Entwurf und Realisierung von Sicherheitsmechanismen für eine Infrastruktur für digitale Bibliotheken

Vortrag zur Diplomarbeit

von
Razi Lotfi-Tabrizi

Juli 2002

INDIGO – Infrastruktur für Digitale Bibliotheken

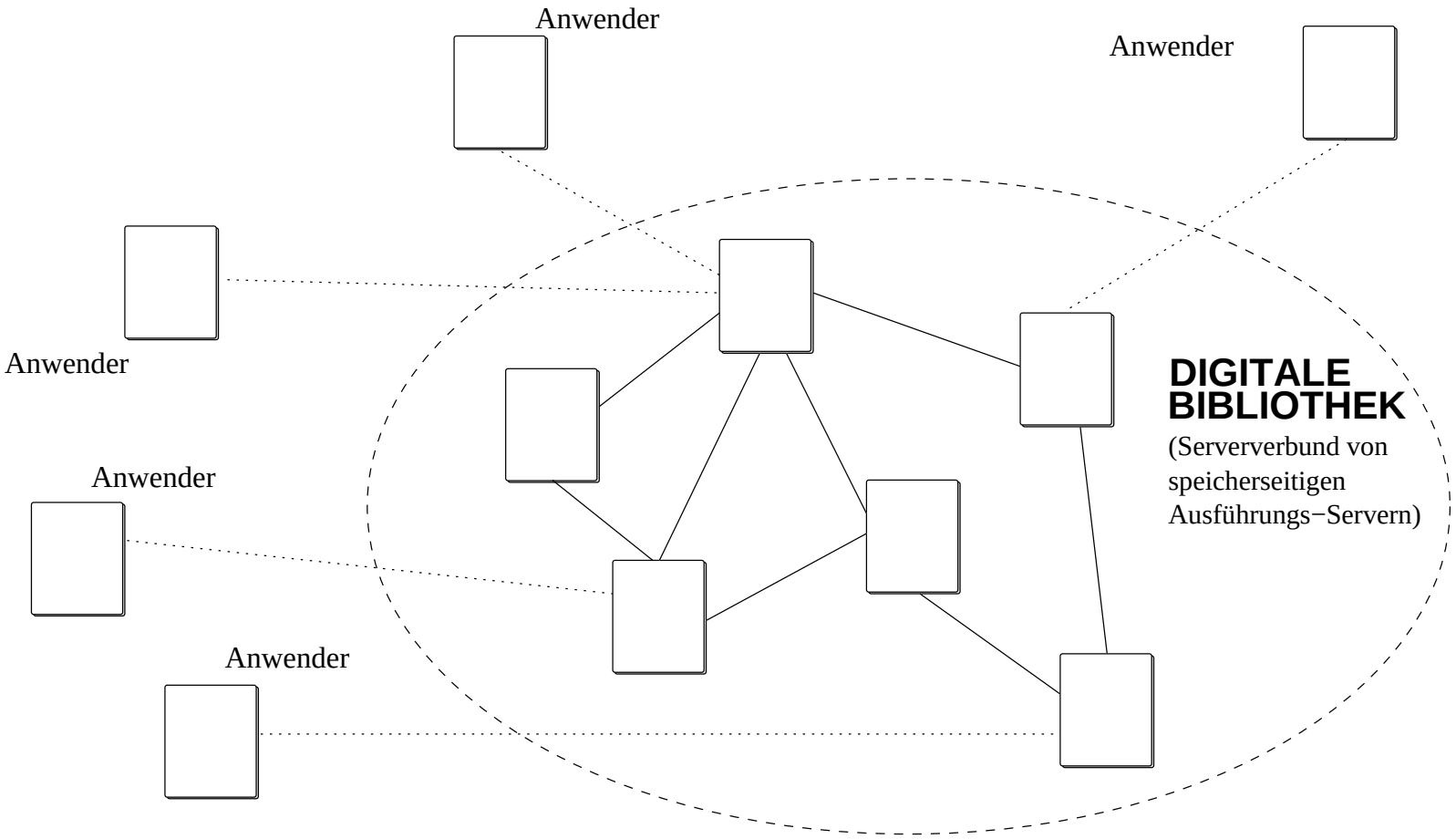


Abbildung 1 Komponenten der INDIGO-Infrastruktur (1)

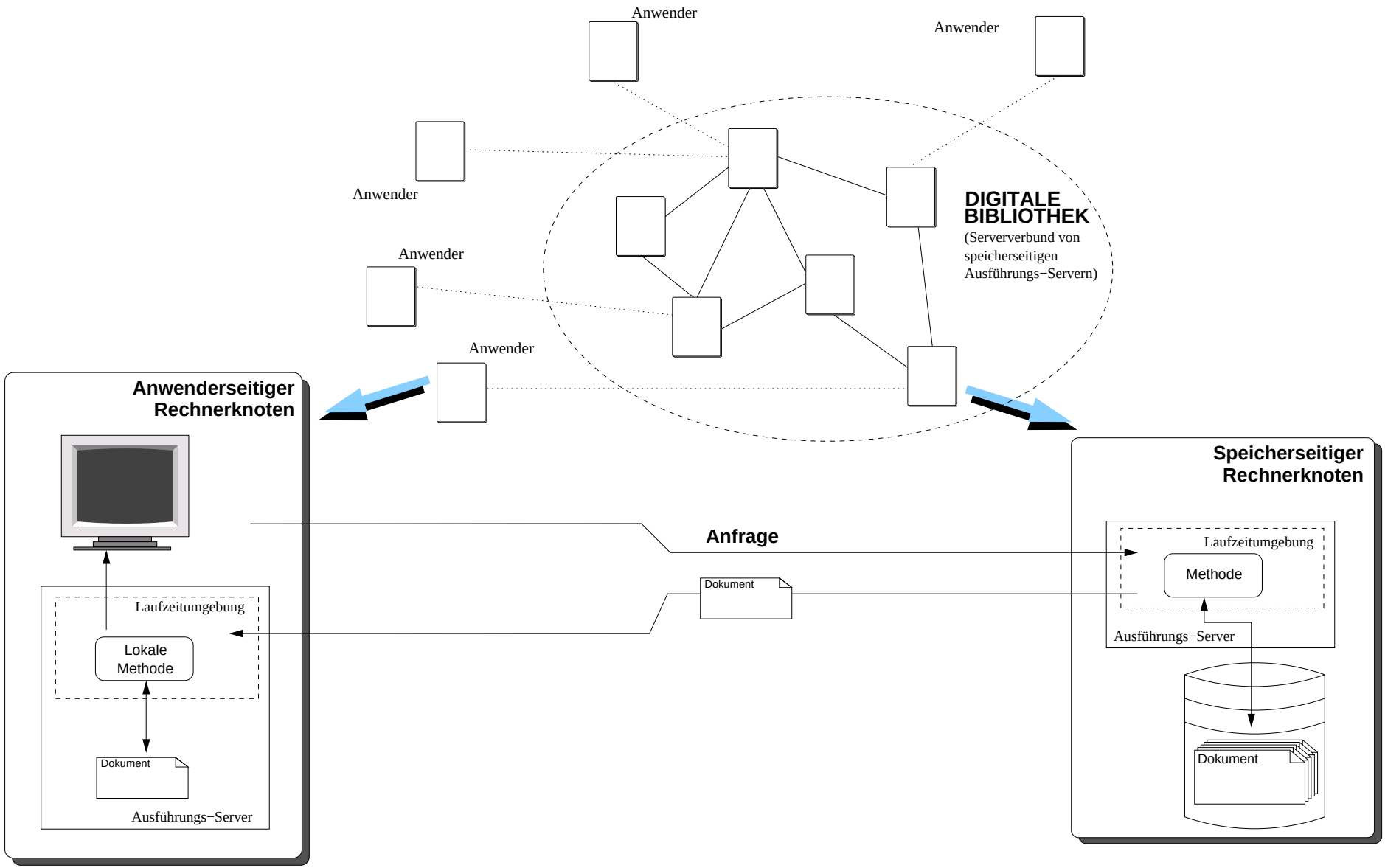


Abbildung 2 Komponenten der INDIGO-Infrastruktur (2)

