

<http://www.e-Voting.at>

---



# **Kryptographische und operationale Aspekte des BVerG2006 unter besonderer Berücksichtigung der §§113-116 und Anhang XVII**

*Alexander Prosser*

*Robert Müller-Török*



# Abgrenzung Public e-Procurement:

- Herstellung eines Vertragsverhältnisses (e-Tendering)
- Abwicklung (z.B. e-shop.gv.at)

# Abgrenzung Public e-Procurement:

- Herstellung eines Vertragsverhältnisses (e-Tendering)
- Abwicklung (z.B. e-shop.gv.at)

# Neuregelung elektronischer Verfahren:

- Abgabe von Angeboten (typischerweise im offenen Verfahren)
- Auktionen
- „dynamische“ Beschaffungssysteme
- Elektronisches Erbringen von Nachweisen

# Neuregelung elektronischer Verfahren:

- Abgabe von Angeboten (typischerweise im offenen Verfahren)
- Auktionen
- „dynamische“ Beschaffungssysteme
- Elektronisches Erbringen von Nachweisen

# Ablauf:

Zusammenstellen/Binden der Angebotsunterlagen	Hashwertberechnung über Dokumente Ein Bit in Dokumenten geändert => anderer Hashwert
Unterschrift	Digitale Signatur von Hashwert und Deckblatt
Versiegeltes Kuvert	Digitale Verschlüsselung

# Ablauf:

Postalische Versendung	„Send Button“
Sicheres Ablegen der Kuverts	Speichern verschlüsselter Angebote und Verwahren Schlüssel zum Öffnen der Angebote
Öffnen der Kuverts	Zurverfügungstellen der Schlüssel und Entschlüsseln der Angebote

## Ablauf:

Prüfen der Angebote	Prüfen Angebote, insb. Hashwert und Signatur (Widerrufslisten)
Kennzeichnen, sodass nachträgliche Änderung nicht möglich	Digitales „stempeln“, z.B. Signatur durch Kommissionsmitglieder

# Abbildung:

## e-Mail

Asynchroner Dienst  
Problem bei Entschlüsselung  
KMU?

Gesicherte End-zu-End  
Verbindung?

