How to create trust in electronic voting over an untrusted platform

The 2nd International Workshop on Electronic Voting 2006

Gerhard Skagestein and Are Vegard Haug
University of Oslo

Einar Nødtvedt
Senit Rådgivning AS

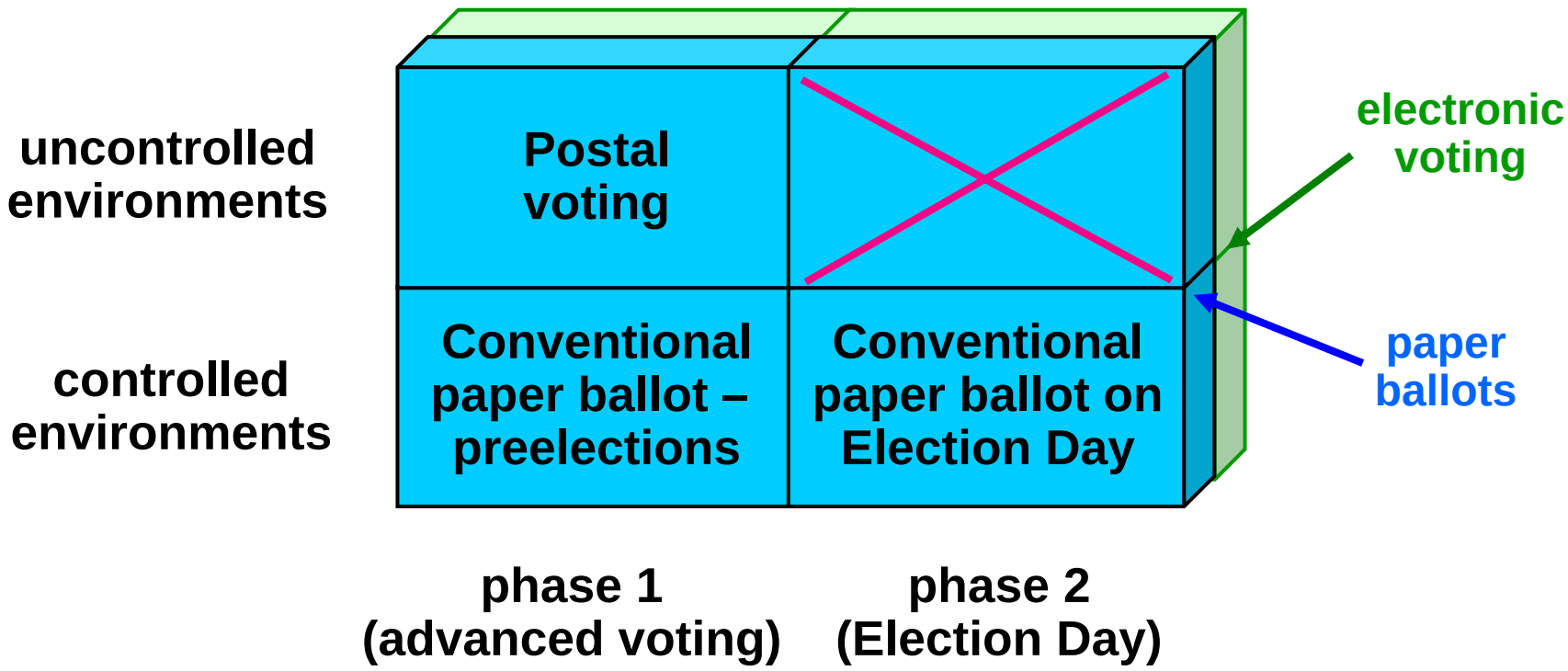
Judith Rossebø
Norwegian University of Science and Technology / Telenor R&D

Bregenz August 2nd to 4th 2006

The background

- In 2004, the Norwegian Ministry of Local Government and Regional Development appointed a working group for giving recommendations on the future of electronic elections in the country
- The results were published in January 2006, see the report Elektronisk stemmegivning – utfordringer og muligheter (Electronic voting – challenges and possibilities) http://odin.dep.no/krd/norsk/dok/andre_dok/rapporter/016051-220023/dok-bn.html (in Norwegian)
- An English version of the report is under production http//:www.e-valg.dep.no
- This presentation (and the paper) discusses one important topic in the report, namely how to achieve trust in e-voting over an insecure system like a home PC connected to Internet
- Three of the authors were members of the working group

