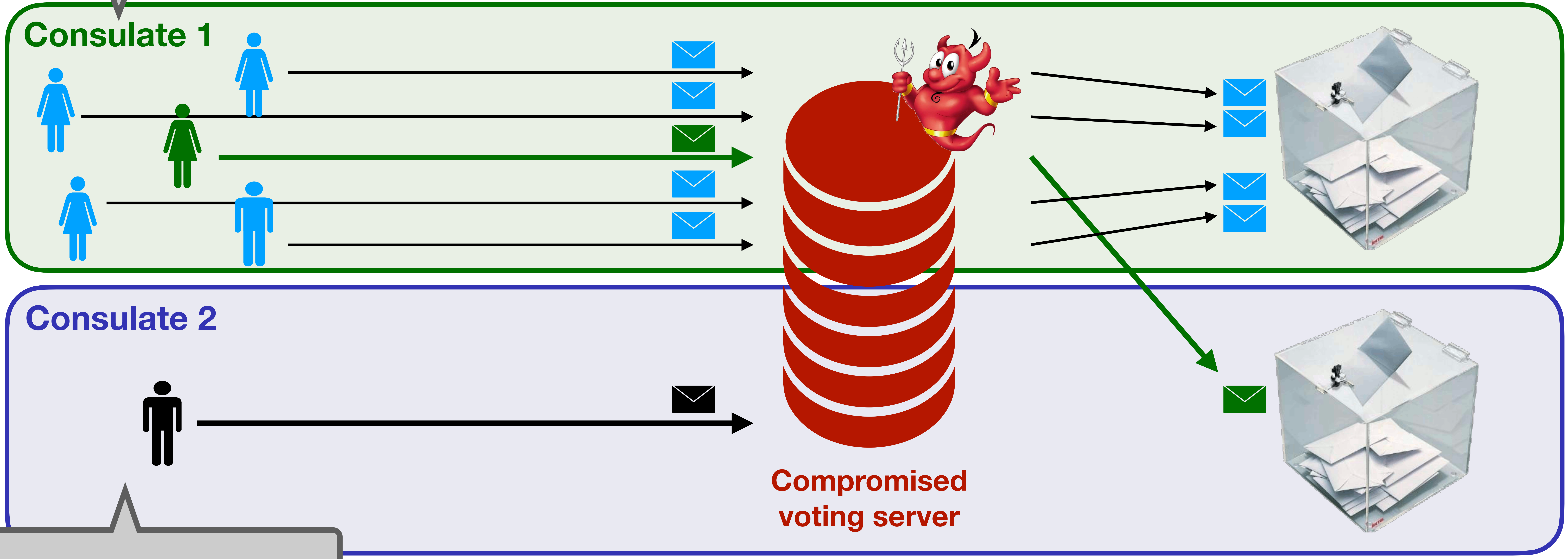
The ballot b are not cryptographically bound to the consulate



