TECHNISCHE UNIVERSITÄT DRESDEN

PrimeLife

Fakultät Informatik Institut für Systemarchitektur, Lehrstuhl für Datenschutz und Datensicherheit

E-Voting Crashkurs

Was an diesem verf***ten E-Voting so unheimlich cool ist. . .

Benjamin.Kellermann@tu-dresden.de
D19E 04A8 8895 020A 8DF6
0092 3501 1A32 491A 3D9C

Dresden, 16. Oktober 2010

PrimeLife is a research project funded by the European Commission's 7th Framework Programme

What the hell is E-Voting?

What the hell is E-Voting?

Vorteile

Nachteile

What the hell is E-Voting?

Vorteile

- Schnellere Auszählung

Nachteile

What the hell is E-Voting?

Vorteile

- Schnellere Auszählung
- Kostenreduktion

Nachteile

What the hell is E-Voting?

Vorteile

- Schnellere Auszählung
- Kostenreduktion

Nachteile

- Überprüfbarkeit

„Я считаю, что совершенно неважно, кто и как будет в партии голосовать; но вот что чрезвычайно важно, это – кто и как будет считать голоса.“

Иосиф Виссарионович Сталин, 1923

„Я считаю, что совершенно неважно, кто и как будет в партии голосовать; но вот что чрезвычайно важно, это – кто и как будет считать голоса.“

Иосиф Виссарионович Сталин, 1923

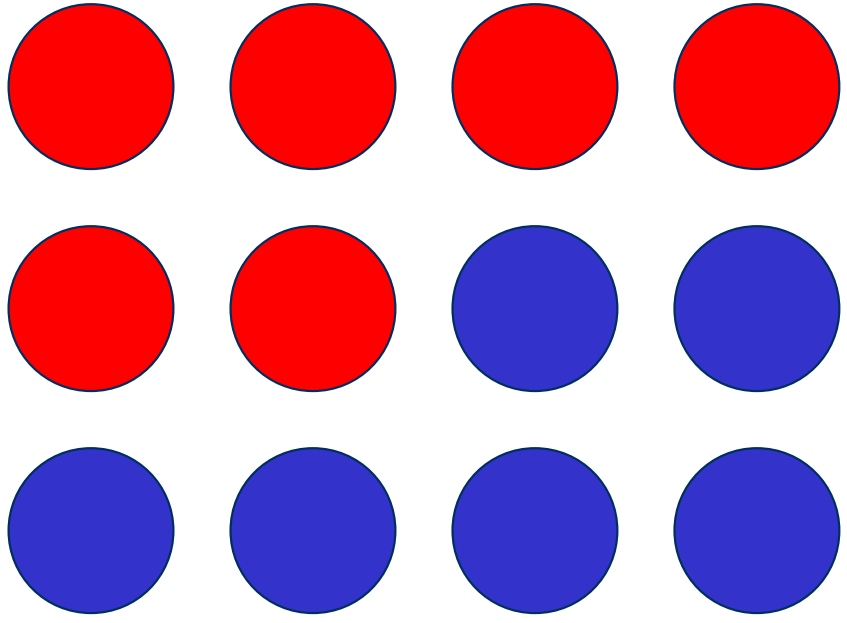
„Wer wählt entscheidet nichts, wer auszählt entscheidet alles.“

Josef Stalin, 1923
(frei übersetzt)

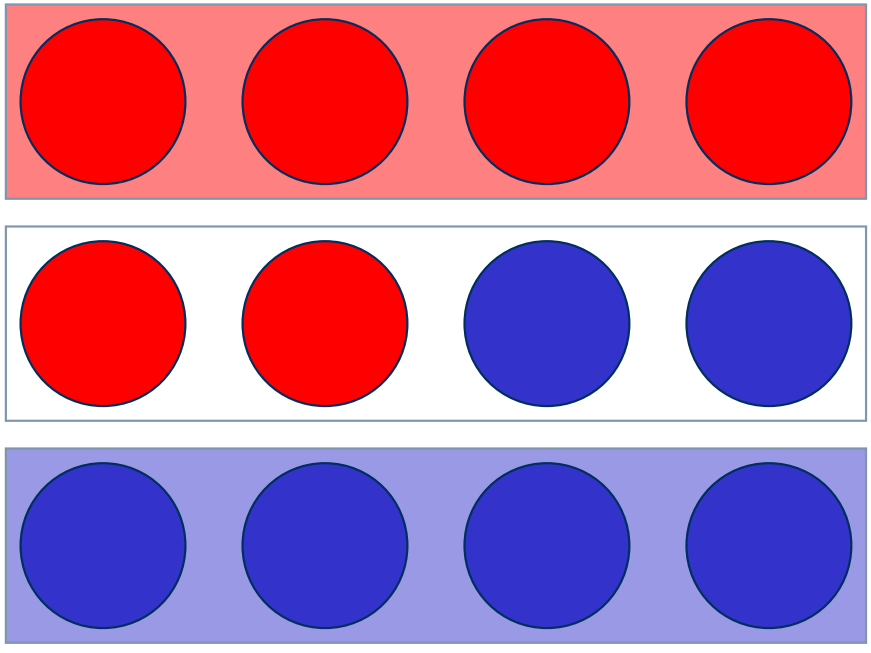
„Es muss demokratisch aussehen, aber wir müssen alles in der Hand haben.“

