

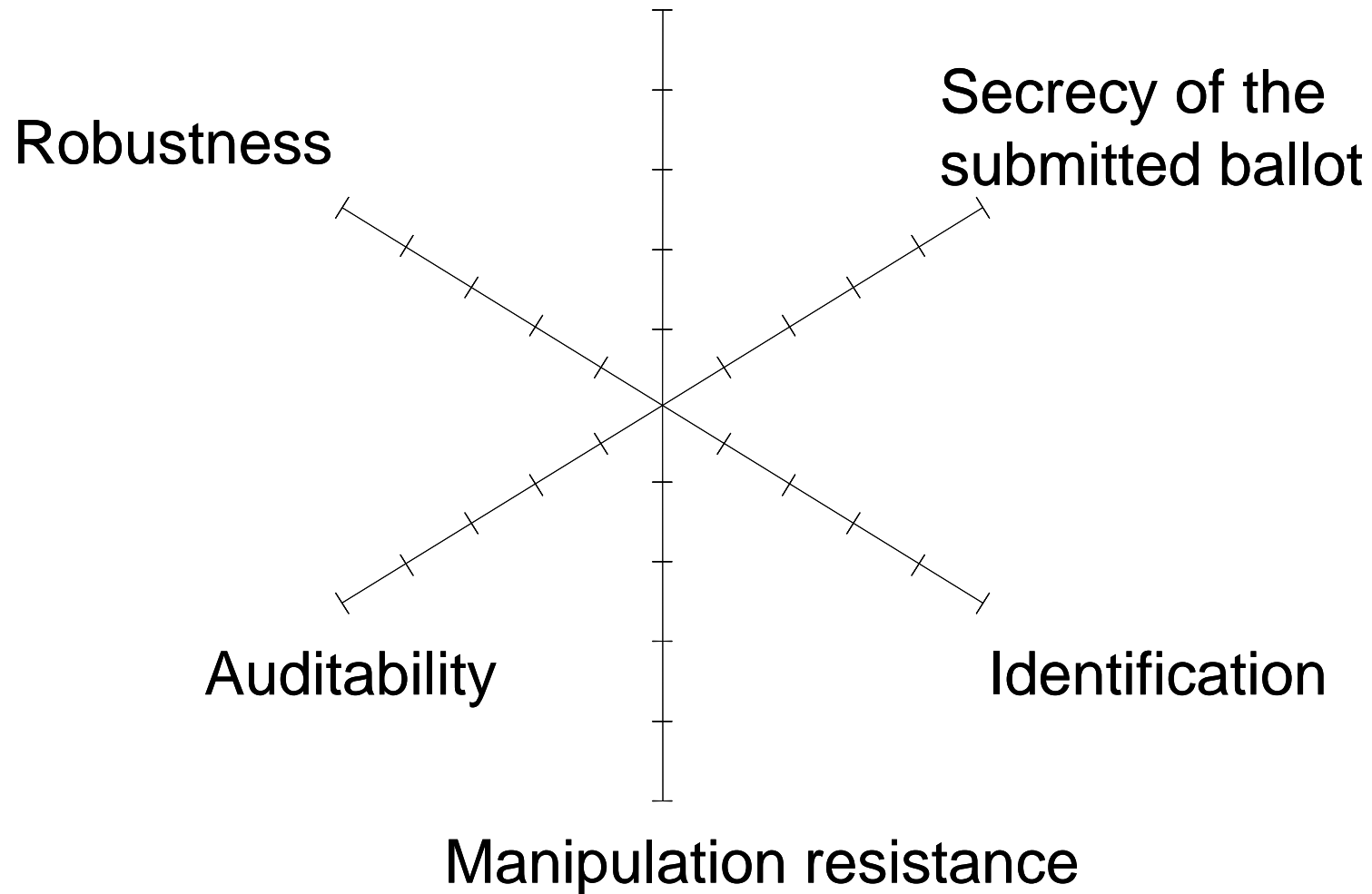
---

# The Voting Client and Rec 2004(11) of the Council of Europe

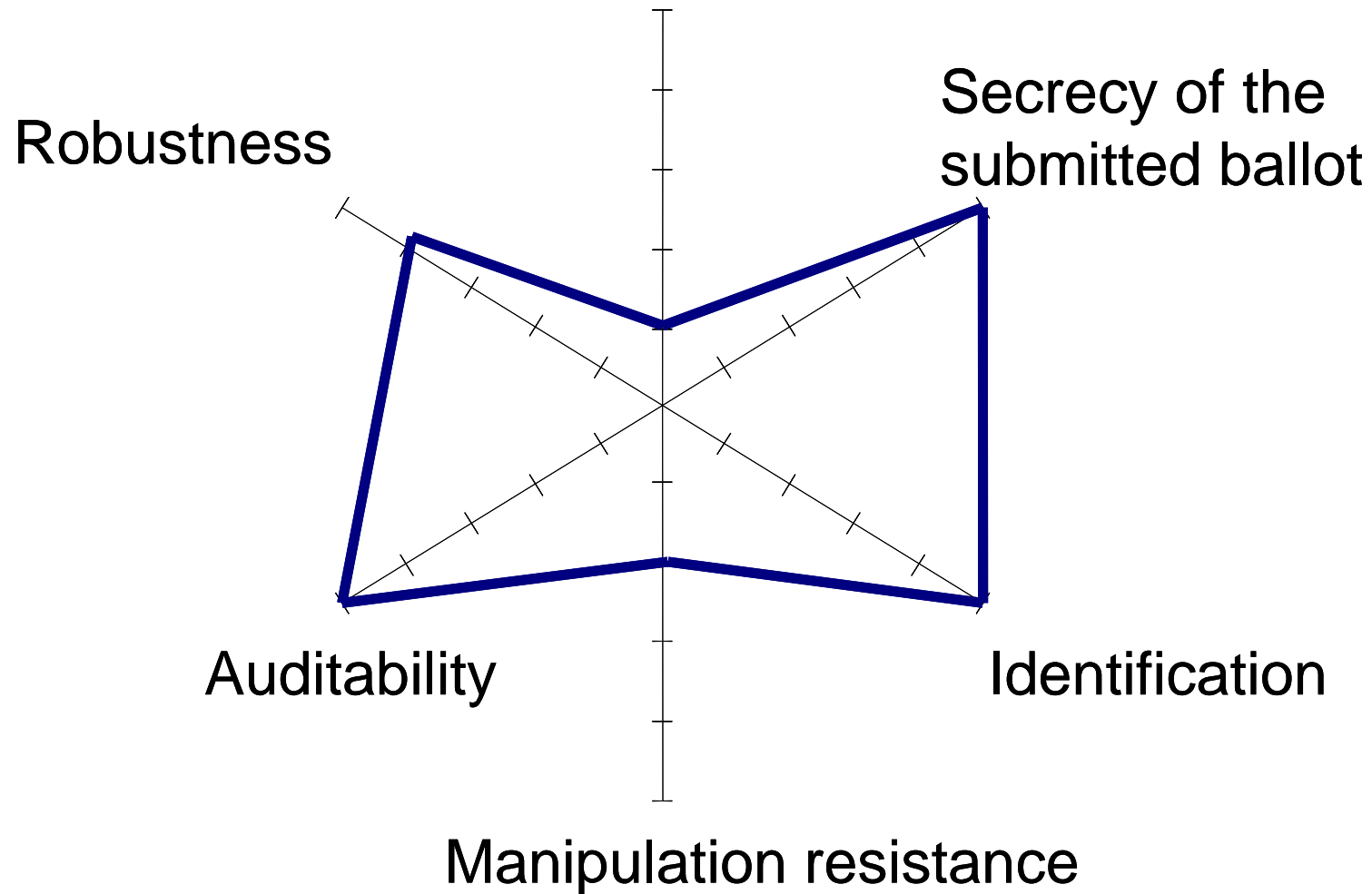
Alexander Prosser



## Protection from vote buying and coercion



## Protection from vote buying and coercion



Council of Europe: Rec 2004(11) for political elections:

- legal
- operational
- technical

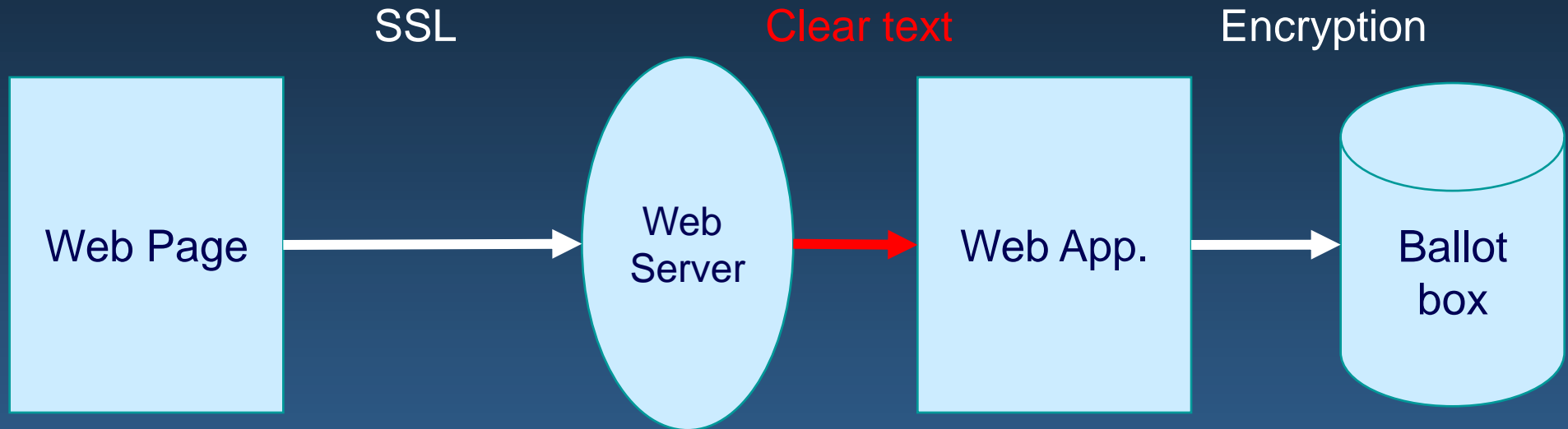
minimum standards for e-voting  
(Internet and terminals)

Includes manipulation of the voting system:

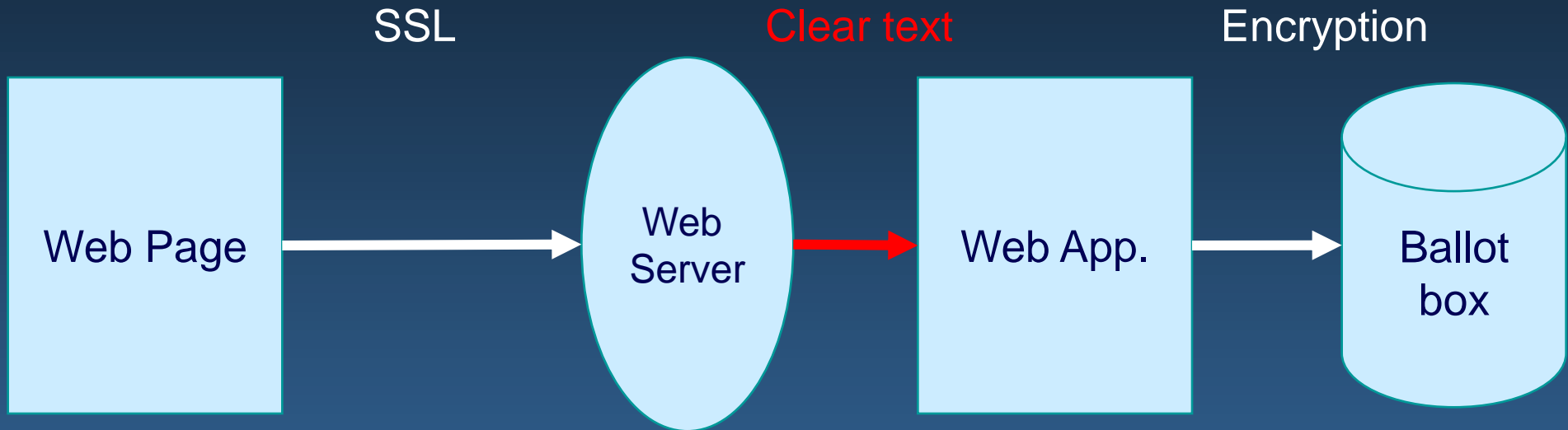
- T.Audit\_Forgery
- T.Hack
- T.System\_Forgery
- T.Ballot\_Forgery (outgoing / incoming)
- T.Vote\_Confidentiality
- T.Vote\_Modify
- ...

