# AppPETs

## Entwurf eines datenschutzfreundlichen Speicherprotokolls

M. Sc. Erik Sy
Sicherheit in verteilten Systemen (SVS)
http://svs.informatik.uni-hamburg.de

Arbeitstreffen des AppPETs-Projektes
Hamburg, 22. August 2016

## Anonymität als Brücke zum Datenschutz

- Schutzziele:
  - Anonymität der veröffentlichenden Person
  - Anonymität der lesenden Person
  - Anonymität des Dokuments
  - Anonymität des Servers
  - Anfrage-Anonymität
  - Integrität eines Dokuments
  - Glaubhafte Bestreitbarkeit für die beteiligten Personen

- Grenzen unseres Speicherprotokolls
  - Anonymität des Verfassers kann nicht technisch von AppPETs umgesetzt werden
  - Server kann nachvollziehen, wann ein bestimmtes Dokument hochgeladen wurde

## Vergleich zu weiteren datenschutzfreundlichen Speicherlösungen

| Projekt | Veröffent-licher | Leser | Server | Dokument | Anfrage | wirtschftl. Konzept |
|---|---|---|---|---|---|---|
| Freenet | + | ? | | | | + |
| Free Haven | + | + | + | + | | + |
| AnonRAM | + | + | | + | (+) | |
| AppPETs | + | + | + | + | + | + |

- Anmerkungen:
  - Konzepte zu Free Haven und AnonRAM sind bisher nicht umgesetzt
  - Freenet und Free Haven basieren auf peer-to-peer
  - Anfrage-Anonymität bei AnonRAM nicht für unser Angreifermodell geeignet

## Wie wird die Anonymität im Detail umgesetzt?

- Anonymität des Dokuments sowie Integritätsüberprüfung
  - Klartext wird gemeinsam mit seinem Hash verschlüsselt auf dem Server gespeichert
  - Es werden jeweils Datenblöcke fester Größe übertragen, zur Geheimhaltung der Dateigröße
  - Integritätskontrolle nach Entschlüsselung mittels Hash

- Anfrage-Anonymität
  - Realisierbar durch Private Information Retrieval (PIR) oder oblivious RAM (ORAM)
  - Sehr hoher Bedarf an Bandbreite und Rechenleistung, sodass die Praktikabilität in Bezug auf Smartphones getestet werden muss
  - Evtl. nur ein ITPIR-Ansatz mit mehreren Servern, welche nicht unerlaubt zusammenwirken, sinnvoll umsetzbar

## Weitere Details zur Umsetzung der Anonymität

- Anonymität des Servers
  - Die Server können als TOR Hidden Services geheim gehalten werden
  - Zugang zu den Servern nur aus dem TOR-Netzwerk möglich
  - Vorteil: nur nach erfolgreicher Anonymisierung kann der Server kontaktiert werden

- Anonymität der Veröffentlicher und Leser
  - Durch das AppPETs-Bezahlsystem können Schreib- oder Lesezugriffe anonym abgerechnet werden
  - Geheimhaltung der wahren Anzahl der Nutzerinnen gegenüber dem Server

## Vergleich zwischen Free Haven und AppPETs

| Free Haven | AppPETs |
|---|---|
| Komplexes Vertrauensmodell | Anonymes Bezahlmodell |
| Datenlöschung nicht möglich | Datenlöschung durch veröffentlichende Person möglich |
| Datenverlust, falls ein großer Teil des Servnets Betrieb einstellt | Serverinhalte können nachverfolgt oder auch dupliziert werden |
| Wartbarkeit ist schwierig | Wartbarkeit ist einfach |
| Niedrige Performance | Verlässliche und performante Infrastruktur |