Walter Ulbricht, 1945

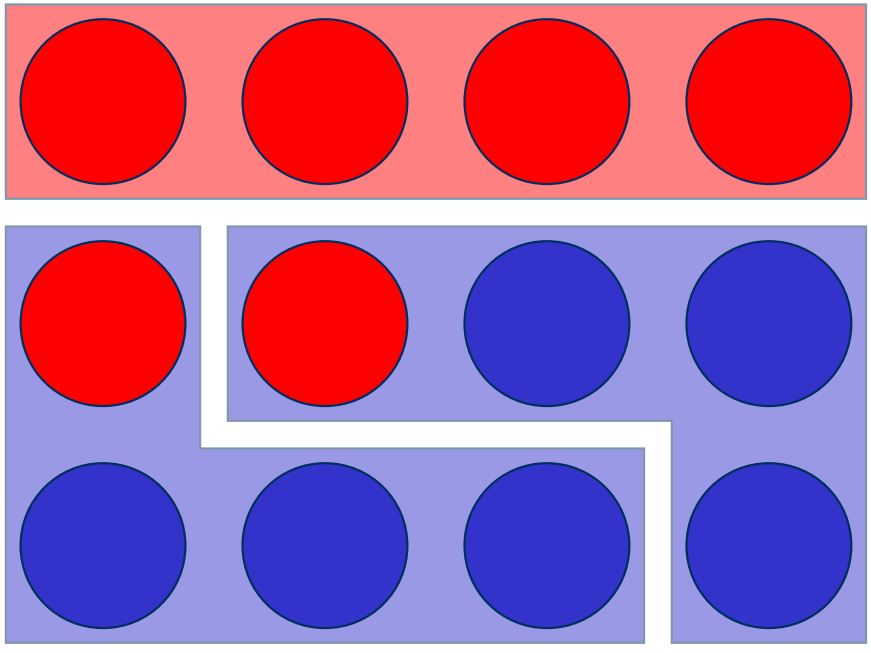
Gerrymandering



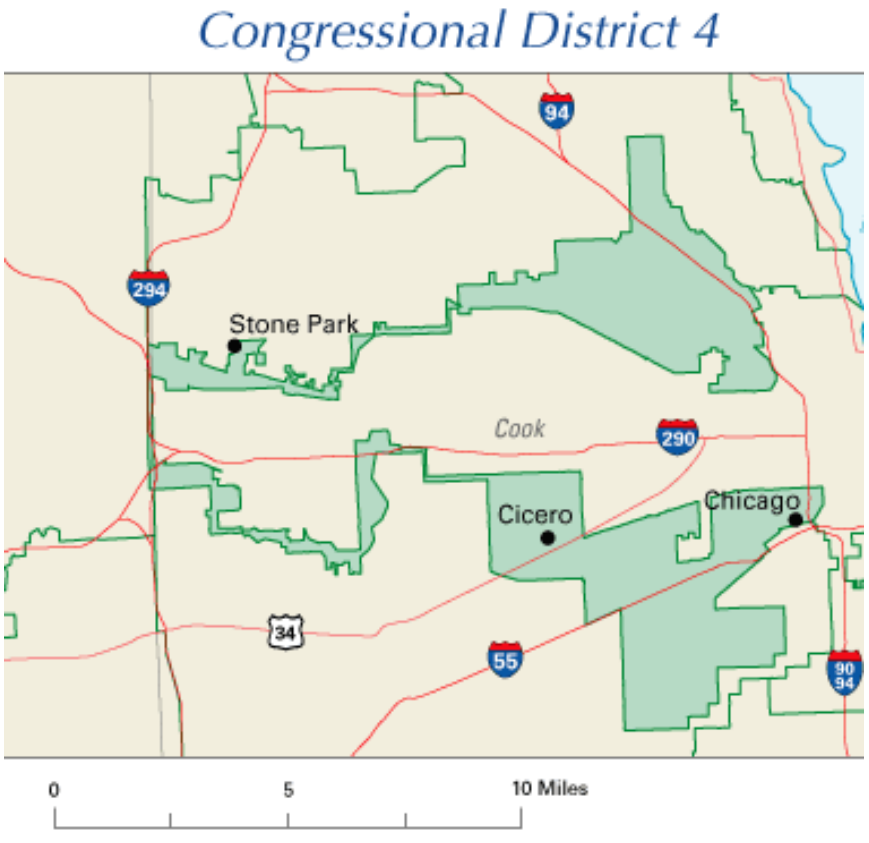
Gerrymandering



Gerrymandering



Gerrymandering



Sicherheit

Bsp: Einkaufen bei Amazon

Sicherheit

Bsp: Einkaufen bei Amazon

amazon.com →

Bitte angeben:

- Geburtsdatum
- Ausweiskopie
- EC und VISA-Nummer
- Arbeitgeber, Gehaltsnachweis
- Krankenkasse, Gesundheitszustand
- sexuelle Orientierung

Sicherheit

Bsp: Einkaufen bei Amazon

amazon.com ←

- unendlich viele Daten
- Einwilligung über Schufaauskunft und Kontoabbuchung
- Bestätigung über Kenntnis der „Kein-Rückgaberecht-Klausel“

Sicherheit

Bsp: Einkaufen bei Amazon

amazon.com

„Die Ware wird versandt, sobald die Frist für den Geldwiderruf vergangen ist.“

Sicherheit

Bsp: Einkaufen bei Amazon

amazon.com

Mehrseitige Sicherheit

Auf die Sicherheitsinteressen aller Teilnehmer wird eingegangen

Sichere Wahlen mit E-Voting?

Vorteile

- Schnellere Auszählung
- Kostenreduktion

Nachteile

- Überprüfbarkeit

Mehrseitig Sichere Wahlen

DIE LINKE. SPD CDU BÜNDNIS 90 DIE GRÜNEN FDP Die Liberalen

Mehrseitig Sichere Wahlen

Mehrseitig Sichere Wahlen

Mehrseitig Sichere Wahlen

ThreeBallot

Alice ☐ Bob ☐ Carol ☐	Alice ☐ Bob ☐ Carol ☐	Alice ☐ Bob ☐ Carol ☐
796210	496186	250105

ThreeBallot

Alice	☒	Alice	☐	Alice	☐
Bob	☐	Bob	☐	Bob	☒
Carol	☐	Carol	☐	Carol	☒
796210		496186		250105	

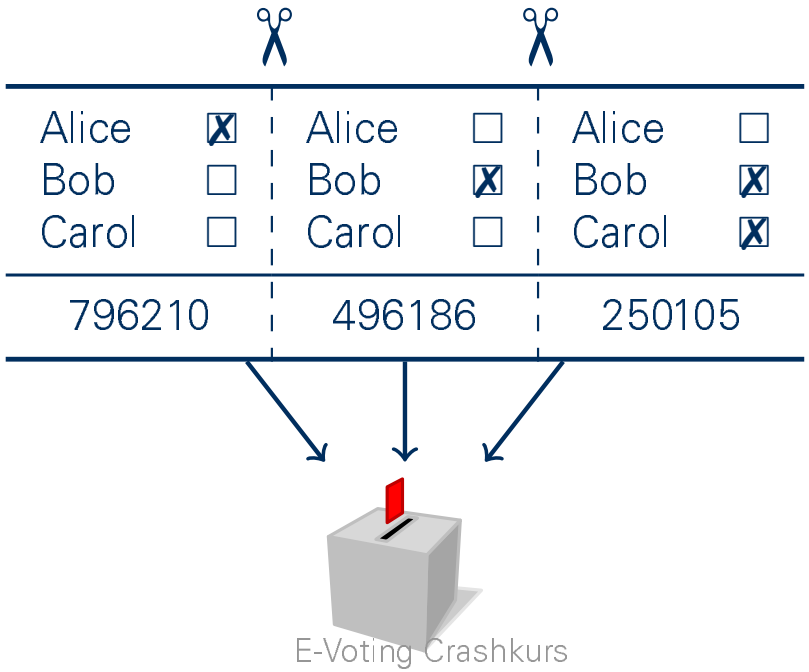
ThreeBallot

Alice	☒	Alice	☐	Alice	☐
Bob	☐	Bob	☒	Bob	☒
Carol	☐	Carol	☐	Carol	☒
796210		496186		250105	

