HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

Ein Verfahren zur passwortlosen Authentifizierung

Mirko Oleszuk

Institut für Informatik
Heinrich-Heine-Universität Düsseldorf

19. Dezember 2013

HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

Einleitung

- Passwörter sind ...!

HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

Einleitung

- Passwörter sind ...!
  - kurz, einfach und werden mehrmals verwendet

HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

Einleitung

- Passwörter sind ...!
  - kurz, einfach und werden mehrmals verwendet
- sich viele Passwörter merken ist nicht komfortabel

HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

Einleitung

- Passwörter sind ...!
  - kurz, einfach und werden mehrmals verwendet
- sich viele Passwörter merken ist nicht komfortabel
- Passwörter werden (manchmal) im Klartext gespeichert

HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

Einleitung

- Passwörter sind ...!
  - kurz, einfach und werden mehrmals verwendet
- sich viele Passwörter merken ist nicht komfortabel
- Passwörter werden (manchmal) im Klartext gespeichert
- $\Rightarrow$ Wir brauchen eine Lösung ohne Passwörter!

HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

Einleitung

- Passwörter sind ...!
  - kurz, einfach und werden mehrmals verwendet
- sich viele Passwörter merken ist nicht komfortabel
- Passwörter werden (manchmal) im Klartext gespeichert
- $\Rightarrow$ Wir brauchen eine Lösung ohne Passwörter!
  - kostenlos, einfach, sicher

HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

Das RSA-Kryptosystem

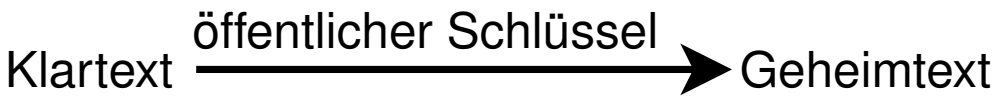
- jeder Benutzer besitzt ein Schlüsselpaar
  - öffentlicher Schlüssel
  - privater Schlüssel

HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

Das RSA-Kryptosystem

- jeder Benutzer besitzt ein Schlüsselpaar
  - öffentlicher Schlüssel
  - privater Schlüssel

Verschlüsselung:

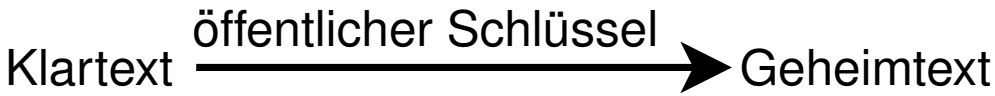


HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

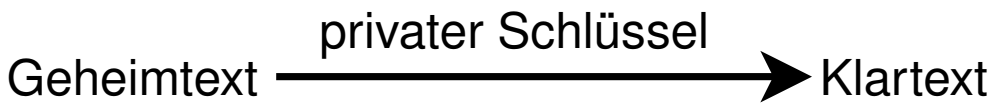
Das RSA-Kryptosystem

- jeder Benutzer besitzt ein Schlüsselpaar
  - öffentlicher Schlüssel
  - privater Schlüssel

Verschlüsselung:



Entschlüsselung:

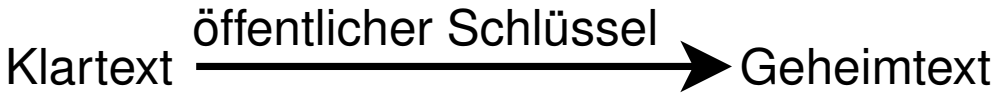


HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

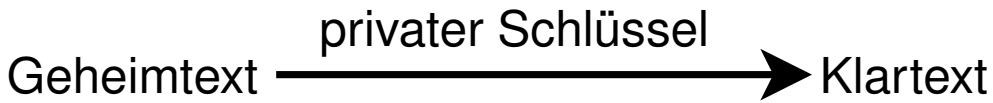
Das RSA-Kryptosystem

- jeder Benutzer besitzt ein Schlüsselpaar
  - öffentlicher Schlüssel
  - privater Schlüssel

Verschlüsselung:



Entschlüsselung:



- asymmetrisch

HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

Das RSA-Kryptosystem

- jeder Benutzer besitzt ein Schlüsselpaar
  - öffentlicher Schlüssel
  - privater Schlüssel

Signieren:

Klartext $\xrightarrow{\text{privater Schlüssel}}$ „Geheimtext“ (signierter Klartext)

Verifizierung:

„Geheimtext“ $\xrightarrow{\text{öffentlicher Schlüssel}}$ Klartext

HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

Das RSA-Kryptosystem

- jeder Benutzer besitzt ein Schlüsselpaar
  - öffentlicher Schlüssel
  - privater Schlüssel

Signieren:

$$\text{Klartext} \xrightarrow{\text{privater Schlüssel}} \text{„Geheimtext“ (signierter Klartext)}$$

Verifizierung:

$$\text{„Geheimtext“} \xrightarrow{\text{öffentlicher Schlüssel}} \text{Klartext}$$

- asymmetrisch $\equiv$ Public-Key-Kryptographie

HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

Überblick & Vorbereitung

Idee:

- signierte Daten identifizieren den Benutzer eindeutig

HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

Überblick & Vorbereitung

Idee:

- signierte Daten identifizieren den Benutzer eindeutig

Der Client

- kennt seinen privaten Schlüssel
- kennt seinen Benutzernamen

HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

Überblick & Vorbereitung

Idee:

- signierte Daten identifizieren den Benutzer eindeutig

Der Client

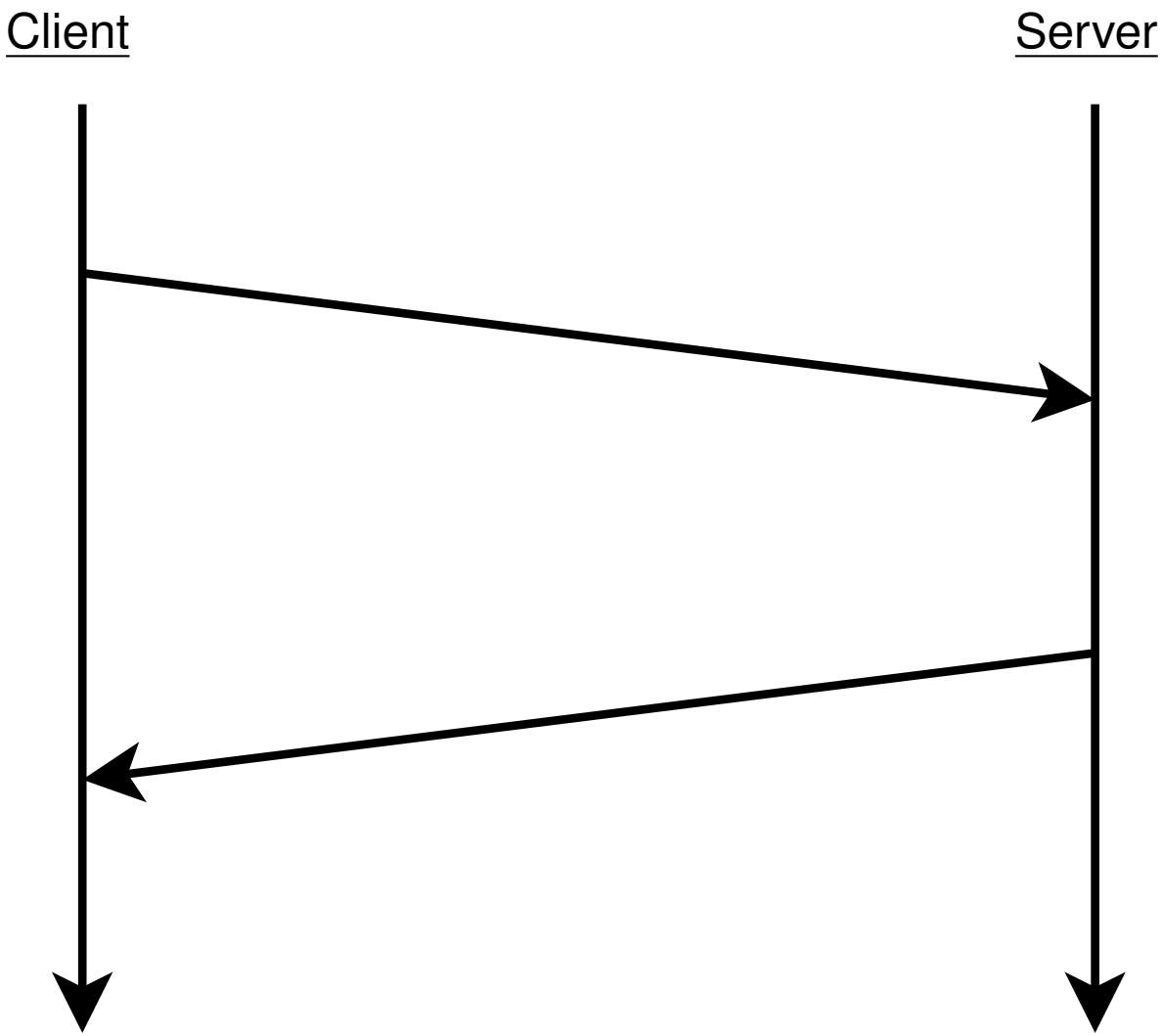
- kennt seinen privaten Schlüssel
- kennt seinen Benutzernamen