Vote casting alternatives



One important regulation

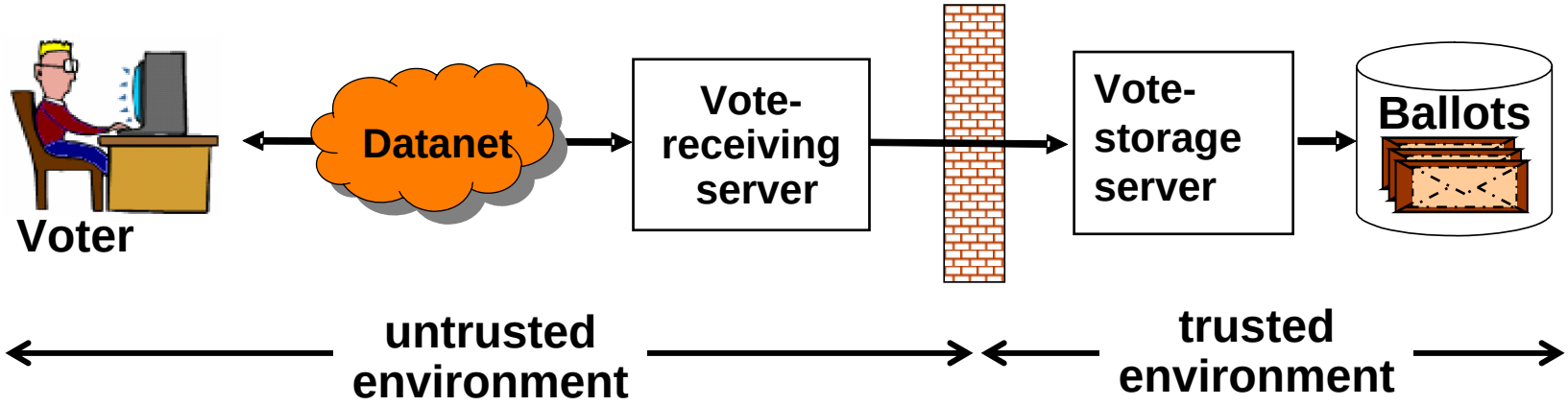
The Legal, Operational and Technical Standards for E-voting

Recommendation Rec(2004)11 adopted by the Committee of Ministers of the Council of Europe **(the "Recommendation") states:**

I. Transparency

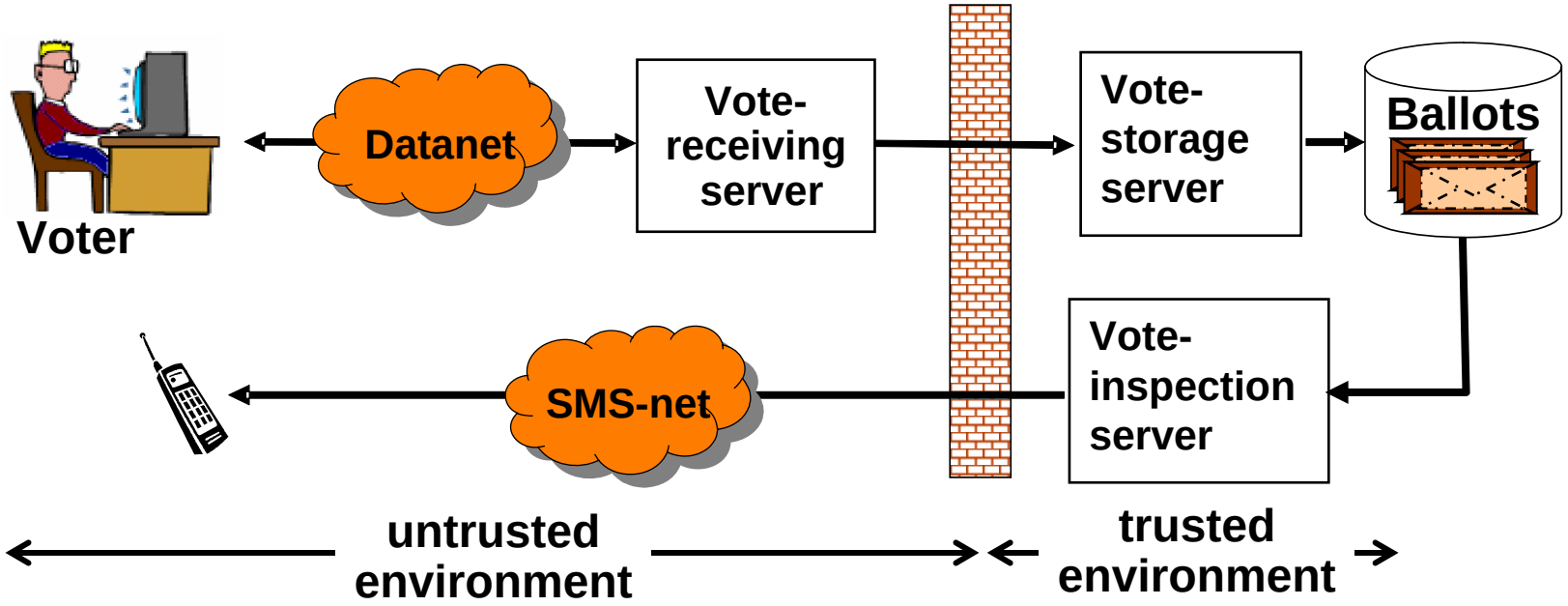
20. Member states shall take steps to ensure that voters understand and have confidence in the e-voting system in use.

