Signatures aveugles:

Une approche pour éviter la confiance aveugle

Eric Dubuis, Rolf Haenni

Haute école spécialisée bernoise

Blinde Signaturen

Ein E-Voting-Ansatz ohne blindes Vertrauen

Rolf Haenni, Eric Dubuis, Stephan Fischli, Reto König

Berner Fachhochschule

Inhaltsverzeichnis

Inhaltsverzeichnis

Rechtliche Grundlagen

StGB Art. 281: Wahlfälschung

Wer ein Stimmregister fälscht, beseitigt oder vernichtet,

wer unbefugt an einer Wahl oder Abstimmung [...] teilnimmt,

wer das Ergebnis einer Wahl oder einer Abstimmung [...] fälscht, insbesondere durch Hinzufügen, Ändern [...] oder Streichen von Stimmzetteln [...], oder durch unrichtiges Auszählen [...] des Ergebnisses,

wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

Rechtliche Grundlagen

StGB Art. 283: Verletzung des Wahlgeheimnisses

Wer sich durch unrechtmässiges Vorgehen Kenntnis davon verschafft, wie einzelne Berechtigte stimmen oder wählen,

wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

Anforderungen

Democracy

Eligibility > nur authorisierte Wähler können eine Stimme abgeben

Uniqueness > authorisierte Wähler können max. 1 Stimme abgeben

Fairness > vor dem Ende der Wahl werden keine Ergebnisse bekannt

Accuracy

Integrity > abgegebene Stimmen können nicht verändert werden

Completeness > jede gültige abgegebene Stimme wird gezählt

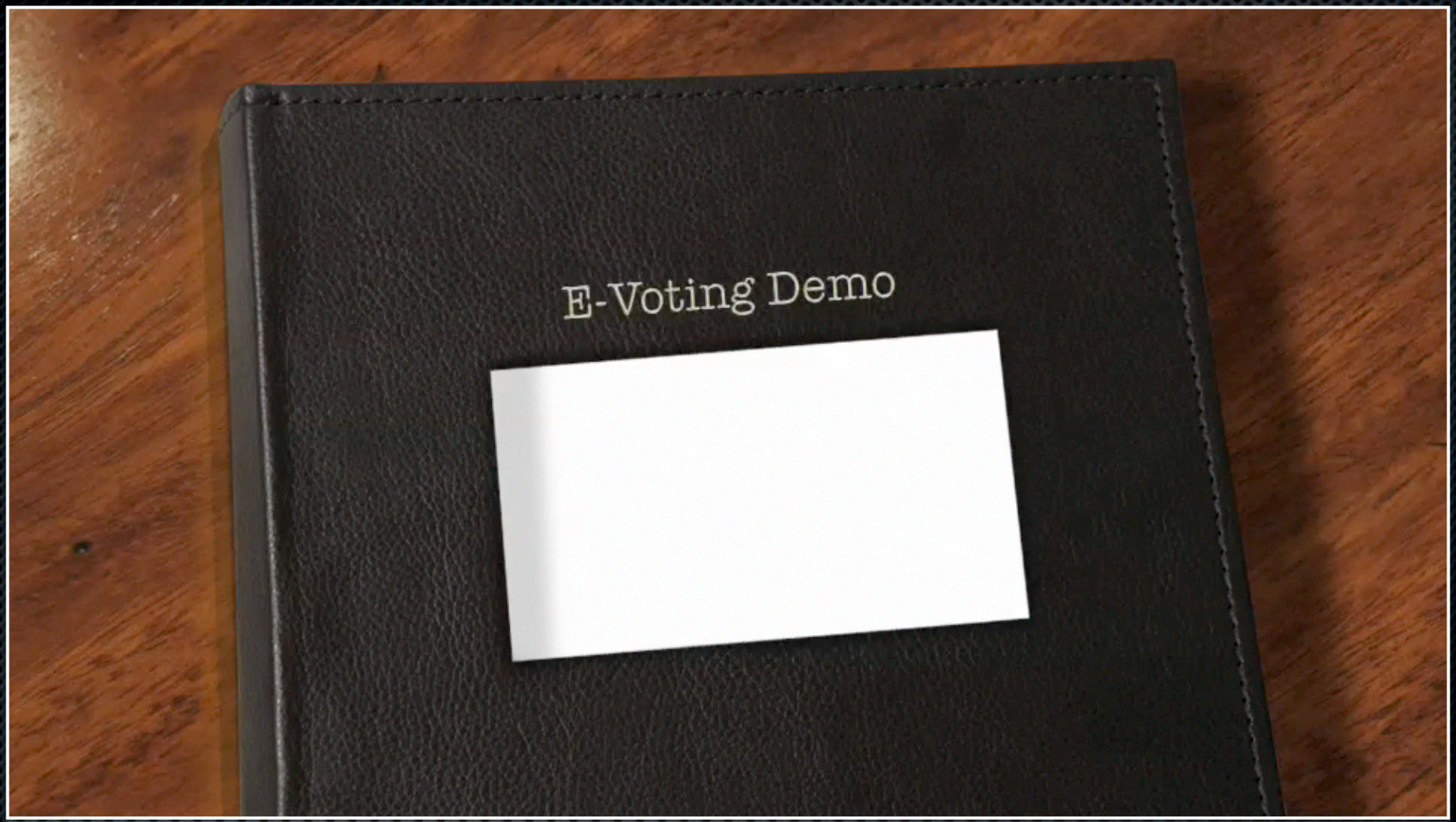
Soundness > ungültige Stimmen werden nicht gezählt

Privacy

Anonymity > eine Stimme kann nicht mit dem Wähler verlinkt werden

Receipt-Freeness > niemand kann beweisen, wie er gestimmt hat

Inhaltsverzeichnis


E-Voting Demo

Blackbox E-Voting

E-Voting-Systeme funktionieren oft nach dem Prinzip einer “Blackbox”:

> Die elektronische Stimme wird abgeschickt und danach in eine “elektronische Wahlurne“ gelegt

> Die elektronische Urne ist geschützt und der Zugriff stark eingeschränkt

> Am Ende der Wahl zählt eine “Zählsoftware” die Stimmen in der Urne und gibt das Resultat aus

Gefahren einer Blackbox

Der einzelne Wähler kann die korrekte Auszählung und das Resultat nicht überprüfen

> Grosse Manipulationsgefahr (intern/extern)

> Entwickler und Betreiber des Systems können erpresst oder gekauft werden

> Hacker können sich Zugriff verschaffen oder Malware einschleusen

> Die Wähler können dem System nicht vertrauen

Weitere Anforderungen

Individual Verifiability

Der Wähler kann überprüfen, dass seine Stimme angekommen ist und korrekt mitgezählt wurde

Universal Verifiability

Unabhängige Parteien oder einzelne Wähler können überprüfen, ob die abgegebenen Stimmen korrekt gezählt wurden

Situation in Deutschland

Leitfaden zum BVerfG-Urteil

1. Der Grundsatz der Öffentlichkeit der Wahl [...] gebietet, dass alle wesentlichen Schritte der Wahl öffentlicher Überprüfbarkeit unterliegen, [...].
2. Beim Einsatz elektronischer Wahlgeräte müssen die wesentlichen Schritte der Wahlhandlung und der Ergebnisermittlung vom Bürger zuverlässig und ohne besondere Sachkenntnis überprüft werden können.

dt. BVerfG, 3. März 2009

Blackbox E-Voting

"Security by Obscurity"

Transparentes E-Voting

"Security by Transparency"

Bulletin Baord I

Bulletin Baord I

Voting Board

nein
ja
nein
hallo!
ja
nein

Integrity Soundness Completeness Eligibility Ind.Verifiability

Fairness Anonymity Receipt-Freeness Uniqueness Univ.Verifiability

Bulletin Baord I

Voting Board

nein
ja
nein
hallo!
ja
nein

Integrity	Soundness	Completeness	Eligibility	Ind.Verifiability
Fairness	Anonymity	Receipt-Freeness	Uniqueness	Univ.Verifiability

Bulletin Baord II

Bulletin Baord II

Voting Board

John: nein
Mike: ja
Oscar: nein
Peter: hallo!
Alice: ja
Bob: nein

Integrity	*Soundness*	*Completeness*	Eligibility	Ind.Verifiability
Fairness	*Anonymity*	*Receipt-Freeness*	Uniqueness	*Univ.Verifiability*

Bulletin Baord II

Voting Board

John: nein
Mike: ja
Oscar: nein
Peter: hallo!
Alice: ja
Bob: nein

Integrity	*Soundness*	*Completeness*	Eligibility	Ind.Verifiability
Fairness	*Anonymity*	*Receipt-Freeness*	Uniqueness	*Univ.Verifiability*

Bulletin Baord III

Voting Board

Fish: nein
Cat: ja
Dog: nein
Bird: hallo!
Horse: ja

Bulletin Baord III

Voting Board

Fish: nein
Cat: ja
Dog: nein
Bird: hallo!
Horse: ja
Cow: nein

Integrity *Soundness* *Completeness* Eligibility *Ind.Verifiability*
Fairness Anonymity Receipt-Freeness *Uniqueness* *Univ.Verifiability*

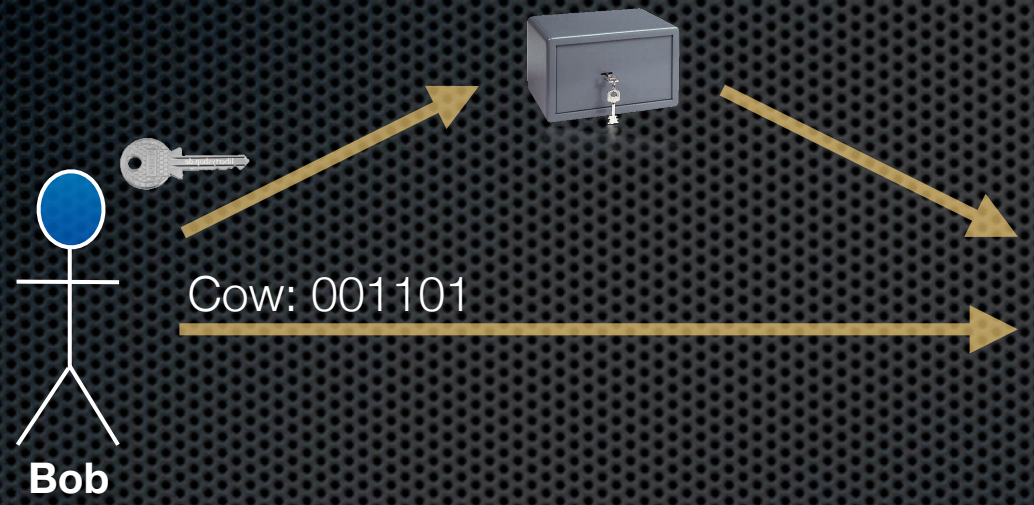
Bulletin Baord III

Voting Board

Fish: nein
Cat: ja
Dog: nein
Bird: hallo!
Horse: ja
Cow: nein

Integrity	*Soundness*	*Completeness*	Eligibility	*Ind.Verifiability*
Fairness	Anonymity	Receipt-Freeness	*Uniqueness*	*Univ.Verifiability*