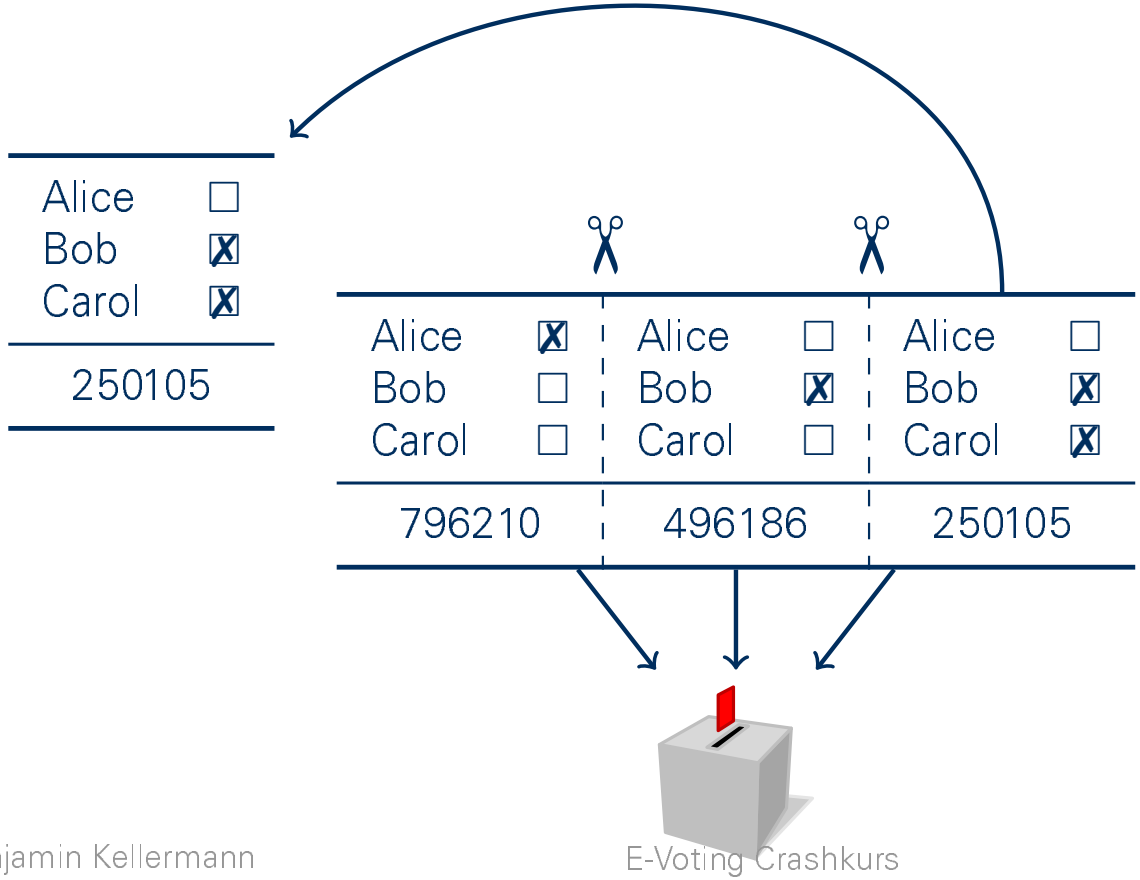
ThreeBallot

Alice	☒	Alice	☐	Alice	☐
Bob	☐	Bob	☒	Bob	☒
Carol	☐	Carol	☐	Carol	☒
796210		496186		250105	