How can the voter know that his vote has been correctly registered?



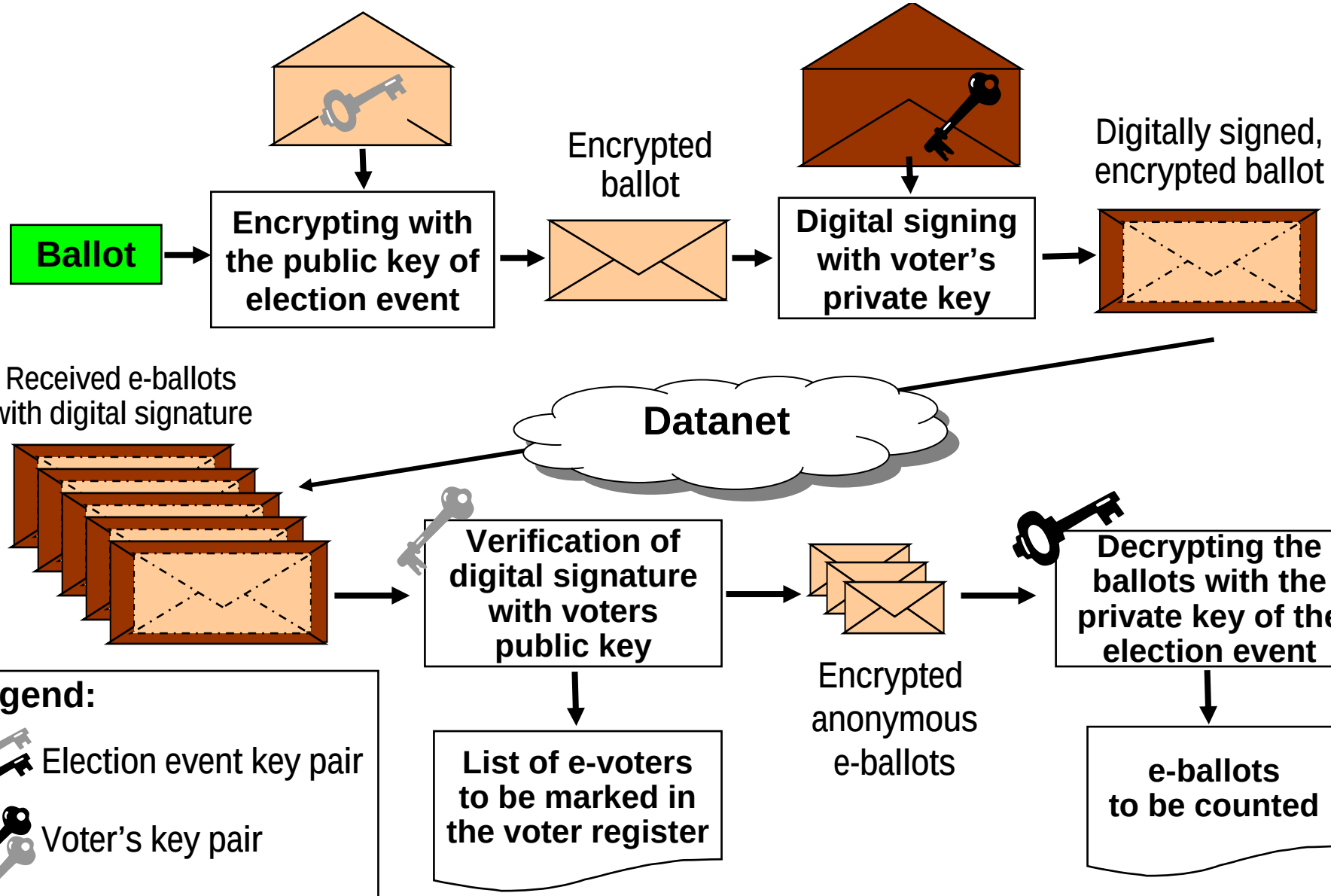
- Ask the voter to cast his vote several times – preferably through different channels – and let the server compare notes and confirm
  - not completely safe
  - cumbersome for the voter
  - the difference between confirmation casting and recasting?
  - the voter may still feel insecure