Zugangsschutz zu e-Mails  
Revisionssicherheit  
Nachweisbarer Eingang

## Web-Applikation

Synchroner Dienst

SSL End-zu-End

Datenbankbasiert  
Protokollierung

# Abbildung:

## ~~e-Mail~~

~~Asynchroner Dienst  
Problem bei Entschlüsselung  
KMU?~~

~~Gesicherte End-zu-End  
Verbindung?~~

~~Zugangsschutz zu e-Mails  
Revisionssicherheit  
Nachweisbarer Eingang~~

## Web-Applikation

Applikation trägt die  
Verantwortung

und

entlastet User auf  
beiden Seiten

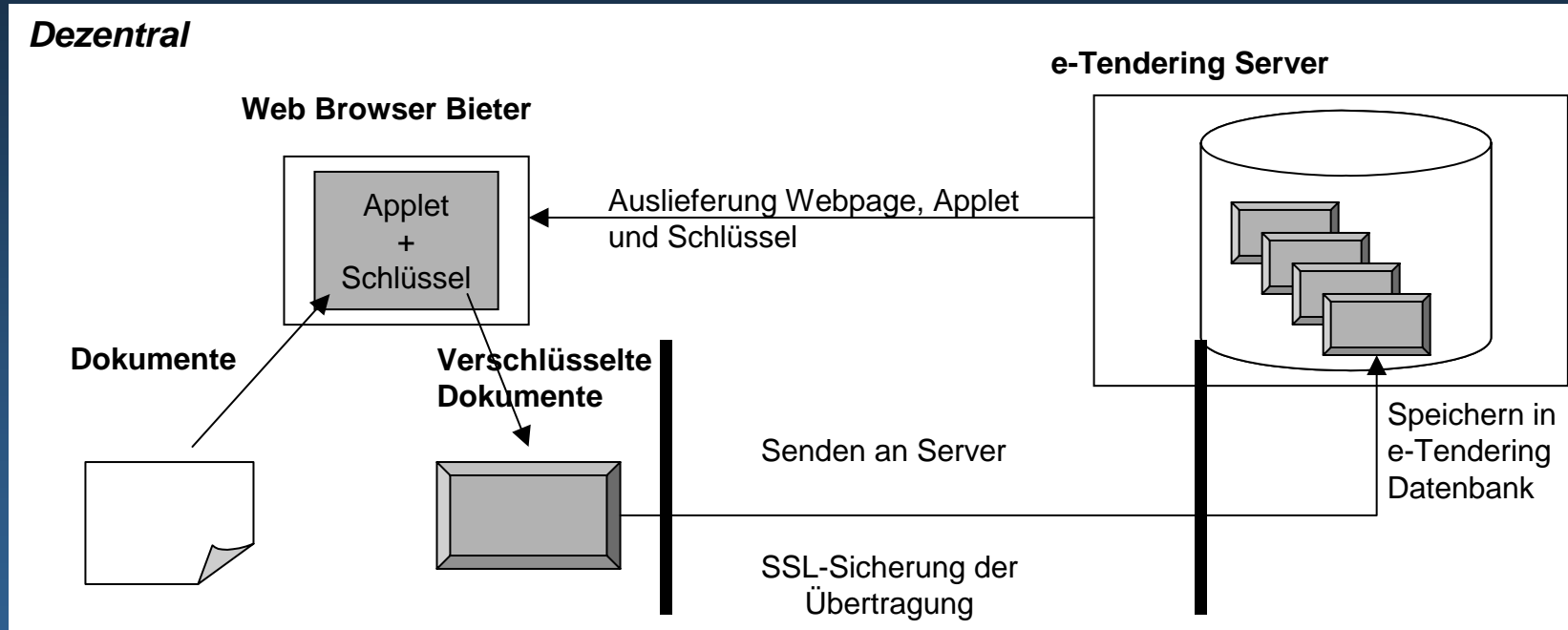


# Verschlüsselung – Entschlüsselung.

Zentral?

Dezentral?

# Verschlüsselung:



=> Sicher, aber Caveats

# Verschlüsselung:

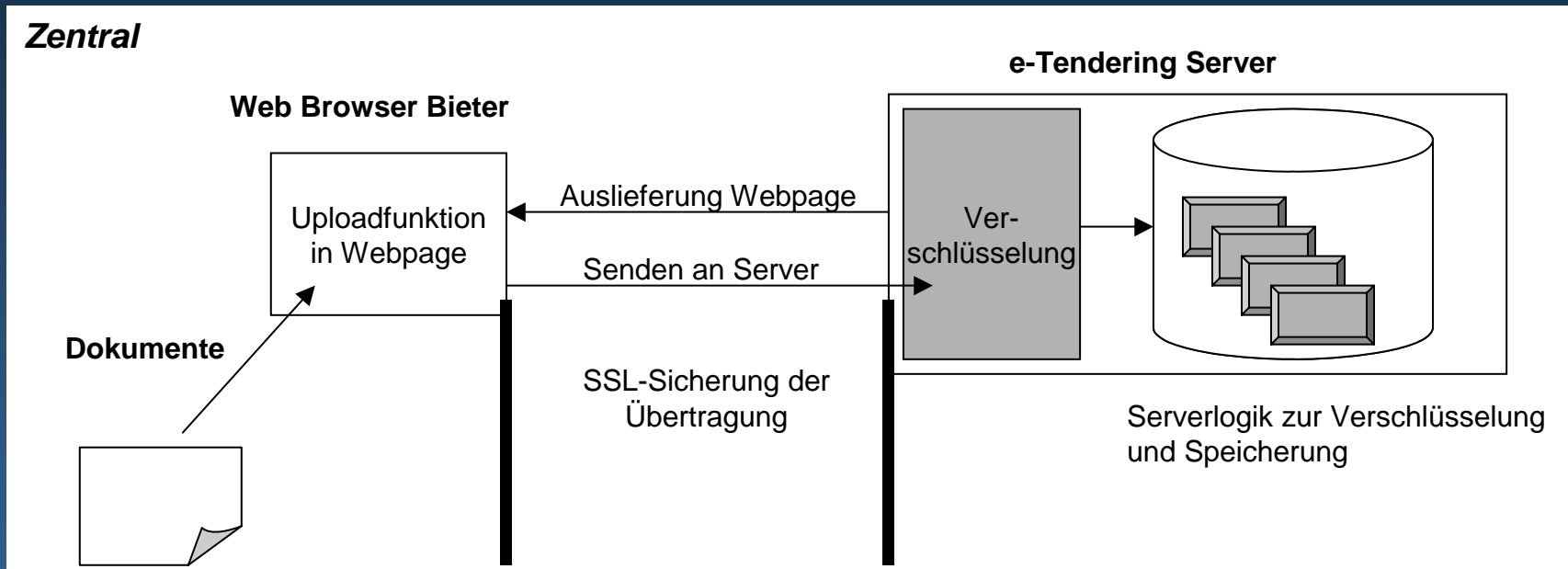
Weitgehend analoge Situation Verschlüsselung Stimmzettel  
in der Stimmabgabe und Abgabe verschlüsselter Angebote