Akteure und schützenswerte Güter

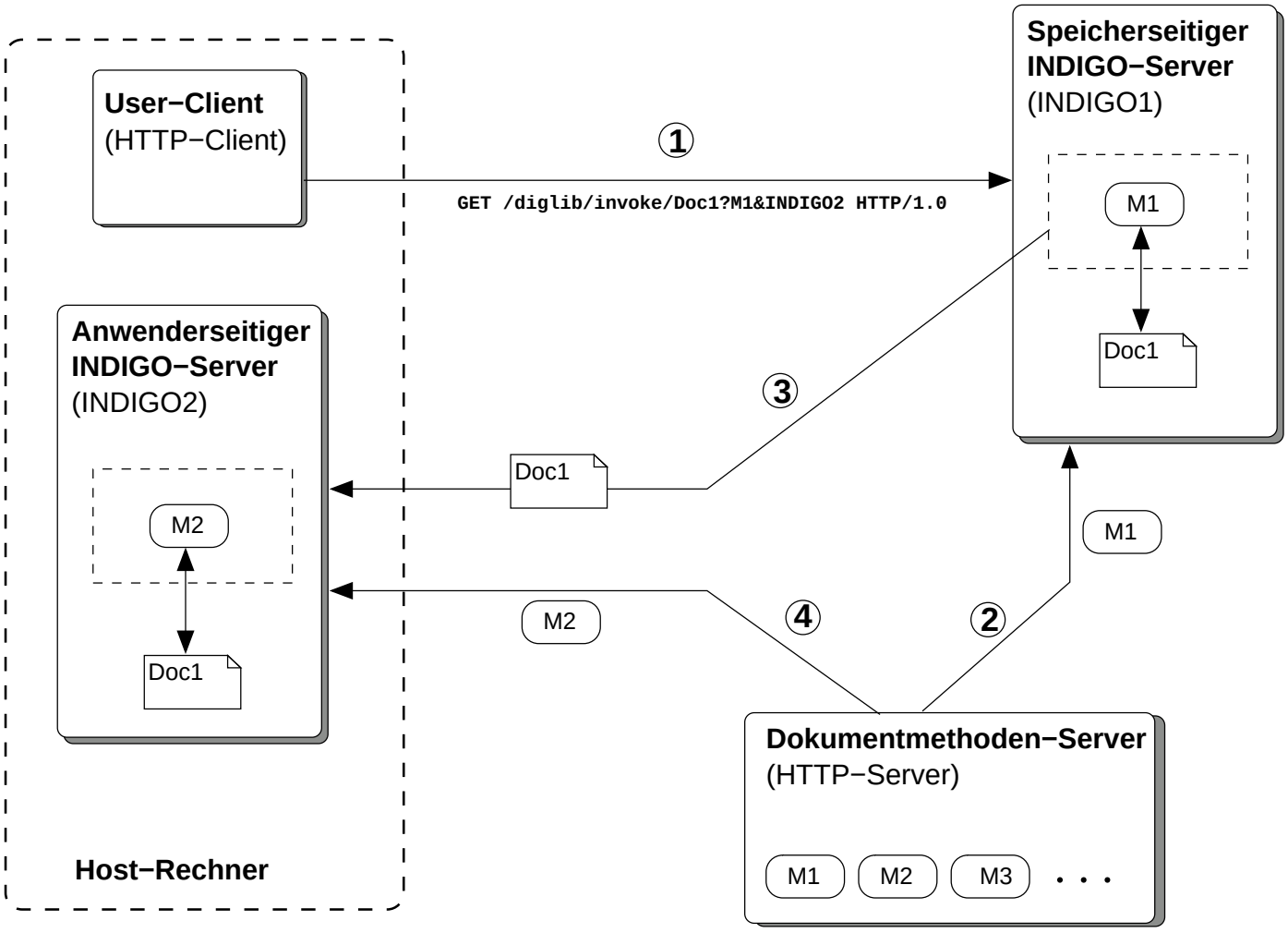


Abbildung 3 Akteure beim INDIGO-System

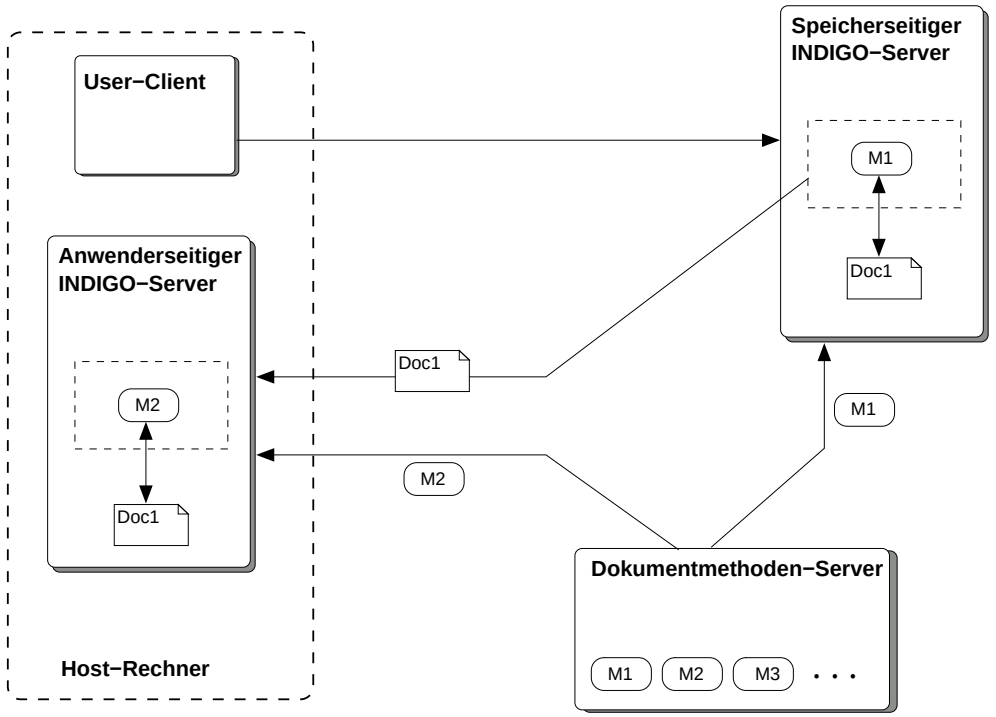
Akteure und schützenswerte Güter

Akteure:

- Dokumentmethoden-Produzent
- Dokumentmethoden-Server-Betreiber
- Autor
- Bibliothek
- Anwender
- Netzwerk-Betreiber

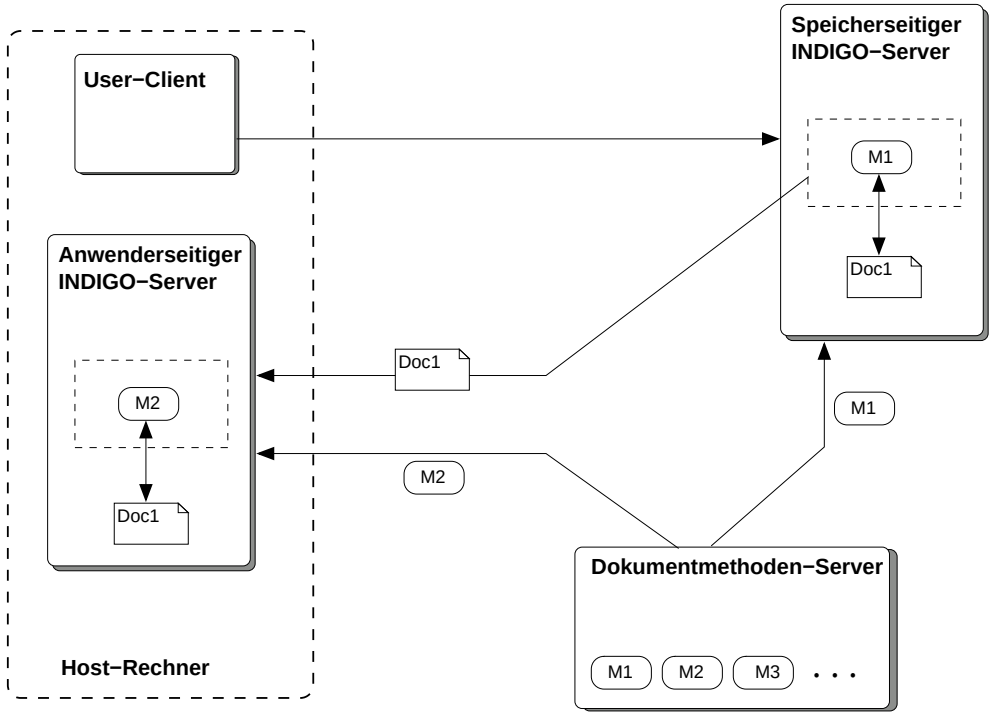
Schützenswerte Güter:

- Metadokumente
- Dokumentmethoden
- INDIGO-Server
- Basis-Infrastruktur



Beispiele für Sicherheitsverletzungen

- Manipulation oder Abhören der Kommunikation.
- Manipulation der Herkunft und Unversehrbarkeit der Metadokumente.
- Manipulation der Methoden bzw. der Dokumentmethoden-Abschnitte.
- Ausführung von böswilligen Dokumentmethoden.
- Unerlaubter Zugriff auf die Dienste des INDIGO-Servers.
- Mißbrauch der indirekten Autorisierung (DDOS-Angriff).

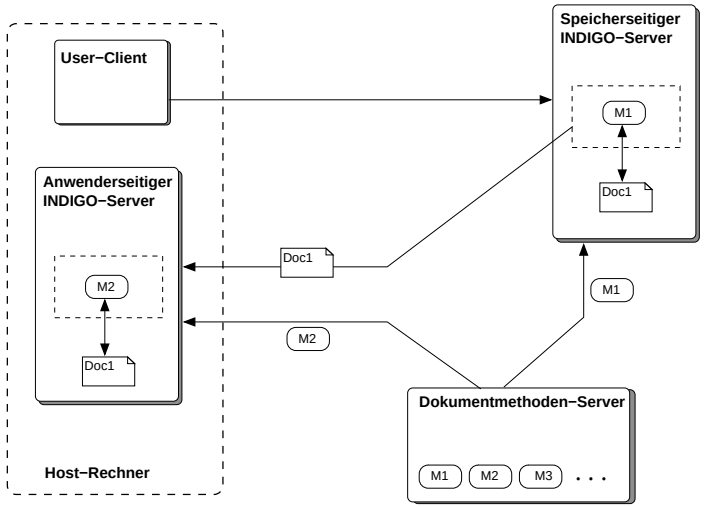


Sicherheitsanforderungen an die schützenswerten Güter

Schützenswerte Güter	Sicherheitsanforderungen
Metadokumente	Vertraulichkeit, Authentizität, Integrität, Verbindlichkeit
Dokumentmethoden	Authentizität, Integrität, Verbindlichkeit
INDIGO-Server	Vertraulichkeit, Authentizität, Integrität, Verbindlichkeit, Autorisierung (Zugriffskontrolle)

Die wichtigsten sicherheitsrelevanten Modifikationen

- Sicherung und Aufbau der verbindlichen Kommunikationskanäle durch den Einsatz von Server-zu-Server Verfahren.
- Eindeutige Identifikation des Ausführungs-Servers mittels eines Zertifikats.
- Durchführung der Client-Authentisierung (optional).
- Realisierung von Sicherheitsmechanismen zur Verifikation der digital signierten Dokumentmethoden.
- Download von Dokumentmethoden auch von HTTPS-Servern.
- Verifikation der digitalen Signatur der Dokumente.
- Erweiterung des INDIGO-Servers um feingranuliert konfigurierbare Zugriffsmechanismen.



Zusammenfassung und Ausblick

- **Sicherheitsanforderungen und ihre Erfüllung:**
  - Vertraulichkeit: SSL, Ende-zu-Ende Verschlüsselung
  - Authentizität, Integrität, Verbindlichkeit: Digitale Signatur, MAC
  - Autorisierung: Zugriffssteuerung verteilt auf drei Ebenen
- **Vorschläge zur Weiterentwicklung:**
  - Urheberrechtsschutz
  - Erweiterte Anwender-Authentisierung
- **Bemerkung zur Implementierung:**
  - SSL-Sockets
  - Zertifikate

Ergänzungsfolien...

Digitale Bibliotheken

Digitale Bibliotheken:

- Verteilte Anwendungen
- Konstruiert für den Umgang mit digitalen Dokumenten

Anforderungen an die digitalen Bibliotheken:

- Skalierbarkeit
- Erweiterbarkeit
- Orthogonalität
- Plattformunabhängigkeit

INDIGO := Infrastruktur für digitale Bibliotheken

Beispiel für ein Metadokument

```
Content-Type: application/x-metadoc;
 boundary="ekidpUnhoJ"

--ekidpUnhoJ
Content-Type: application/x-metadoc-attributes

author: Razi Lotfi-Tabrizi
uses: base self global io
type: text/plain
title: Testdokument fuer die INDIGO
--ekidpUnhoJ
Content-Type: application/x-metadoc-methods

Present http://62.104.191.241/Text/present.zip application/java
Describe http://62.104.191.241/Text/describe.zip application/java
private.localPresent http://62.104.191.241/Text/lpresent.zip application/java
--ekidpUnhoJ
Content-Type: application/x-metadoc-content

Dies ist ein Testdokument fuer die INDIGO Infrastruktur.
Es enthaelt als Inhalt nur diese beiden Zeilen.
```

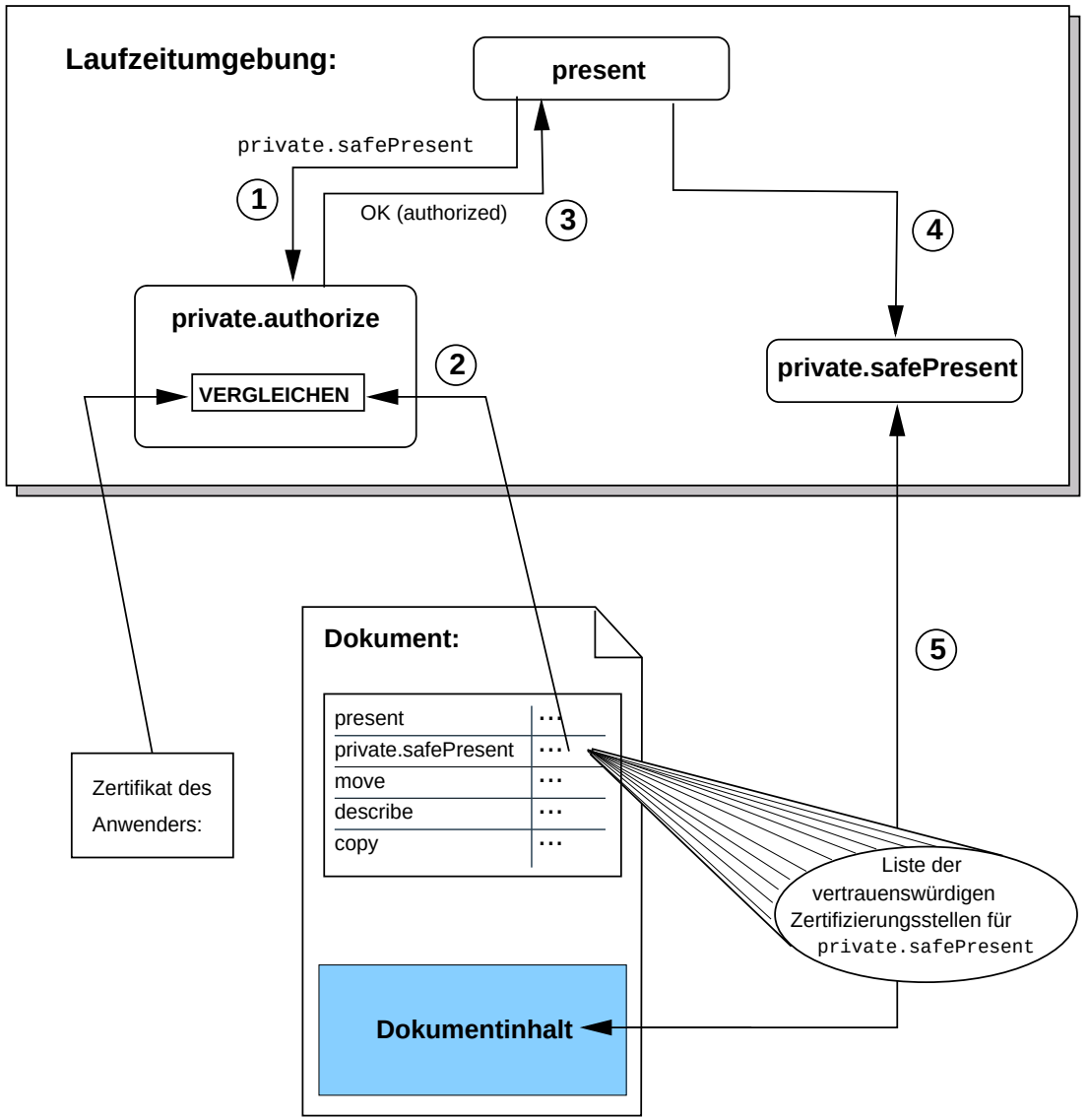
Dokumentmethoden

Die Dokumentmethoden führen Operationen auf die Dokumente aus.

