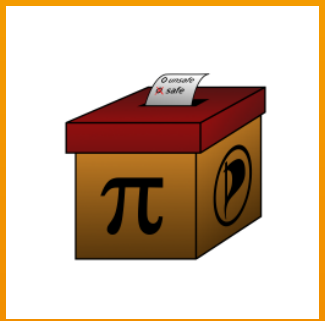
# Π-Vote

## Sicherheit, Verbesserungen

Thomas Bruderer, Stefan Thöni, Simon Rupf

Piratenpartei Schweiz

26. Mai 2006



piratenpartei

# Index



piratenpartei

# Index



piratenpartei

# Index



piratenpartei

# Index



piratenpartei

# Kategorie 1 - Erschleichen von Zertifikaten

- Notare werden über die Identität getäuscht

piratenpartei

# Kategorie 1 - Erschleichen von Zertifikaten

- Notare werden über die Identität getäuscht
- Notare sind korrupt

piratenpartei

# Kategorie 1 - Erschleichen von Zertifikaten

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

piratenpartei

# Kategorie 1 - Erschleichen von Zertifikaten

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

piratenpartei

# 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

piratenpartei

# 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 stielht das Zertifikat bzw. den privaten Schlüssel von Pirat A

piratenpartei

# 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 stielht das Zertifikat bzw. den privaten Schlüssel von Pirat A

piratenpartei

# 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 stielht das Zertifikat bzw. den privaten Schlüssel von Pirat A

piratenpartei

# 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 stielht das Zertifikat bzw. den privaten Schlüssel von Pirat A

piratenpartei

# 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 stielht das Zertifikat bzw. den privaten Schlüssel von Pirat A

piratenpartei

# 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 stielht das Zertifikat bzw. den privaten Schlüssel von Pirat A

piratenpartei

# 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 stielht das Zertifikat bzw. den privaten Schlüssel von Pirat A

piratenpartei

# Kategorie 2 - Sabotage von Abstimmungen

- DoS auf den Server

piratenpartei

# Kategorie 2 - Sabotage von Abstimmungen

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

piratenpartei

# Kategorie 2 - Sabotage von Abstimmungen

- DoS auf den Server
- Authoritäten weigert sich eine Abstimmung zu starten
- Mindestens 2 Authoriäten weigern sich die Abstimmung zu entschüsseln

piratenpartei

# Kategorie 2 - Sabotage von Abstimmungen

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

piratenpartei

# Kategorie 2 - Sabotage von Abstimmungen

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

piratenpartei

# Kategorie 2 - Sabotage von Abstimmungen

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

piratenpartei

# Kategorie 2 - Sabotage von Abstimmungen

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

piratenpartei

# Kategorie 2 - Sabotage von Abstimmungen

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

piratenpartei

# Kategorie 3 - Kryptographische Schwächen

- Es sind Bugs in den Genutzen Libraries vorhanden

piratenpartei

# Kategorie 3 - Kryptographische Schwächen

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

piratenpartei

# Kategorie 3 - Kryptographische Schwächen

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

piratenpartei

# Kategorie 3 - Kryptographische Schwächen

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

piratenpartei

# Kategorie 3 - Kryptographische Schwächen

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

piratenpartei

# Kategorie 3 - Kryptographische Schwächen

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

piratenpartei

# Kategorie 3 - Kryptographische Schwächen

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

piratenpartei

# Kategorie 3 - Kryptographische Schwächen

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

piratenpartei

# Das ist ja furchtbar...

## Ich will es absolut Sicher haben

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

piratenpartei

# ...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.

piratenpartei

# Neues Sicherheitsmerkmal

## QR-Code

- Menschliche Fehler ausschliessen
- Überprüfung der Echtheit der Unterschriften

piratenpartei

# Art. 14

## Art. 14 (neu)

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

piratenpartei

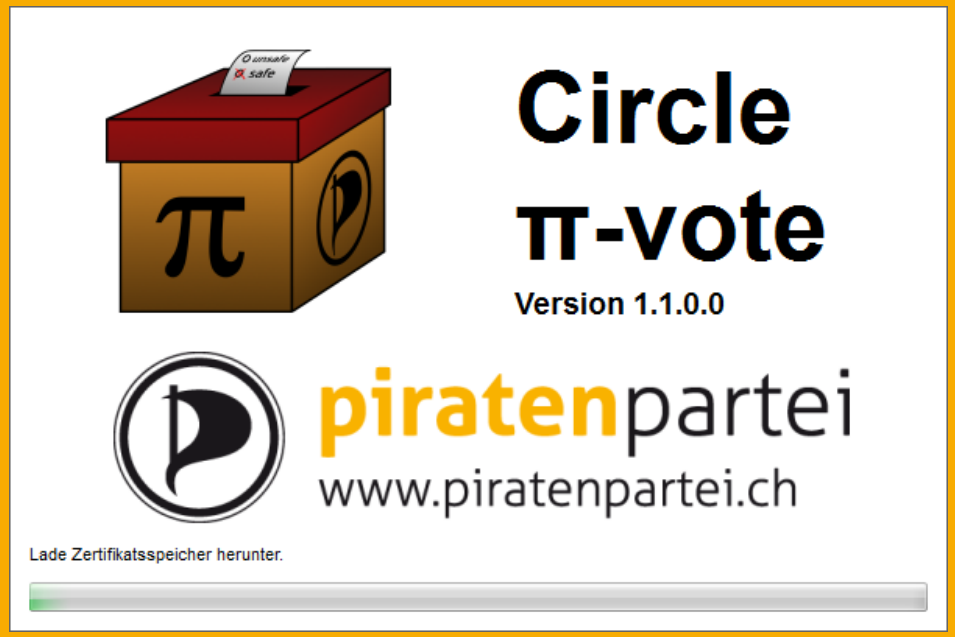
# Fortschritte...

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

piratenpartei

# Die neue Benutzer-Oberfläche

## Presentation




piratenpartei