Der Server

- kennt den öffentlichen Schlüssel des Clients
- und dieser ist mit dem Benutzerkonto assoziiert

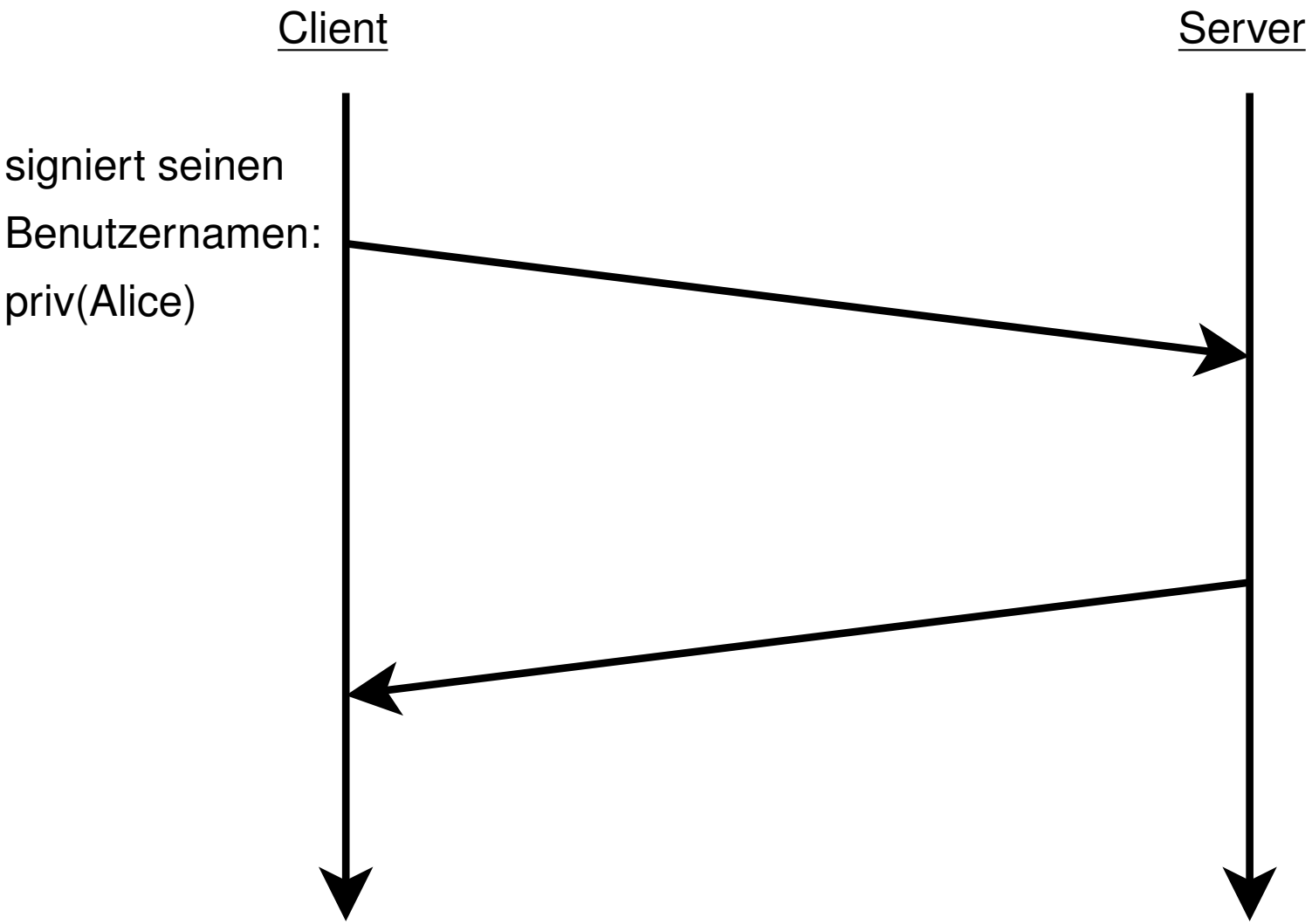
HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

PKWL 1.0 - Signierte Nachrichten



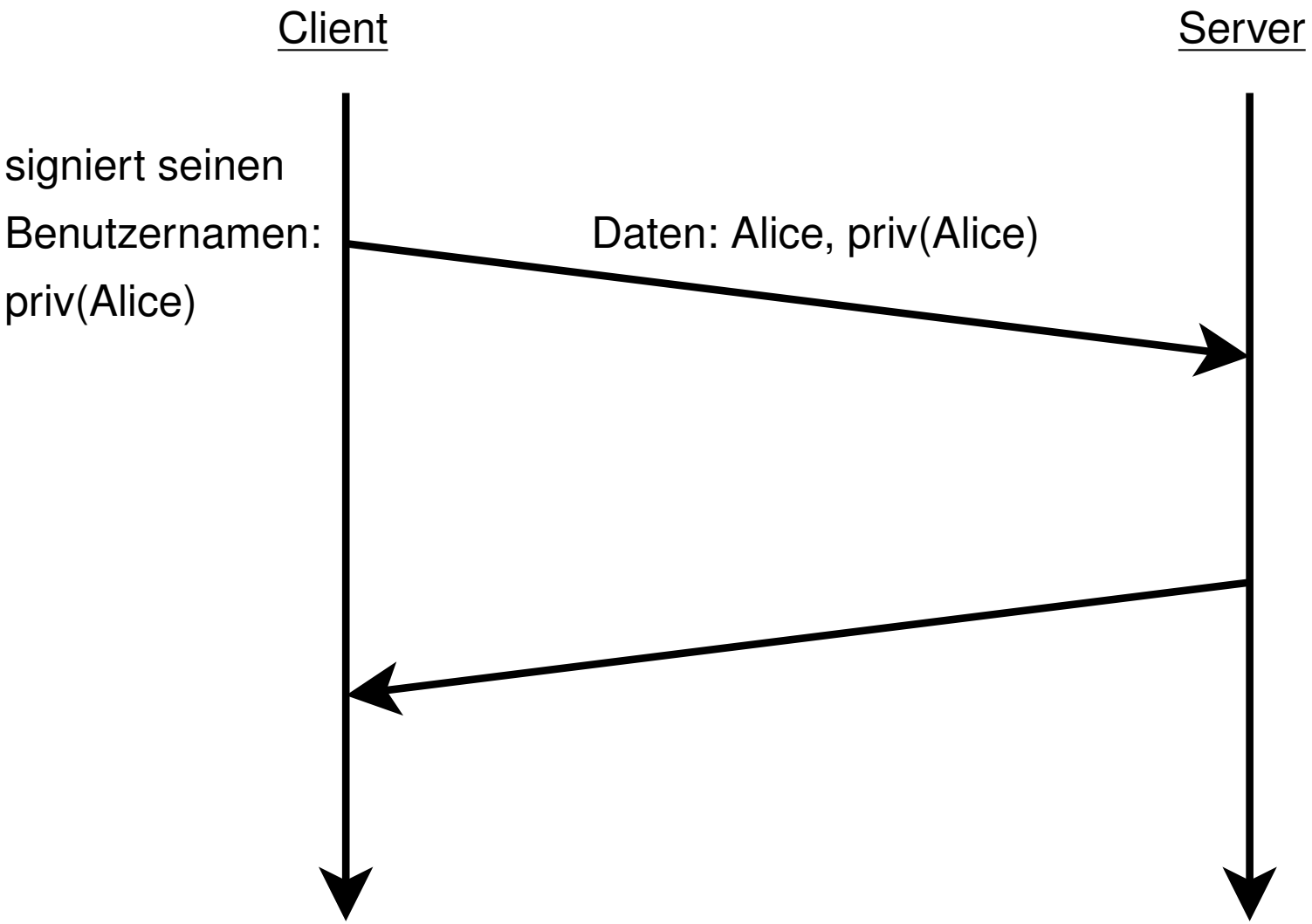
HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