Die **Operationsarten** bei der INDIGO-Infrastruktur sind:

- Orthogonale Operationen
  - Present
  - Describe
  - Copy
  - Move
- Private Operationen

Dokumentspezifische Autorisation



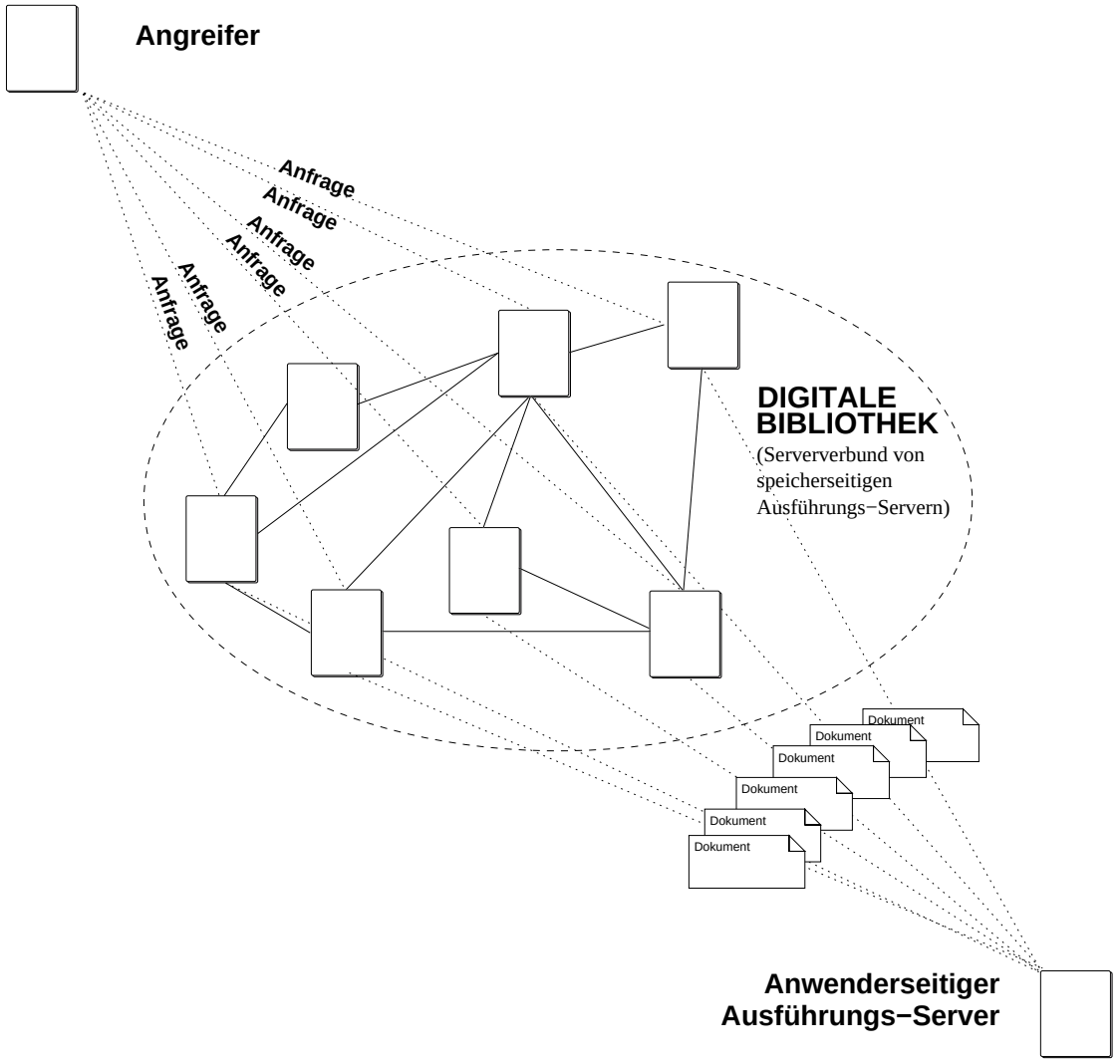


Abbildung 4 Beispiel für den Mißbrauch der indirekten Autorisierung

Zurück Lösung

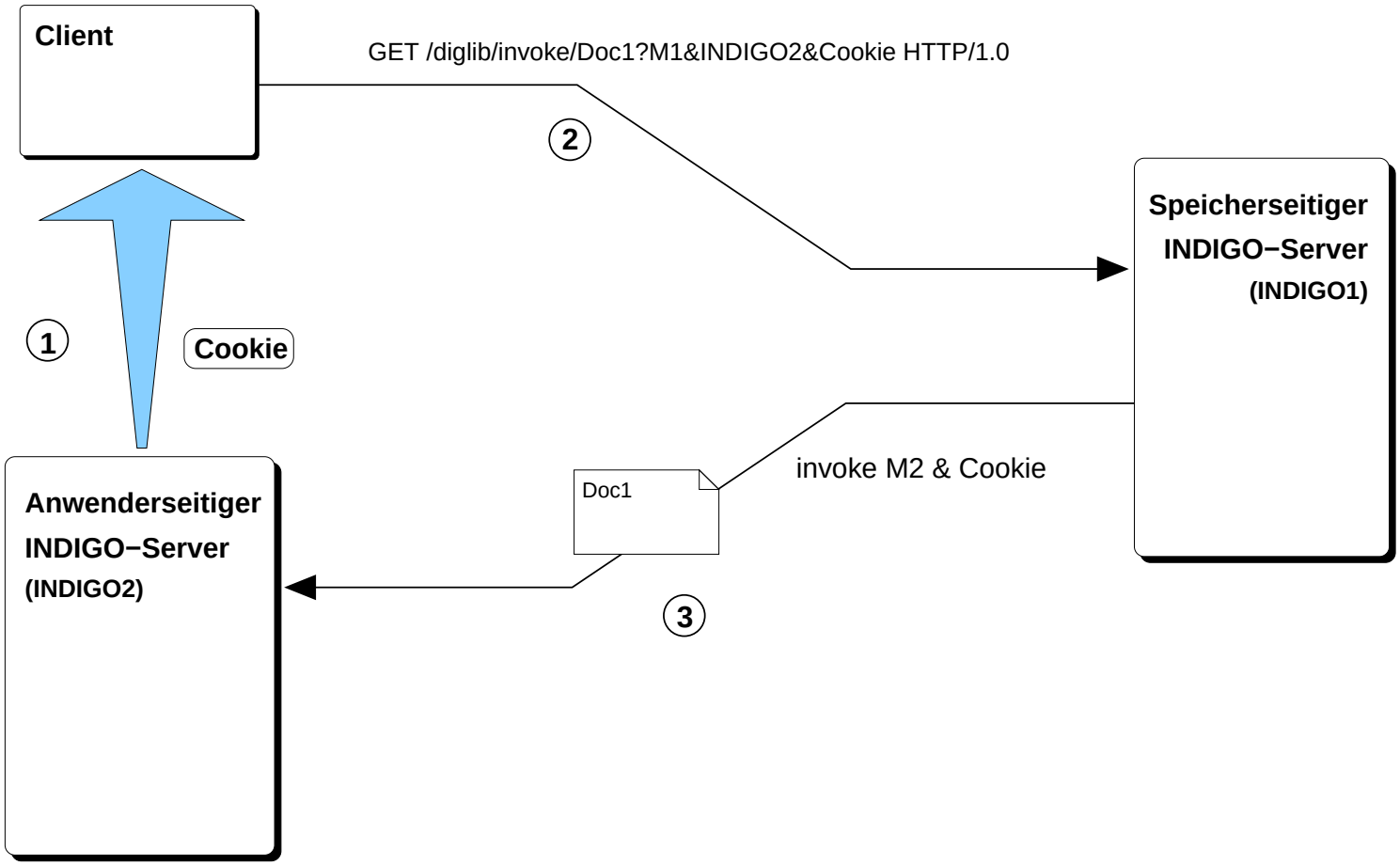