Attack against vote secrecy

The ballot b are not cryptographically bound to the consulate

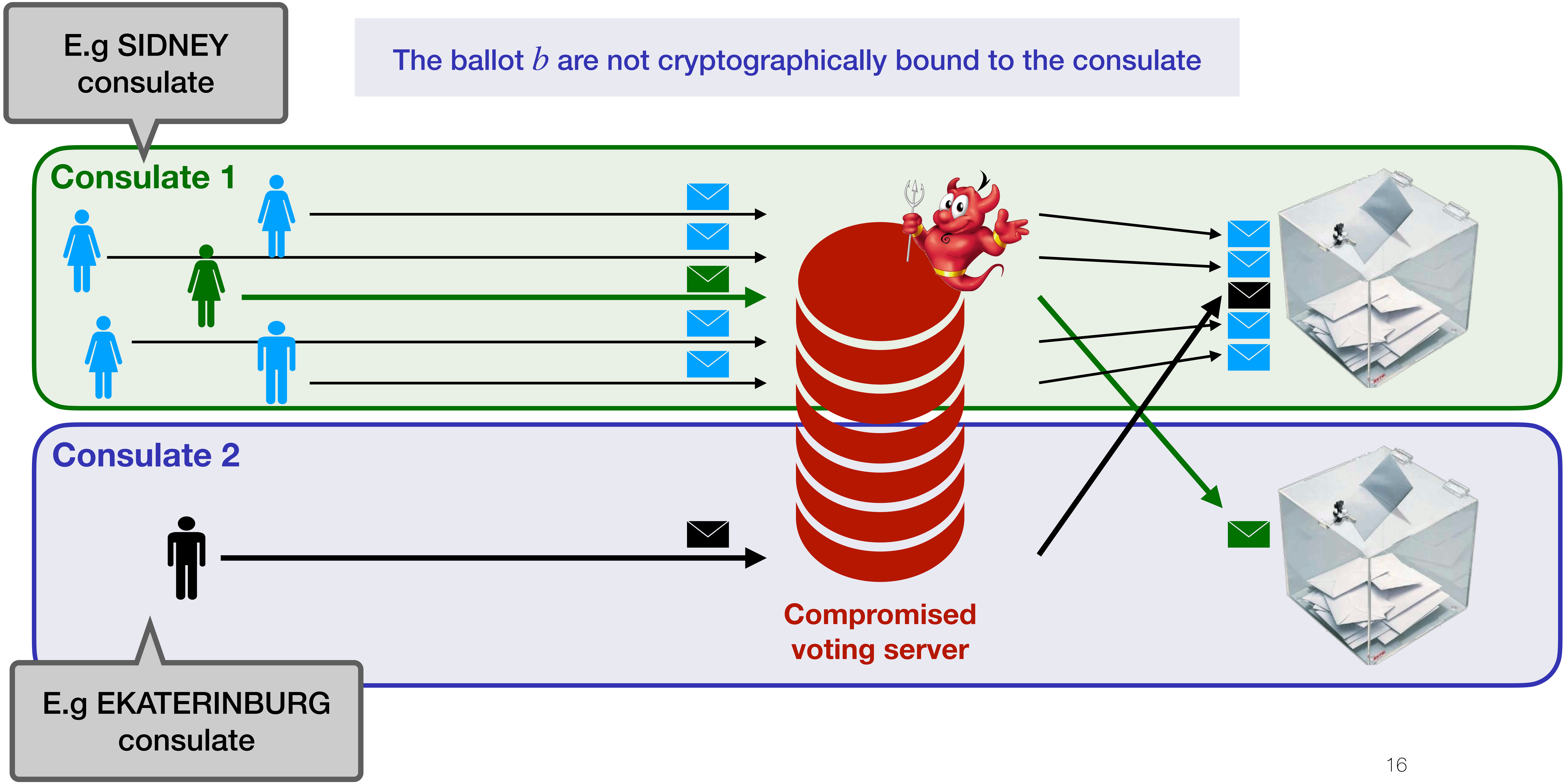
E.g SIDNEY consulate



E.g EKATERINBURG consulate

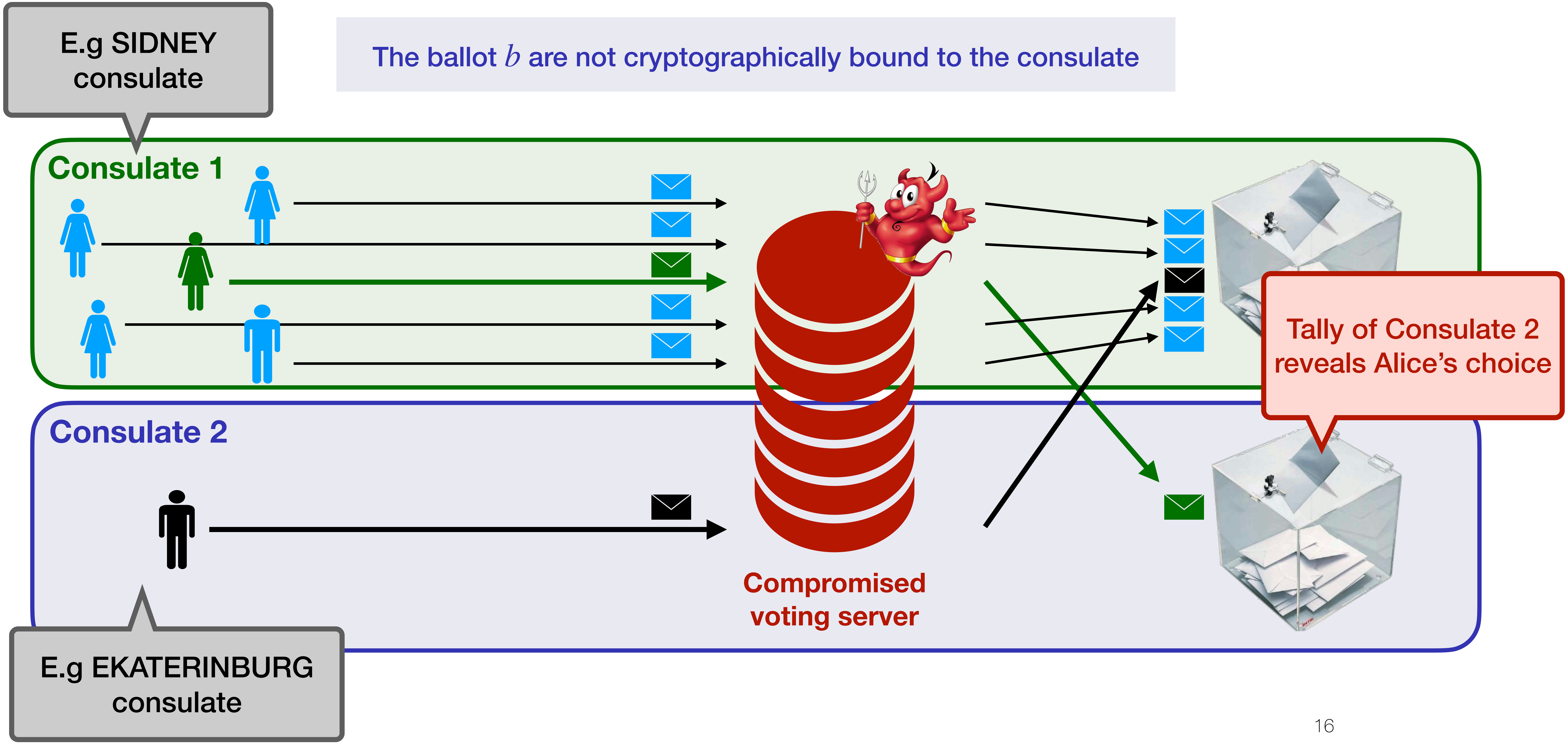
Attack against vote secrecy

The ballot b are not cryptographically bound to the consulate



Attack against vote secrecy

The ballot b are not cryptographically bound to the consulate



Impact of the attack

Assumptions to mount a completely undetectable attack:

- a channel attacker is enough
- at least as many corrupted voter as candidates
- at least as many expressed votes as candidates in the small consulate
- at least one vote per candidate in the large consulate

Impact of the attack

Assumptions to mount a completely undetectable attack:

- a channel attacker is enough
- at least as many corrupted voter as candidates
- at least as many expressed votes as candidates in the small consulate
- at least one vote per candidate in the large consulate

Impact

- can learn the choice or a bias on the choice of target voters: one per “small” consulate
- could contribute to remote coercion attacks: gather and isolate all coerced voters ballots in the same consulate
- is completely undetectable

Summary of attacks

1- Individual verifiability does not hold
Despite the use of a third-party verifier, an attacker who compromises the communication channels (or even worse the voting server) can significantly modify the outcome of the election by dropping and replacing ballots.

2- Vote secrecy does not hold
An attacker who compromises the communication channels (or even more so the voting server) can learn the plaintext vote of arbitrary target voters. The number of voters who can be targeted is immediately related to the number of consulates with a small number of votes cast.

Summary of attacks

1- Individual verifiability does not hold
Despite the use of a third-party verifier, an attacker who compromises the communication channels (or even worse the voting server) can significantly modify the outcome of the election by dropping and replacing ballots.

2- Vote secrecy does not hold