ThreeBallot



ThreeBallot



ThreeBallot

Alice	☐
Bob	☒
Carol	☒
250105	

ThreeBallot

Alice	☐
Bob	☒
Carol	☒
250105	

Alice	☐
Bob	☐
Carol	☐
824438	

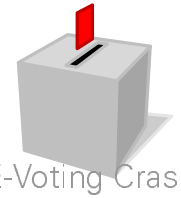
Alice	☐
Bob	☒
Carol	☒
250105	

Alice	☐
Bob	☒
Carol	☒
954315	

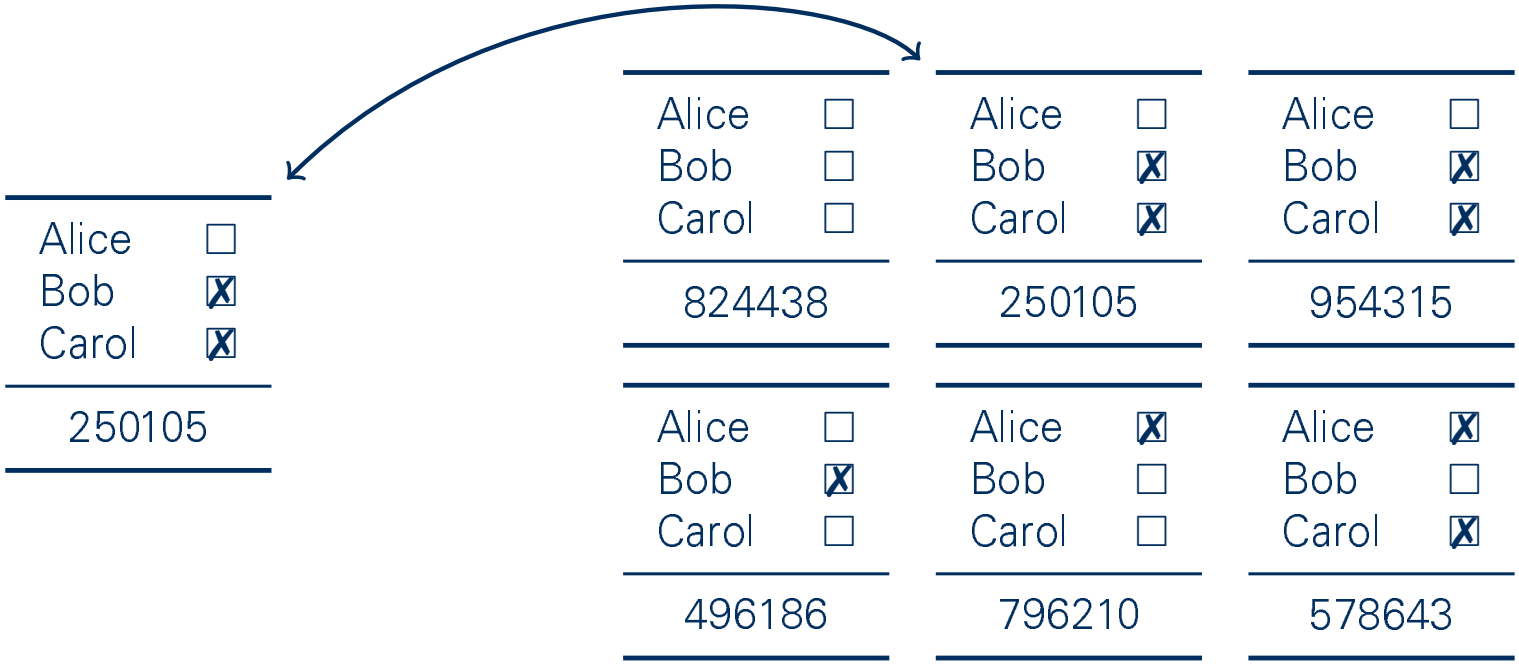
Alice	☐
Bob	☒
Carol	☐
496186	

Alice	☒
Bob	☐
Carol	☐
796210	

Alice	☒
Bob	☐
Carol	☒
578643	



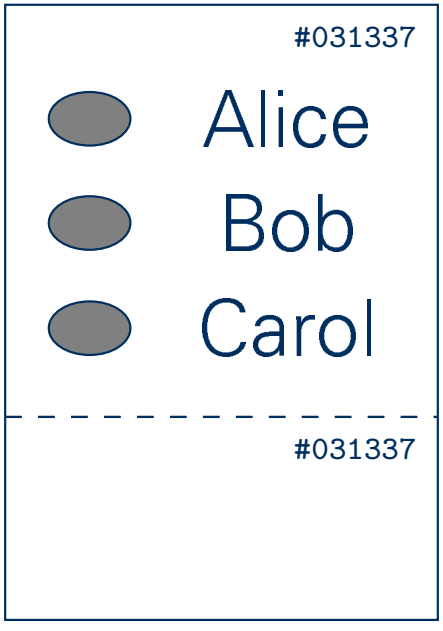
ThreeBallot



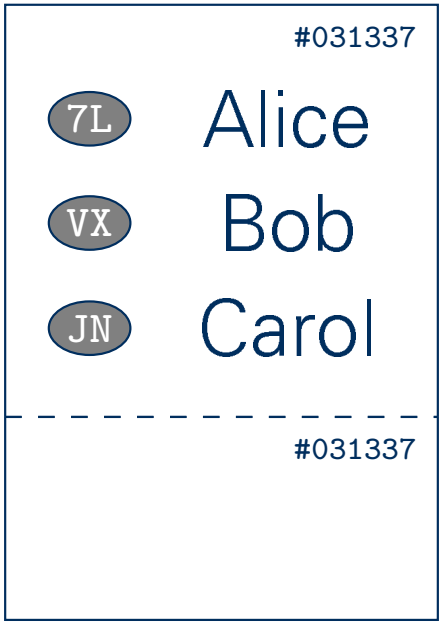
Ende-zu-Ende Überprüfung

1. Meine Stimme ist in den Ergebnisstimmen.
2. Alle Ergebnisstimmen wurden richtig zusammengezählt.

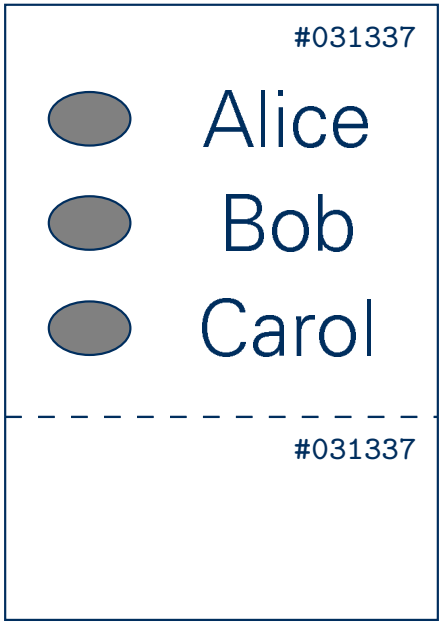
Scantegrity II



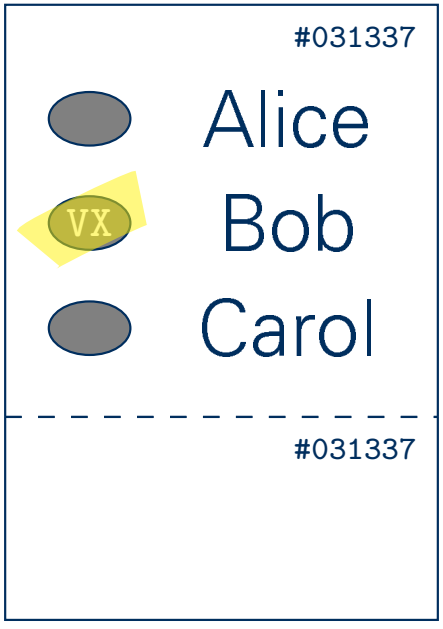
Scantegrity II



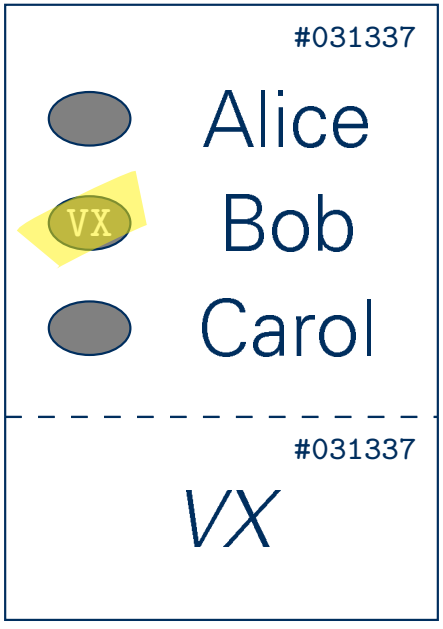
Scantegrity II



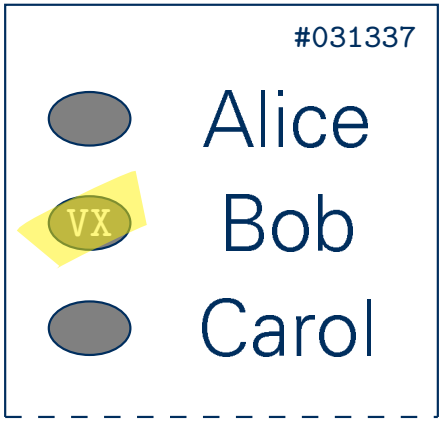
Scantegrity II

