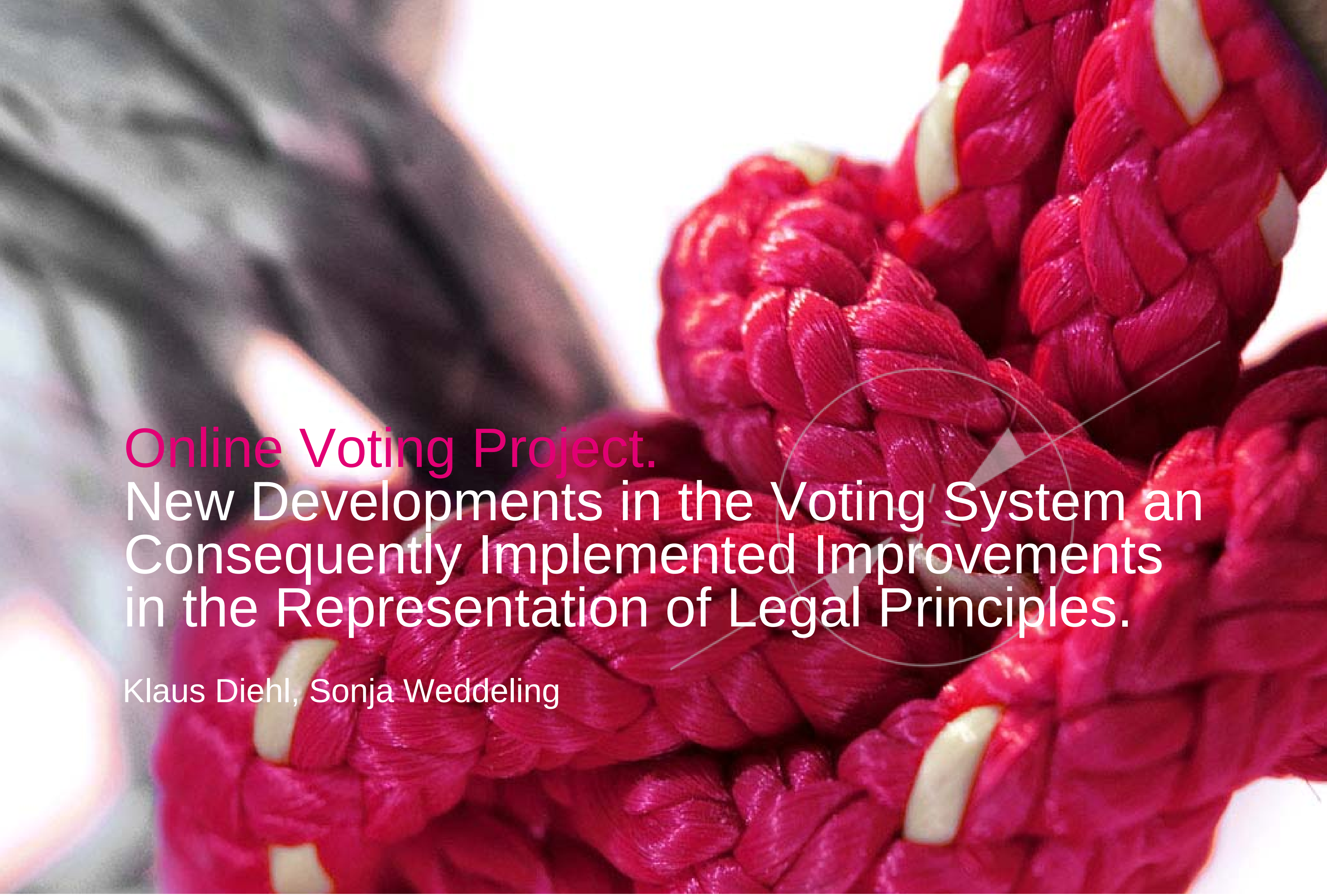


Online Voting Project.

New Developments in the Voting System an Consequently Implemented Improvements in the Representation of Legal Principles.