Abbildung 5 Sichere indirekte Autorisierung mittels Cookies

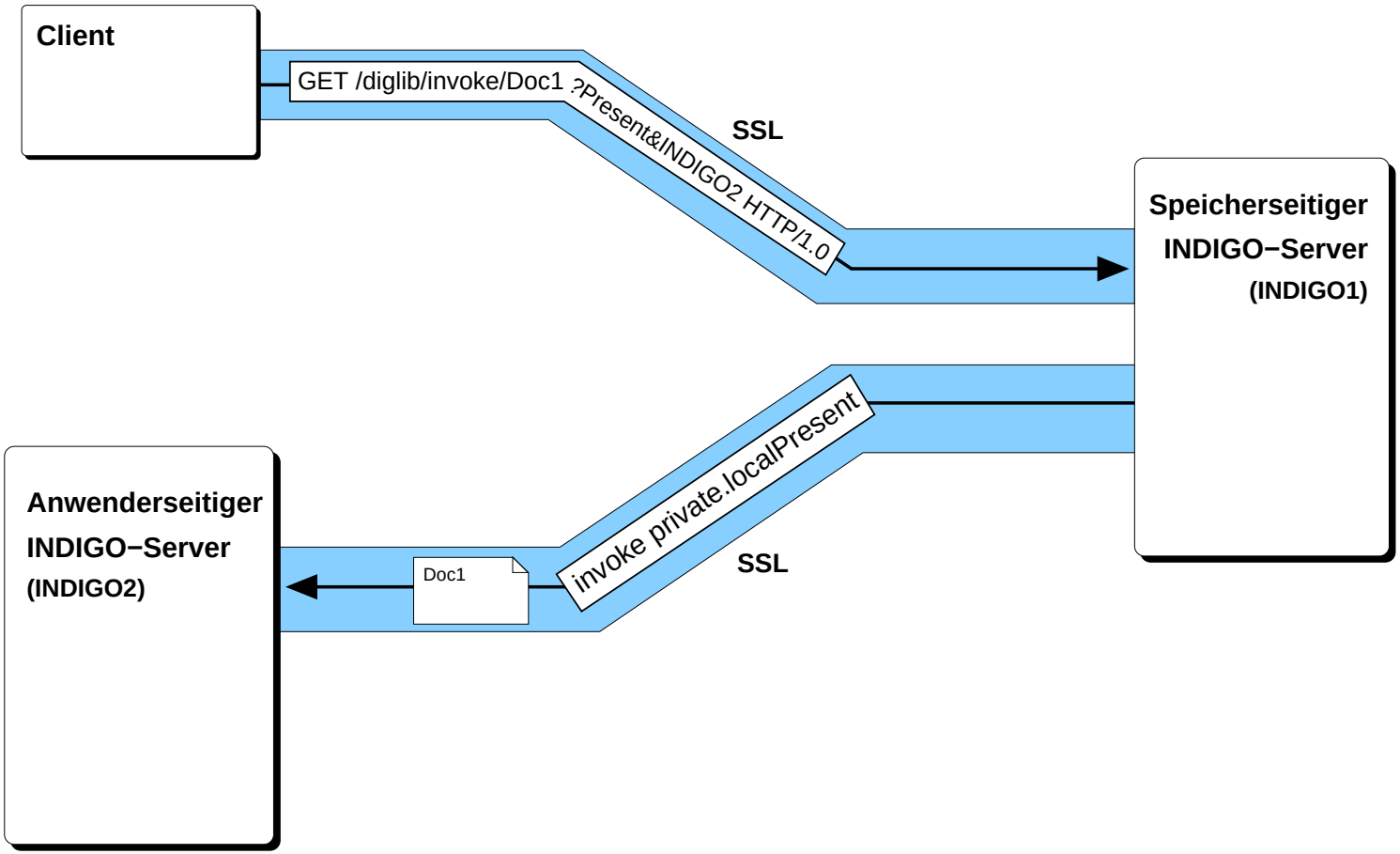


Abbildung 6 Sichere indirekte Autorisierung mittels verbindlicher Kommunikationskanäle

DDOS | Sicherheitsverletzungen | Zurück

Zugriffssteuerungsebenen

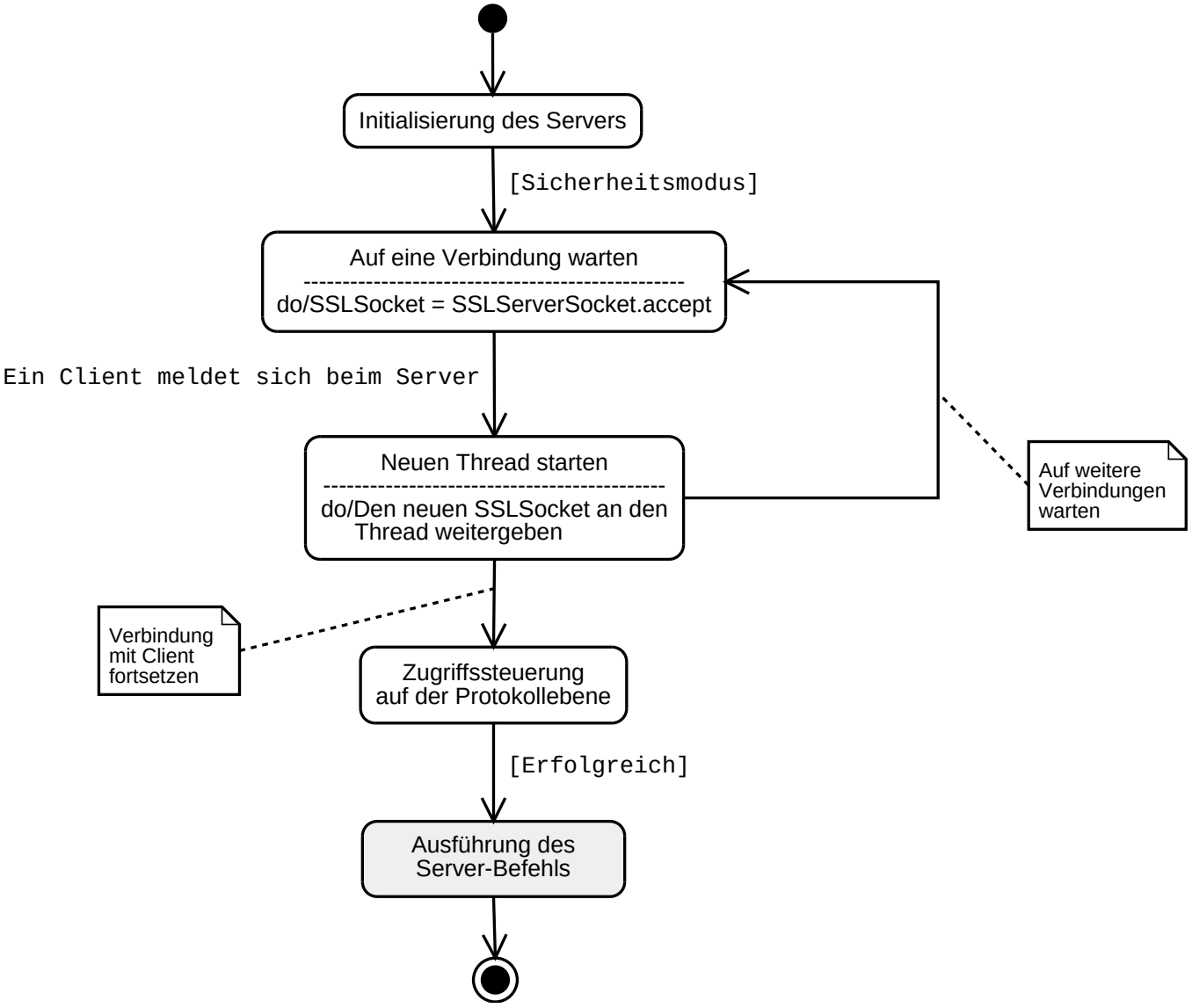


Abbildung 7 Zugriffssteuerungsebenen beim INDIGO-Server (1)