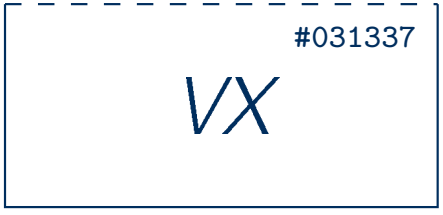


Scantegrity II

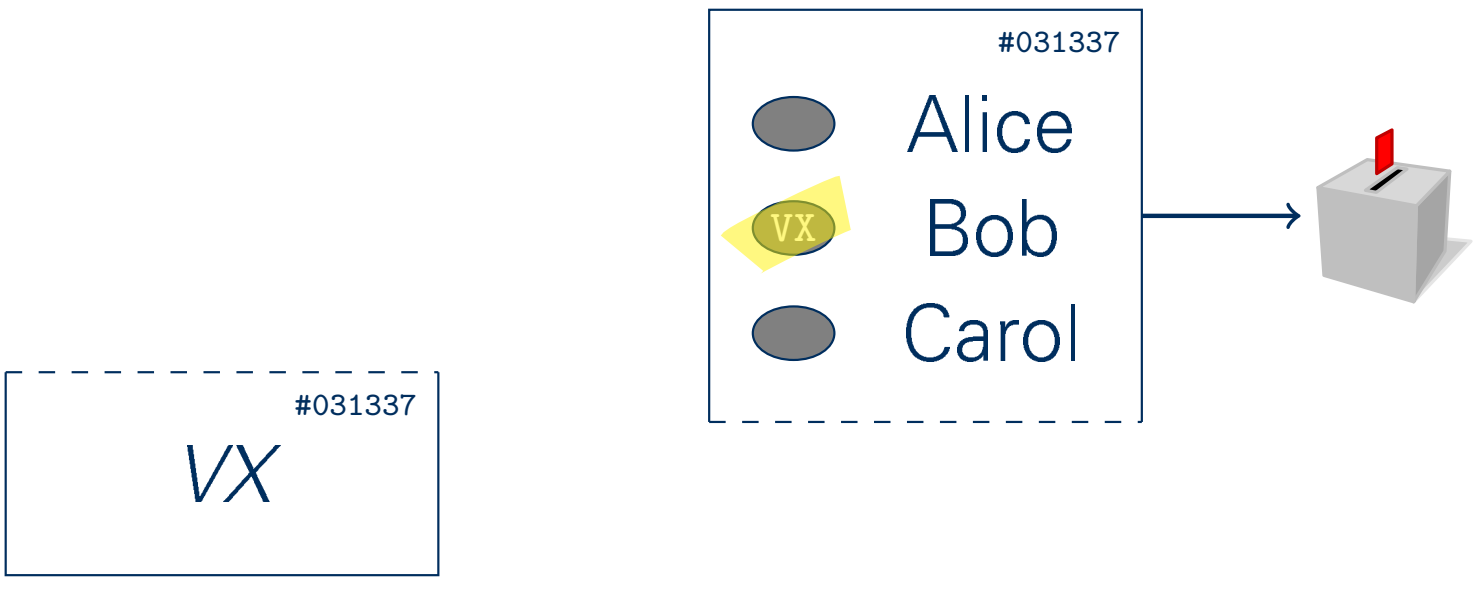


Scantegrity II

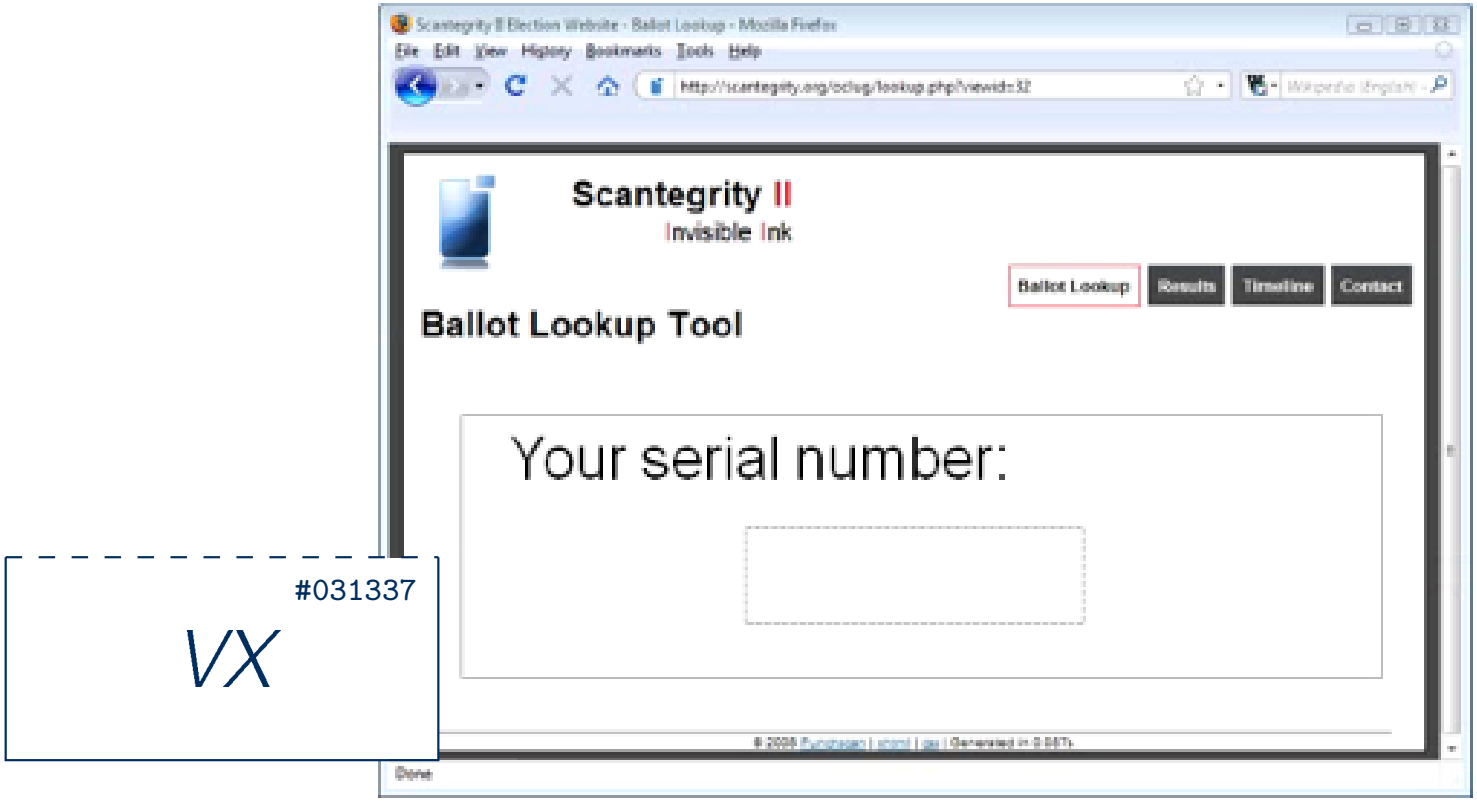




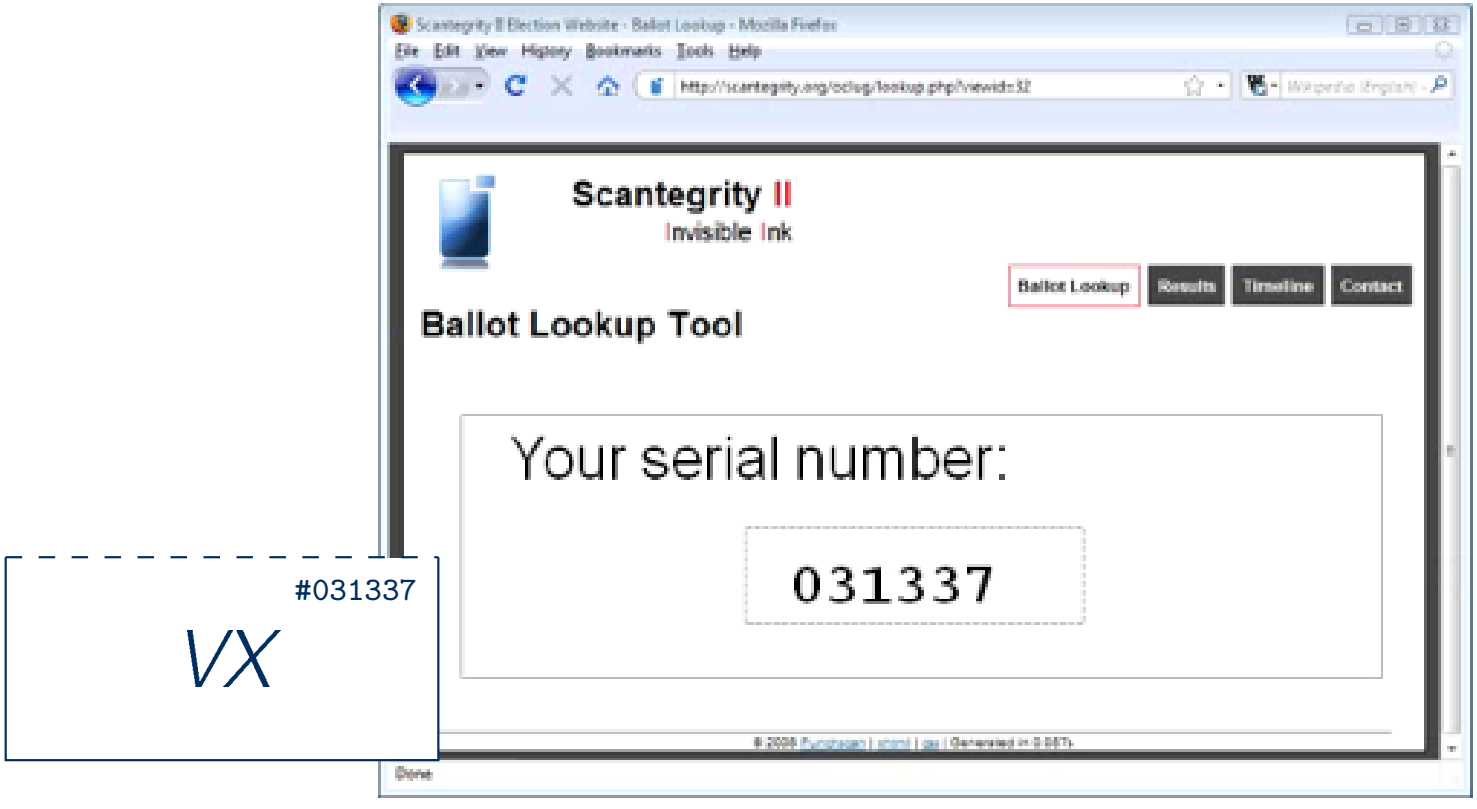
Scantegrity II



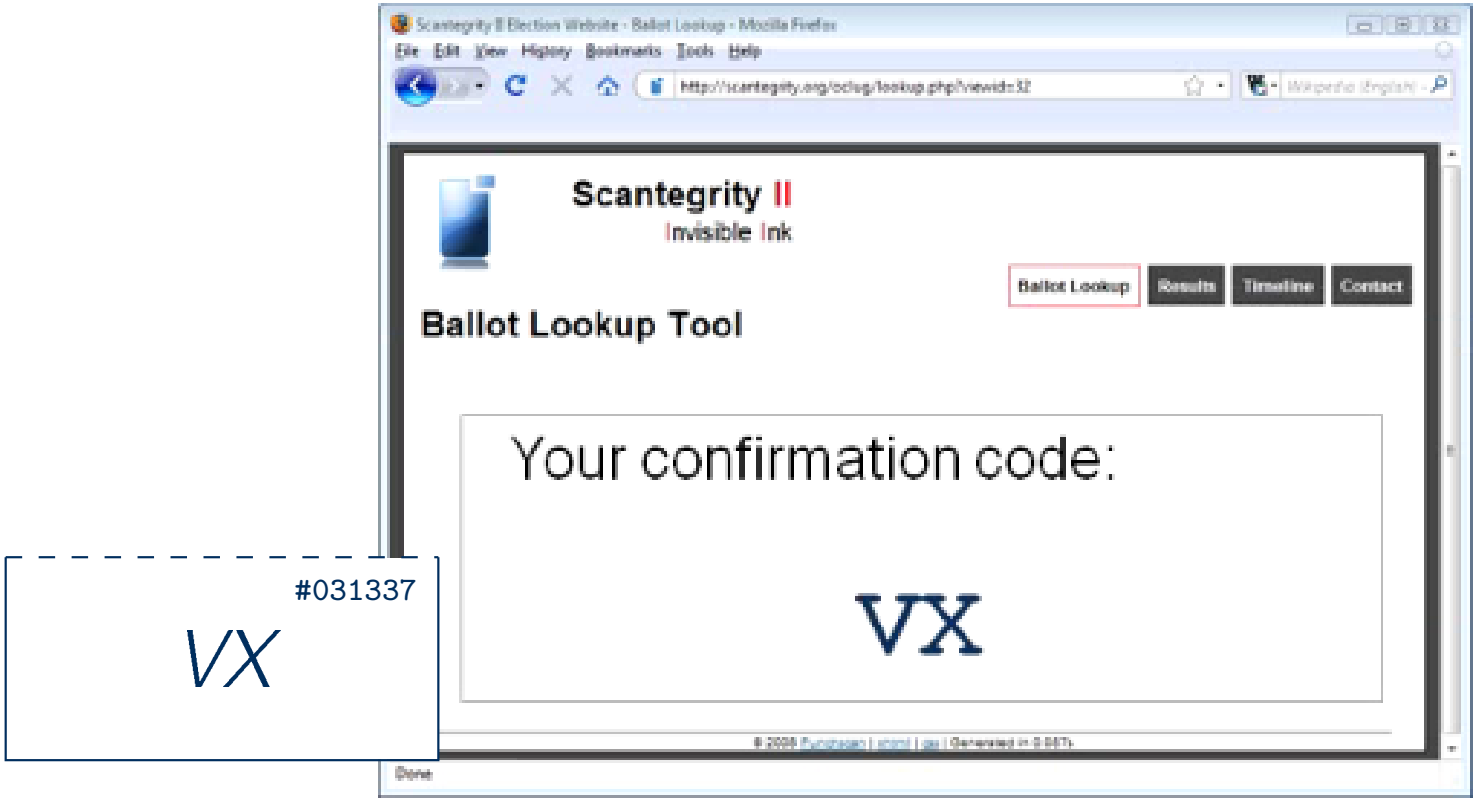
Scantegrity II



Scantegrity II



Scantegrity II



Ende-zu-Ende Überprüfung

1. Meine Stimme ist in den Ergebnisstimmen.
2. Alle Ergebnisstimmen wurden richtig zusammengezählt.

Scantegrity II – Stimmen Zählen

ID	A	B	C
#031336	XA	QB	2F
#031337	7L	VX	JN
#031338	23	FM	LI
#031339	NA	TN	B5

Scantegrity II – Stimmen Zählen

ID	A	B	C
#031336	XA	QB	2F
#031337	7L	VX	JN
#031338	23	FM	LI
#031339	NA	TN	B5

ID	α	β	γ
#031336	QB	XA	2F
#031337	VX	7L	JN
#031338	LI	FM	23
#031339	B5	NA	TN

(#031338,β)	(B,1)
(#031339,α)	(C,1)
(#031338,α)	(C,4)
(#031339,γ)	(B,4)
(#031337,γ)	(C,3)
(#031339,β)	(A,3)
(#031336,γ)	(C,2)
(#031337,β)	(A,1)