Erfahrung mit dezentraler Verschlüsselung im Bereich  
e-Voting (Wahltests 2003 und 2004)

Im Bereich e-Voting dezentrale Verschlüsselung gefordert

Probleme mit Softwareinstallation und Firewall-Einstellungen

# Verschlüsselung:

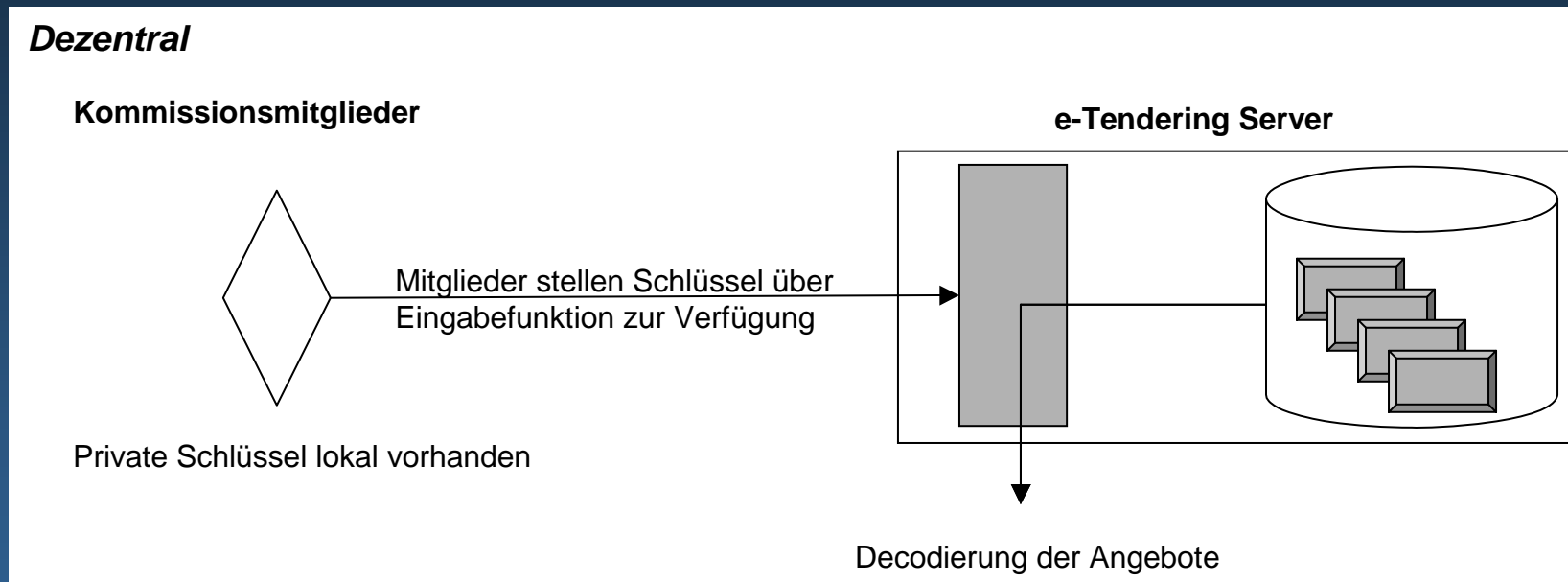


=> Robust, Zugriff durch Unbefugte möglich

# Entschlüsselung (Aufbewahrung):

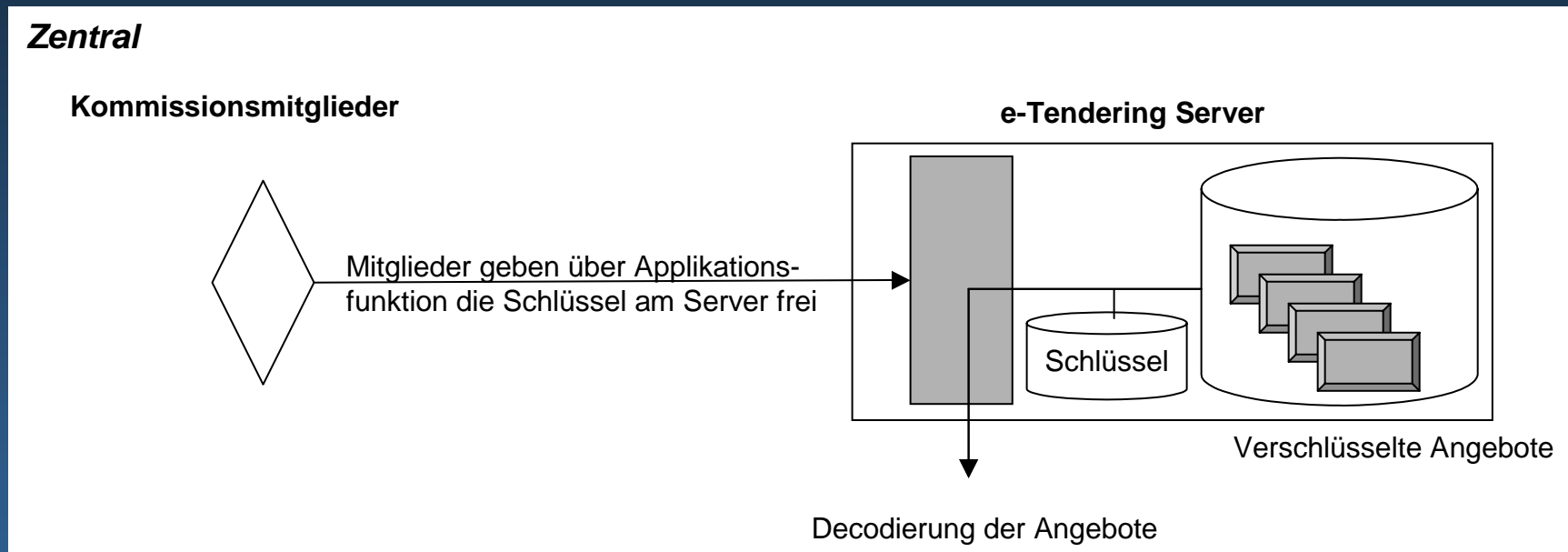
- Kein unbefugter Zugriff vor Ablauf der Angebotsfrist
- Termine ausschließlich von Ermächtigten änderbar
- Zugang zu Daten indem Ermächtigte gleichzeitig tätig werden