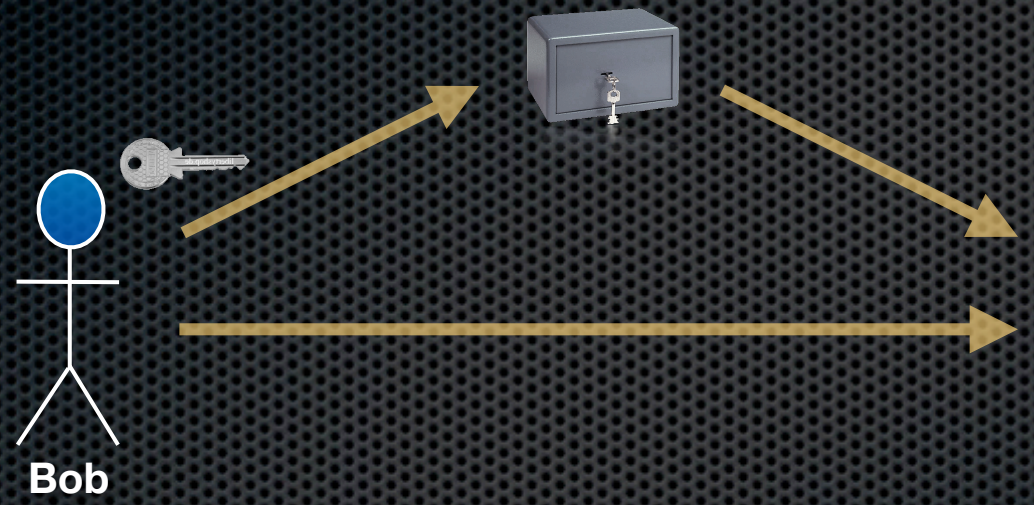
Bulletin Baord IV



Voting Board

Fish: 010110
Cat: 110010
Dog: 011001
Bird: 100110
Horse: 00010

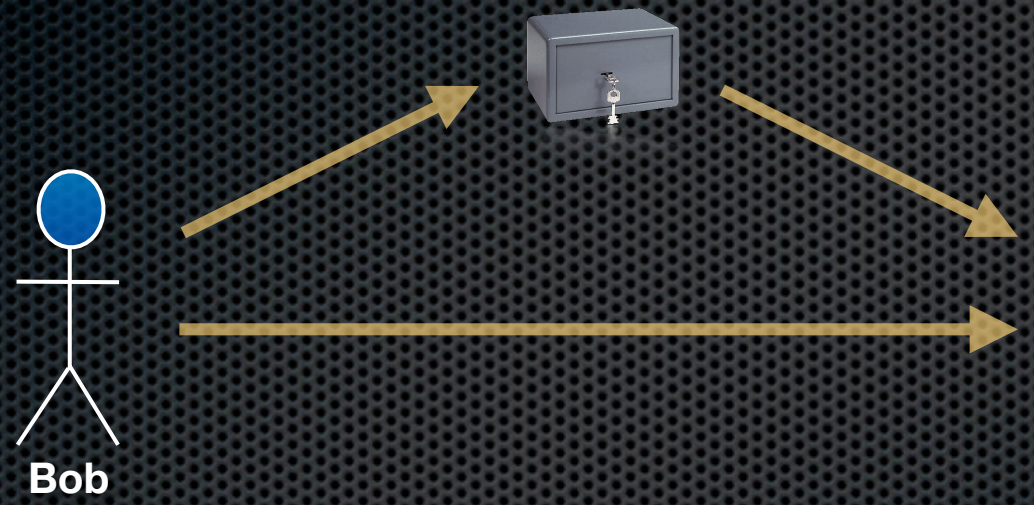
Bulletin Baord IV



Voting Board

Fish: 010110
Cat: 110010
Dog: 011001
Bird: 100110
Horse: 00010
Cow: 001101

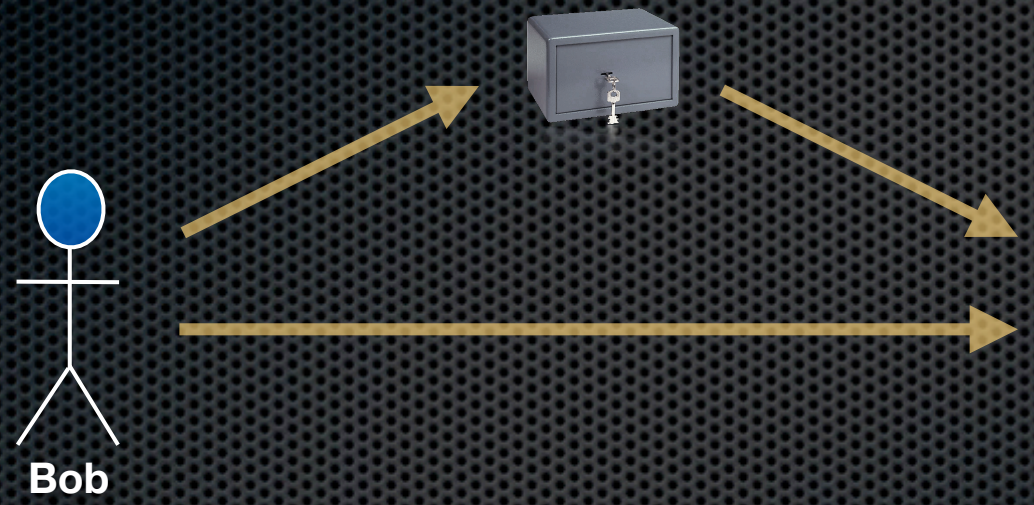
Bulletin Baord IV



Voting Board

Fish: 010110
Cat: 110010
Dog: 011001
Bird: 100110
Horse: 00010
Cow: 001101

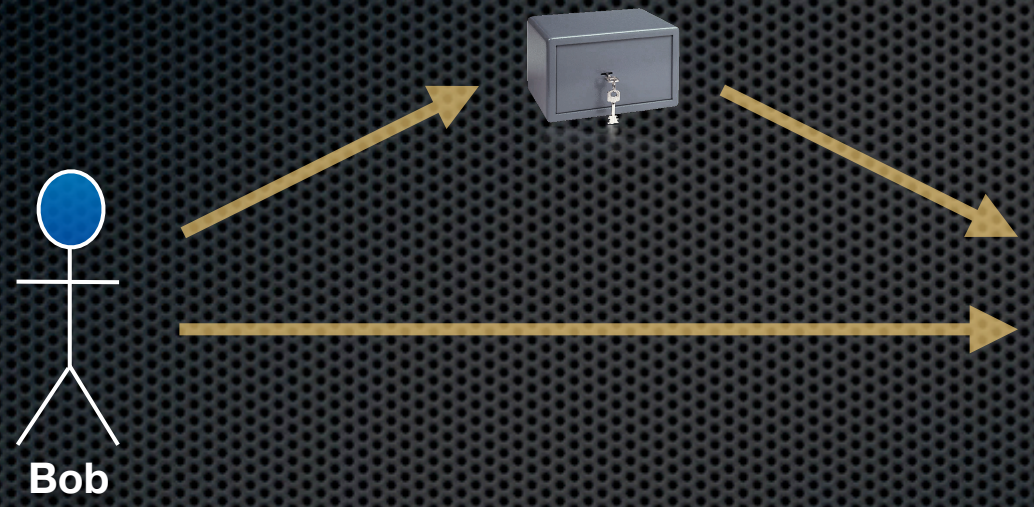
Bulletin Baord IV



Integrity *Soundness* *Completeness* Eligibility *Ind.Verifiability*

Fairness *Anonymity* Receipt-Freeness Uniqueness *Univ.Verifiability*

Bulletin Baord IV



Voting Board

Fish: 010110
Cat: 110010
Dog: 011001
Bird: 100110
Horse: 00010
Cow: 001101

Integrity	*Soundness*	*Completeness*	Eligibility	*Ind.Verifiability*
Fairness	*Anonymity*	Receipt-Freeness	Uniqueness	*Univ.Verifiability*

Bulletin Baord V

(*k*,*n*)-Threshold Secret Sharing Scheme

Bob

Cow: 001101

Voting Board

Fish: 010110
Cat: 110010
Dog: 011001
Bird: 100110
Horse: 00010

Bulletin Baord V

(*k*,*n*)-Threshold Secret Sharing Scheme

Voting Board

Fish: 010110
Cat: 110010
Dog: 011001
Bird: 100110
Horse: 00010
Cow: 001101

Bulletin Baord V

(*k*,*n*)-Threshold Secret Sharing Scheme

Voting Board

Fish: 010110
Cat: 110010
Dog: 011001
Bird: 100110
Horse: 00010
Cow: 001101

Bulletin Baord V

(*k*,*n*)-Threshold Secret Sharing Scheme

Integrity *Soundness* *Completeness* Eligibility *Ind.Verifiability*

Fairness *Anonymity* Receipt-Freeness Uniqueness *Univ.Verifiability*

Bulletin Baord V

(*k*,*n*)-Threshold Secret Sharing Scheme

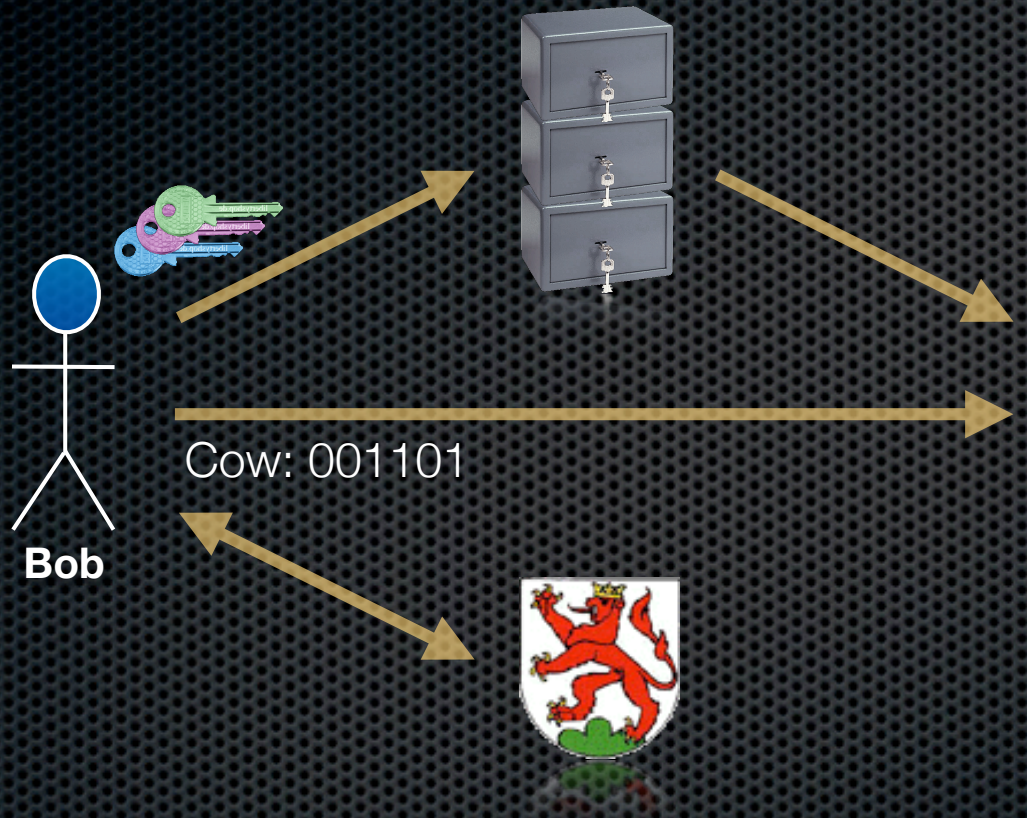
Voting Board

Fish: 010110
Cat: 110010
Dog: 011001
Bird: 100110
Horse: 00010
Cow: 001101

Integrity	*Soundness*	*Completeness*	Eligibility	*Ind.Verifiability*
Fairness	*Anonymity*	Receipt-Freeness	Uniqueness	*Univ.Verifiability*

Inhaltsverzeichnis

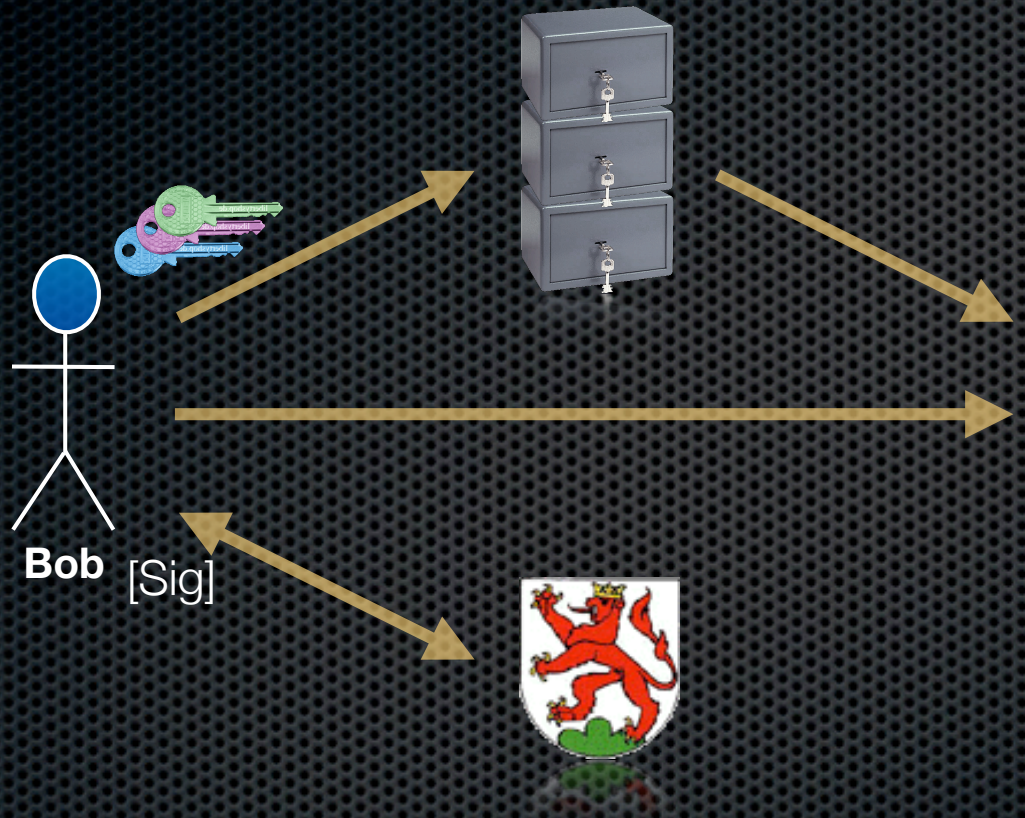
Bulletin Baord VI



Voting Board

Fish: 010110 [Sig]
Cat: 110010 [Sig]
Dog: 011001 [Sig]
Bird: 100110 [Sig]
Horse: 00010 [Sig]