PKWL 1.0 - Signierte Nachrichten



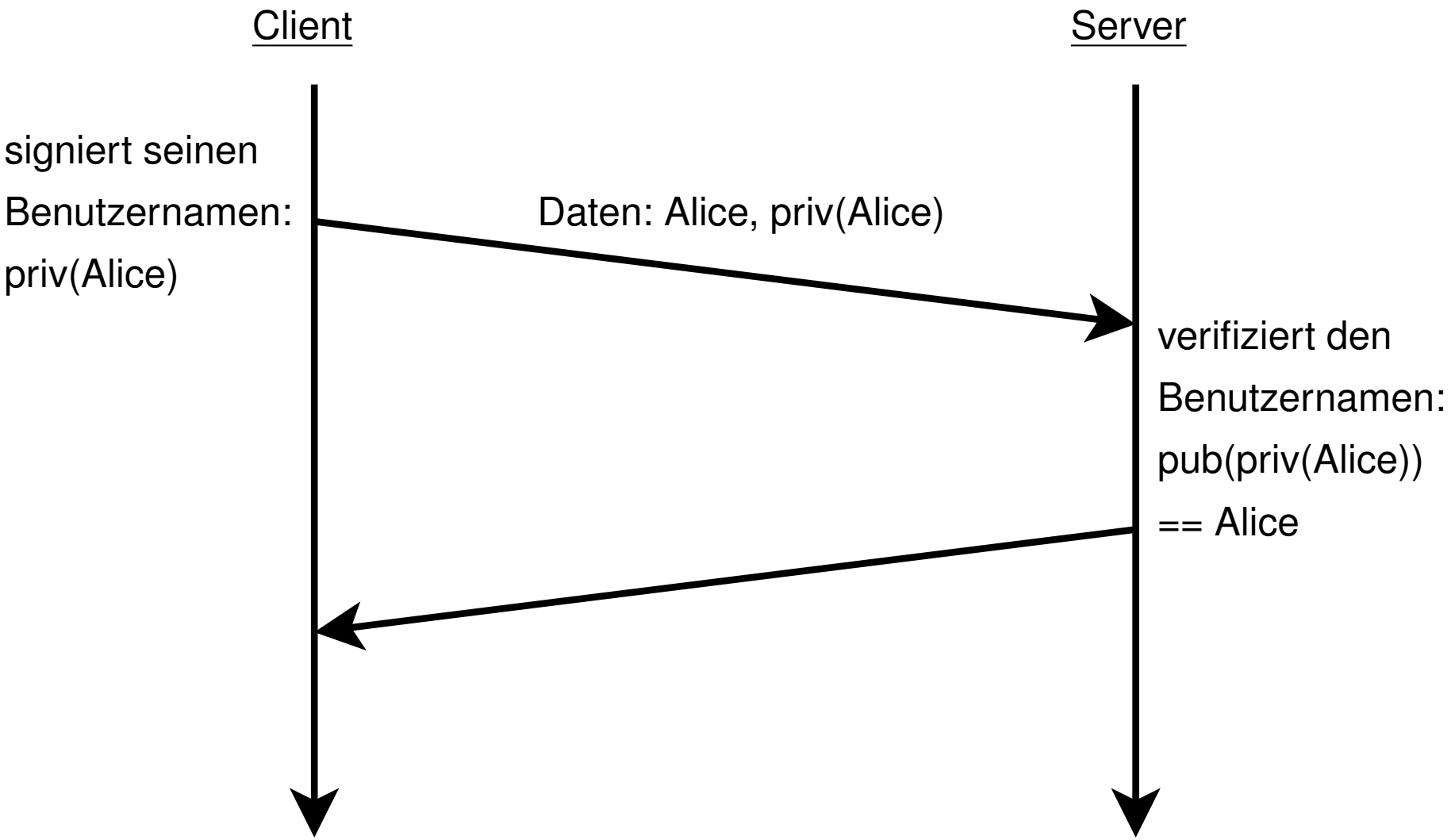
HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

PKWL 1.0 - Signierte Nachrichten



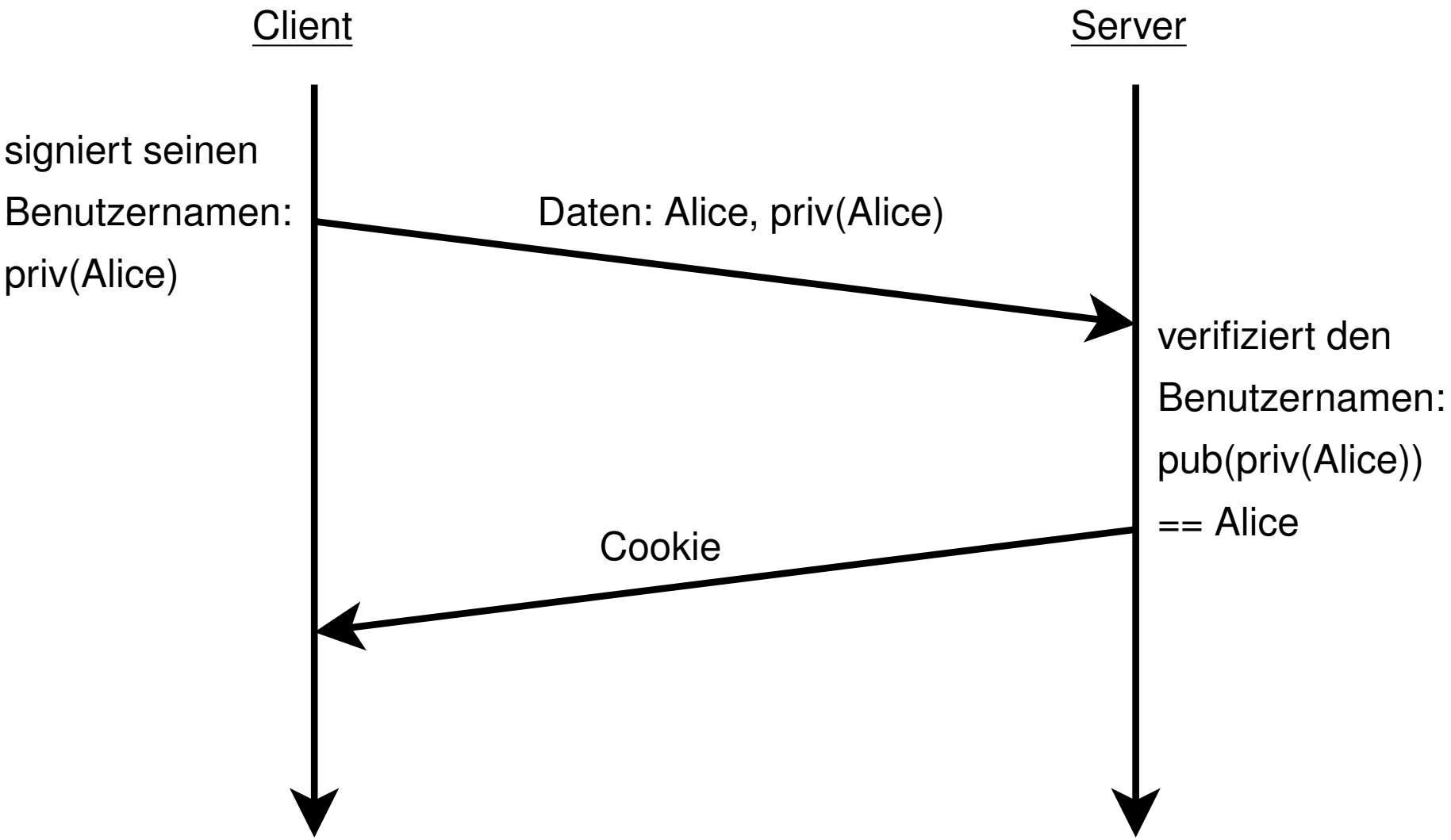
HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