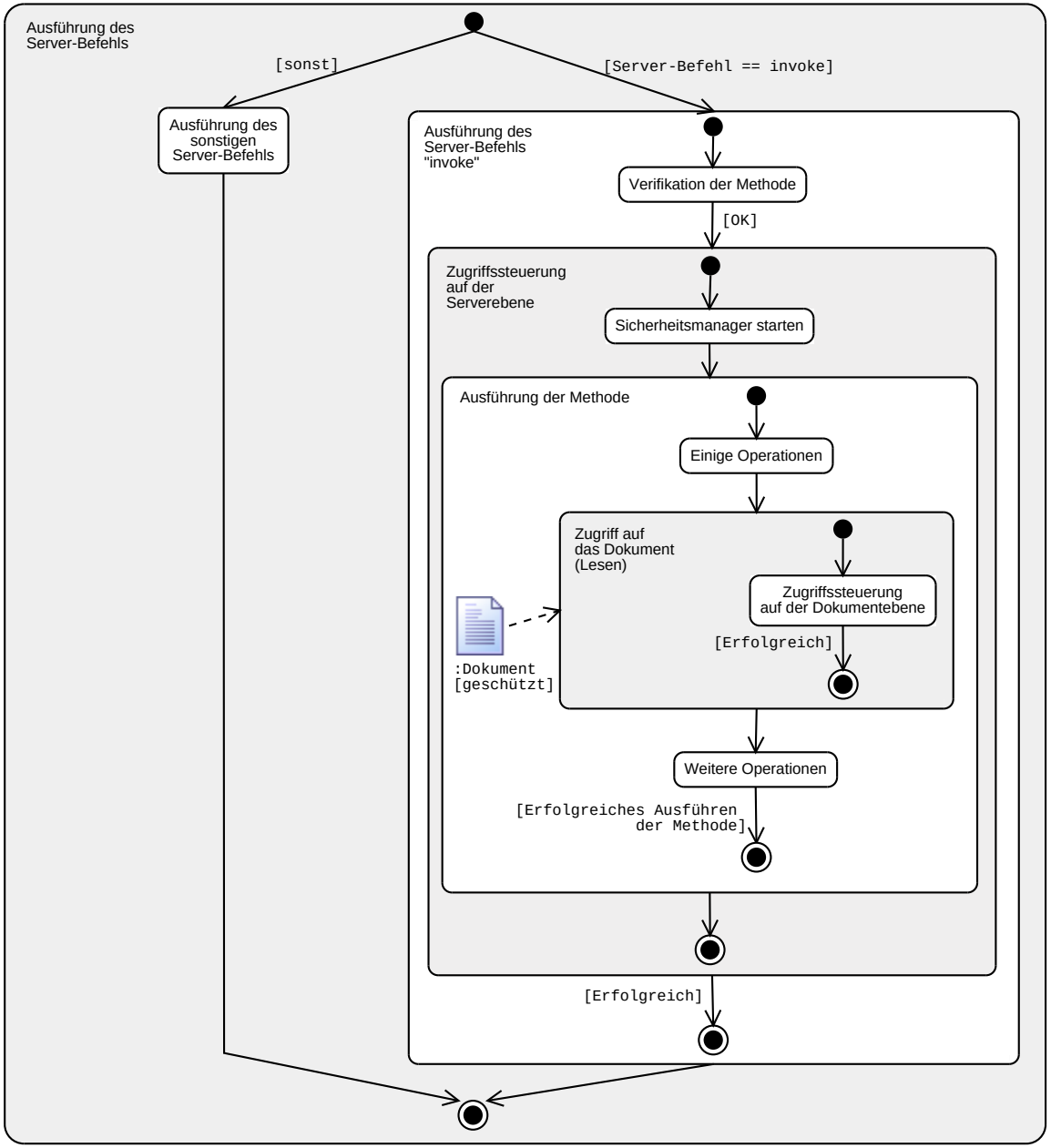


Abbildung 8 Zugriffssteuerungsebenen beim INDIGO-Server (2)

Zugriffssteuerung auf der Protokollebene

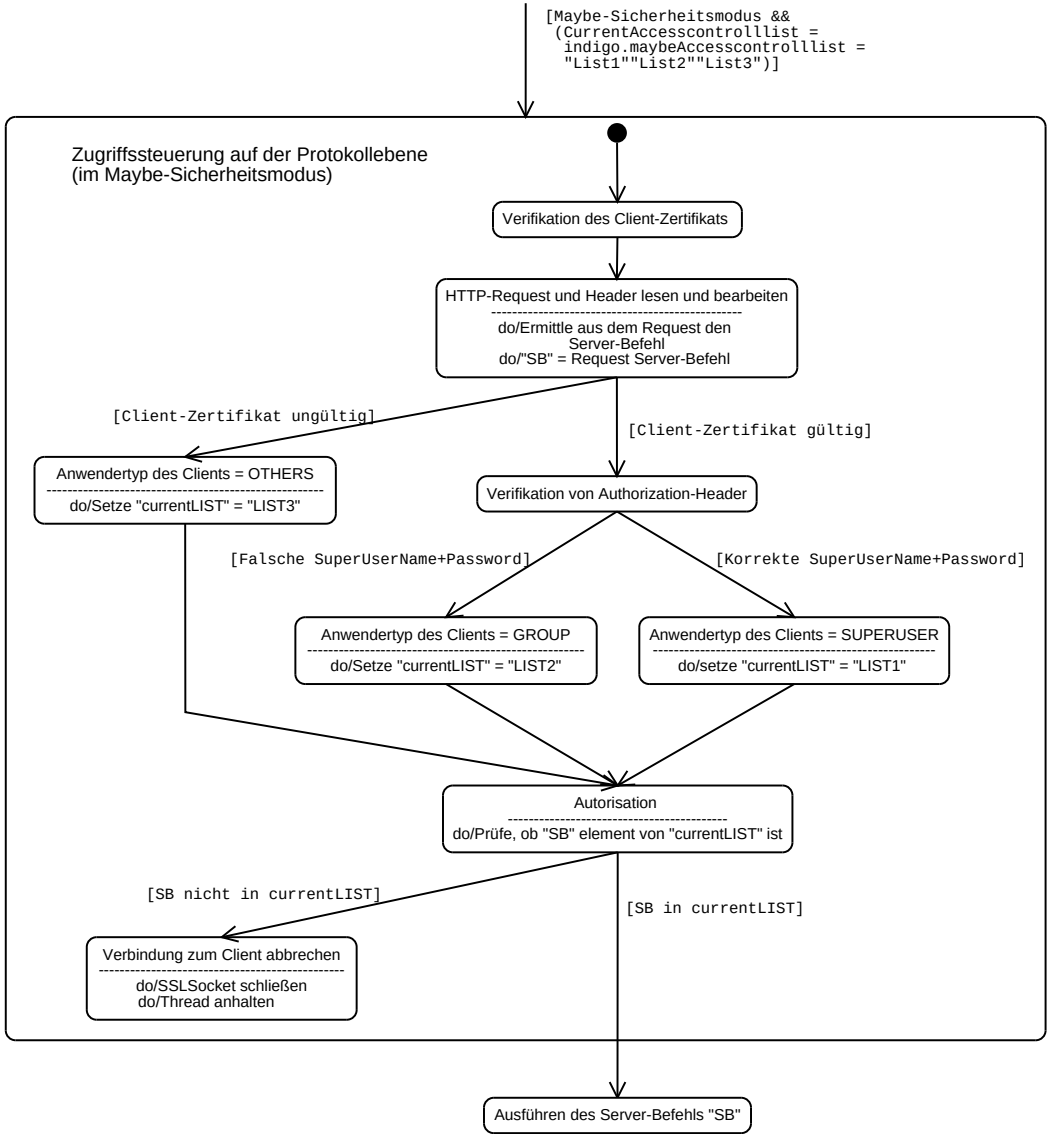


Abbildung 9 Zugriffssteuerung auf der Protokollebene im Maybe-Sicherheitsmodus

Offline-Präsentation (1)