# Entschlüsselung (Aufbewahrung):



=> Sicher, wenig robust

# Entschlüsselung (Aufbewahrung):

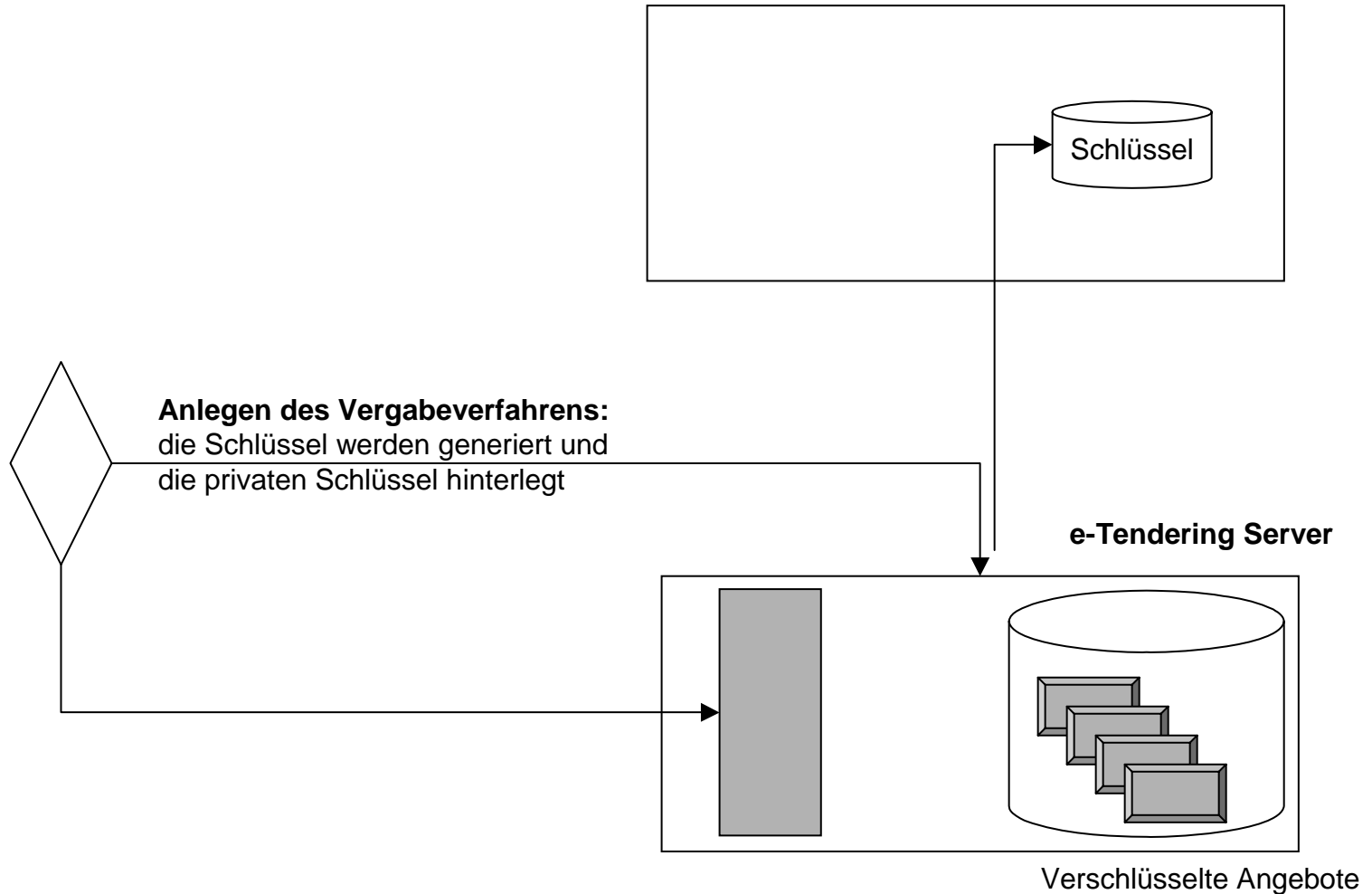


=> Robust, Zugriff durch Unbefugte möglich

### Hinterlegung

Kommissionsmitglieder

Hinterlegungsserver



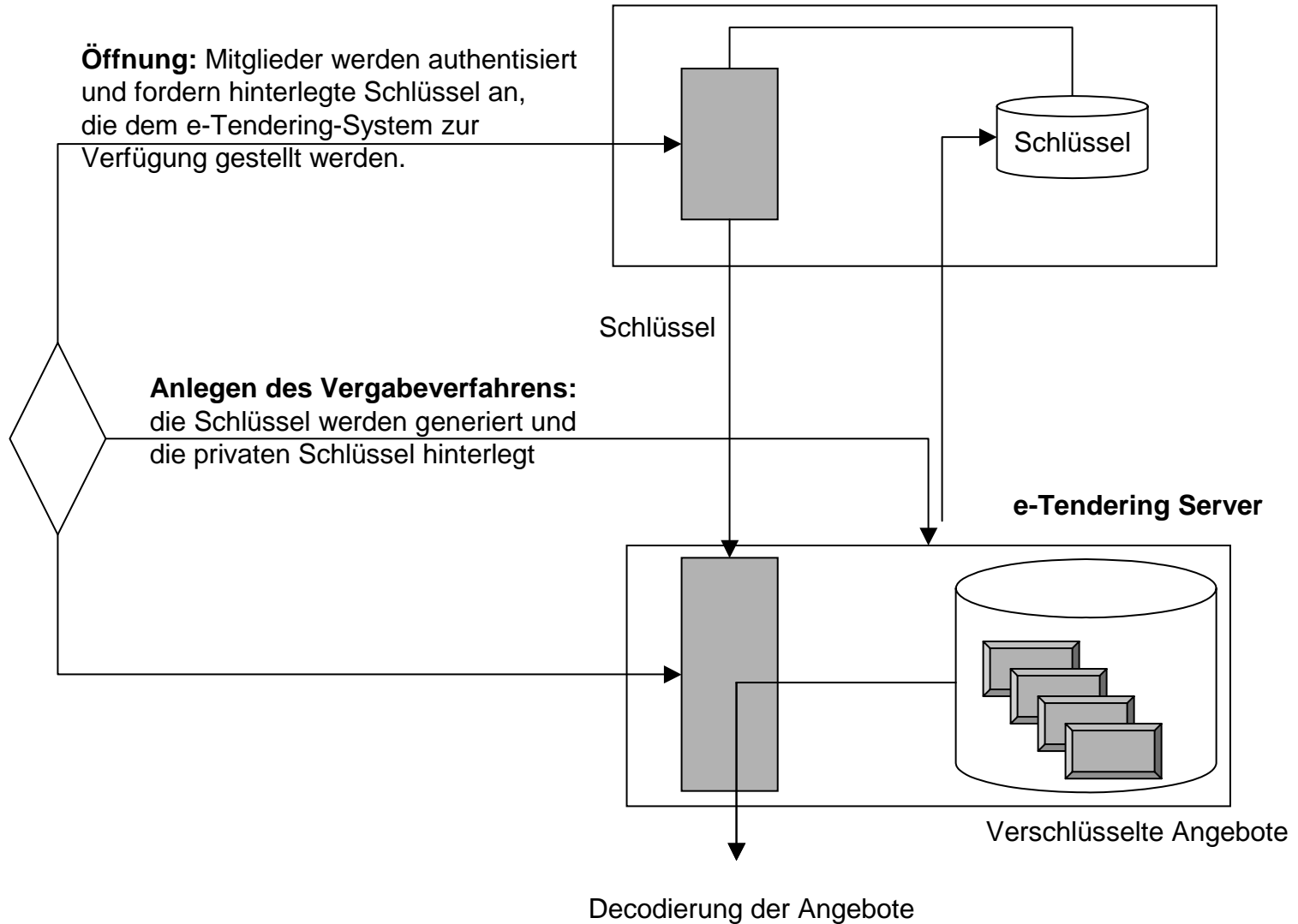
## Hinterlegung

Kommissionsmitglieder

Hinterlegungsserver

**Öffnung:** Mitglieder werden authentisiert und fordern hinterlegte Schlüssel an, die dem e-Tendering-System zur Verfügung gestellt werden.

**Anlegen des Vergabeverfahrens:** die Schlüssel werden generiert und die privaten Schlüssel hinterlegt



# Zusammenfassung:

- => E-Tendering als komplexe Applikation
- => Haftungsrisiken
- => Neuland für Bieter und Ausschreibende
  
- => TCO von Fixkosten dominiert
- => Kritische Größe für Helpdesk, Support etc.
  
- => Sinnvolle Ausgestaltung:
  - Implementierung: Webapplikation
  - Organisatorisch: Provider
  - Kryptographisch: Hinterlegungslösung

# Wirtschaftsuniversität Wien

**Prof. Alexander Prosser**

*Institut für Informationsverarbeitung und Prozessmanagement*

**Dr. Robert Müller-Török**

*Institut für Klein- und Mittelbetriebe*

Augasse 2-6, 1090 Wien

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

[robert.mueller-toeroek@wu-wien.ac.at](mailto:robert.mueller-toeroek@wu-wien.ac.at)