PKWL 1.0 - Signierte Nachrichten



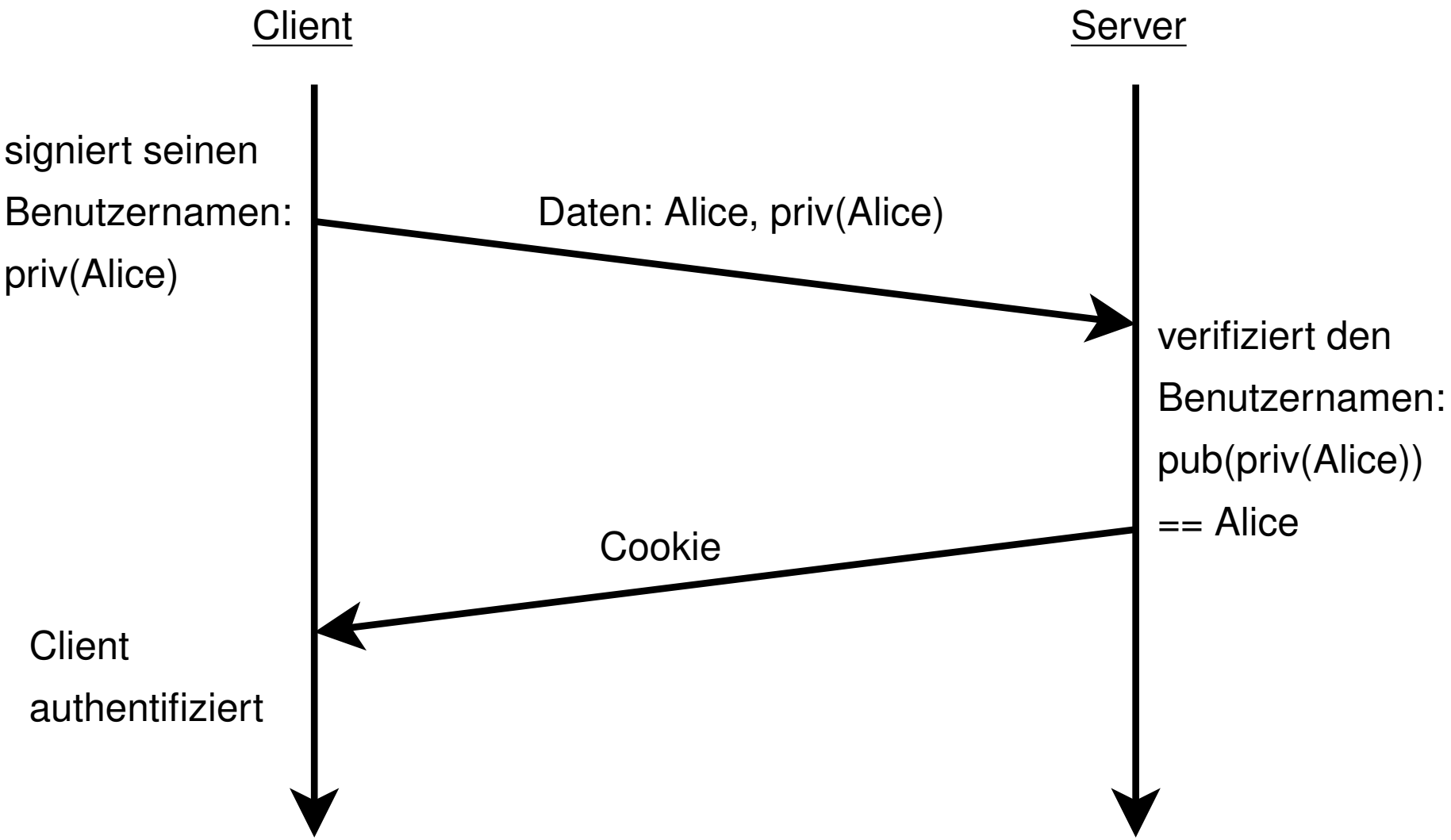
HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

PKWL 1.0 - Signierte Nachrichten



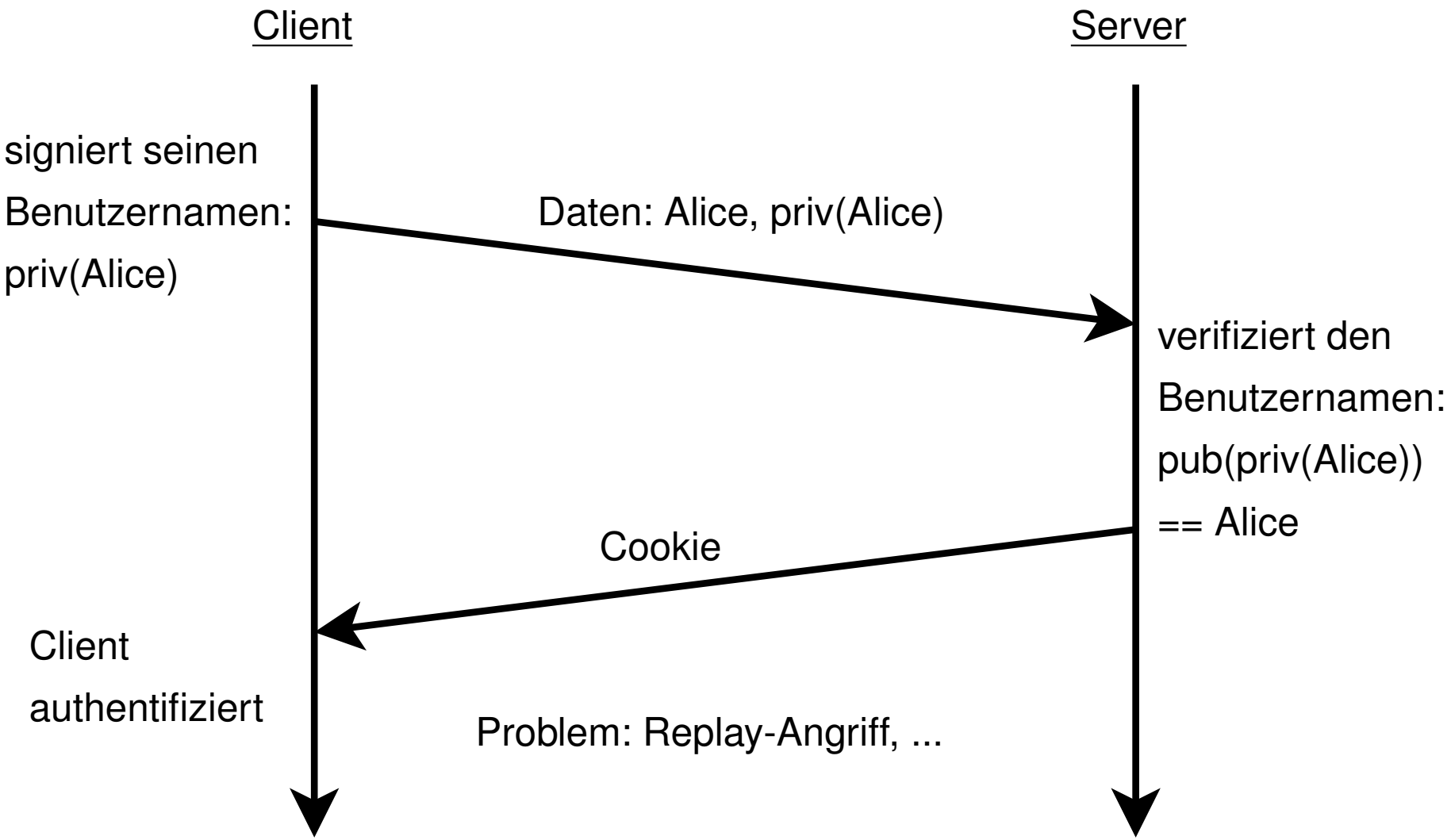
HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