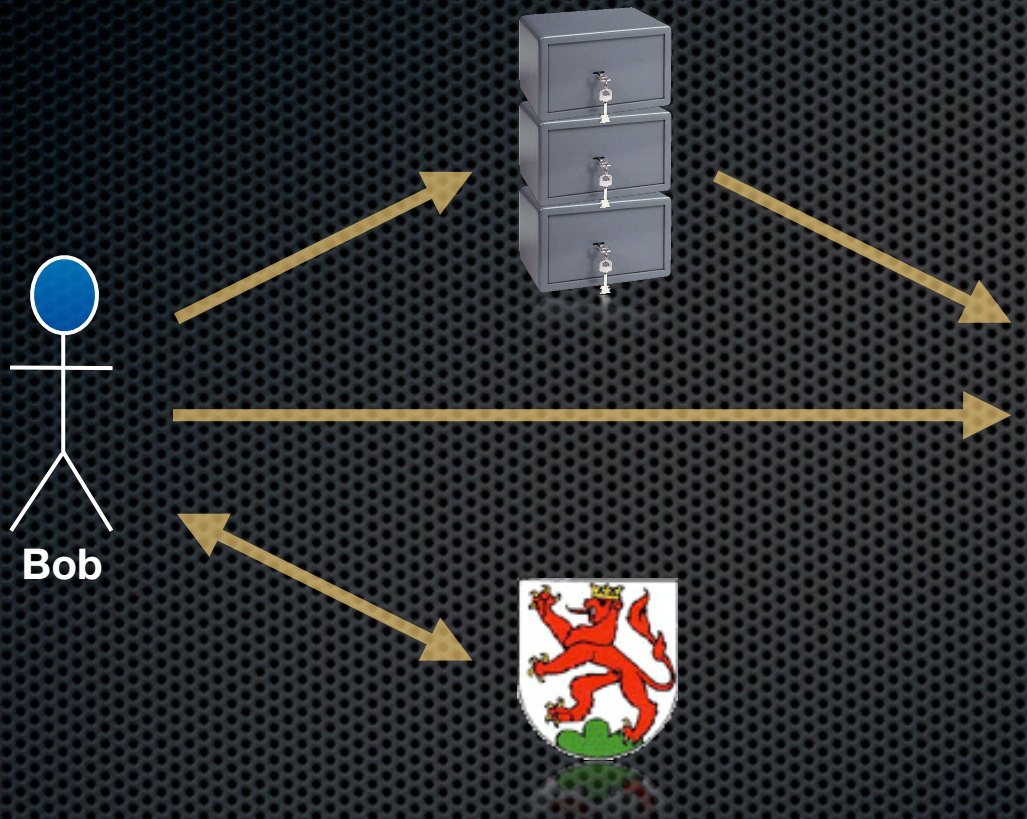
Bulletin Baord VI



Voting Board

Fish: 010110 [Sig]
Cat: 110010 [Sig]
Dog: 011001 [Sig]
Bird: 100110 [Sig]
Horse: 00010 [Sig]

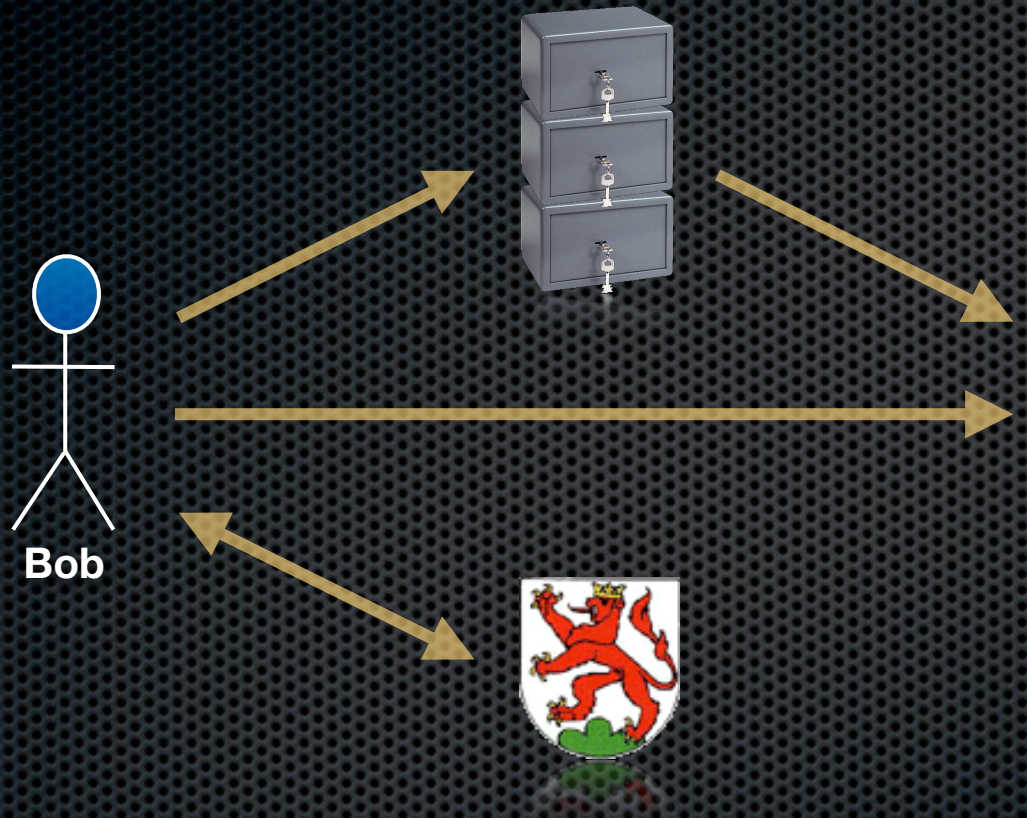
Bulletin Baord VI



Voting Board

Fish: 010110 [Sig]
Cat: 110010 [Sig]
Dog: 011001 [Sig]
Bird: 100110 [Sig]
Horse: 00010 [Sig]
Cow: 001101 [Sig]

Bulletin Baord VI

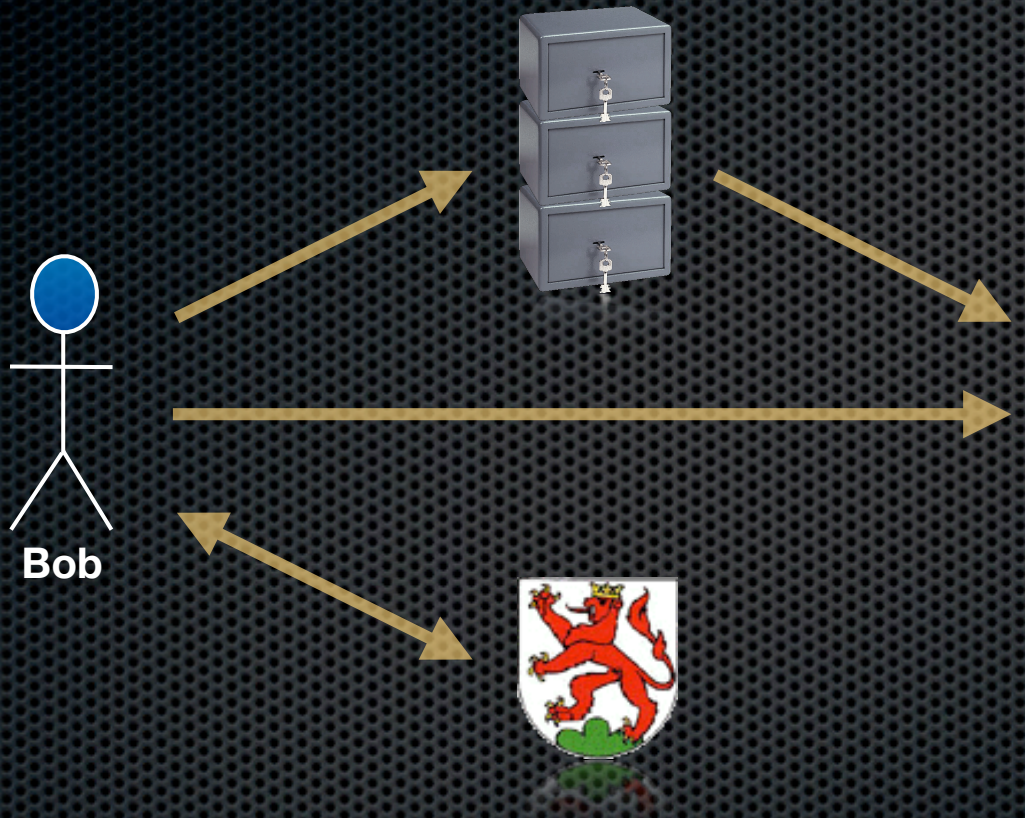


Voting Board

Fish: 010110 [Sig]
Cat: 110010 [Sig]
Dog: 011001 [Sig]
Bird: 100110 [Sig]
Horse: 00010 [Sig]
Cow: 001101 [Sig]

Integrity *Soundness* *Completeness* Eligibility *Ind.Verifiability*
Fairness *Anonymity* Receipt-Freeness Uniqueness *Univ.Verifiability*

Bulletin Baord VI

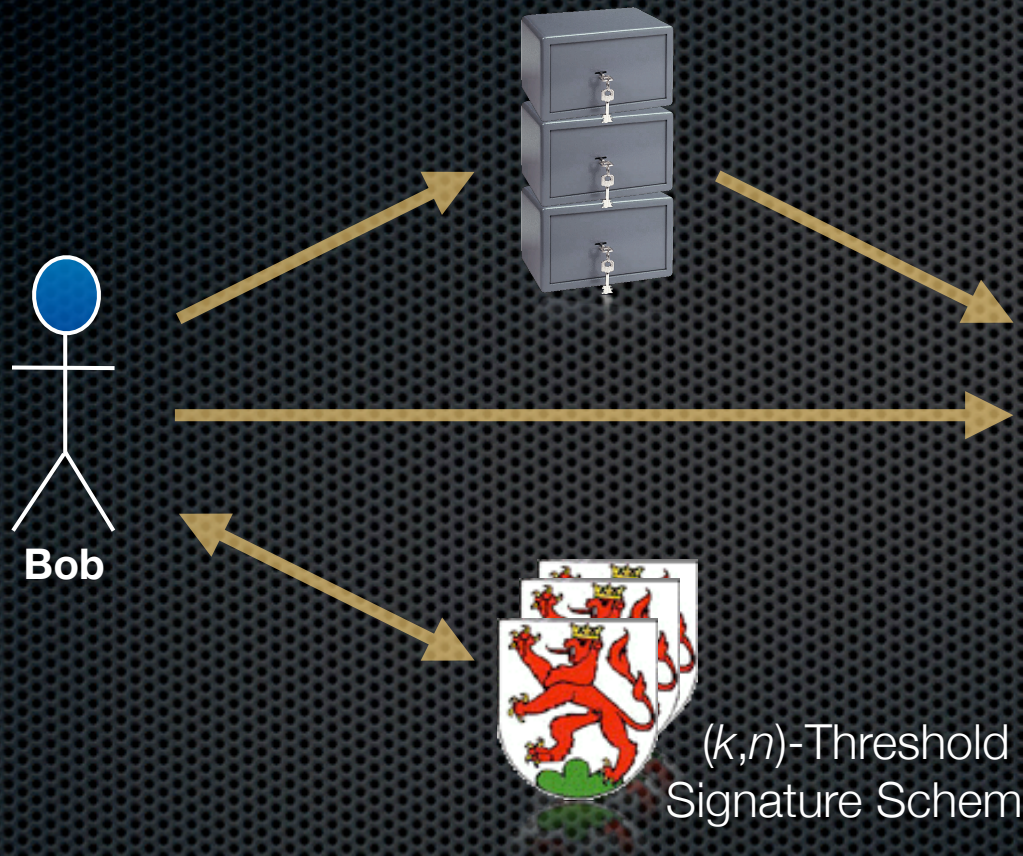


Voting Board

Fish: 010110 [Sig]
Cat: 110010 [Sig]
Dog: 011001 [Sig]
Bird: 100110 [Sig]
Horse: 00010 [Sig]
Cow: 001101 [Sig]

