

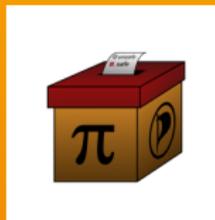
II-Vote

Sicherheit, Verbesserungen

Thomas Bruderer, Stefan Thöni, Simon Rupf

Piratenpartei Schweiz

26. Mai 2006



piratenpartei

Index

- 1 Inhalt
 - Titel
 - Index

Index

- 1 Inhalt
 - Titel
 - Index
- 2 Sicherheit
 - Schwächen Zertifikate
 - Schwächen Abstimmungen
 - Schwächen Kryptographie
 - Schlussfolgerung

Index

- 1 Inhalt
 - Titel
 - Index
- 2 Sicherheit
 - Schwächen Zertifikate
 - Schwächen Abstimmungen
 - Schwächen Kryptographie
 - Schlussfolgerung
- 3 Verbesserungen
 - Fingerprints
 - Klarere Regeln
 - Besser Benutzbar

Index

- 1 Inhalt
 - Titel
 - Index
- 2 Sicherheit
 - Schwächen Zertifikate
 - Schwächen Abstimmungen
 - Schwächen Kryptographie
 - Schlussfolgerung
- 3 Verbesserungen
 - Fingerprints
 - Klarere Regeln
 - Besser Benutzbar
- 4 Neuer Client
 - Circle

Kategorie 1 - Erschleichen von Zertifikaten

- Notare werden über die Identität getäuscht

Kategorie 1 - Erschleichen von Zertifikaten

- Notare werden über die Identität getäuscht
- Notare sind korrupt

Kategorie 1 - Erschleichen von Zertifikaten

- Notare werden über die Identität getäuscht
- Notare sind korrupt
- Die Unterschriften von Notaren sind gefälscht

Kategorie 1 - Erschleichen von Zertifikaten

- Notare werden über die Identität getäuscht
- Notare sind korrupt
- Die Unterschriften von Notaren sind gefälscht
- Der Aktuar ist korrupt

Kategorie 1 - Erschleichen von Zertifikaten

- Notare werden über die Identität getäuscht
- Notare sind korrupt
- Die Unterschriften von Notaren sind gefälscht
- Der Aktuar ist korrupt
- Pirat A überlässt Pirat B das Zertifikat bzw. den privaten Schlüssel

Kategorie 1 - Erschleichen von Zertifikaten

- Notare werden über die Identität getäuscht
- Notare sind korrupt
- Die Unterschriften von Notaren sind gefälscht
- Der Aktuar ist korrupt
- Pirat A überlässt Pirat B das Zertifikat bzw. den privaten Schlüssel
- Pirat B stiehlt das Zertifikat bzw. den privaten Schlüssel von Pirat A

Kategorie 1 - Erschleichen von Zertifikaten

- Notare werden über die Identität getäuscht
- Notare sind korrupt
- Die Unterschriften von Notaren sind gefälscht
- Der Aktuar ist korrupt
- Pirat A überlässt Pirat B das Zertifikat bzw. den privaten Schlüssel
- Pirat B stiehlt das Zertifikat bzw. den privaten Schlüssel von Pirat A

Kategorie 1 - Erschleichen von Zertifikaten

- Notare werden über die Identität getäuscht
- Notare sind korrupt
- Die Unterschriften von Notaren sind gefälscht
- Der Aktuar ist korrupt
- Pirat A überlässt Pirat B das Zertifikat bzw. den privaten Schlüssel
- Pirat B stiehlt das Zertifikat bzw. den privaten Schlüssel von Pirat A

Kategorie 1 - Erschleichen von Zertifikaten

- Notare werden über die Identität getäuscht
- Notare sind korrupt
- Die Unterschriften von Notaren sind gefälscht
- Der Aktuar ist korrupt
- Pirat A überlässt Pirat B das Zertifikat bzw. den privaten Schlüssel
- Pirat B stiehlt das Zertifikat bzw. den privaten Schlüssel von Pirat A

Kategorie 1 - Erschleichen von Zertifikaten

- Notare werden über die Identität getäuscht
- Notare sind korrupt
- Die Unterschriften von Notaren sind gefälscht
- Der Aktuar ist korrupt
- Pirat A überlässt Pirat B das Zertifikat bzw. den privaten Schlüssel
- Pirat B stiehlt das Zertifikat bzw. den privaten Schlüssel von Pirat A

Kategorie 1 - Erschleichen von Zertifikaten

- Notare werden über die Identität getäuscht
- Notare sind korrupt
- Die Unterschriften von Notaren sind gefälscht
- Der Aktuar ist korrupt
- Pirat A überlässt Pirat B das Zertifikat bzw. den privaten Schlüssel
- Pirat B stiehlt das Zertifikat bzw. den privaten Schlüssel von Pirat A

Kategorie 1 - Erschleichen von Zertifikaten

- Notare werden über die Identität getäuscht
- Notare sind korrupt
- Die Unterschriften von Notaren sind gefälscht
- Der Aktuar ist korrupt
- Pirat A überlässt Pirat B das Zertifikat bzw. den privaten Schlüssel
- Pirat B stiehlt das Zertifikat bzw. den privaten Schlüssel von Pirat A