PKWL 1.0 - Signierte Nachrichten



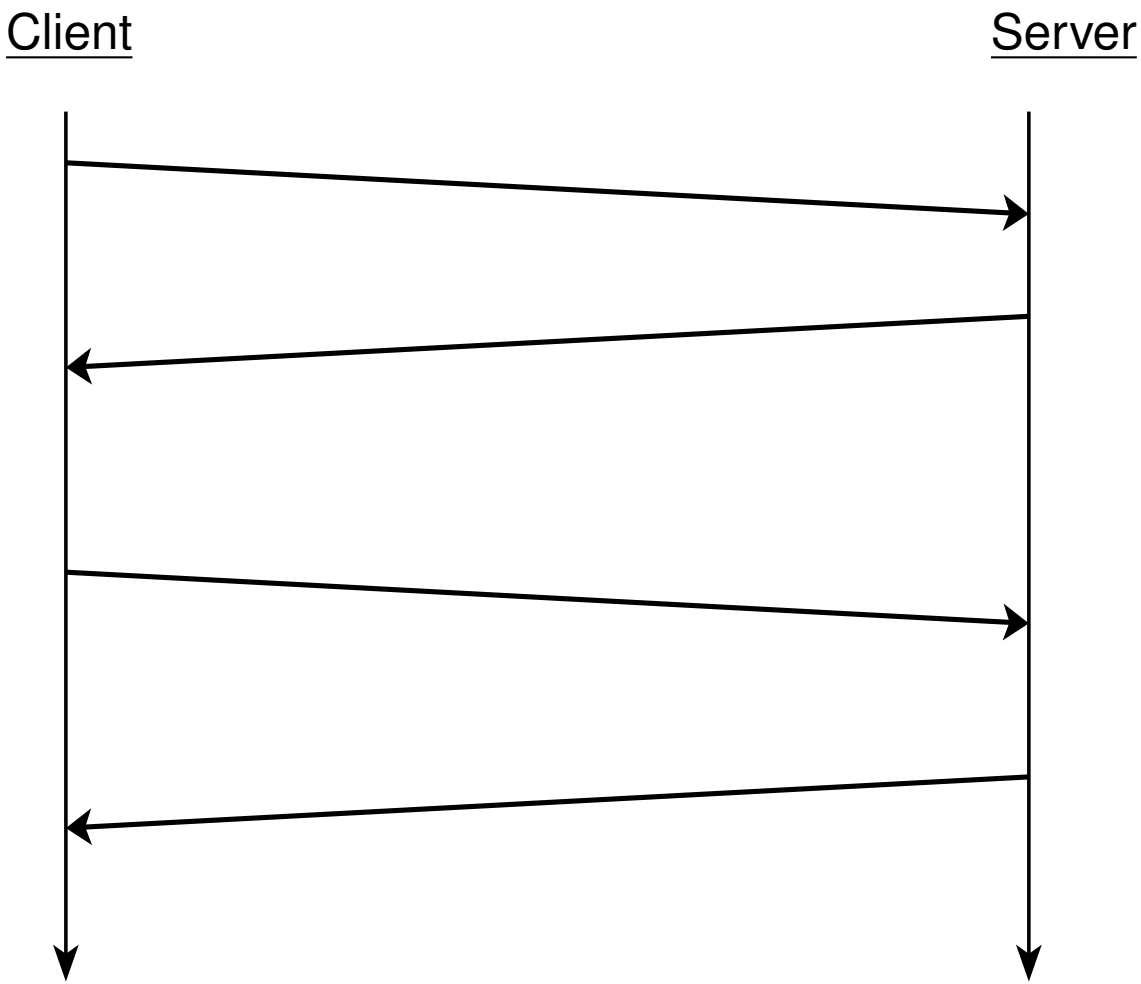
HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

PKWL 1.0 - Signierte Nachrichten



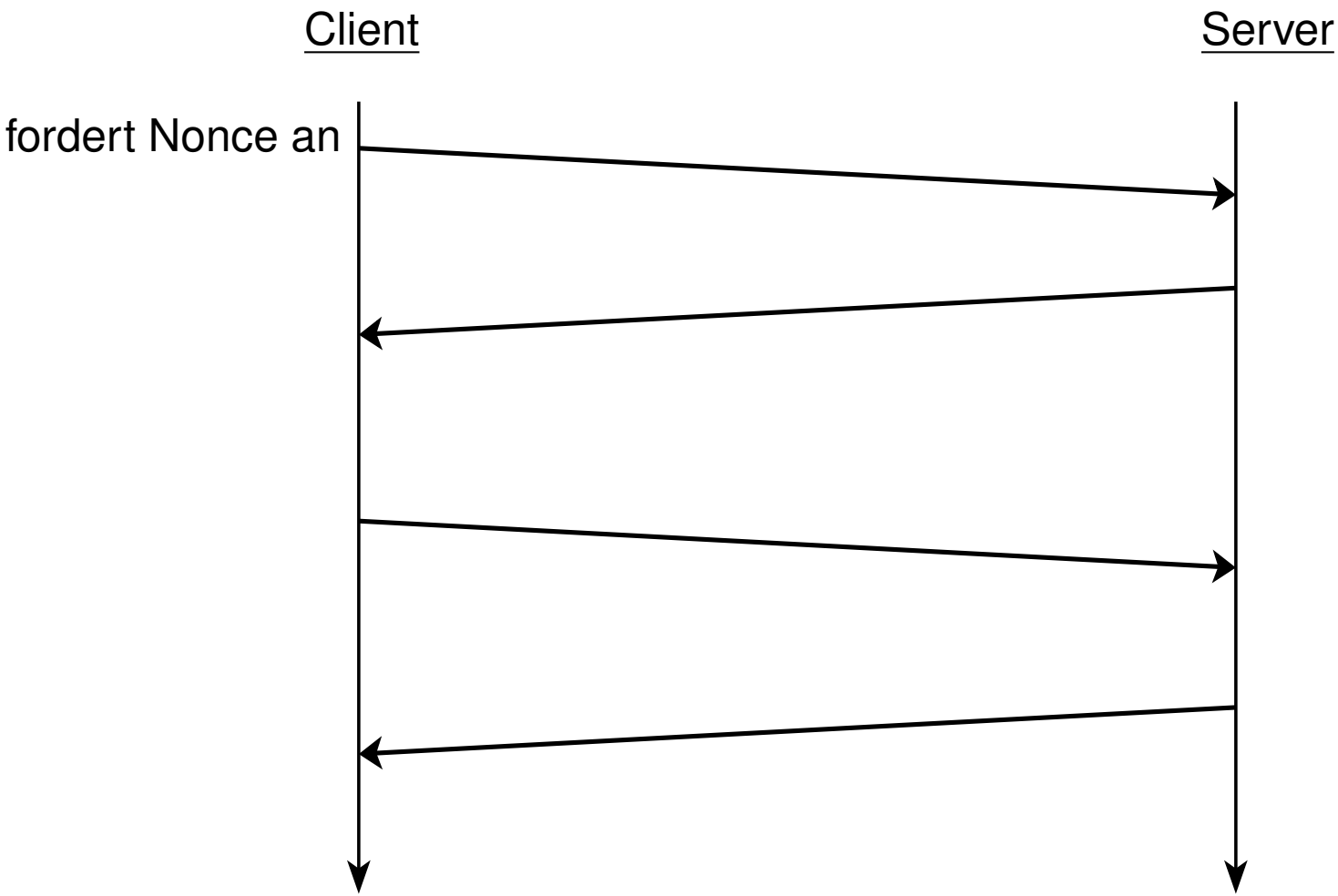
HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