How can the voter know that his vote has been correctly registered? (cont.)



- The voter may ask the trusted system to return the content of his vote, possibly through an alternative channel
  - gives the voter high confidence in correct registration
  - … but how keep the vote secret to everybody else?

The double envelope principle



The double envelope principle…

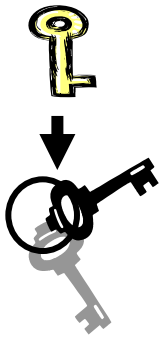
…ensures

- **the secrecy and the authenticity of the vote**
- **that the voters identity and the content of the vote can never be connected**
- **but how is it possible for the vote-inspecting server to break the inner envelope without access to the private key of the election event?**

The hybrid crypto principle

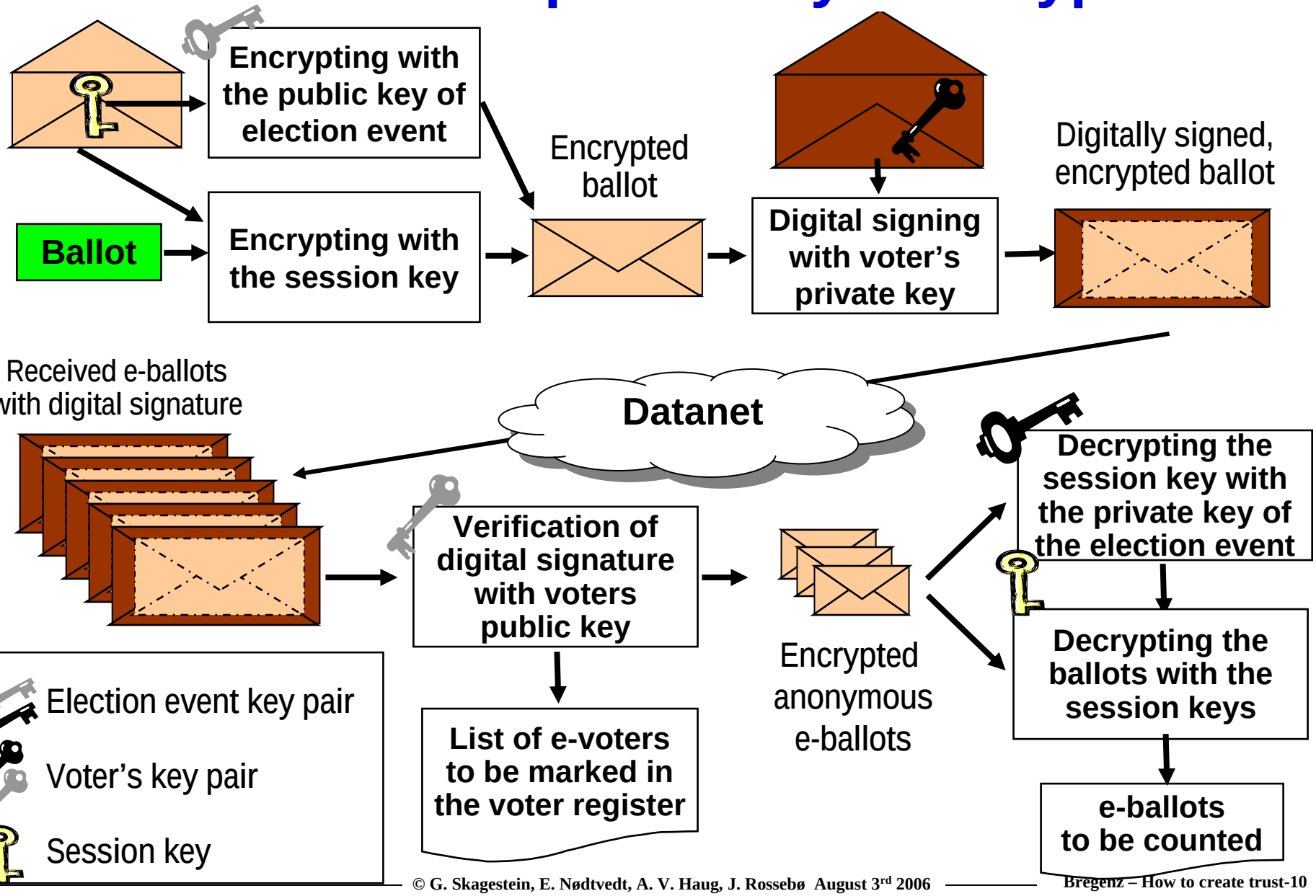
- **Symmetric cryptography:**
  The same key is used for encryption and decryption