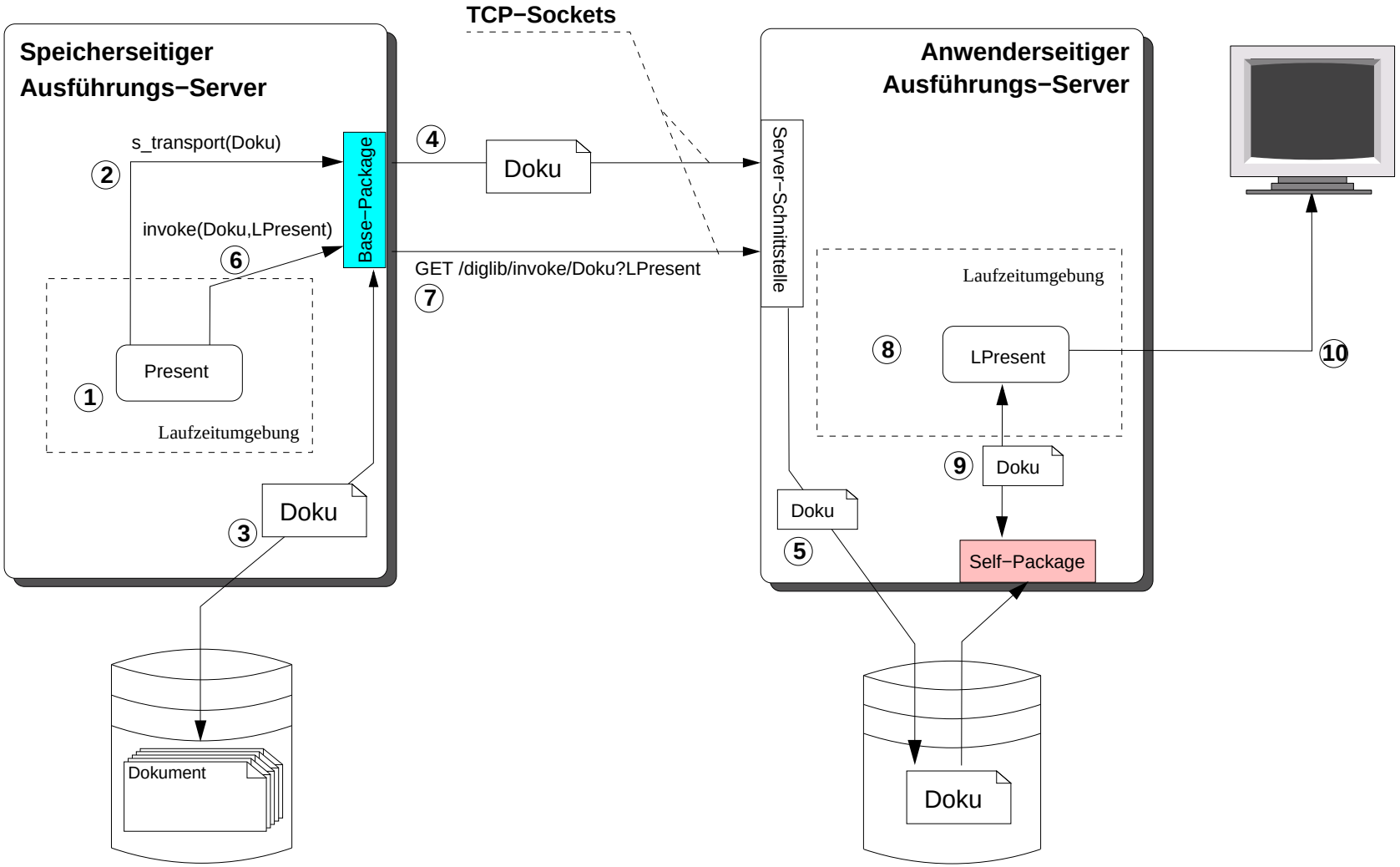


Abbildung 10 Base-Package mit TCP-Sockets

Offline-Präsentation (2)

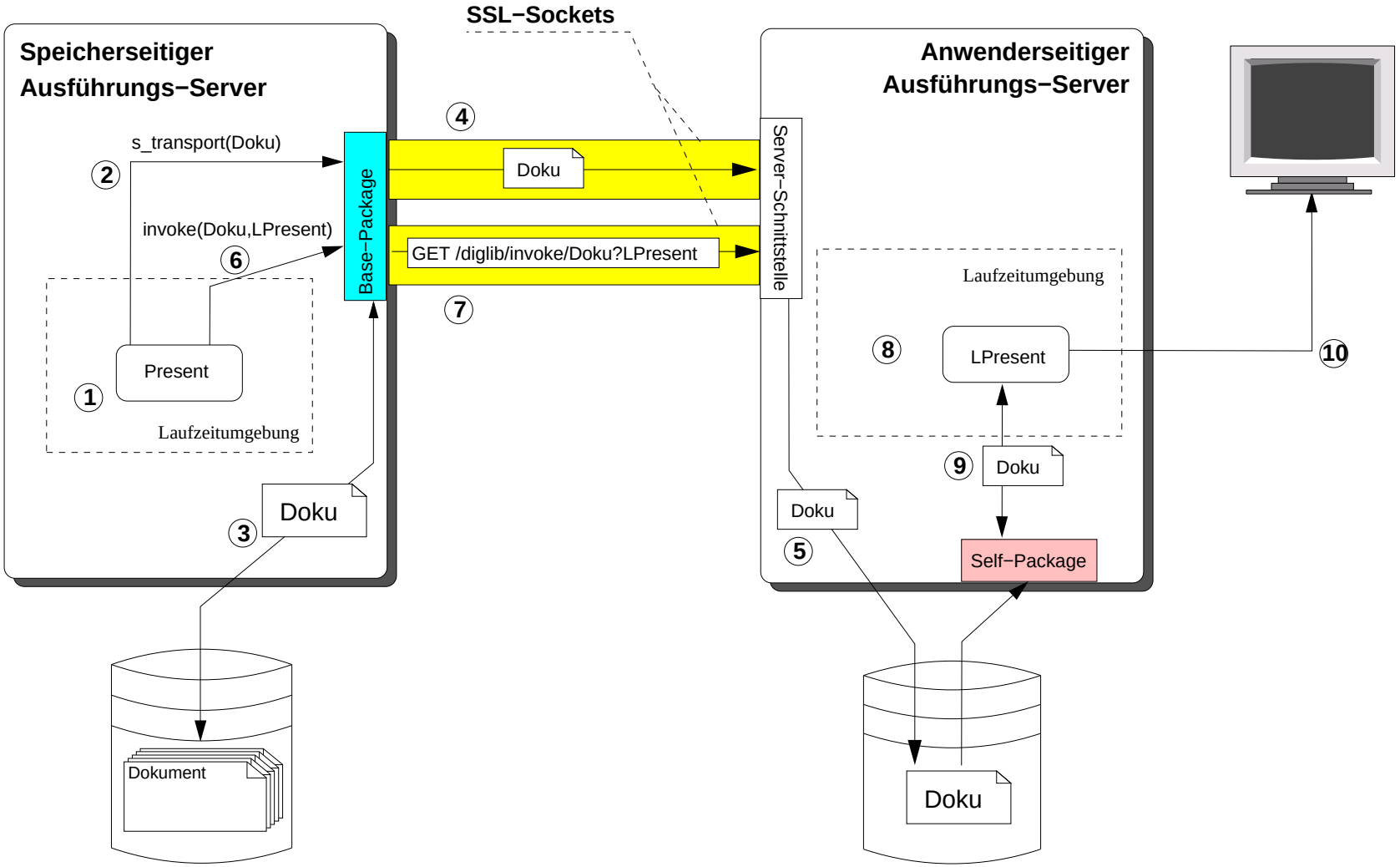


Abbildung 11 Base-Package mit SSL-Sockets

Online-Präsentation (1)