PKWL 1.1 - Signierte Noncen



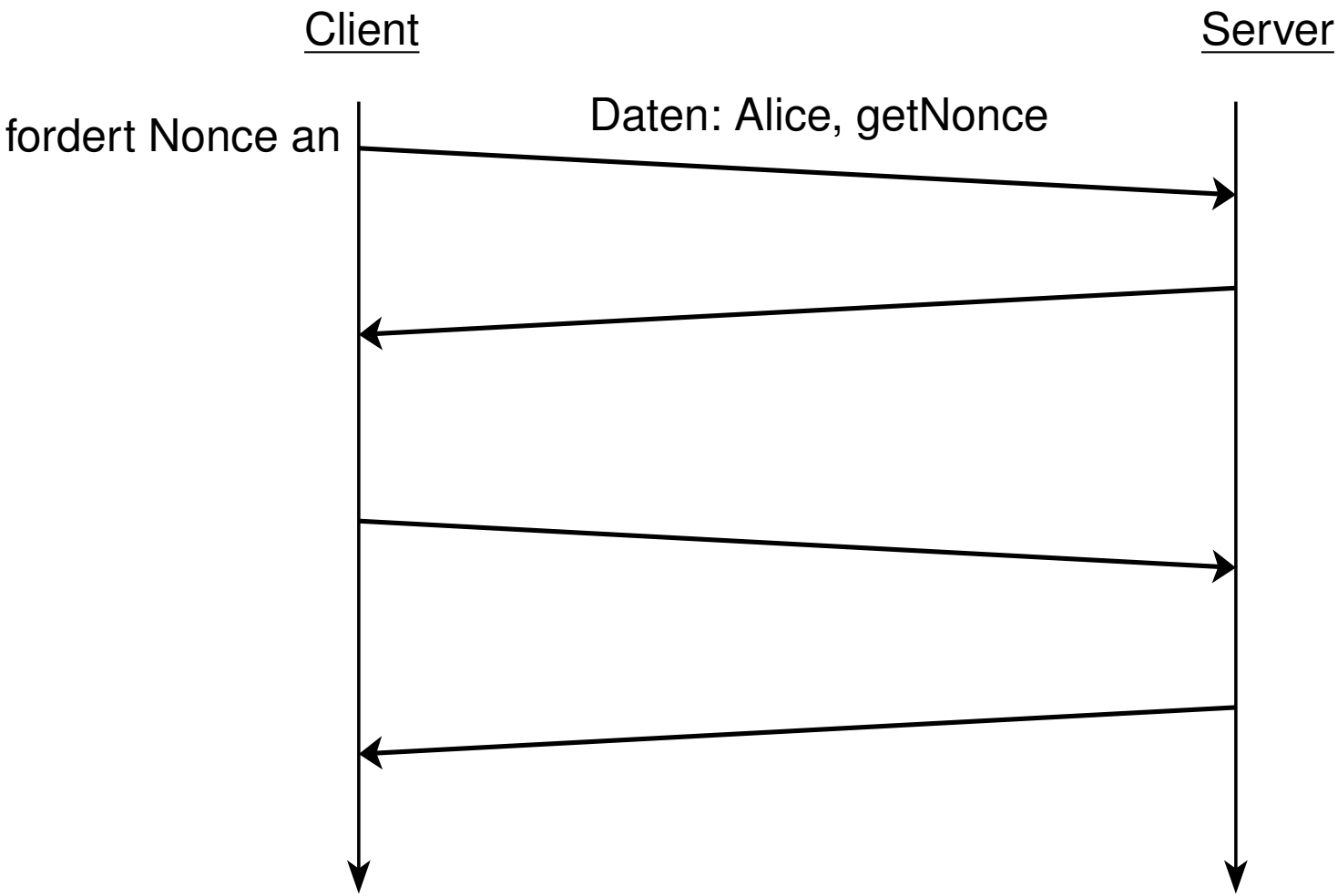
HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

PKWL 1.1 - Signierte Noncen



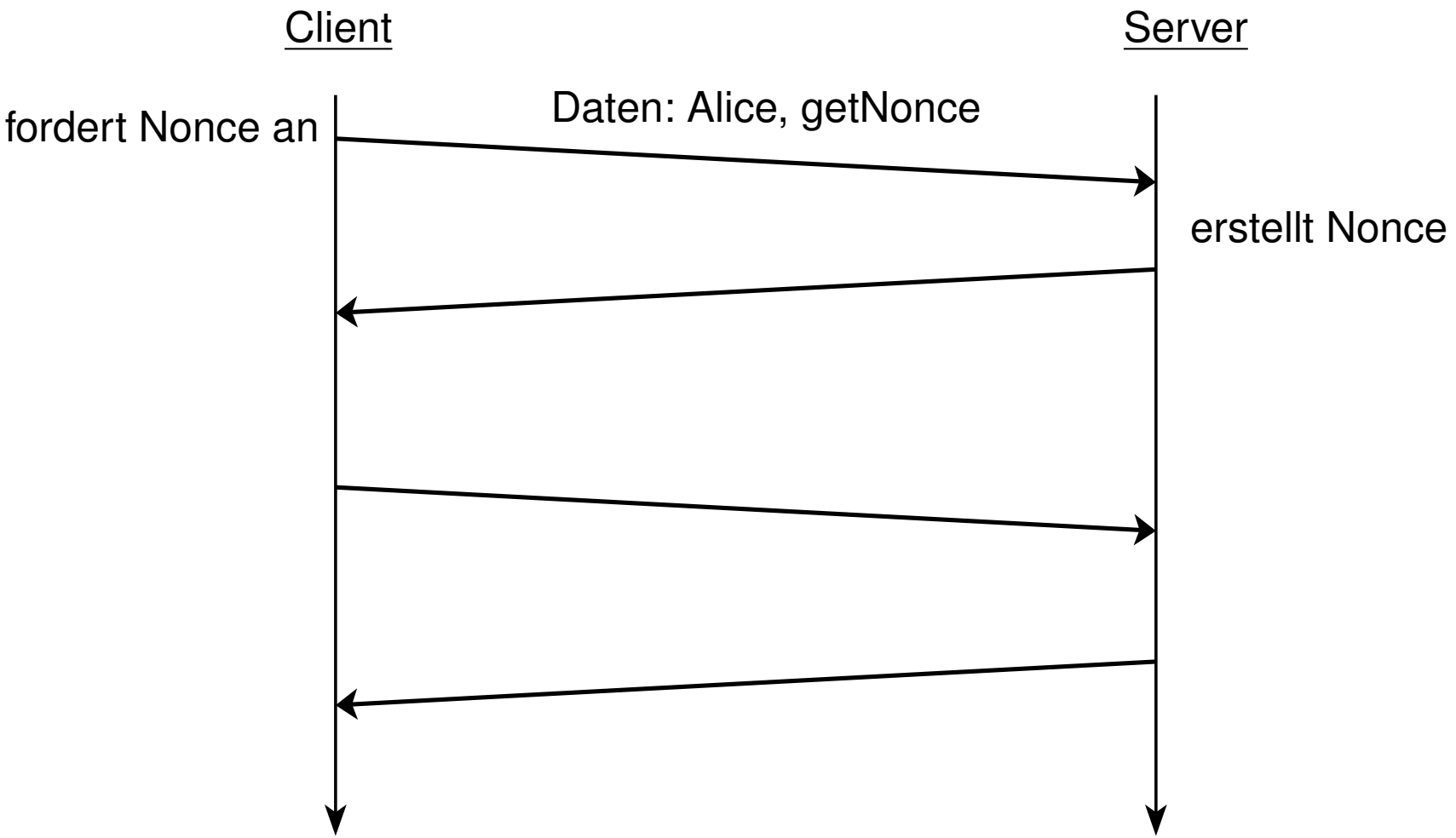
HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