Klaus Diehl, Sonja Weddeling

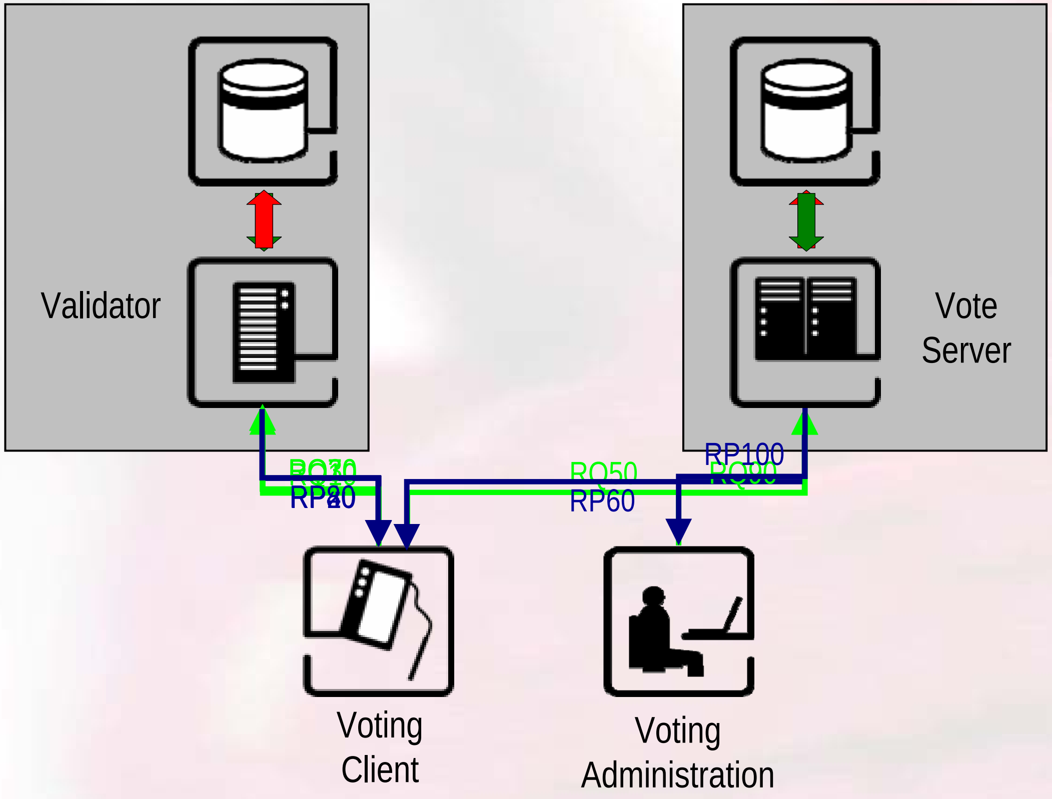
T · · Systems

Online Voting Project.
Introduction.

- Since 2001 T-Systems made research on secure online voting systems in cooperation with the PTB and other prominent institutes under the support of the Federal Ministry of Economics
- Last year the voting systems developed in the W.I.E.N. project underwent a security review by the Technical University of Darmstadt
- Because of some security flaws the whole architecture of the system was rebuild with regard to special cryptological add-on modules and the optimization of the client-server communication
- At this time the project is in the planning of a certification process on the Common Criteria for the new implemented system which runs in cooperation with the BSI and an accredited testing centre. Besides, the voting system should be subject to a comprehensive check by the PTB
- The system is now being developed to a remote voting system

Online Voting Project.
Technical Modification of the Voting System.

Previous voting protocol



RQ10: Registration of Voting
RP20: Issue of Voting Documents
Voting phase
RQ30: Request of blinded Voter Signature
RP40: Issue of blinded Voting Register Signature
RQ50: Delivery of the Vote
RP60: Confirmation of Ballot Box
RQ70: Confirmation for Register of Voters
RP80: Confirmation of Register of Voters
RQ90: Initiate counting
RP100: Receipt Votes for counting

Online Voting Project.
Technical Modification of the Voting System.