- **Asymmetric cryptography:**
  One key of a key pair is used for encryption, the other key of the key pair for decryption



- **Hybrid cryptography:**
  The message is encrypted symmetrically by a randomly selected session key, which is then encrypted asymmetrically.
  To decrypt, the session key is decrypted asymmetrically, then the message is decrypted symmetrically with the session key.

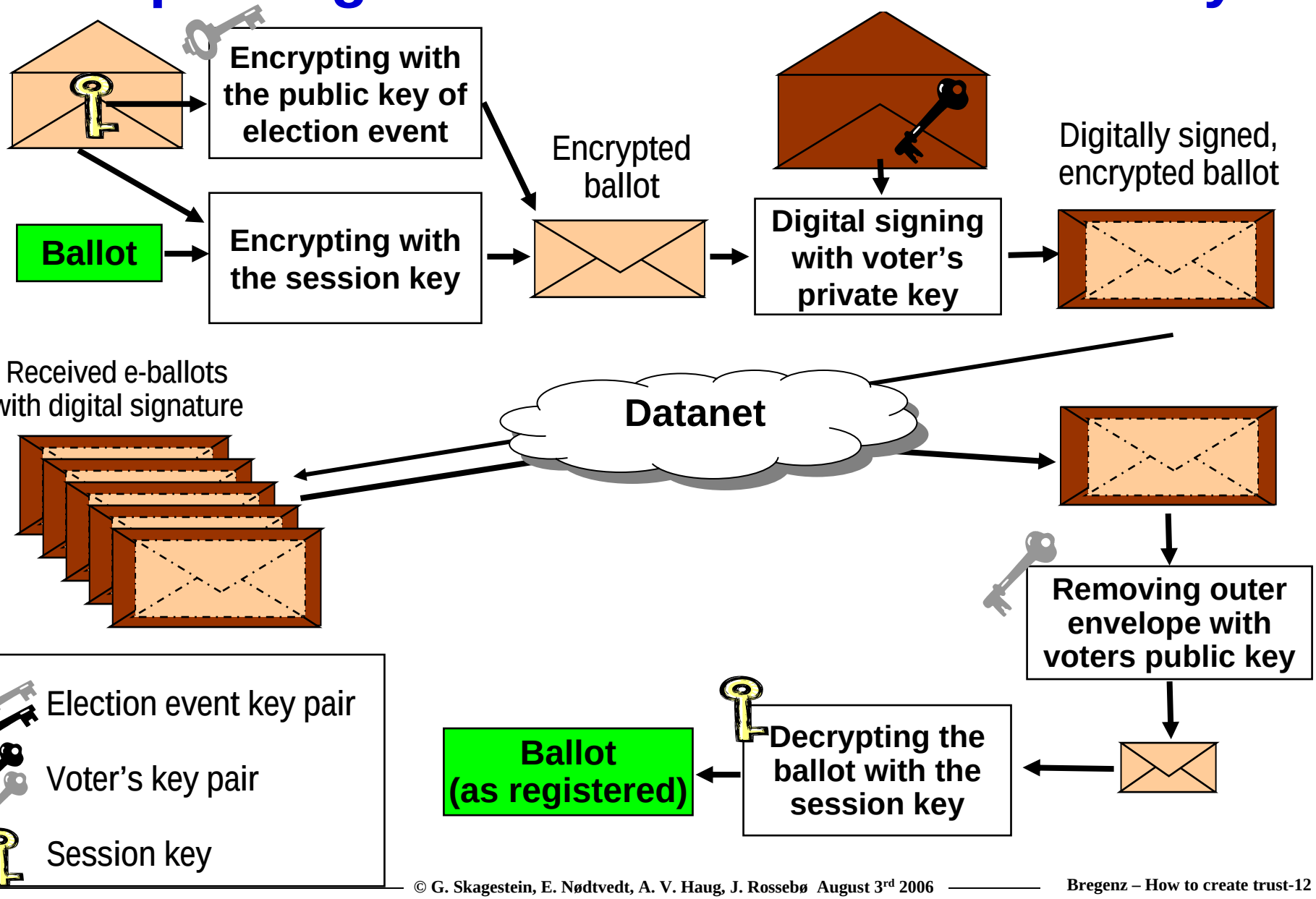
Double envelope with hybrid crypto



The session key

- Hybrid crypto with a session key is traditionally used for *efficiency reasons*
- In this solution, we will use the session key also to allow the voter to inspect his registered ballot
- For inspecting the ballot, the voting client must keep the session key
- For inspecting the ballot through other channels, the session key must be transferable to the client on the other channels

Inspecting the vote with the session key



Another important regulation

The Legal, Operational and Technical Standards for E-voting

Recommendation Rec(2004)11 adopted by the Committee of Ministers of the Council of Europe **(the "Recommendation") states:**

IV. Voting

51. A remote e-voting system shall not enable a proof of the content of the vote cast.

The importance of allowing recasting of votes

- Recasting of votes eliminates the well-known problems with voting in uncontrolled environments
  - coercion – “family voting”
  - buying/selling votes
  - compromising the secrecy of the vote

  because nobody can know whether the current vote will be the final one
- The working group proposes that the final vote may be cast on Election Day in controlled environments by means of a paper ballot
- The technical solution comes at almost no additional cost