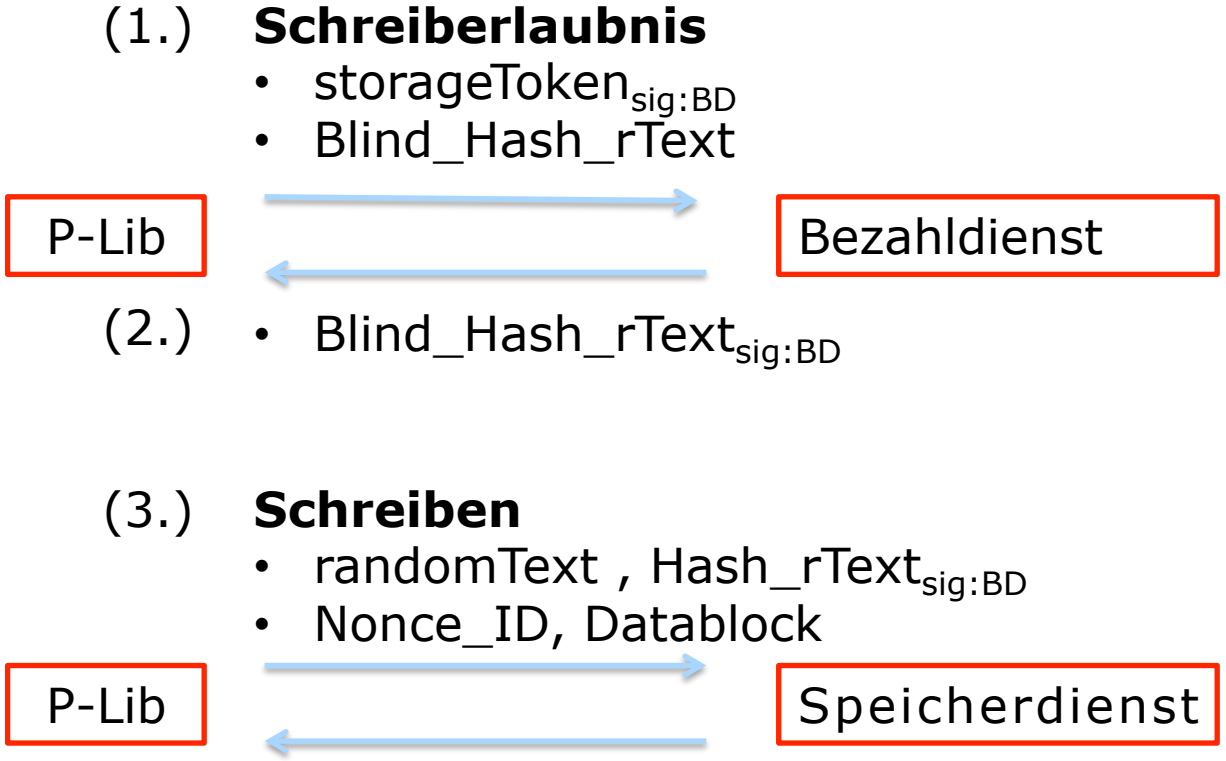
# Schreiboperation

## Hintergrund

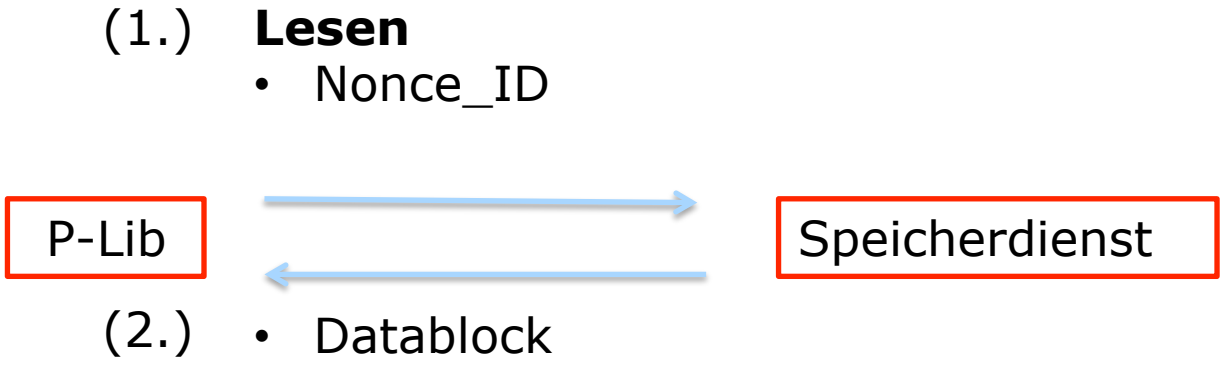
**Kauf von Guthaben**
- $storageToken_{sig:BD}$

**Kryptographie**
- randomText
- Hash_rText
- Nonce_ID

**Blinde Signaturen**
- Blind_Hash_rText
- $Hash\_rText_{sig:BD}$



## Leseoperation




- Leseabfrage erfolgt auf Basis eines PIR-Verfahrens
- Ein Schema zur Leistungsabrechnung kann auf Grundlage der Blinden Signaturen ergänzt werden

# Löschoperation

(1.) **Löschen**
- Nonce_ID
- Hash_rText$_{sig:BD}$

P-Lib → Speicherdienst

(2.) **Status**
- Erfolg/Misserfolg?

## Relevante Angriffsvektoren und Gegenmaßnahmen

- Replay-Angriffe
  - Zielen auf eine Mehrfachnutzung von Bezahl-Token ab
  - Abwehr durch Speicherung aller akzeptierten storageToken durch den Bezahldienst sowie der Kontrolle ob Tokens bereits eingelöst wurden
  - analoges Vorgehen für randomText und Hash_rText bei dem Speicherdienst

- Denial of service-Angriffe
  - Zielen auf ein Überfluten der Service-Infrastrukturen mit Anfragen ab
  - Abwehr durch vorübergehendes Blockieren von IP-Adressen mit hohem Aufkommen an missbräuchlichen Anfragen
  - sind ein reales Problem Service-Infrastruktur

## Weitere relevante Angriffsvektoren und Gegenmaßnahmen

- Kollusion-Angriffe
  - Zielen auf die Enttarnung von Nutzern ab mittels geheimer Zusammenarbeit anderer Nutzer oder Teile der Service-Infrastruktur
  - Bei Verwendung des IT-PIR-Verfahren kann somit die Anfrage-Anonymität aufgehoben werden
  - Diese Angriffe sind wirksam gegen Anonymisierungsdienste, wenn eine bestimmte Anzahl von Knoten/Mixe zusammenwirken

- Angriffe gegen die Anonymität der Leser
  - Ein Angreifer kann Dokumente bereitstellen, welche während der Ausführung eine Verbindung zu anderen Servern aufbauen und somit Informationen über den Leser übertragen
  - Als Abwehrmaßnahme sollten Dokumente nur auf vom Netzwerk getrennten Geräten ausgeführt werden

# AppPETs

## Entwurf eines datenschutzfreundlichen Speicherprotokolls

M. Sc. Erik Sy
Sicherheit in verteilten Systemen (SVS)
http://svs.informatik.uni-hamburg.de

Arbeitstreffen des AppPETs-Projektes
Hamburg, 22. August 2016