- This voting protocol devised previously in W.I.E.N. entails the physical and administrative separation of the voting register and the ballot box and also includes the separation of vote and identity
- The most important elements are the *Validator* (provides the electronic voter register), the *Ballot Box* (contains the electronic ballot box) and the voting *Client* himself
- Separated storage of persistent dates (Problem: redundant data management – inconsistency of communication problems)
- For the purpose of anonymity the identity is strictly separated during the whole communication (the voting register knows the identity, the Ballot Box does not)

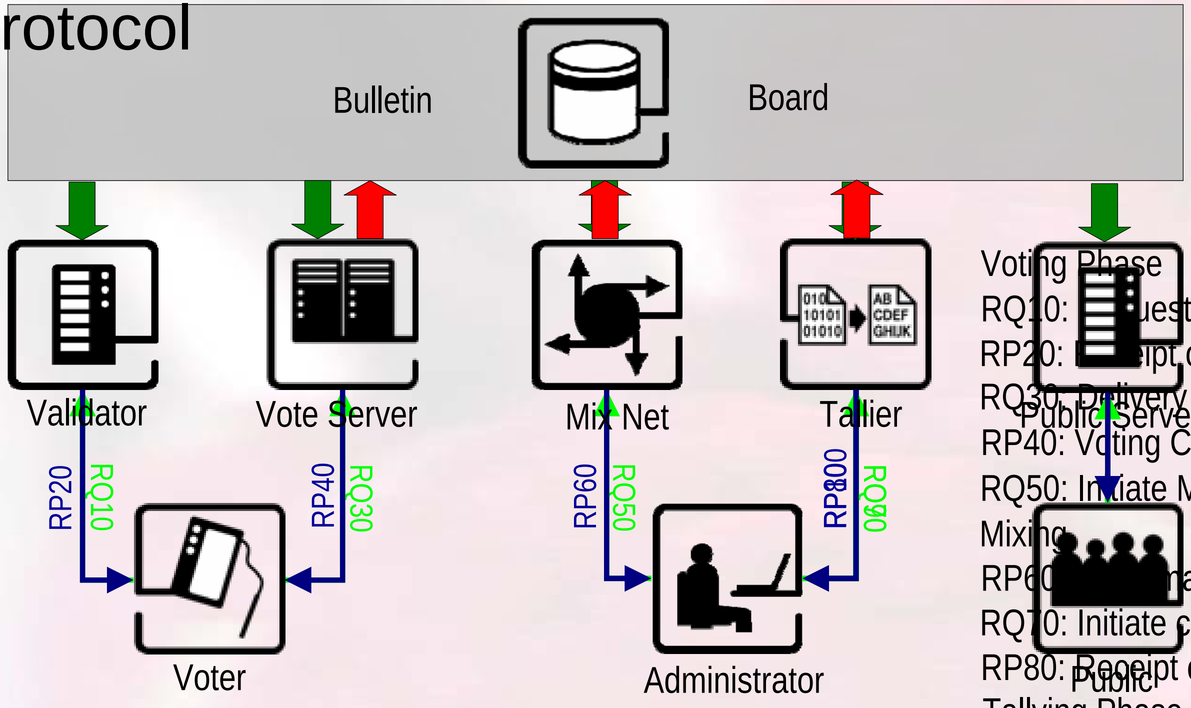
Online Voting Project.
Technical Modification of the Voting System.

- Technically laborious recovery procedure in case of incidents
- The protocol is based on the use of blind signatures and other cryptographic procedures but remains time-consuming, laborious and insecure in some important aspects
- That’s why T-Systems developed by means of the TU Darmstadt a new voting scheme, which is simpler and easier to implement and offers a better security level
- The main principles of the former architecture have remained the same, like the use of blinding or the division of powers

Online Voting Project.

Technical Modification of the Voting System.