An attacker who compromises the communication channels (or even more so the voting server) can learn the plaintext vote of arbitrary target voters. The number of voters who can be targeted is immediately related to the number of consulates with a small number of votes cast.

Very easy fixes

- display locally created data to the voter only (i.e. create the PDF in local)
- add $ballotBoxId$ in the context of the ZKPs

Summary of attacks

1- Individual verifiability does not hold
Despite the use of a third-party verifier, an attacker who compromises the communication channels (or even worse the voting server) can significantly modify the outcome of the election by dropping and replacing ballots.

2- Vote secrecy does
An attacker who compr ... so the voting server) can learn the plaintext vote ... can be targeted is immediately related to t ... es cast.

We detail 6 different variants of these attacks and propose fixes in the full report!
[ePrint 2022/1653]

Very easy fixes

- display locally created data to the voter only (i.e. create the PDF in local)
- add $ballotBoxId$ in the context of the ZKPs

Outline

1. Reverse the threat model and the protocol

2. Vulnerabilities, attacks, and fixes
   - how to defeat verifiability?
   - how to defeat vote privacy?

3. Other concerns and take away

On the importance of…
the voting device

Regarding security, the key element is the voting device…
(not the voting server)

On the importance of…
the voting device

Regarding security, the key element is the voting device…
(not the voting server)

☺ = trustworthy
👹 = untrustworthy

	Voter	Voting device	Com. channels	Voting server	Dec. auth.	3rd-party
Verifiability	☺	☺	👹	👹	👹	☺
Confidentiality	☺	☺	👹	👹	☺	☺

It's the unique trustworthy component

On the importance of…
the voting device

Regarding security, the key element is the voting device…
(not the voting server)

🙂 = trustworthy
👹 = untrustworthy

	Voter	Voting device	Com. channels	Voting server	Dec. auth.	3rd-party
Verifiability	🙂	🙂	👹	👹	👹	🙂
Confidentiality	🙂	🙂	👹	👹	🙂	🙂

It's the unique trustworthy component

Now, the voting client is a Javascript program provided by the server…

➡ need to find a solution to make it really trustworthy? (transparency, audibility…)
➡ ensure cast-as-intended?