Integrity	*Soundness*	*Completeness*	Eligibility	*Ind.Verifiability*
Fairness	*Anonymity*	Receipt-Freeness	Uniqueness	*Univ.Verifiability*

Bulletin Baord VI

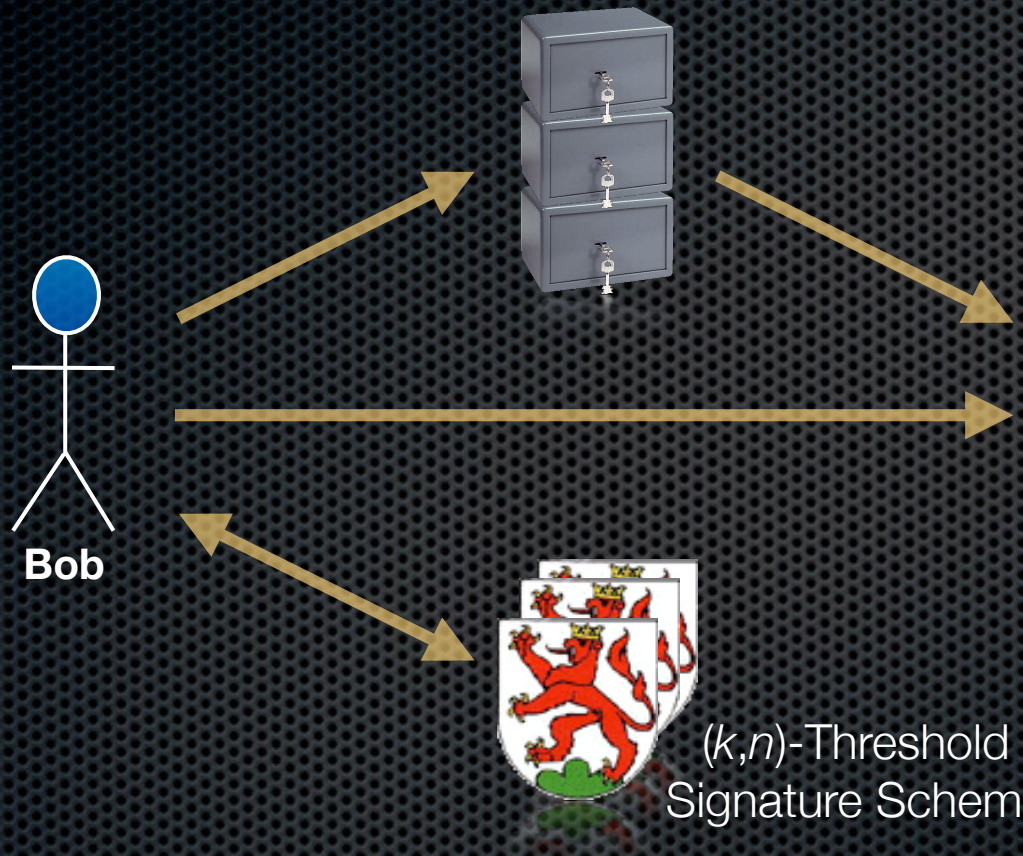


Voting Board

Fish: 010110 [Sig]
Cat: 110010 [Sig]
Dog: 011001 [Sig]
Bird: 100110 [Sig]
Horse: 00010 [Sig]
Cow: 001101 [Sig]

Integrity	*Soundness*	*Completeness*	Eligibility	*Ind.Verifiability*
Fairness	*Anonymity*	Receipt-Freeness	Uniqueness	*Univ.Verifiability*

Bulletin Baord VI



Voting Board

Fish: 010110 [Sig]
Cat: 110010 [Sig]
Dog: 011001 [Sig]
Bird: 100110 [Sig]
Horse: 00010 [Sig]
Cow: 001101 [Sig]

Integrity	*Soundness*	*Completeness*	Eligibility	*Ind.Verifiability*
Fairness	*Anonymity*	Receipt-Freeness	Uniqueness	*Univ.Verifiability*

WAHLBÜRO
der Stadt Murten
Postfach 326
3280 MURTEN

Abstimmungen/Wahlen **17. Mai 2009**
Votations/Elections ***17 mai 2009***

Öffnung des Stimmlokals / *Le bureau de vote est ouvert:*
Sonntag / *Dimanche*: 10.00–12.00 (keine Öffnungen an Freitagen und Samstagen mehr / *plus d'ouverture les vendredis et samedis*)

VORZEITIGE STIMMABGABE / *VOTE ANTICIPÉ*:

Die vorzeitige Stimmabgabe ist nur mit Ihrer eigenhändigen Unterschrift gültig. Per Post/Briefkasten bei der Stadtverwaltung/Empfangsbüro der Stadtverwaltung. *Sous peine de nullité, veuillez apposer votre signature manuscrite à l'endroit indiqué. Par poste / dans la boîte aux lettres de l'administration communale / Réception de l'Hôtel de Ville.*

Unterschrift / *Signature*:

BRIEFLICHE STIMMABGABE / *VOTE PAR CORRESPONDANCE*:

Streichen Sie Ihre Adresse durch, jedoch so, dass sie noch lesbar ist.
Veuillez biffer votre adresse qui doit toutefois rester lisible.

Geschäftsantwortsendung Invio commerciale-risposta
Envoi commercial-réponse

A

Nicht frankieren
Ne pas affranchir
Non affrancare

Stimmrechtsausweis
Certificat de capacité civique

Stadt Murten / *Ville de Morat*

Abstimmungslokal: Aula Schulhaus Längmatt
Bureau de vote: ***Aula de l'école Längmatt***

Dieses Couvert ist im Stimmlokal abzugeben. Bei vorzeitiger Stimmabgabe dient es als Antwortcouvert und muss rechtzeitig der Post übergeben werden, so dass es vor der Schliessung des Urnengangs beim Wahlbüro eintrifft. Es kann auch bis spätestens eine Stunde vor Öffnung des Stimmlokals (9.00 Uhr) am Sonntag in den **Briefkasten der Stadtverwaltung** beim Rathaus eingeworfen werden.

Cette enveloppe doit être présentée au bureau de vote. Pour le vote anticipé, elle sert d'enveloppe-réponse et doit être postée de manière à parvenir au bureau électoral avant la clôture du scrutin. Elle peut aussi être déposée ***dans la boîte aux lettres de l'administration communale*** *auprès de la maison communale, au plus tard jusqu'au dimanche du scrutin, une heure avant l'ouverture du local de vote (9h00)*

Wer unbefugt an einer Wahl oder Abstimmung teilnimmt, wird nach Artikel 282 StGB mit Gefängnis oder Busse bestraft.

En vertu de l'article 282 CP, celui qui, sans en avoir le droit, aura pris part à une élection ou une votation sera puni de l'emprisonnement ou de l'amende.

PP
3280 Murten

3360

Herr
Rolf Haenni
Altavilla 13
3280 Murten

Sceau communal

Gemeindestempel

Votation fédérale du 17 mai 2009

Eidgenössische Abstimmung vom 17. Mai 2009

Insérer dans cette enveloppe le bulletin de vote
Stimmzettel in diesen Umschlag einlegen

3042

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

1

Bulletin de vote pour la votation populaire du 17 mai 2009
Stimmzettel für die Volksabstimmung vom 17. Mai 2009

	Réponse Antwort
Acceptez-vous l'**article constitutionnel «Pour la prise en compte des médecines complémentaires»**? (Contre-projet à l'initiative populaire «Oui aux médecines complémentaires», qui a été retirée) Wollen Sie den **Verfassungsartikel «Zukunft mit Komplementärmedizin»** annehmen? (Gegenentwurf zur zurückgezogenen Volksinitiative «Ja zur Komplementärmedizin»)	

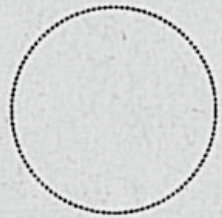
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

1

Bulletin de vote pour la votation populaire du 17 mai 2009
Stimmzettel für die Volksabstimmung vom 17. Mai 2009

	Réponse Antwort
Acceptez-vous l'**article constitutionnel «Pour la prise en compte des médecines complémentaires»**? (Contre-projet à l'initiative populaire «Oui aux médecines complémentaires», qui a été retirée)	
Wollen Sie den **Verfassungsartikel «Zukunft mit Komplementärmedizin»** annehmen? (Gegenentwurf zur zurückgezogenen Volksinitiative «Ja zur Komplementärmedizin»)	Nein

Sceau communal



Gemeindestempel

Votation fédérale du 17 mai 2009

Eidgenössische Abstimmung vom 17. Mai 2009

Insérer dans cette enveloppe le bulletin de vote
Stimmzettel in diesen Umschlag einlegen

3042

WAHLBÜRO
der Stadt Murten
Postfach 326
3280 MURTEN

Abstimmungen/Wahlen **17. Mai 2009**
Votations/Elections ***17 mai 2009***

Öffnung des Stimmlokals / *Le bureau de vote est ouvert:*
Sonntag / *Dimanche*: 10.00–12.00 (keine Öffnungen an Freitagen und Samstagen mehr / *plus d'ouverture les vendredis et samedis*)

VORZEITIGE STIMMABGABE / *VOTE ANTICIPÉ*:

Die vorzeitige Stimmabgabe ist nur mit Ihrer eigenhändigen Unterschrift gültig. Per Post/Briefkasten bei der Stadtverwaltung/Empfangsbüro der Stadtverwaltung. *Sous peine de nullité, veuillez apposer votre signature manuscrite à l'endroit indiqué. Par poste / dans la boîte aux lettres de l'administration communale / Réception de l'Hôtel de Ville.*

Unterschrift / *Signature*:

Stimmrechtsausweis
Certificat de capacité civique

Stadt Murten / *Ville de Morat*

Abstimmungslokal: Aula Schulhaus Längmatt
Bureau de vote:* *Aula de l'école Längmatt

Dieses Couvert ist im Stimmlokal abzugeben. Bei vorzeitiger Stimmabgabe dient es als Antwortcouvert und muss rechtzeitig der Post übergeben werden, so dass es vor der Schliessung des Urnengangs beim Wahlbüro eintrifft. Es kann auch bis spätestens eine Stunde vor Öffnung des Stimmlokals (9.00 Uhr) am Sonntag in den **Briefkasten der Stadtverwaltung** beim Rathaus eingeworfen werden.

*Cette enveloppe doit être présentée au bureau de vote. Pour le vote anticipé, elle sert d'enveloppe-réponse et doit être postée de manière à parvenir au bureau électoral avant la clôture du scrutin. Elle peut aussi être déposée **dans la boîte aux lettres de l'administration communale** auprès de la maison communale, au plus tard jusqu'au dimanche du scrutin, une heure avant l'ouverture du local de vote (9h00)*

Wer unbefugt an einer Wahl oder Abstimmung teilnimmt, wird nach Artikel 282 StGB mit Gefängnis oder Busse bestraft.

En vertu de l'article 282 CP, celui qui, sans en avoir le droit, aura pris part à une élection ou une votation sera puni de l'emprisonnement ou de l'amende.

BRIEFLICHE STIMMABGABE / *VOTE PAR CORRESPONDANCE*:

Streichen Sie Ihre Adresse durch, jedoch so, dass sie noch lesbar ist.
Veuillez biffer votre adresse qui doit toutefois rester lisible.

PP
3280 Murten

3360

Herr
Rolf Haenni
Altavilla 13
3280 Murten

Geschäftsantwortsendung Invio commerciale-risposta
Envoi commercial-réponse

A

Nicht frankieren
Ne pas affranchir
Non affrancare

WAHLBÜRO
der Stadt Murten
Postfach 326
3280 MURTEN

Stimmrechtsausweis
Certificat de capacité civique

Stadt Murten / *Ville de Morat*

Abstimmungslokal: Aula Schulhaus Längmatt
Bureau de vote:* *Aula de l'école Längmatt

Dieses Couvert ist im Stimmlokal abzugeben. Bei vorzeitiger Stimmabgabe dient es als Antwortcouvert und muss rechtzeitig der Post übergeben werden, so dass es vor der Schliessung des Urnengangs beim Wahlbüro eintrifft. Es kann auch bis spätestens eine Stunde vor Öffnung des Stimmlokals (9.00 Uhr) am Sonntag in den **Briefkasten der Stadtverwaltung** beim Rathaus eingeworfen werden.