Newly implemented voting protocol



Voting Phase

RQ10: Request vote validation

RP20: Receipt of blinded Validator Signature

RQ30: Delivery of the vote with Validator Signature

RP40: Voting Confirmation

RQ50: Initiate Mixing / Collection of the votes

Mixing

RP60: Confirmation of Mixing

RQ70: Initiate counting of the mixed votes

RP80: Receipt of the mixed Votes for counting

Tallying Phase

RQ90: Publishing election result / tallier key

RP100: Conformation of successful publishing

Online Voting Project.
Technical Modification of the Voting System.

- The new implemented voting protocol has five main players: The *Voting Client* (which can be found at home, in a working station, in a special polling station or from any other end device), the *Mix Net* (separates the encrypted votes from the identity of the voter and randoms the order), the *Tallier* (counts and encrypts the mixed votes) , the *Validator* (proof of voter authorisation and issue of Validator signature) and the *Bulletin Board* (central data storage)
- The *Bulletin Board*
  - is a consistent data base for all participants
  - plays an absolutely passive role and is not able to communicate with the other players.
  - It has the function as a placard, because after the election the public has the possibility to check if certain votes are counted and if they are counted in a correct manner. It shows not only the counted votes but also the the Tallier key.
  - It is not possible for anyone to delete or to overwrite messages on it

Online Voting Project.
Technical Modification of the Voting System.

- The protocol is supplemented with some cryptographic components like
  - the use of blinding and mixing by David Chaum and
  - the use of a public key system
- Furthermore it is assumed that
  - a trustworthy PKI is available,
  - the use of a communication protocol like TCP/IP based on TLS, which guarantees authentication of parties
  - the voting booth, the mix net and the bulletin board are considered trustworthy
- Policies regulate the logical and organisational separation of identity and vote

Online Voting Project.
Technical Modification of the Voting System.

The main advantages of the new protocol are the following:

- **Public transparency by the bulletin board (publication of tallier key, etc.)**
- **Inured to technical troubles like interruption of access, etc, uncomplicated recovery**
- **Possibility of configuration for different voting models by policies**
- **Greater performance**

Online Voting Project.
Adherence to Voting Legislation Principles.

- The five main voting legislation principles in Germany for publicly regulated elections are
  - **universality** (everyone has the same rights to vote)
  - **directness** (everyone has to vote by himself without deputies)
  - **freedom** (everyone should vote without impact of any kind)
  - **equality** (everyone's vote has the same weight)
  - **secrecy** (everyone must cast his vote unobserved)
- Apart from that, the **accessibility to the public** in the voting procedure plays a special role, which means that the voting result can be monitored, although casting of the votes has to be secret as a matter of course. Accessibility to the public is necessary for all voting stages and is performed by the electoral committee, but also by any member of the public.

Problem: Remote Internet Voting removes the location of voting from public view!

Online Voting Project.
Adherence to Voting Legislation Principles.