Why we need the identity of the voter connected to the e-ballot

The rule: One voter – one vote

How to enforce it?

- **On the client side**
  - **invalidate credential, then cast anonymous vote**
  - **cast anonymous vote, then invalidate credential**

  – both are unsafe!
- **On the server side**
  - **reject or throw away duplicate ballots from the same voter**

  – then we need the identity of the voter or of his credentials

How to handle duplicate e-votes

Duplicate e-ballots from the same voter may be handled in several ways:

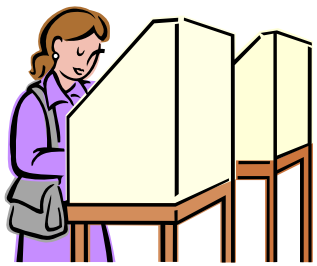
- **Reject e-ballot if there already exist a e-ballot from this voter**
  - **difficult to handle if the e-ballots are stored on several servers**
  - **may cause delays during online voting**
- **Delete the previous e-ballot, store the new one on the fly (overwrite)**
  - **allows recasting of e-votes**
  - **difficult to handle if the e-ballots are stored on several servers**
  - **may cause delays during online voting**
- **Accept and store all the e-ballots,**
  pick the last one at the end of the voting period
  - **allows recasting of e-votes**
  - **duplicate ballots can be thrown out offline in a batch process**

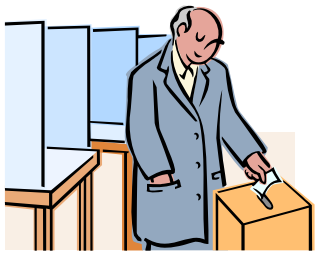
Identification and authentication of the voter

- Identification and authentication of the voter should be done by a generally available PKI-system (citizen identity card)
  - cheaper that a special purpose election credential
  - the voter will not be tempted to sell it
- The e-vote may be connected to the voters real identity, or to a derived pseudo-identity
  - the working group recommends using the real identity, since this makes the canceling of e-votes in case of revoting on Election Day easier