Cette enveloppe doit être présentée au bureau de vote. Pour le vote anticipé, elle sert d'enveloppe-réponse et doit être postée de manière à parvenir au bureau électoral avant la clôture du scrutin. Elle peut aussi être déposée ***dans la boîte aux lettres de l'administration communale*** *auprès de la maison communale, au plus tard jusqu'au dimanche du scrutin, une heure avant l'ouverture du local de vote (9h00)*

Wer unbefugt an einer Wahl oder Abstimmung teilnimmt, wird nach Artikel 282 StGB mit Gefängnis oder Busse bestraft.

En vertu de l'article 282 CP, celui qui, sans en avoir le droit, aura pris part à une élection ou une votation sera puni de l'emprisonnement ou de l'amende.

Abstimmungen/Wahlen **17. Mai 2009**
Votations/Elections ***17 mai 2009***

Öffnung des Stimmlokals / *Le bureau de vote est ouvert:*
Sonntag / *Dimanche*: 10.00–12.00 (keine Öffnungen an Freitagen und Samstagen mehr / *plus d'ouverture les vendredis et samedis*)

VORZEITIGE STIMMABGABE / *VOTE ANTICIPÉ*:

Die vorzeitige Stimmabgabe ist nur mit Ihrer eigenhändigen Unterschrift gültig. Per Post/Briefkasten bei der Stadtverwaltung/Empfangsbüro der Stadtverwaltung.
Sous peine de nullité, veuillez apposer votre signature manuscrite à l'endroit indiqué. Par poste / dans la boîte aux lettres de l'administration communale / Réception de l'Hôtel de Ville.

Unterschrift / *Signature*: Rolf Haenni

BRIEFLICHE STIMMABGABE / *VOTE PAR CORRESPONDANCE*:

Streichen Sie Ihre Adresse durch, jedoch so, dass sie noch lesbar ist.
Veuillez biffer votre adresse qui doit toutefois rester lisible.

PP
3280 Murten

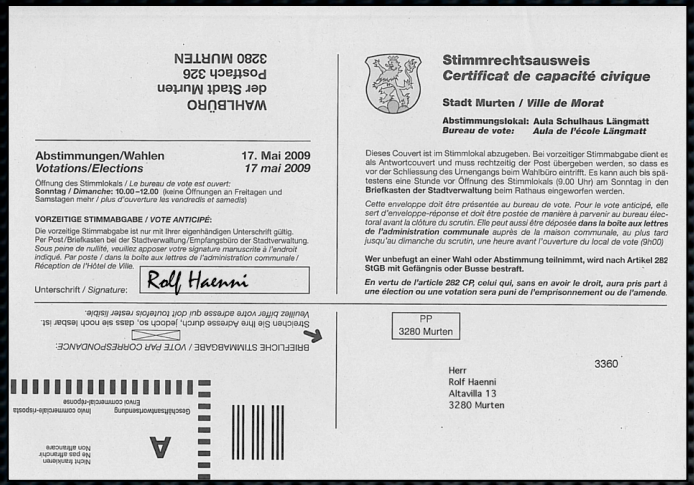
3360

Herr
Rolf Haenni
Altavilla 13
3280 Murten

Geschäftsantwortsendung
Envoi commercial-réponse
Invio commerciale-risposta

A

Nicht frankieren
Ne pas affranchir
Non affrancare



WAHLBÜRO
der Stadt Murten
Postfach 326
3280 MURTEN

Stimmrechtsausweis
Certificat de capacité civique

Stadt Murten / *Ville de Morat*

Abstimmungslokal: Aula Schulhaus Längmatt
Bureau de vote: Aula de l'école Längmatt

Abstimmungen/Wahlen 17. Mai 2009
Votations/Elections *17 mai 2009*

Öffnung des Stimmlokals / *Le bureau de vote est ouvert:*
Sonntag / *Dimanche*: 10.00–12.00 (keine Öffnungen an Freitagen und Samstagen mehr / *plus d'ouverture les vendredis et samedis*)

VORZEITIGE STIMMABGABE / *VOTE ANTICIPÉ*:
Die vorzeitige Stimmabgabe ist nur mit Ihrer eigenhändigen Unterschrift gültig. Per Post/Briefkasten bei der Stadtverwaltung/Empfangsbüro der Stadtverwaltung. *Sous peine de nullité, veuillez apposer votre signature manuscrite à l'endroit indiqué. Par poste / dans la boîte aux lettres de l'administration communale / Réception de l'hôtel de Ville.*

Unterschrift / *Signature:* Rolf Haenni

Dieses Couvert ist im Stimmlokal abzugeben. Bei vorzeitiger Stimmabgabe dient es als Antwortcouvert und muss rechtzeitig der Post übergeben werden, so dass es vor der Schliessung des Urnengangs beim Wahlbüro eintrifft. Es kann auch bis spätestens eine Stunde vor Öffnung des Stimmlokals (9.00 Uhr) am Sonntag in den **Briefkasten der Stadtverwaltung** beim Rathaus eingeworfen werden.

*Cette enveloppe doit être présentée au bureau de vote. Pour le vote anticipé, elle sert d'enveloppe-réponse et doit être postée de manière à parvenir au bureau électoral avant la clôture du scrutin. Elle peut aussi être déposée **dans la boîte aux lettres de l'administration communale** auprès de la maison communale, au plus tard jusqu'au dimanche du scrutin, une heure avant l'ouverture du local de vote (9h00)*

Wer unbefugt an einer Wahl oder Abstimmung teilnimmt, wird nach Artikel 282 StGB mit Gefängnis oder Busse bestraft.

En vertu de l'article 282 CP, celui qui, sans en avoir le droit, aura pris part à une élection ou une votation sera puni de l'emprisonnement ou de l'amende.

BRIEFLICHE STIMMABGABE / *VOTE PAR CORRESPONDANCE:*
Stecken Sie Ihre Adresse durch, jedoch so, dass sie noch lesbar ist.
Veuillez biffer votre adresse qui doit toutefois rester lisible.

PP
3280 Murten

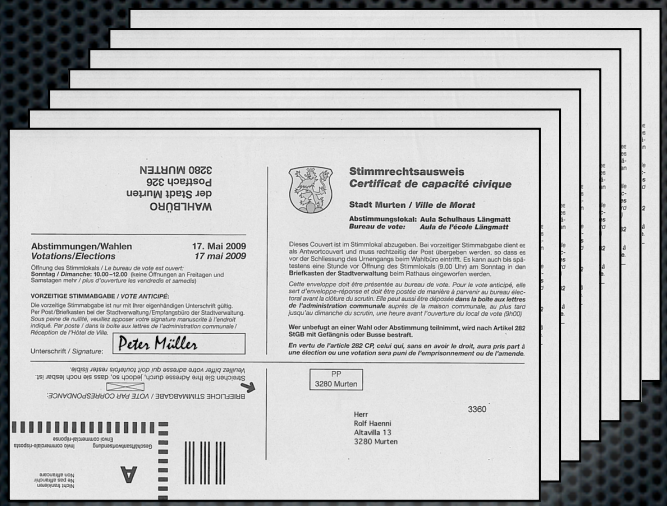
3360

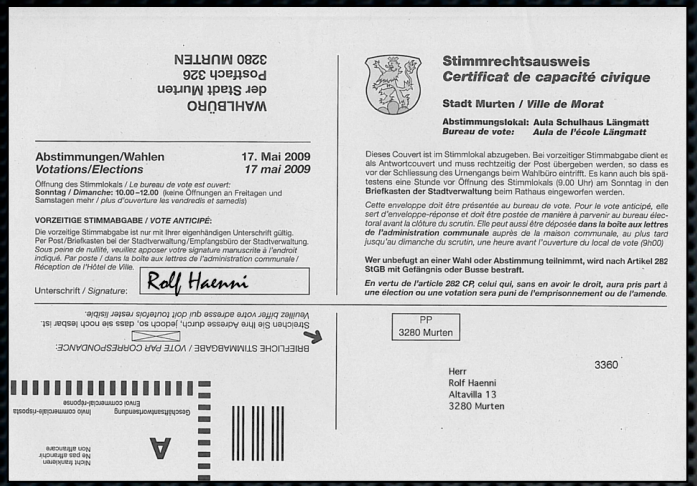
Herr
Rolf Haenni
Altavilla 13
3280 Murten

Nicht frankieren
Ne pas affranchir
Non affrancare

A

Geschäftsantwortsendung
Envoi commercial-réponse
Invio commerciale-risposta





WAHLBÜRO
der Stadt Murten
Postfach 326
3280 MURTEN

Stimmrechtsausweis
Certificat de capacité civique

Stadt Murten / *Ville de Morat*

Abstimmungslokal: **Aula Schulhaus Längmatt**
Bureau de vote: ***Aula de l'école Längmatt***

Abstimmungen/Wahlen **17. Mai 2009**
Votations/Elections ***17 mai 2009***

Öffnung des Stimmlokals / *Le bureau de vote est ouvert:*
Sonntag / *Dimanche:* 10.00–12.00 (keine Öffnungen an Freitagen und Samstagen mehr / *plus d'ouverture les vendredis et samedis*)

VORZEITIGE STIMMABGABE / *VOTE ANTICIPÉ*:
Die vorzeitige Stimmabgabe ist nur mit Ihrer eigenhändigen Unterschrift gültig. Per Post/Briefkasten bei der Stadtverwaltung/Empfangsbüro der Stadtverwaltung. *Sous peine de nullité, veuillez apposer votre signature manuscrite à l'endroit indiqué. Par poste / dans la boîte aux lettres de l'administration communale / Réception de l'hôtel de Ville.*

Unterschrift / *Signature:* Rolf Haenni

Dieses Couvert ist im Stimmlokal abzugeben. Bei vorzeitiger Stimmabgabe dient es als Antwortcouvert und muss rechtzeitig der Post übergeben werden, so dass es vor der Schliessung des Urnengangs beim Wahlbüro eintrifft. Es kann auch bis spätestens eine Stunde vor Öffnung des Stimmlokals (9.00 Uhr) am Sonntag in den **Briefkasten der Stadtverwaltung** beim Rathaus eingeworfen werden.

*Cette enveloppe doit être présentée au bureau de vote. Pour le vote anticipé, elle sert d'enveloppe-réponse et doit être postée de manière à parvenir au bureau électoral avant la clôture du scrutin. Elle peut aussi être déposée **dans la boîte aux lettres de l'administration communale** auprès de la maison communale, au plus tard jusqu'au dimanche du scrutin, une heure avant l'ouverture du local de vote (9h00)*

Wer unbefugt an einer Wahl oder Abstimmung teilnimmt, wird nach Artikel 282 StGB mit Gefängnis oder Busse bestraft.

En vertu de l'article 282 CP, celui qui, sans en avoir le droit, aura pris part à une élection ou une votation sera puni de l'emprisonnement ou de l'amende.

BRIEFLICHE STIMMABGABE / *VOTE PAR CORRESPONDANCE:*
Bitte achten Sie Ihre Adresse durch, jedoch so, dass sie noch lesbar ist. *Veuillez biffer votre adresse qui doit toutefois rester lisible.*

PP
3280 Murten

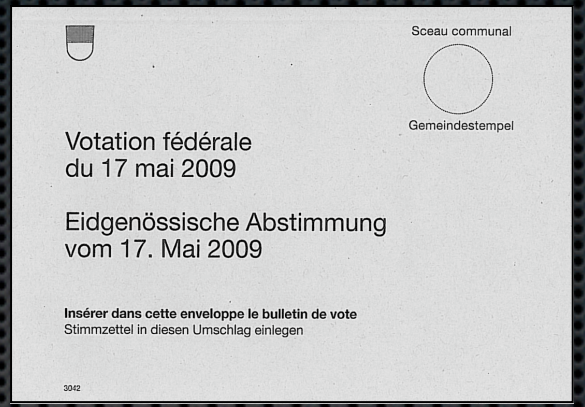
3360

Herr
Rolf Haenni
Altavilla 13
3280 Murten

Nicht frankieren
Ne pas affranchir
Non affrancare

A

Geschäftsantwortsendung
Envoi commercial-réponse
Invio commerciale-risposta



Sceau communal

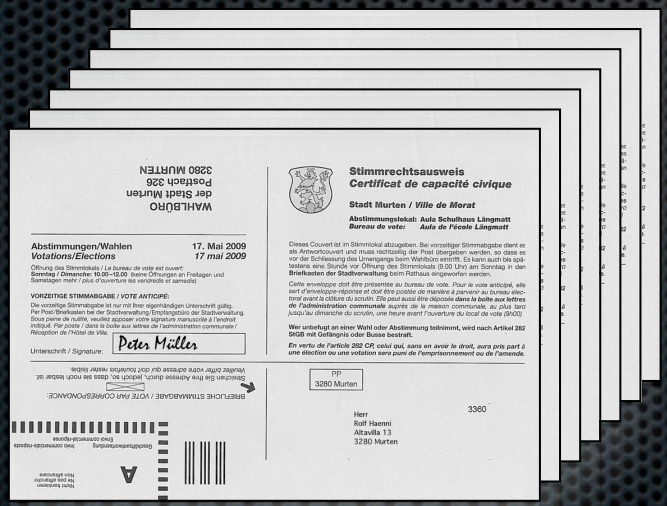
Gemeindestempel

Votation fédérale
du 17 mai 2009

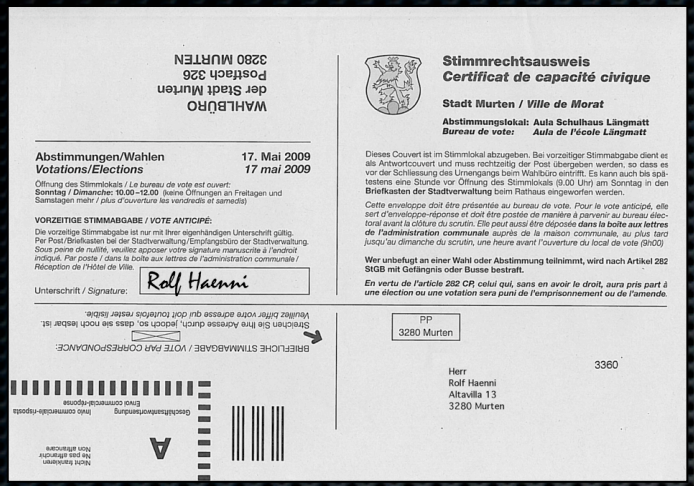
Eidgenössische Abstimmung
vom 17. Mai 2009