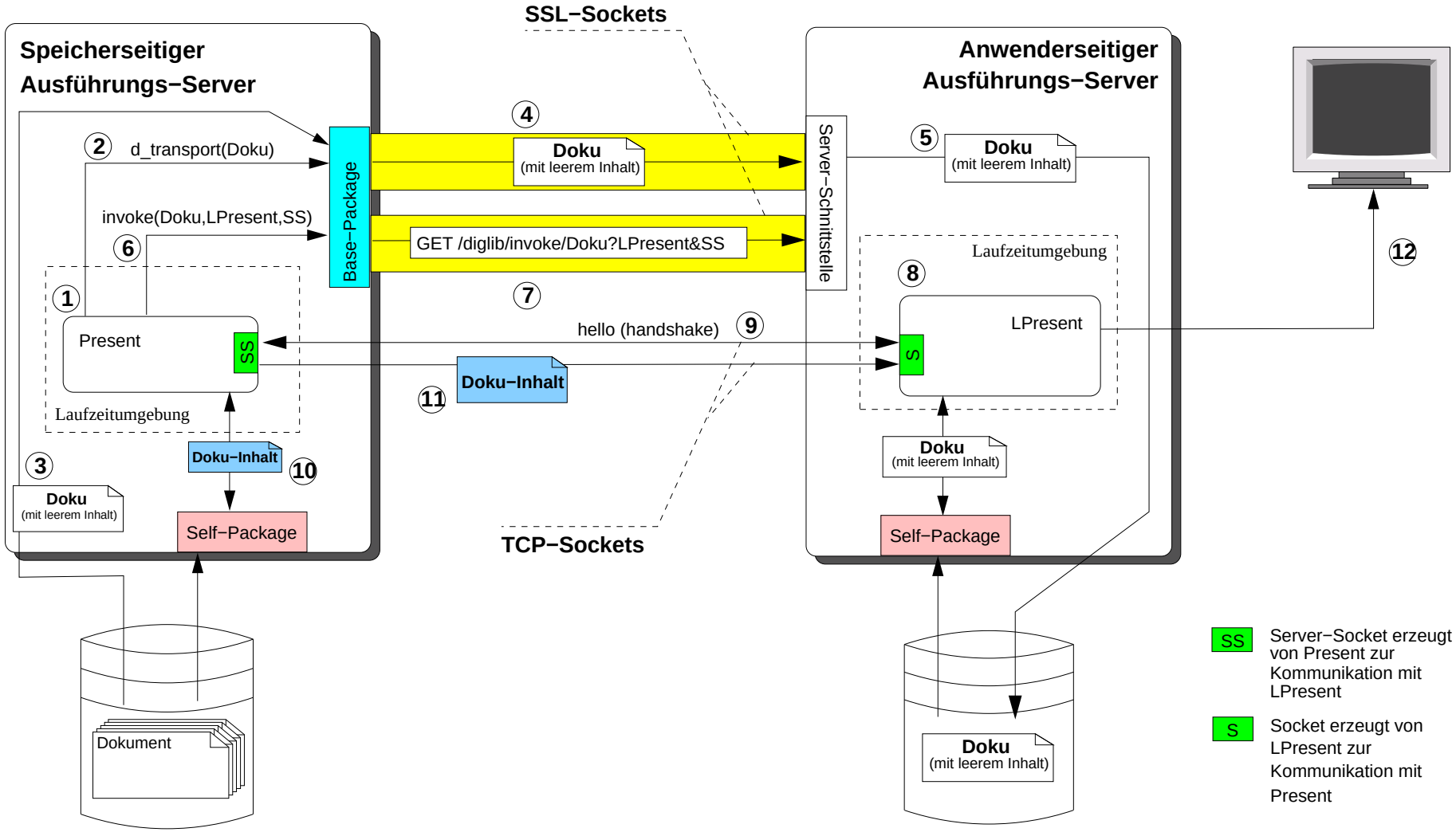


Abbildung 12 Online-Präsentation ohne NetSSL

Online-Präsentation (2)

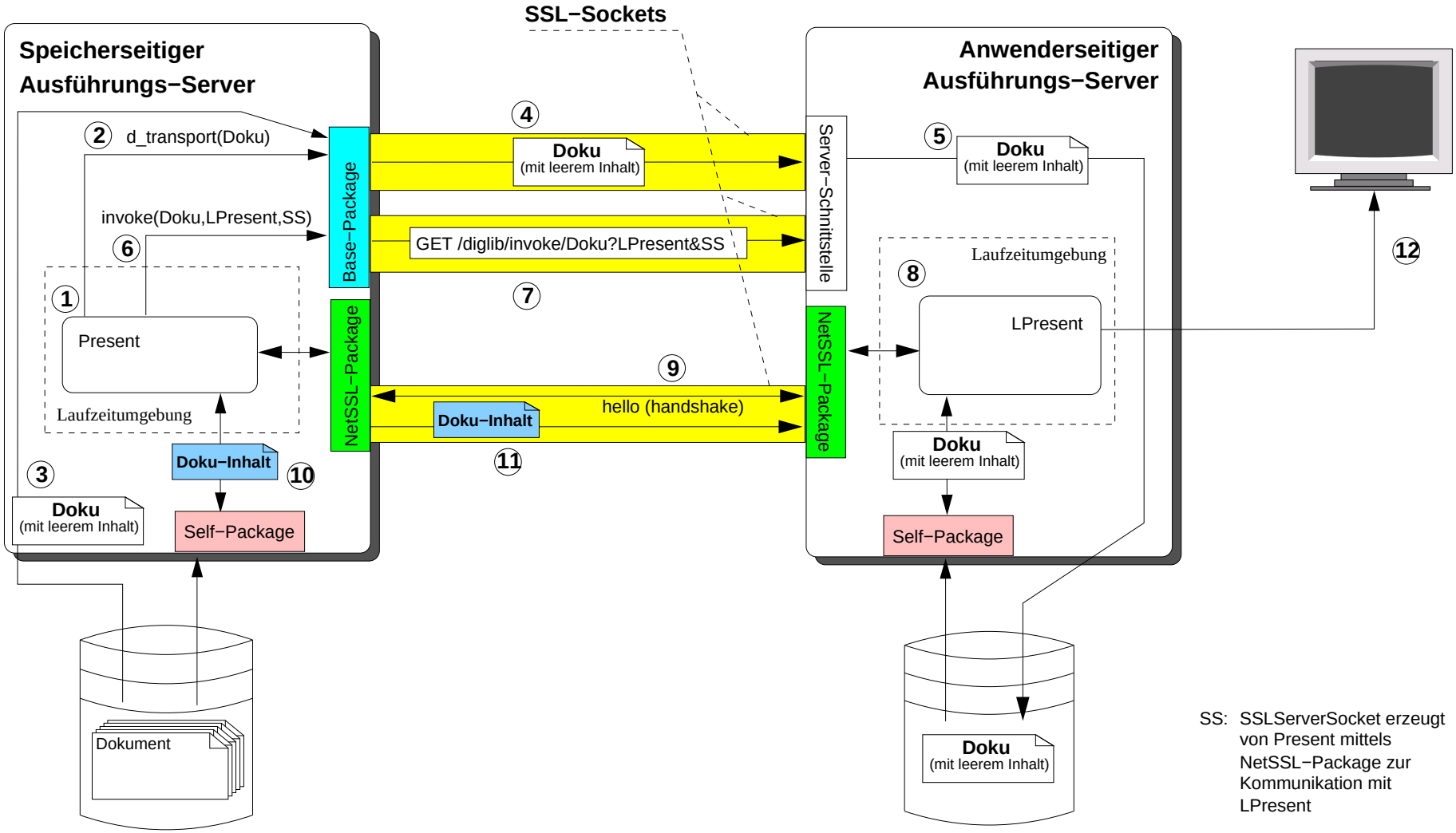


Abbildung 13 Online-Präsentation mit NetSSL