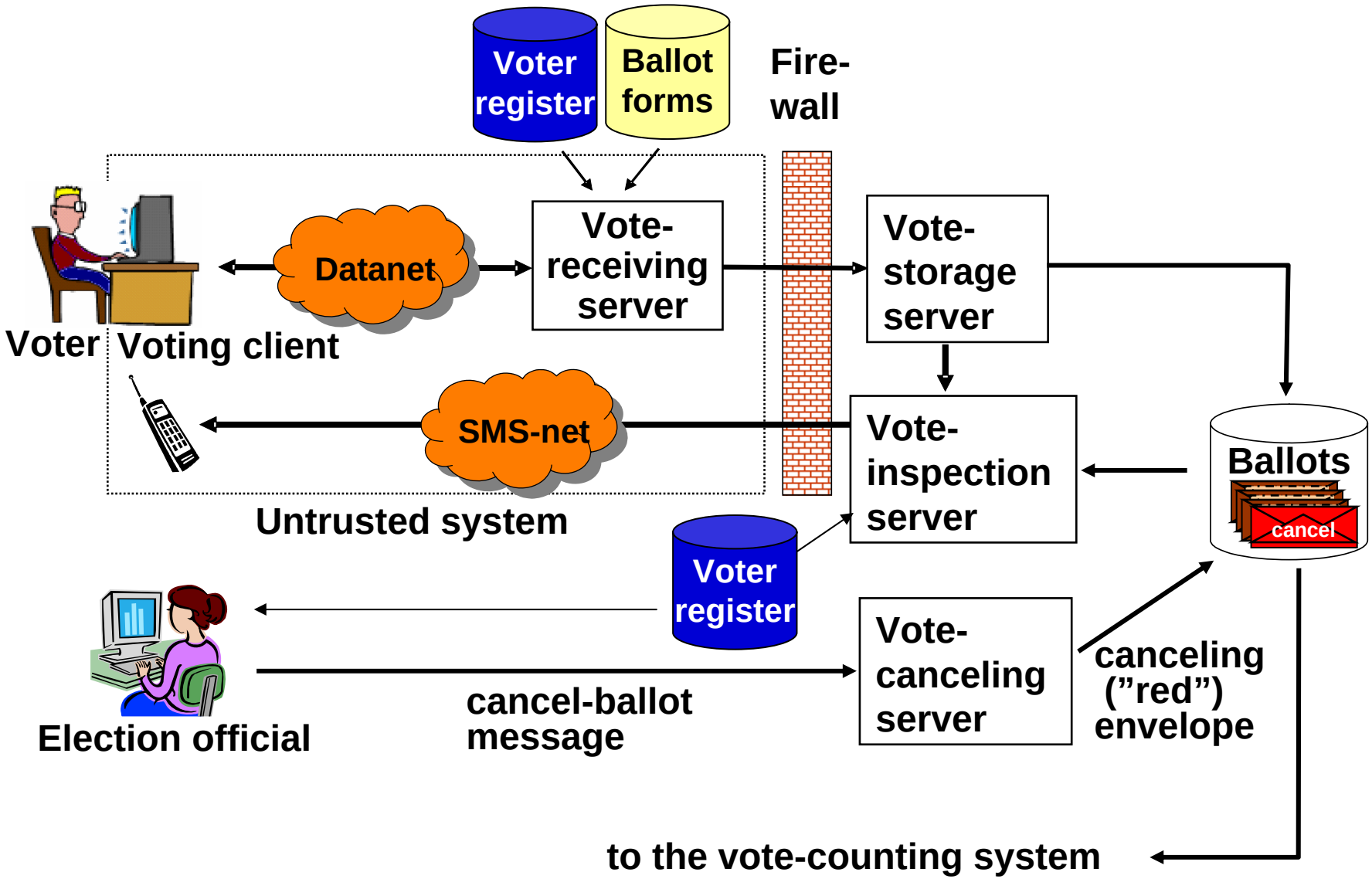
On Election Day…

- … the Election officials will have access to an updated Voter register, where the e-voters have been marked
- When an e-voter shows up in the polling station, the Election official will send a ”cancel-ballot”-message to the e-voting system before allowing the voter to vote by traditional means (i.e. anonymous paper ballot in controlled environment)