Insérer dans cette enveloppe le bulletin de vote
Stimmzettel in diesen Umschlag einlegen

3042



GEMEINDE MURTEN



WAHLBÜRO
der Stadt Murten
Postfach 326
3280 MURTEN

Stimmrechtsausweis
Certificat de capacité civique

Stadt Murten / *Ville de Morat*

Abstimmungslokal: Aula Schulhaus Längmatt
Bureau de vote: Aula de l'école Längmatt

Abstimmungen/Wahlen 17. Mai 2009
Votations/Elections *17 mai 2009*

Öffnung des Stimmlokals / *Le bureau de vote est ouvert:*
Sonntag / *Dimanche:* 10.00–12.00 (keine Öffnungen an Freitagen und Samstagen mehr / *plus d'ouverture les vendredis et samedis*)

VORZEITIGE STIMMABGABE / *VOTE ANTICIPÉ*:
Die vorzeitige Stimmabgabe ist nur mit Ihrer eigenhändigen Unterschrift gültig. Per Post/Briefkasten bei der Stadtverwaltung/Empfangsbüro der Stadtverwaltung.
Sous peine de nullité, veuillez apposer votre signature manuscrite à l'endroit indiqué. Par poste / dans la boîte aux lettres de l'administration communale / Réception de l'hôtel de Ville.

Unterschrift / *Signature:* Rolf Haenni

Dieses Couvert ist im Stimmlokal abzugeben. Bei vorzeitiger Stimmabgabe dient es als Antwortcouvert und muss rechtzeitig der Post übergeben werden, so dass es vor der Schliessung des Urnengangs beim Wahlbüro eintrifft. Es kann auch bis spätestens eine Stunde vor Öffnung des Stimmlokals (9.00 Uhr) am Sonntag in den **Briefkasten der Stadtverwaltung** beim Rathaus eingeworfen werden.

*Cette enveloppe doit être présentée au bureau de vote. Pour le vote anticipé, elle sert d'enveloppe-réponse et doit être postée de manière à parvenir au bureau électoral avant la clôture du scrutin. Elle peut aussi être déposée **dans la boîte aux lettres de l'administration communale** auprès de la maison communale, au plus tard jusqu'au dimanche du scrutin, une heure avant l'ouverture du local de vote (9h00)*

Wer unbefugt an einer Wahl oder Abstimmung teilnimmt, wird nach Artikel 282 StGB mit Gefängnis oder Busse bestraft.

En vertu de l'article 282 CP, celui qui, sans en avoir le droit, aura pris part à une élection ou une votation sera puni de l'emprisonnement ou de l'amende.

BRIEFLICHE STIMMABGABE / *VOTE PAR CORRESPONDANCE:*
Bitte achten Sie Ihre Adresse durch, falls sie nicht lesbar ist. *Veuillez biffer votre adresse qui doit toutefois rester lisible.*

PP
3280 Murten

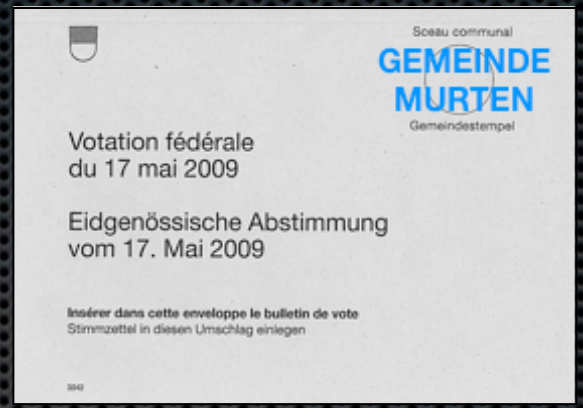
3360

Herr
Rolf Haenni
Altavilla 13
3280 Murten

Nicht frankieren
Ne pas affranchir
Non affrancare

A

Geschäftsantwortsendung
Envoi commercial-réponse
Invio commerciale-risposta



Sceau communal

GEMEINDE
MURTEN

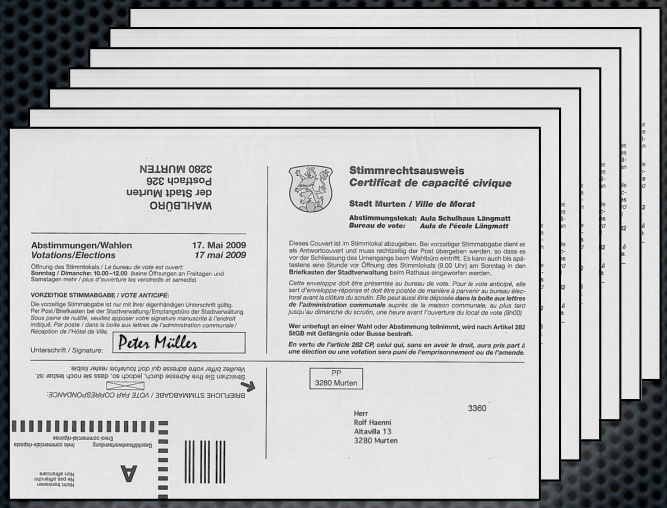
Gemeindestempel

Votation fédérale
du 17 mai 2009

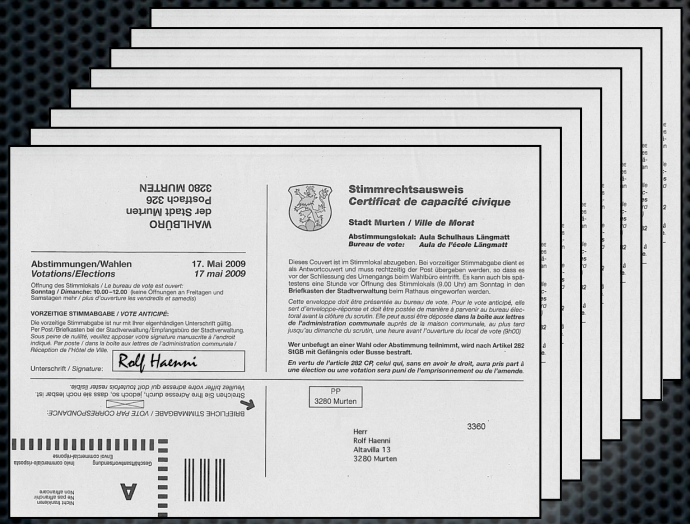
Eidgenössische Abstimmung
vom 17. Mai 2009

Insérer dans cette enveloppe le bulletin de vote
Stimmzettel in diesen Umschlag einlegen

3343



GEMEINDE MURTEN


WAHLBÜRO
der Stadt Murten
Postfach 326
3280 MURTEN
Stimmrechtsausweis
Certificat de capacité civique
Stadt Murten / Ville de Morat
Abstimmungslokal: Aula Schulhaus Längmatt
Bureau de vote: Aula de l'école Längmatt
Abstimmungen/Wahlen 17. Mai 2009
Votations/Elections 17 mai 2009
Rolf Haenni
PP
3280 Murten
3360
Herr
Rolf Haenni
Altavilla 13
3280 Murten


GEMEINDE MURTEN

Blinde Signaturen

Bei einer blinden Signatur wird eine Nachricht *m* digital unterschrieben, ohne dass der Unterschreibende die Nachricht sieht

> zuerst wird die Nachricht “versalzen” $\underline{m} = \text{salt}(m,r)$

> die versalzene Nachricht wird signiert $\underline{s} = \text{sign}(\underline{m},d)$

> die versalzene Signatur wird “entsalzen” $s = \text{unsalt}(\underline{s},r)$

> die Signatur kann normal überprüft werden $\text{verify}(m,s,e)$

Dabei muss gelten: $\text{unsalt}(\text{sign}(\text{salt}(m,r),d),r)=\text{sign}(m,d)$

Blinde Signaturen mit RSA

Beim RSA-Verfahren können blinde Signaturen wie folgt generiert werden:

> zuerst wird die Nachricht “versalzen” $\underline{m} = m \times r^e$

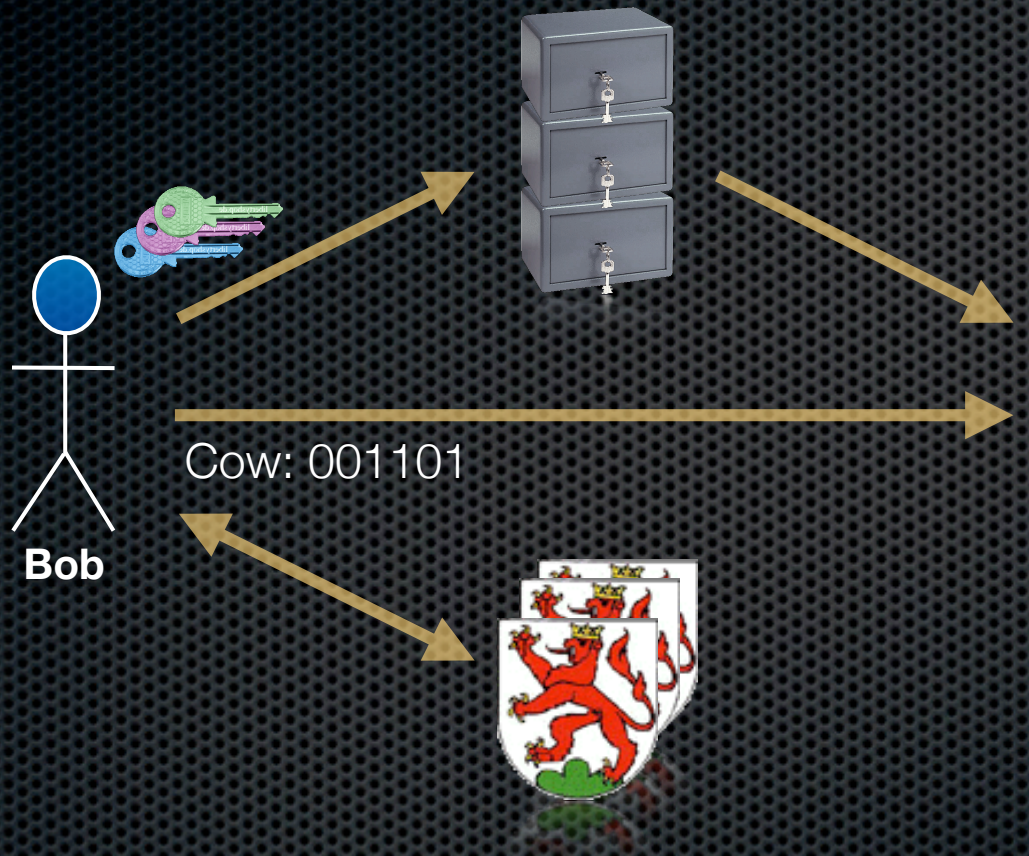
> die versalzene Nachricht wird signiert $\underline{s} = \underline{m}^d$

> die versalzene Signatur wird “entsalzen” $s = \underline{s} \times r^{-1}$

> die Signatur kann normal überprüft werden $m = s^e$?