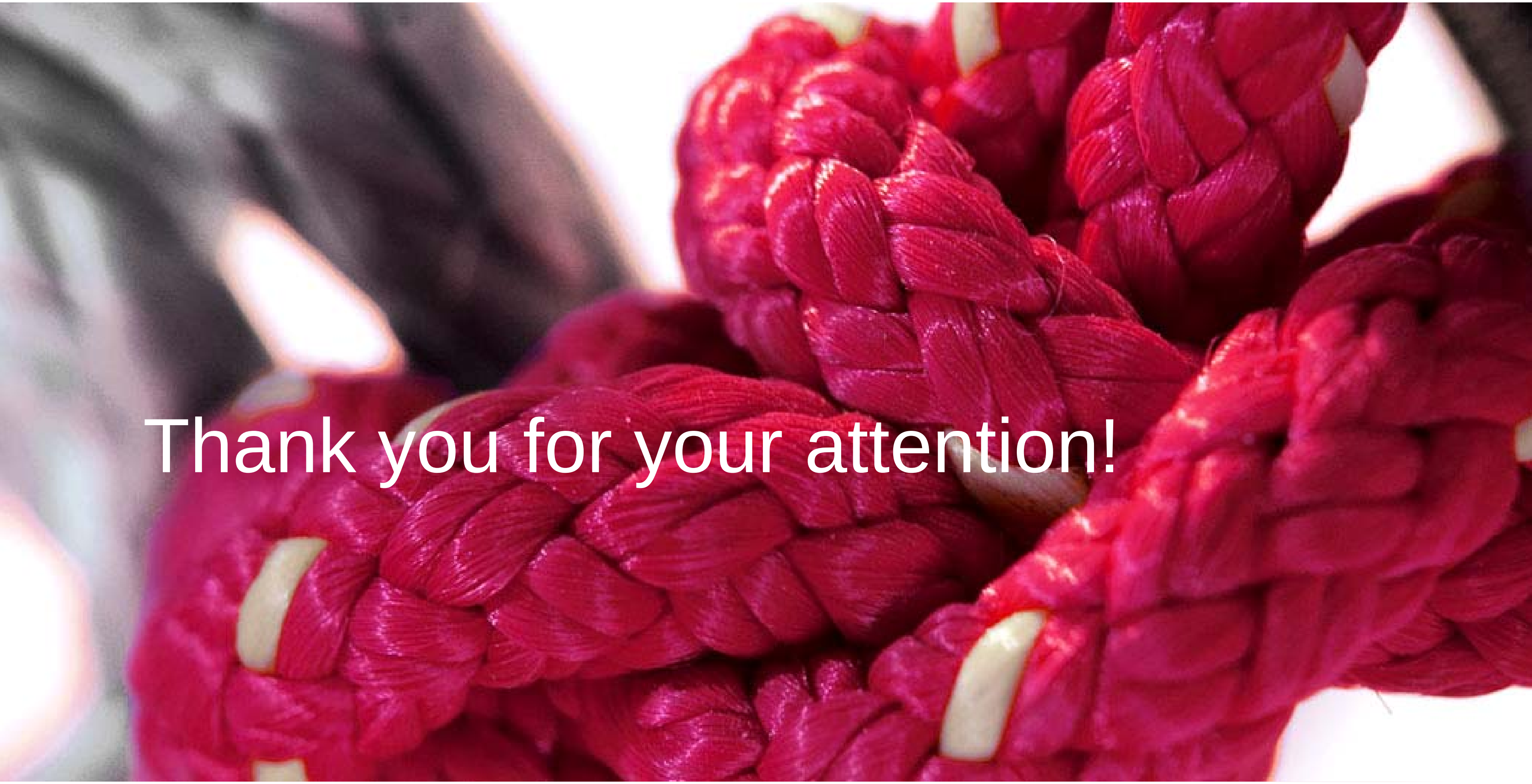
- Furthermore there are several auxiliary principles for the voting act like
  - comprehensibility (everyone must be confronted with a simple voting act)
  - simultaneity (everyone must cast his vote in the same period)
  - free of charge (everyone's voting act must be free of charge for the voter)
- In conclusion these aspects should be considered by creating an electronic voting system

Online Voting Project.
Adherence to Voting Legislation Principles.

- The new developed voting system considered the prevailing legislation principles like the Federal Electoral Law
- The addition of the bulletin board comprehensively delivers an advantage of postal voting by increasing the principle of **accessibility to the public**
- The public must be able to monitor the correct implementation of the election at all times – that’s why they have available access to contend on the bulletin board if this aspect is desired by the electoral boarder
- Moreover the principle of **universality** is also increased by giving more access options to the voter

Online Voting Project.
Conclusions.

- Most legal reservations against electronic voting were rebutted
- The new voting protocol became not only simpler and got a higher security level but also now offers a better integration of the general public – a special criticism point often mentioned in the public discussion
- All this brings us one step closer to feasible electronic voting models for elections in the range of operational but also political elections
- Recently accomplished voting projects in the Germany Telekom Group exemplified the simple use of online voting systems and the great advantages concerning economics and democracy



Thank you for your attention!