PKWL 1.1 - Signierte Noncen



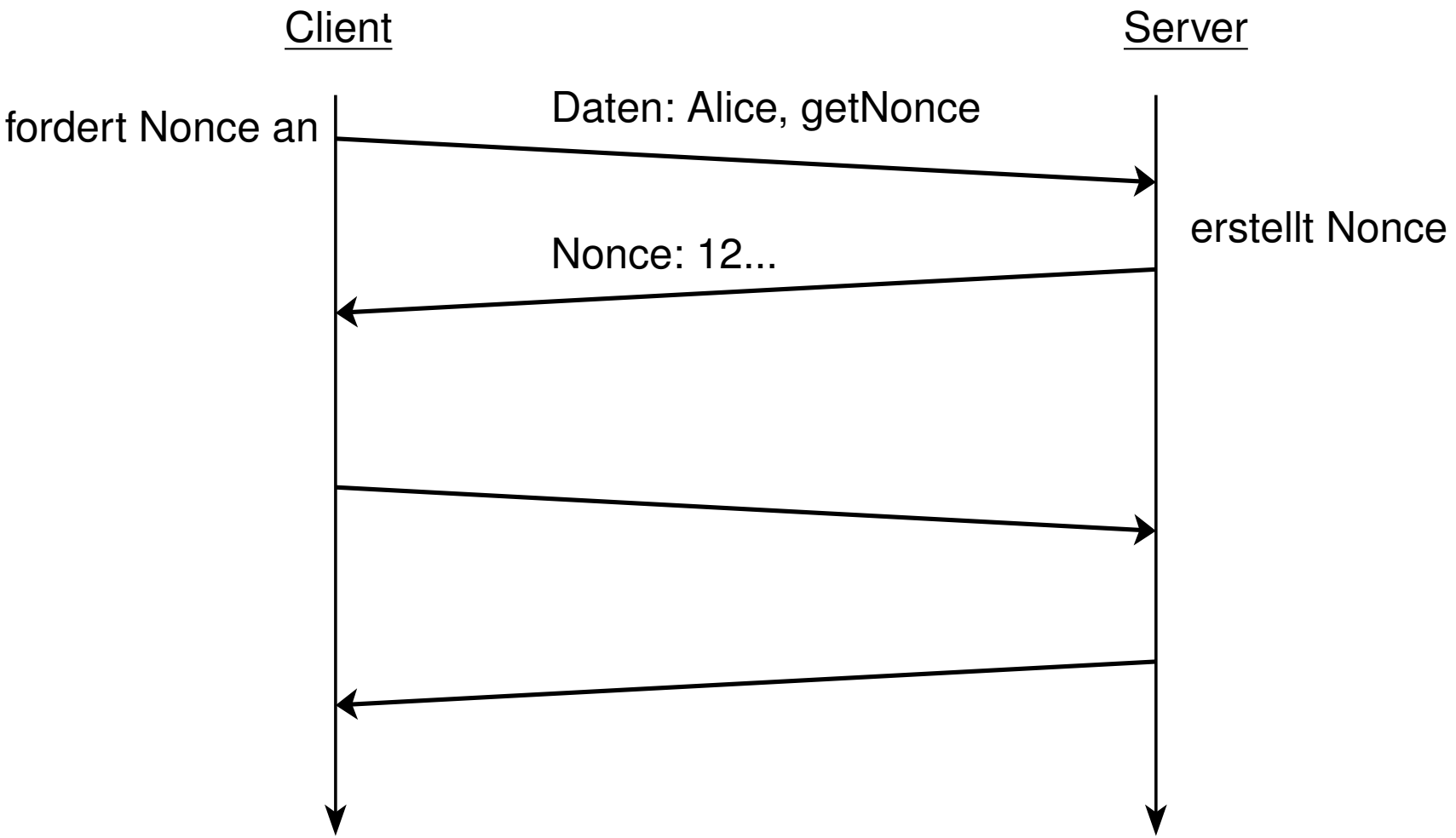
HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

PKWL 1.1 - Signierte Noncen



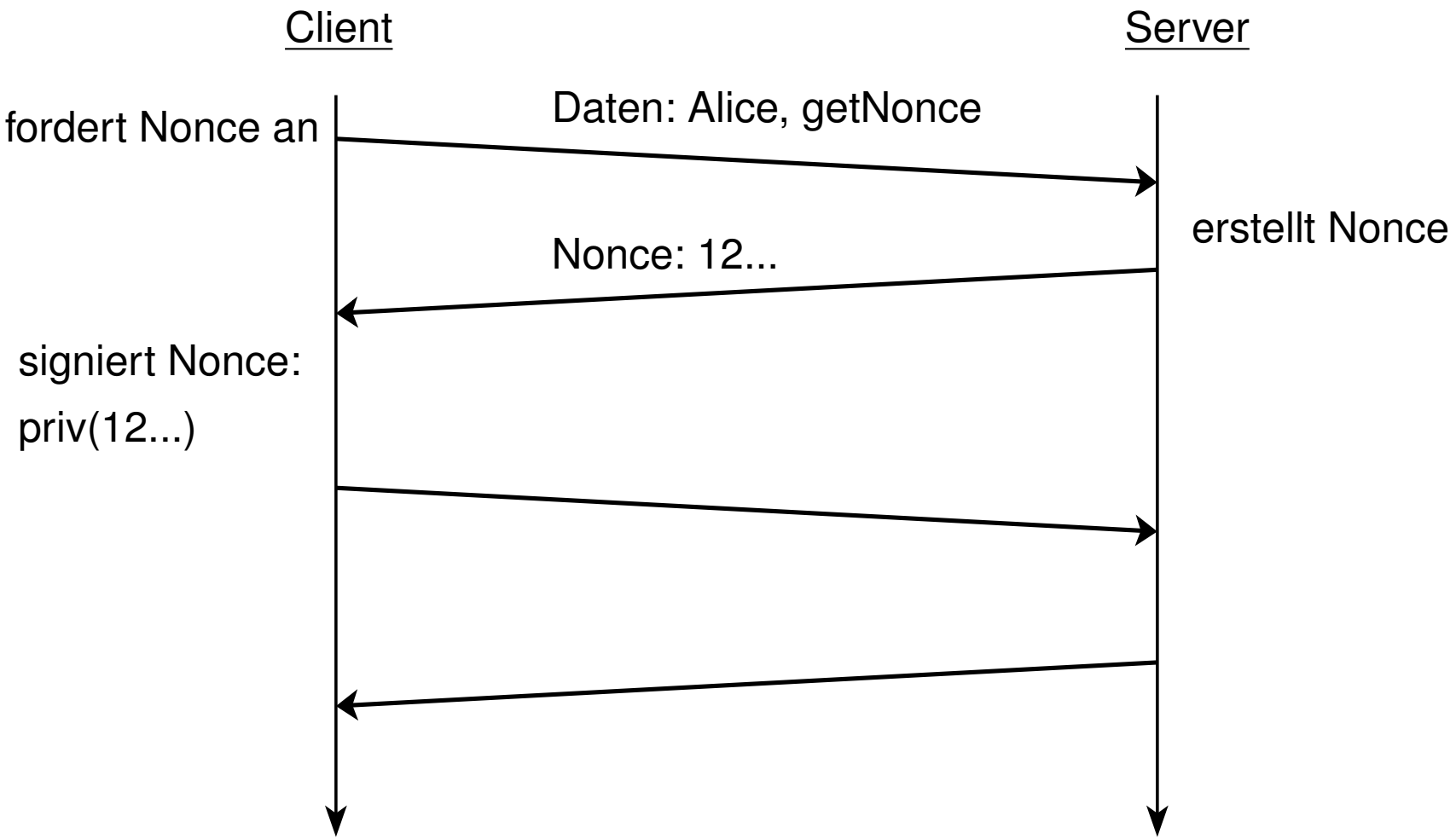
HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