(#031338,γ)	(A,2)
(#031336,α)	(B,2)
(#031337,α)	(B,3)
(#031336,β)	(A,4)

#	A	B	C
1			
2			
3			
4			

Scantegrity II – Stimmen Zählen

ID	A	B	C
#031336	XA	QB	2F
#031337	7L	VX	JN
#031338	23	FM	LI
#031339	NA	TN	B5

ID	α	β	γ
#031336	QB	XA	2F
#031337	VX	7L	JN
#031338	LI	FM	23
#031339	B5	NA	TN

(#031338,β)	(B,1)
(#031339,α)	(C,1)
(#031338,α)	(C,4)
(#031339,γ)	(B,4)
(#031337,γ)	(C,3)
(#031339,β)	(A,3)
(#031336,γ)	(C,2)
(#031337,β)	(A,1)
(#031338,γ)	(A,2)
(#031336,α)	(B,2)
(#031337,α)	(B,3)
(#031336,β)	(A,4)

#	A	B	C
1			
2			
3		✗	
4			

Scantegrity II – Stimmen Zählen

ID	A	B	C
#031336	XA	QB	2F
#031337	7L	VX	JN
#031338	23	FM	LI
#031339	NA	TN	B5

ID	α	β	γ

#	A	B	C
1			
2			
3			
4			

Scantegrity II – Stimmen Zählen

ID	A	B	C
#031336	XA	QB	2F
#031337	7L	VX	JN
#031338	23	FM	LI
#031339	NA	TN	B5

ID	α	β	γ
#031336		XA	
#031337	VX		
#031338	LI	FM	23
#031339		NA	