Kategorie 2 - Sabotage von Abstimmungen

- DoS auf den Server



Kategorie 2 - Sabotage von Abstimmungen

- DoS auf den Server
- Autoritäten weigert sich eine Abstimmung zu starten

Kategorie 2 - Sabotage von Abstimmungen

- DoS auf den Server
- Autoritäten weigert sich eine Abstimmung zu starten
- Mindestens 2 Autoritäten weigern sich die Abstimmung zu entschlüsseln

Kategorie 2 - Sabotage von Abstimmungen

- DoS auf den Server
- Autoritäten weigert sich eine Abstimmung zu starten
- Mindestens 2 Autoritäten weigern sich die Abstimmung zu entschlüsseln
- Mindestens 4 Autoritäten entschlüsseln einzelne Stimmen

Kategorie 2 - Sabotage von Abstimmungen

- DoS auf den Server
- Autoritäten weigert sich eine Abstimmung zu starten
- Mindestens 2 Autoritäten weigern sich die Abstimmung zu entschlüsseln
- Mindestens 4 Autoritäten entschlüsseln einzelne Stimmen

Kategorie 2 - Sabotage von Abstimmungen

- DoS auf den Server
- Autoritäten weigert sich eine Abstimmung zu starten
- Mindestens 2 Autoritäten weigern sich die Abstimmung zu entschlüsseln
- Mindestens 4 Autoritäten entschlüsseln einzelne Stimmen

Kategorie 2 - Sabotage von Abstimmungen

- DoS auf den Server
- Autoritäten weigert sich eine Abstimmung zu starten
- Mindestens 2 Autoritäten weigern sich die Abstimmung zu entschlüsseln
- Mindestens 4 Autoritäten entschlüsseln einzelne Stimmen



Kategorie 2 - Sabotage von Abstimmungen

- DoS auf den Server
- Autoritäten weigert sich eine Abstimmung zu starten
- Mindestens 2 Autoritäten weigern sich die Abstimmung zu entschlüsseln
- Mindestens 4 Autoritäten entschlüsseln einzelne Stimmen



Kategorie 3 - Kryptographische Schwächen

- Es sind Bugs in den Genutzen Libraries vorhanden



Kategorie 3 - Kryptographische Schwächen

- Es sind Bugs in den Genutzen Libraries vorhanden
- Es sind Bugs in II-Vote oder Circle vorhanden

Kategorie 3 - Kryptographische Schwächen

- Es sind Bugs in den Genutzen Libraries vorhanden
- Es sind Bugs in II-Vote oder Circle vorhanden
- Der Diskrete Logarithmus kann Effizient berechnet werden

Kategorie 3 - Kryptographische Schwächen

- Es sind Bugs in den Genutzen Libraries vorhanden
- Es sind Bugs in II-Vote oder Circle vorhanden
- Der Diskrete Logarithmus kann Effizient berechnet werden
- Schlechter Zufall

Kategorie 3 - Kryptographische Schwächen

- Es sind Bugs in den Genutzen Libraries vorhanden
- Es sind Bugs in II-Vote oder Circle vorhanden
- Der Diskrete Logarithmus kann Effizient berechnet werden
- Schlechter Zufall

Kategorie 3 - Kryptographische Schwächen

- Es sind Bugs in den Genutzen Libraries vorhanden
- Es sind Bugs in II-Vote oder Circle vorhanden
- Der Diskrete Logarithmus kann Effizient berechnet werden
- Schlechter Zufall

Kategorie 3 - Kryptographische Schwächen

- Es sind Bugs in den Genutzen Libraries vorhanden
- Es sind Bugs in II-Vote oder Circle vorhanden
- Der Diskrete Logarithmus kann Effizient berechnet werden
- Schlechter Zufall

Kategorie 3 - Kryptographische Schwächen

- Es sind Bugs in den Genutzen Libraries vorhanden
- Es sind Bugs in II-Vote oder Circle vorhanden
- Der Diskrete Logarithmus kann Effizient berechnet werden
- Schlechter Zufall



Das ist ja furchtbar...

Ich will es absolut Sicher haben

Wenn es soviele Möglichkeiten gibt - dann werden wir das ja nie Sicher haben.

...oder auch nicht

Fairer Vergleich

Absolute Sicherheits gibt es nirgends. Auch bei richtigen Abstimmungen kann man manipulieren, auch an einer PV, und erst Recht bei Nationalratswahlen. Nur wenn man fair vergleicht macht elektronische Abstimmungen Sinn.

Neues Sicherheitsmerkmal

QR-Code



- Menschliche Fehler ausschliessen
- Überprüfung der Echtheit der Unterschriften

Art. 14

Art. 14 (neu)

Wer versucht bei II-Vote zu betrügen ... begeht eine schwere Missachtung der Vereinsgrundsätze.

Fortschritte...

- Mehr Notare www.piratenpartei.ch/Notare
- Adresse auf dem Zertifikat
- Alternative Oberfläche
- Videoerklärungen

Die neue Benutzer-Oberfläche

Presentation



The screenshot shows the main interface of the Circle π-vote application. On the left is a 3D ballot box with a red top and a brown body. The Greek letter π is on the front, and a circular logo with a stylized 'P' is on the side. A ballot is being inserted into the top. To the right of the box, the text reads: **Circle**, **π-vote**, and Version 1.1.0.0. Below this is the logo of the Piratenpartei (a circle with a stylized 'P') followed by the text **piratenpartei** and www.piratenpartei.ch. At the bottom left, there is a small text prompt: "Lade Zertifikatsspeicher herunter." and a progress bar.