Dabei gilt: $((m \times r^e)^d) \times r^{-1} = m^d$

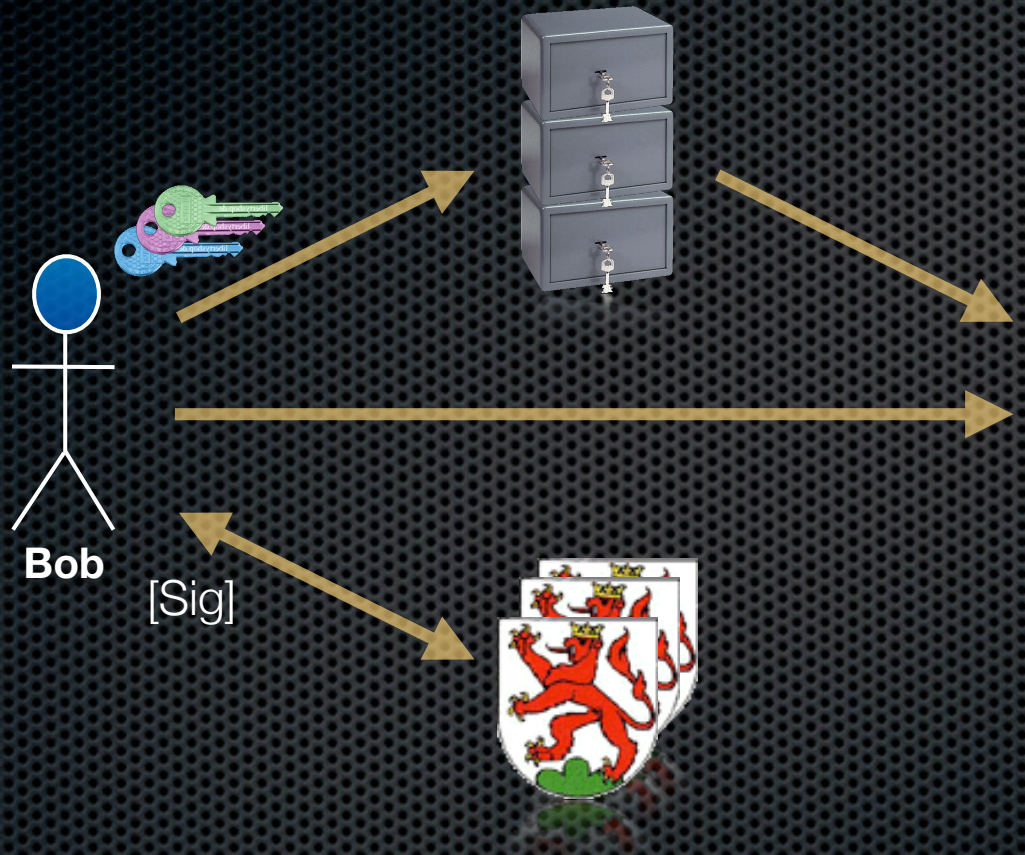
Bulletin Baord VII



Voting Board

Fish: 010110 [Sig]
Cat: 110010 [Sig]
Dog: 011001 [Sig]
Bird: 100110 [Sig]
Horse: 00010 [Sig]

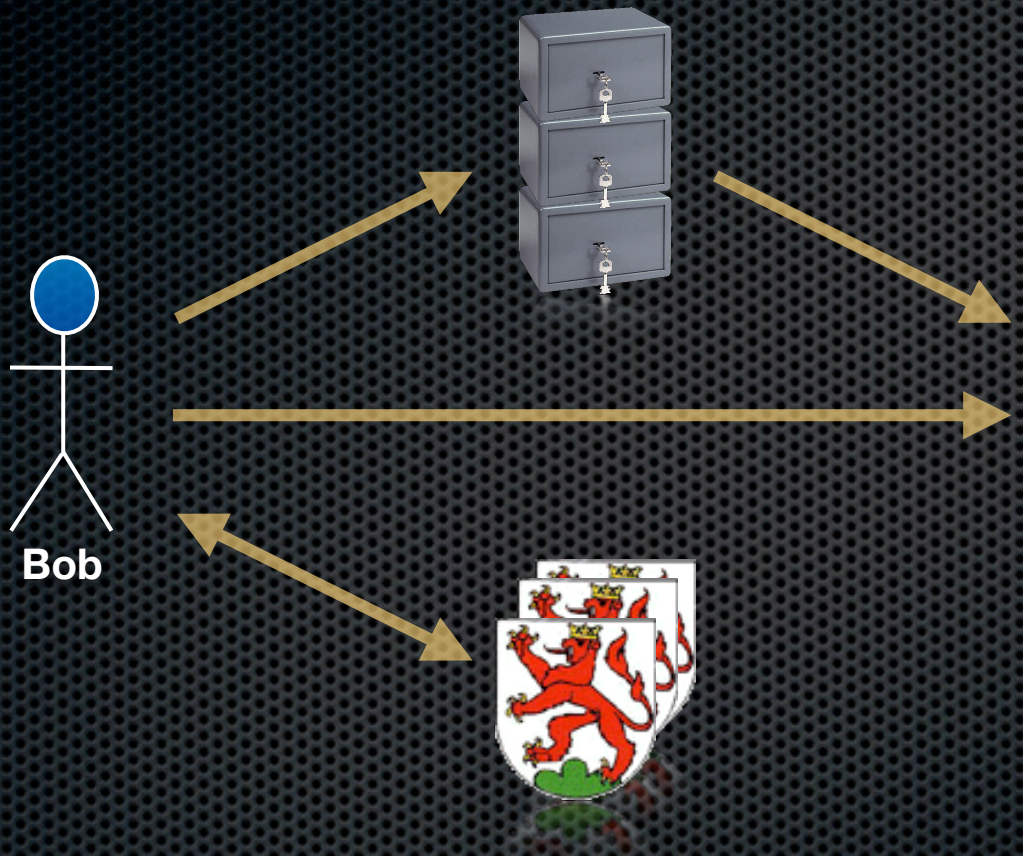
Bulletin Baord VII



Voting Board

Fish: 010110 [Sig]
Cat: 110010 [Sig]
Dog: 011001 [Sig]
Bird: 100110 [Sig]
Horse: 00010 [Sig]

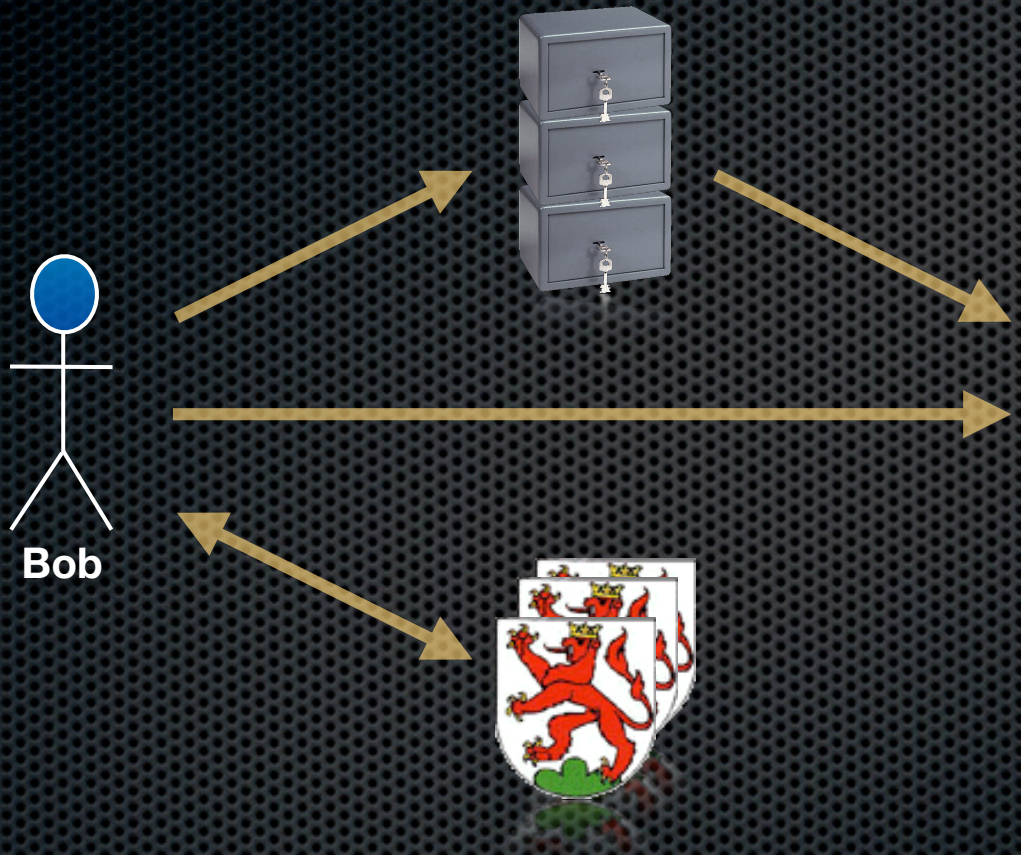
Bulletin Baord VII



Voting Board

Fish: 010110 [Sig]
Cat: 110010 [Sig]
Dog: 011001 [Sig]
Bird: 100110 [Sig]
Horse: 00010 [Sig]
Cow: 001101 [Sig]

Bulletin Baord VII

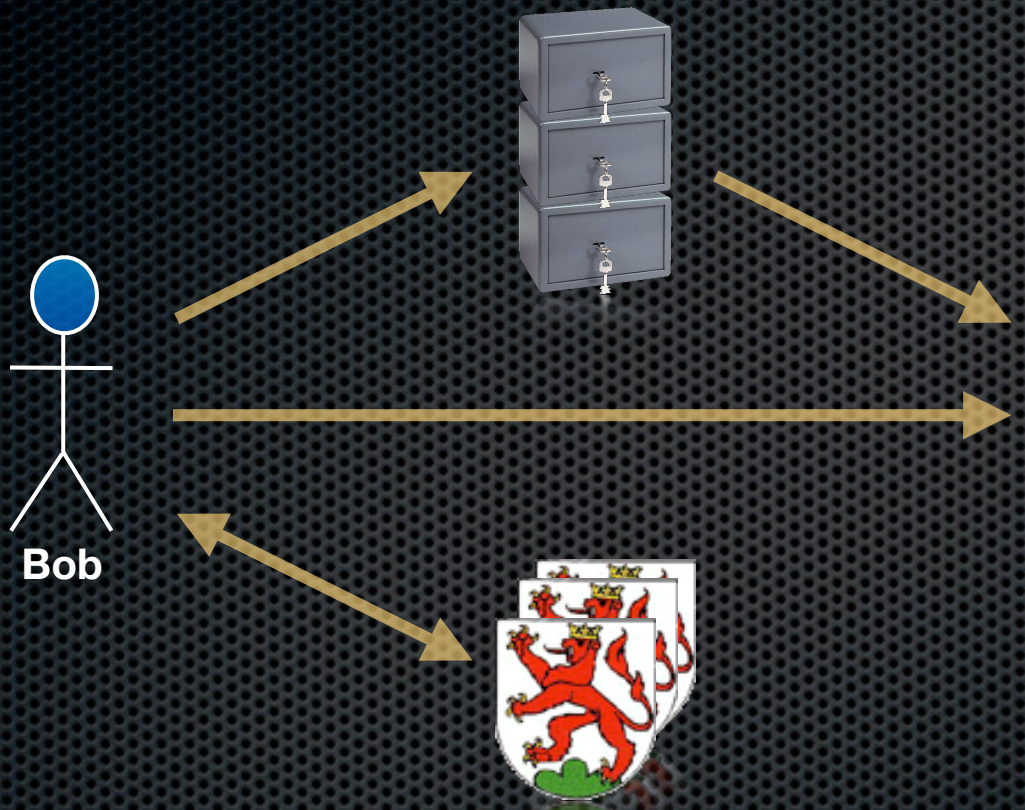


Voting Board

Fish: 010110 [Sig]
Cat: 110010 [Sig]
Dog: 011001 [Sig]
Bird: 100110 [Sig]
Horse: 00010 [Sig]
Cow: 001101 [Sig]

Integrity *Soundness* *Completeness* Eligibility *Ind.Verifiability*
Fairness Anonymity Receipt-Freeness Uniqueness *Univ.Verifiability*

Bulletin Baord VII



Voting Board

Fish: 010110 [Sig]
Cat: 110010 [Sig]
Dog: 011001 [Sig]
Bird: 100110 [Sig]
Horse: 00010 [Sig]
Cow: 001101 [Sig]

Integrity	*Soundness*	*Completeness*	Eligibility	*Ind.Verifiability*
Fairness	Anonymity	Receipt-Freeness	Uniqueness	*Univ.Verifiability*

Inhaltsverzeichnis

Rechtliche Grundlagen

StGB Art. 283: Wahlbestechung

Wer einem Stimmberechtigten ein Geschenk oder einen andern Vorteil anbietet [...] oder zukommen lässt,damit er in einem bestimmten Sinne stimme oder wähle, [...], oder damit er an einer Wahl oder Abstimmung nicht teilnehme,

wer sich als Stimmberechtigter einen solchen Vorteil versprechen oder geben lässt,

wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

Rechtliche Grundlagen

StGB Art. 282bis: Stimmenfang

Wer Wahl- oder Stimmzettel planmässig einsammelt, ausfüllt oder ändert,

wer derartige Wahl- oder Stimmzettel verteilt,

wird mit Busse bestraft.