#	A	B	C
1			
2			
3			
4			

Scantegrity II – Stimmen Zählen

ID	A	B	C
#031336	XA	QB	2F
#031337	7L	VX	JN
#031338	23	FM	LI
#031339	NA	TN	B5

ID	α	β	γ	
#031336		XA		✗
#031337	VX			
#031338	LI	FM	23	
#031339		NA		✗
				✗

#	A	B	C
1			
2			
3	✗	✗	
4	✗		

Scantegrity II – Stimmen Zählen

ID	A	B	C
#031336	XA	QB	2F
#031337	7L	VX	JN
#031338	23	FM	LI
#031339	NA	TN	B5

ID	α	β	γ
#031336		XA	
#031337	VX		
#031338	LI	FM	23
#031339		NA	

(#031338,β)	(B,1)	
(#031338,α)	(C,4)	
		✗
(#031338,γ)	(A,2)	
		✗
		✗

#	A	B	C
1			
2			
3	✗	✗	
4	✗		

Scantegrity II – Stimmen Zählen

ID	A	B	C
#031336	XA	QB	2F
#031337	7L	VX	JN
#031338	23	FM	LI
#031339	NA	TN	B5

ID	α	β	γ
#031336		XA	
#031337	VX		
#031338	LI	FM	23
#031339		NA	

(#031338,β)	(B,1)	
(#031339,α)		
(#031338,α)	(C,4)	
(#031339,γ)		
	(C,3)	
(#031339,β)		✗
(#031336,γ)		
	(A,1)	
(#031338,γ)	(A,2)	
(#031336,α)		
	(B,3)	✗
	(A,4)	✗