On the importance of…
the eligibility

Today, authentication is ensured by an untrustworthy server and an (almost) inaccessible signing sheet….

On the importance of…
the eligibility

Today, authentication is ensured by an untrustworthy server and an (almost) inaccessible signing sheet….

3 authentication element:

- a login sent by the service provider Orange by email
- a password sent by the service provider mTarget
- an activation code sent on-the-flight by Orange too

On the importance of…
the eligibility

Today, authentication is ensured by an untrustworthy server and an (almost) inaccessible signing sheet….

3 authentication element:

- a login sent by the service provider Orange by email
- a password sent by the service provider mTarget
- an activation code sent on-the-flight by Orange too

But a ballot contains none of them… the voting server can vote for absentees…

On the importance of…
the eligibility

Today, authentication is ensured by an untrustworthy server and an (almost) inaccessible signing sheet….

3 authentication element:

- a login sent by the service provider Orange by email
- a password sent by the service provider mTarget
- an activation code sent on-the-flight by Orange too

But a ballot contains none of them… the voting server can vote for absentees…

Can we improve the protocol to prevent such a weakness? Yes, we think so!
(but we have no solution to present for now…)

On the importance of…
the literature

the system suffers from well-known vulnerabilities…

On the importance of…
the literature

the system suffers from well-known vulnerabilities…

A lack of elements in the ZKPs contexts leads to attacks…

- our vote secrecy attacks
- Cortier and Smyth attack (2011) to break verifiability and vote secrecy
- (maybe) Cortier, Gaudry and Yang attack (2020) to break verifiability

On the importance of…
the literature

the system suffers from well-known vulnerabilities…

A lack of elements in the ZKPs contexts leads to attacks…

- our vote secrecy attacks
- Cortier and Smyth attack (2011) to break verifiability and vote secrecy
- (maybe) Cortier, Gaudry and Yang attack (2020) to break verifiability

Fixes are really easy to implement!

On the importance of…
the literature

the system suffers from well-known vulnerabilities…

A lack of elements in the ZKPs contexts leads to attacks…

- our vote secrecy attacks
- Cortier and Smyth attack (2011) to break verifiability and vote secrecy
- (maybe) Cortier, Gaudry and Yang attack (2020) to break verifiability

Fixes are really easy to implement!

No weeding makes ballot replay attacks possible…

- an attacker can replay Alice's ballot to bias the result and learn Alice's choice
- impact recently studied by Mestel *et. al.* (2022)

On the importance of…
the literature

the system suffers from well-known vulnerabilities…

A lack of elements in the ZKPs contexts leads to attacks…

- our vote secrecy attacks
- Cortier and Smyth attack (2011) to break verifiability and vote secrecy
- (maybe) Cortier, Gaudry and Yang attack (2020) to break verifiability

✔ **Fixes are really easy to implement!**

No weeding makes ballot replay attacks possible…

- an attacker can replay Alice's ballot to bias the result and learn Alice's choice
- impact recently studied by Mestel *et. al.* (2022)

✔ **Everything is in place to make ballot weeding…**
but they weren't aware of…

Summary

We provide the first public and comprehensive specification of the protocol

We show that the system fails to ensure verifiability and vote secrecy under a reasonable threat model:

- assumes a channel attacker only
- 6 attacks, some of them being completely undetectable

We propose fixes for each attack and recall well-known vulnerability and fixes of the literature that the protocol should implement.

Some of our fixes is will be implemented for future elections,
others will depend on the timeline…

Hope for the future

We hope our recommandations will be taken into account for the next public tender…

- define a clearer threat model
- pay attention to the threats and vulnerabilities we pointed out
- push for more transparency, in particular regarding the voting device

Hope for the future

We hope our recommandations will be taken into account for the next public tender…

- define a clearer threat model
- pay attention to the threats and vulnerabilities we pointed out
- push for more transparency, in particular regarding the voting device

Still open questions to improve the system:

- **Eligibility:** develop new techniques or convince authorities to use existing ones…?
- **Cast-as-intended:** random audits or plaintext verification don't seem acceptable… what can we do?
- **Vote secrecy:** 4 out of 16 is not acceptable… can we do better?

Hope for the future

We hope our recommandations will be taken into account for the next public tender…

- define a clearer threat model
- pay attention to the threats and vulnerabilities we pointed out
- push for more transparency, in particular regarding the voting device

Still open questions to improve the system:

- **Eligibility:** develop new techniques or convince authorities to use existing ones…?
- **Cast-as-intended:** random audits or plaintext verification don't seem acceptable… what can we do?
- **Vote secrecy:** 4 out of 16 is not acceptable… can we do better?

Thank you!