Stimmenkauf im Internet

www.wahlgeld.com

www.sell-your-vote.com

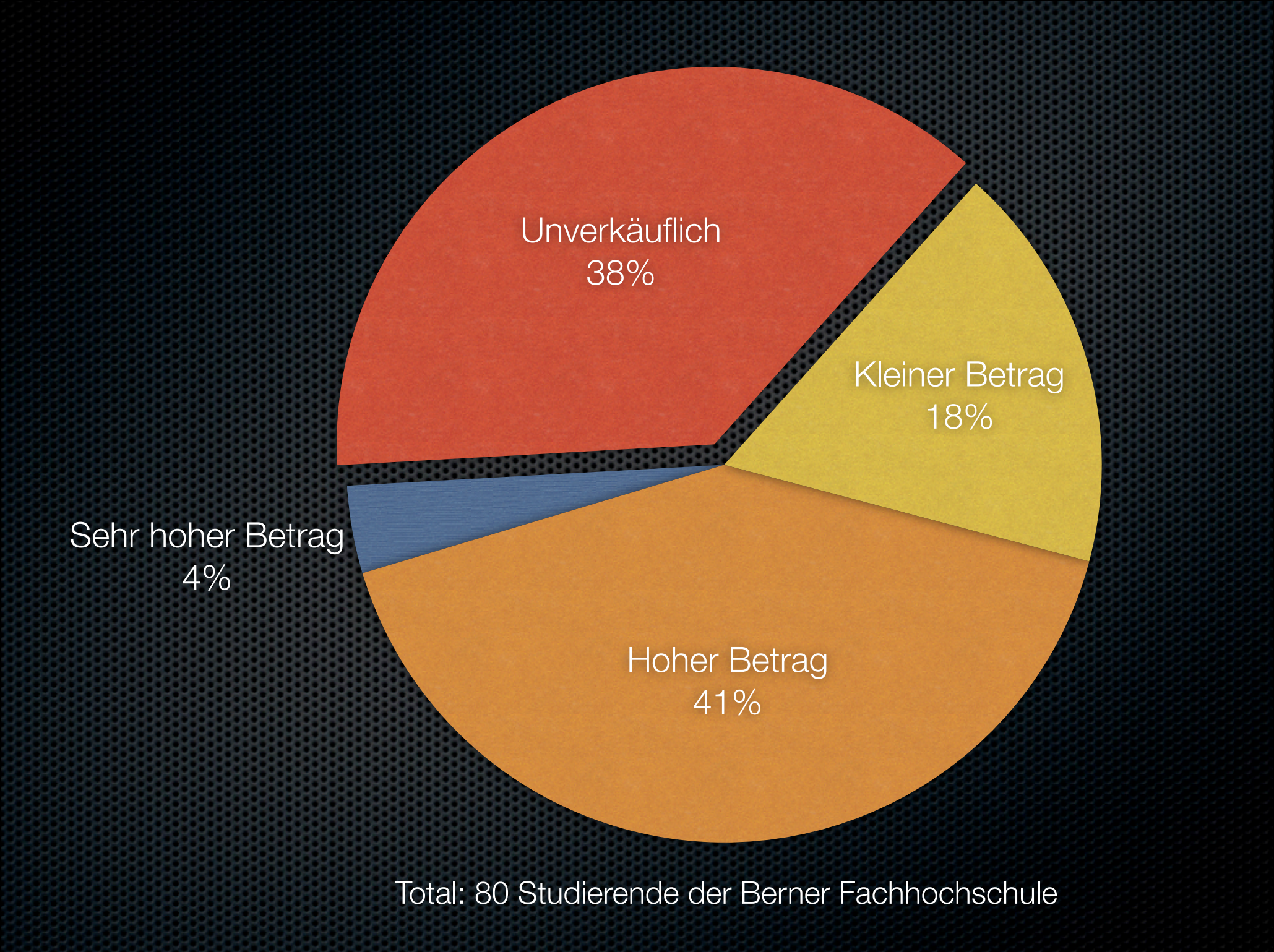

Umfrage Stimmenkauf

Umfrage Stimmenkauf I

Nehmen Sie an, Sie erhalten von Ihrer Gemeinde die Zugangsdaten (Username/PIN/etc.), um bei der nächsten eidg. Abstimmung Ihre Stimme elektronisch über das Internet abzugeben.

Stellen Sie sich zudem vor, es gäbe eine Web-Seite, auf welcher Sie Ihre Zugangsdaten diskret (z.B. über Paypal) verkaufen können.

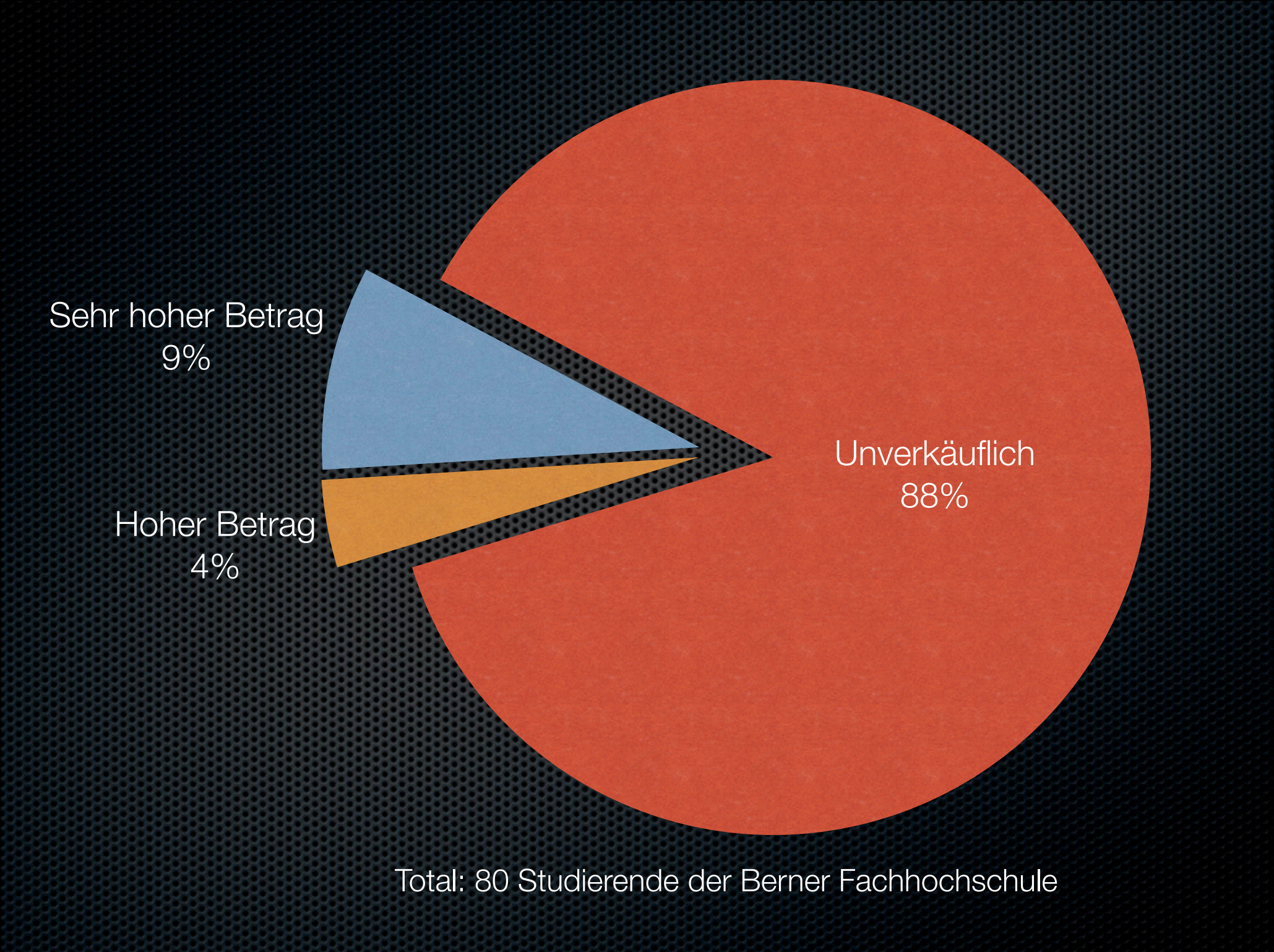
Für welchen Betrag wären Sie bereit, Ihre Zugangsdaten zu verkaufen?


Unverkäuflich
38%
Kleiner Betrag
18%
Sehr hoher Betrag
4%
Hoher Betrag
41%
Total: 80 Studierende der Berner Fachhochschule

Umfrage Stimmenkauf

Nehmen Sie an, Sie hätten vom Staat eine elektronische ID (d.h. ein digitales Zertifikat) erhalten, welche Sie für alle zukünftigen elektronischen Abstimmungen einsetzen können, wie auch für alle anderen Online-Dienste der Gemeinde, des Kantons und des Bundes (Führerschein, Steuererklärung, etc.).

Für welchen Betrag wären Sie bereit, Ihre elektronische ID zu verkaufen?



Total: 80 Studierende der Berner Fachhochschule

Vote Updating

Das E-Voting System in Estland erlaubt eine mehrmalige elektronische Stimmabgabe, wobei nur die letzte Stimme zählt

> beim Verkauf der Zugangsdaten kann die verkaufte Stimme durch eine zweite Stimme annuliert werden

> eine unter direktem Zwang abgegene Stimme kann durch eine zweite Stimme annuliert werden

> bei einem quittungsfreien System kann eine verkaufte Stimme durch eine zweite Stimme annuliert werden

Hybrides E-Voting

In einem hybriden E-Voting System kann eine elektronisch abgegebene Stimme durch eine zweite Stimme an der Urne (oder per Briefwahl) annuliert werden

> eine unter direktem Zwang abgegene Stimme kann durch eine zweite Stimme an der Urne annuliert werden

> beim Verkauf der Zugangsdaten kann die verkaufte Stimme durch eine zweite Stimme an der Urne annuliert werden

> ein nicht-quittungsfreies System wird quittungsfrei

Stimmenkauf

Lösungsansätze

1. Der Wähler-Authentifizierung eines E-Voting-Systems sollte mit Hilfe eines digitalen Zertifikates realisiert sein

2. Eine elektronische Stimme sollte entweder
   > durch eine andere elektronische Stimme
   > durch eine Stimme an der Urne
   > durch eine brieflich abgegebene Stimme
   annuliert werden können

Inhaltsverzeichnis

Fazit

1. “Security by Transparency” statt “Security by Obscurity”
2. Transparenz mit Hilfe eines Bulletin Boards ermöglicht das individuelle und universelle Verifizieren
3. Blinde Signaturen lösen den Konflikt zwischen genauer Authentifizierung und Anonymität
4. Authentifizierung mitttels elektronischer ID (Zertifikat) reduziert das Risiko des Stimmenverkaufs
5. Vote Updating und hybride Systeme sind gute Lösungs-Ansätze für das Problem des Stimmenkaufs

Schlusswort

"We will work together to ensure the public trust and establish a system of transparency [...]."

Barack Obama, 21. Januar 2009

TrustVote Protokoll

TrustVote: A Hybrid E-Voting System for Large-Scale Elections

Rolf Haenni, Reto Koenig, Stephan Fischli, and Eric Dubuis

Bern University of Applied Sciences, Höheweg 80, CH-2501 Biel
{rolf.haenni,reto.koenig,stephan.fischli,eric.dubuis}@bfh.ch

Abstract. This paper presents a hybrid e-voting system, in which a transparent e-voting protocol is embedded in a traditional paper-based voting procedure. To guarantee vote anonymity, the protocol itself is based on a scalable blind signature scheme with multiple authorities. An anonymous channel is used to cast the encrypted votes onto the public board. To prevent vote buying and vote coercion, we depart from the mainstream approach of taking additional measures to guarantee receipt-freeness. Instead, we propose to exploit the existence of a receipt to allow vote revocations over the enclosing paper-based voting procedure.