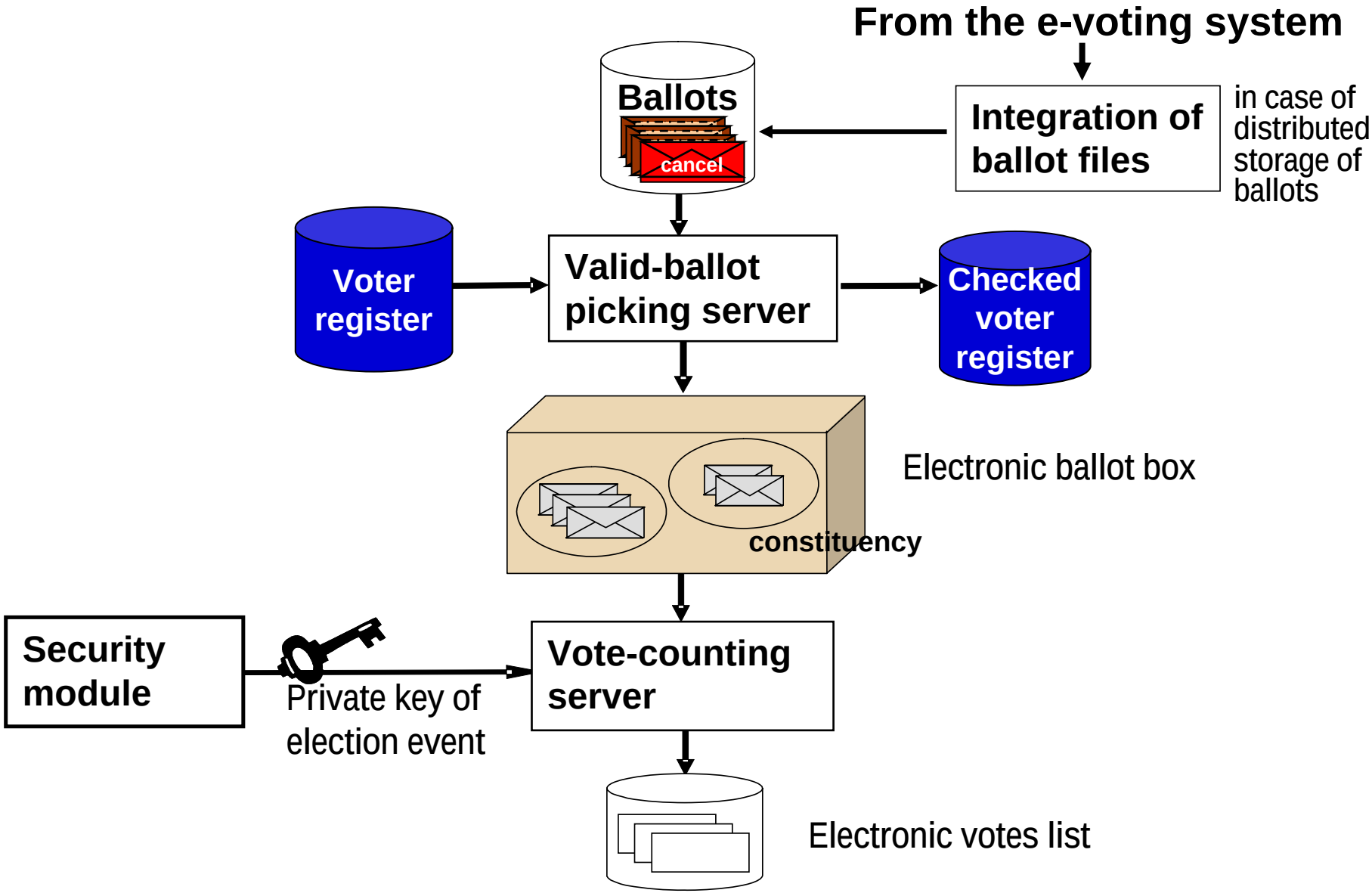




Architecture of the e-voting system



Election is closed – time to count



Basic Design Principles

- E-voting is allowed in phase 1 only
- Repeated casting of e-votes is allowed
  - last ballot counts
- The e-voter is allowed to inspect his e-ballot as it is registered
- Traditional voting with paper ballots in controlled environments on election Day is maintained
- Any paper ballot takes precedence over the e-ballot

What about the secrecy of the vote?

Wouldn't this solution increase the risk for disclosing the secret vote to other people?

Yes, but

- **the vote-inspection server should authenticate the voter just as thoroughly as the vote-receiving server**
- **with the session key, the vote can only be inspected, not modified**
- **it is the responsibility of the voter to keep the session key unavailable to other people**
- ***if the vote is disclosed, there is no way to know whether this is the final vote***

Summary

- We have shown that by relaxing there requirement for an absolute secrecy of the vote, the vote as registered may be inspected by the voter
- This possibility for inspection gives the voter trust in the untrusted part of the system
- The loss of secrecy is compensated by the possibility to revote, even by traditional means on Election Day
- The Election Day should be kept free of any kind of e-voting
- § 51 of the Recommandation should read
  A remote e-voting system shall not enable a proof of the content of the *final* vote cast.

And then?

- Because the voter has complete freedom in how to vote, the possible shift towards e-voting will be driven by the voters themselves, not by the authorities or the technology
- The working group recommends progress at a slow pace
  - Introduction of e-voting in controlled environments
  - … in the beginning, only for selected elections and for advisory polls
  - release in uncontrolled environments for selected groups of voters only (replacing most of the postal voting)
  - full scale offering if the voters and the society want it