#	A	B	C
1			
2			
3	✗	✗	
4	✗		

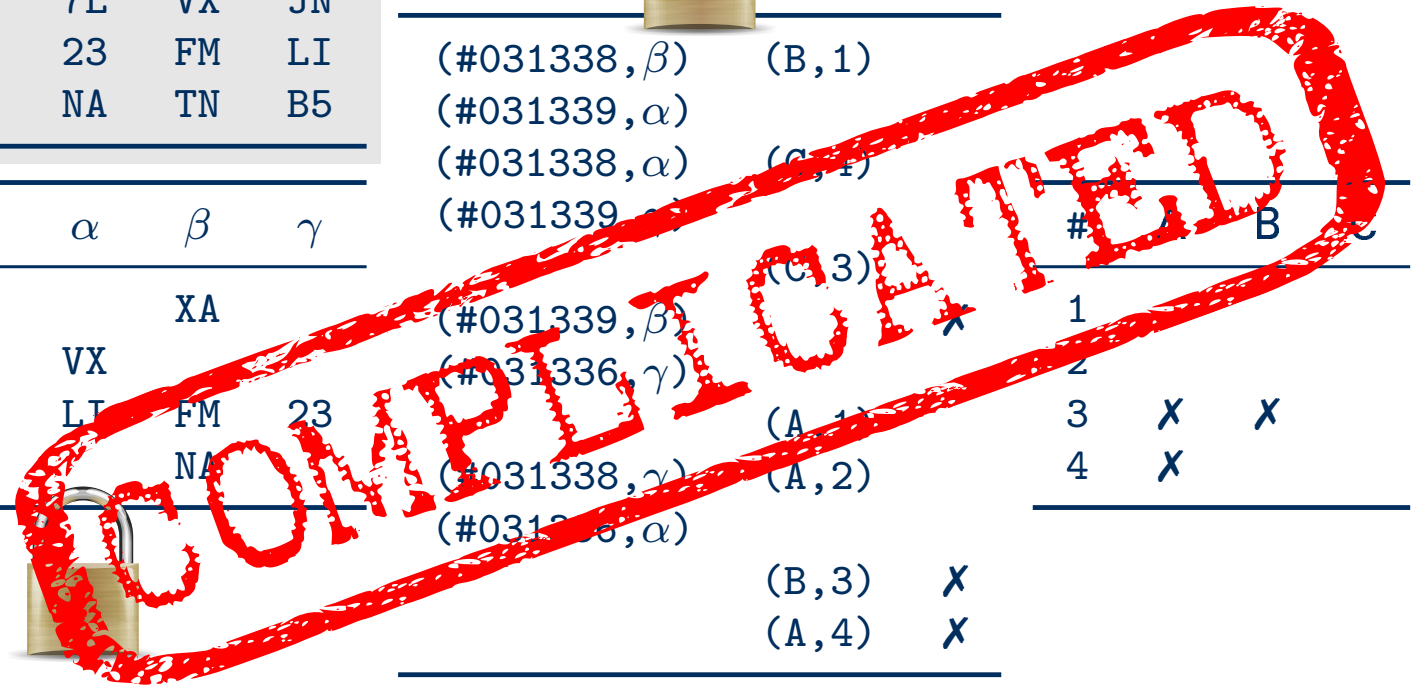
Scantegrity II – Stimmen Zählen

ID	A	B	C
#031336	XA	QB	2F
#031337	7L	VX	JN
#031338	23	FM	LI
#031339	NA	TN	B5

ID	α	β	γ
#031336		XA	
#031337	VX		
#031338	LI	FM	23
#031339		NA	

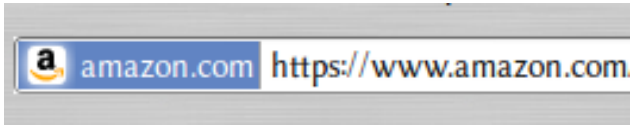
(#031338,β)	(B,1)
(#031339,α)	
(#031338,α)	(C,1)
(#031339,	
	(C,3)
(#031339,β)	✗
(#031336,γ)	
	(A,1)
(#031338,γ)	(A,2)
(#031 ,α)	
	(B,3) ✗
	(A,4) ✗

#	A	B	C
1			
2			
3	✗	✗	
4	✗		



Intermezzo

- Wer hat einen dieser Dienste schon benutzt?

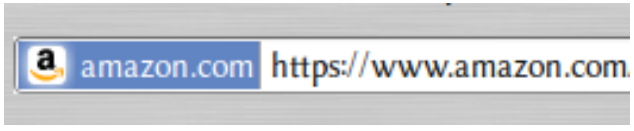


GnuPG

PGP

Intermezzo

- Wer hat einen dieser Dienste schon benutzt?
- Wer weiß, welche Algorithmen für die Sicherheit benutzt werden?



GnuPG

PGP

Intermezzo

- Wer hat einen dieser Dienste schon benutzt?
- Wer weiß, welche Algorithmen für die Sicherheit benutzt werden?
- Wer weiß, wie RSA/ElGamal funktioniert?

GnuPG

PGP

Intermezzo

- Wer hat einen dieser Dienste schon benutzt?
- Wer weiß, welche Algorithmen für die Sicherheit benutzt werden?
- Wer weiß, wie RSA/ElGamal funktioniert?
- Wer hat den Quellcode dieser System schon gegen RSA/ElGamal verglichen?

GnuPG

PGP

Intermezzo

- Wer hat einen dieser Dienste schon benutzt?
- Wer weiß, welche Algorithmen für die Sicherheit benutzt werden?
- Wer weiß, wie RSA/ElGamal funktioniert?
- Wer hat den Quellcode dieser System schon gegen RSA/ElGamal verglichen?

GnuPG

PGP

- Vertrauen kommt durch externe Validierung

Zusammenfassung

Vorteile

- Schnellere Auszählung
- Kostenreduktion

Nachteile

- Überprüfbarkeit

Zusammenfassung

Machthaber überprüfen

TECHNISCHE UNIVERSITÄT DRESDEN

PrimeLife

Fakultät Informatik Institut für Systemarchitektur, Lehrstuhl für Datenschutz und Datensicherheit

Diskussion!

Was meint ihr?

Benjamin.Kellermann@tu-dresden.de
D19E 04A8 8895 020A 8DF6
0092 3501 1A32 491A 3D9C

Dresden, 16. Oktober 2010

PrimeLife is a research project funded by the European Commission's 7th Framework Programme