What does protection from administrator fraud imply for the voting client ?

# Implementation of the voting client:



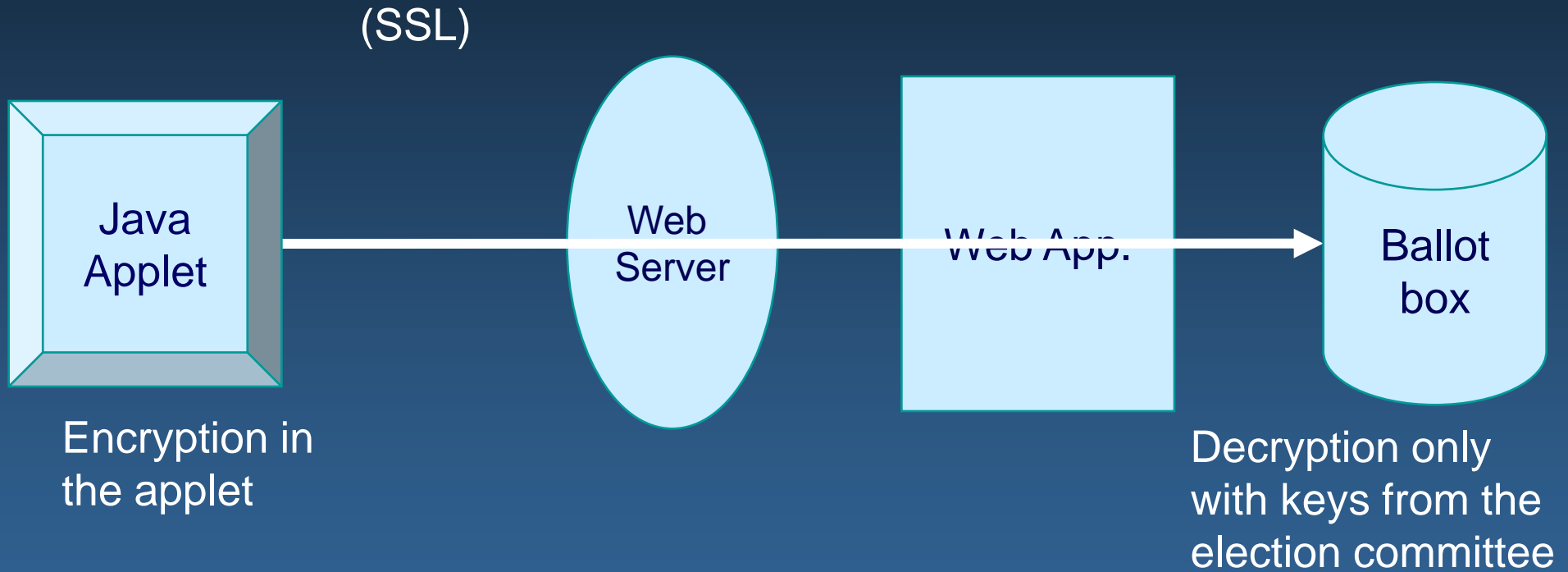
# Implementation of the voting client:



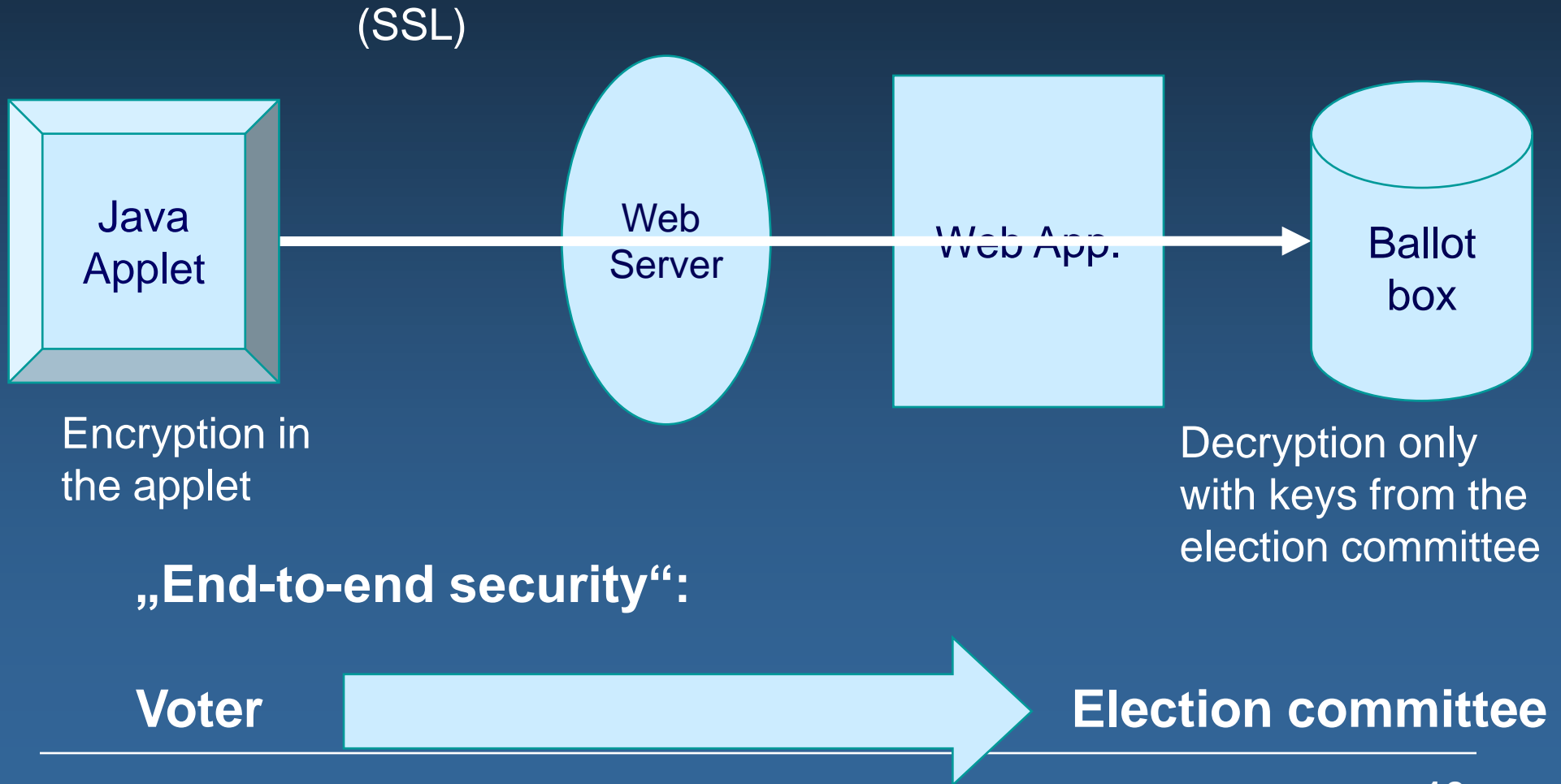
- T.Vote\_Confidentiality
- T.Vote\_Modify
- T.Ballot\_Forgery
- ...

=> Following encryption is a „placebo“

# Implementation of the voting client:



# Implementation of the voting client:



# Authentication of the voting client:



Web page with SSL:

Is this the right Web server?

Yes

Is this the right voting client?

No

- T.System\_Forgery
- T.Audit\_Forgery
- T.Ballot\_Forgery
- T-Vote\_Modify
- ...

# Authentication of the voting client:



Java applet (with/without SSL):

Is this the right Web server?

Yes

Is this the right voting client?

Yes

## Refutable hypothesis:

No election system, whose voting client is a mere Web application can meet the requirements of Rec. 2004(11) – independent of the cryptographic protocol implemented.



# Alexander Prosser

Dept. for Information systems and operations, Univ. Economics and Business

Administration, Augasse 2-6, A-1090 Vienna

[alexander.prosser@wu-wien.ac.at](mailto:alexander.prosser@wu-wien.ac.at)

# Domenica Bagnato

Hierodiction GmbH, Rabengasse 6, A-2230 Gänserndorf

[domenica.bagnato@hierodiction.com](mailto:domenica.bagnato@hierodiction.com)

# Robert Müller-Török

Inteco GmbH, Stethaimerstr. 32-34, D-84034 Landshut

[r.mueller-toeroek@inteco.de](mailto:r.mueller-toeroek@inteco.de)