PKWL 1.1 - Signierte Noncen



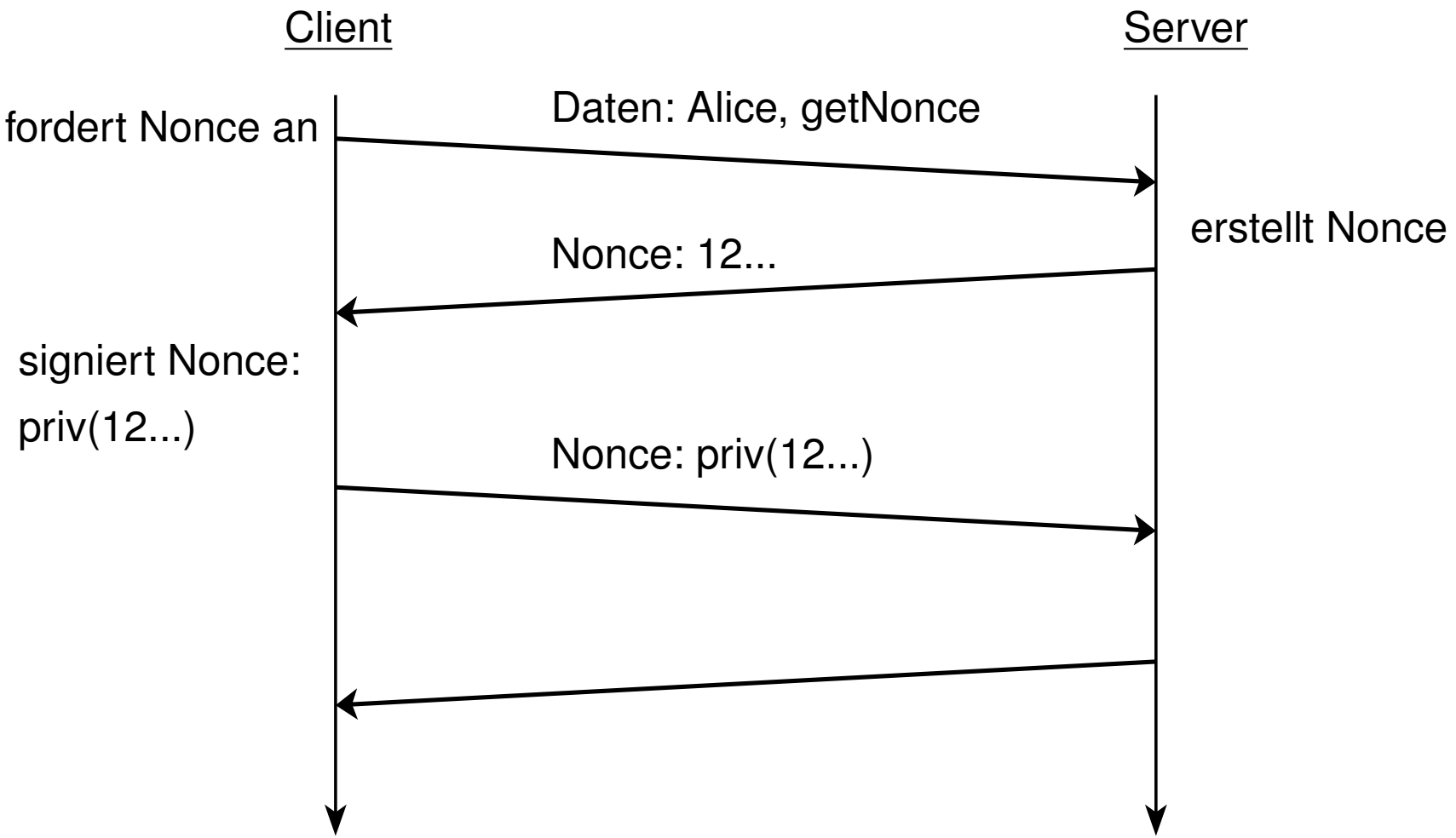
HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

PKWL 1.1 - Signierte Noncen



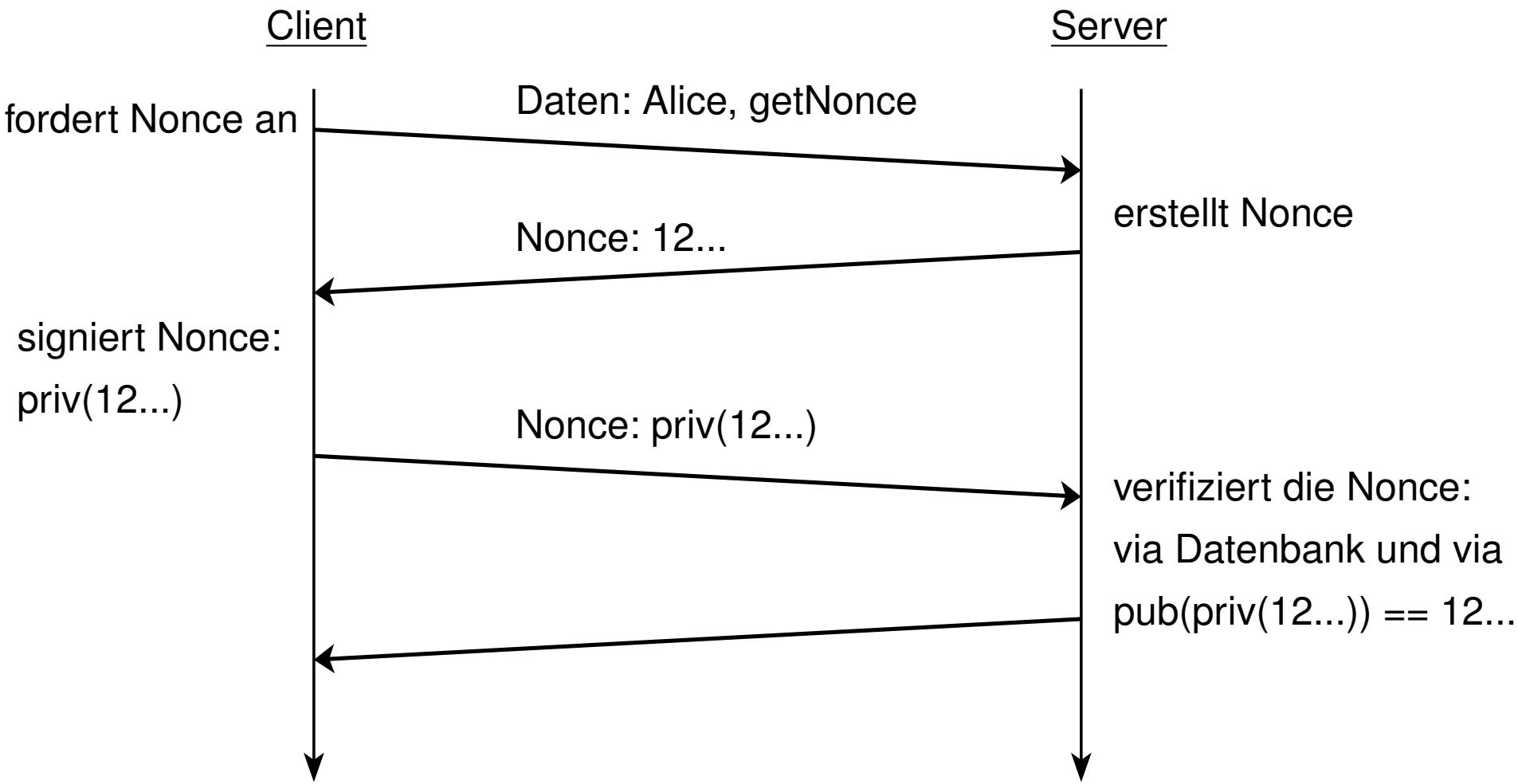
HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

PKWL 1.1 - Signierte Noncen



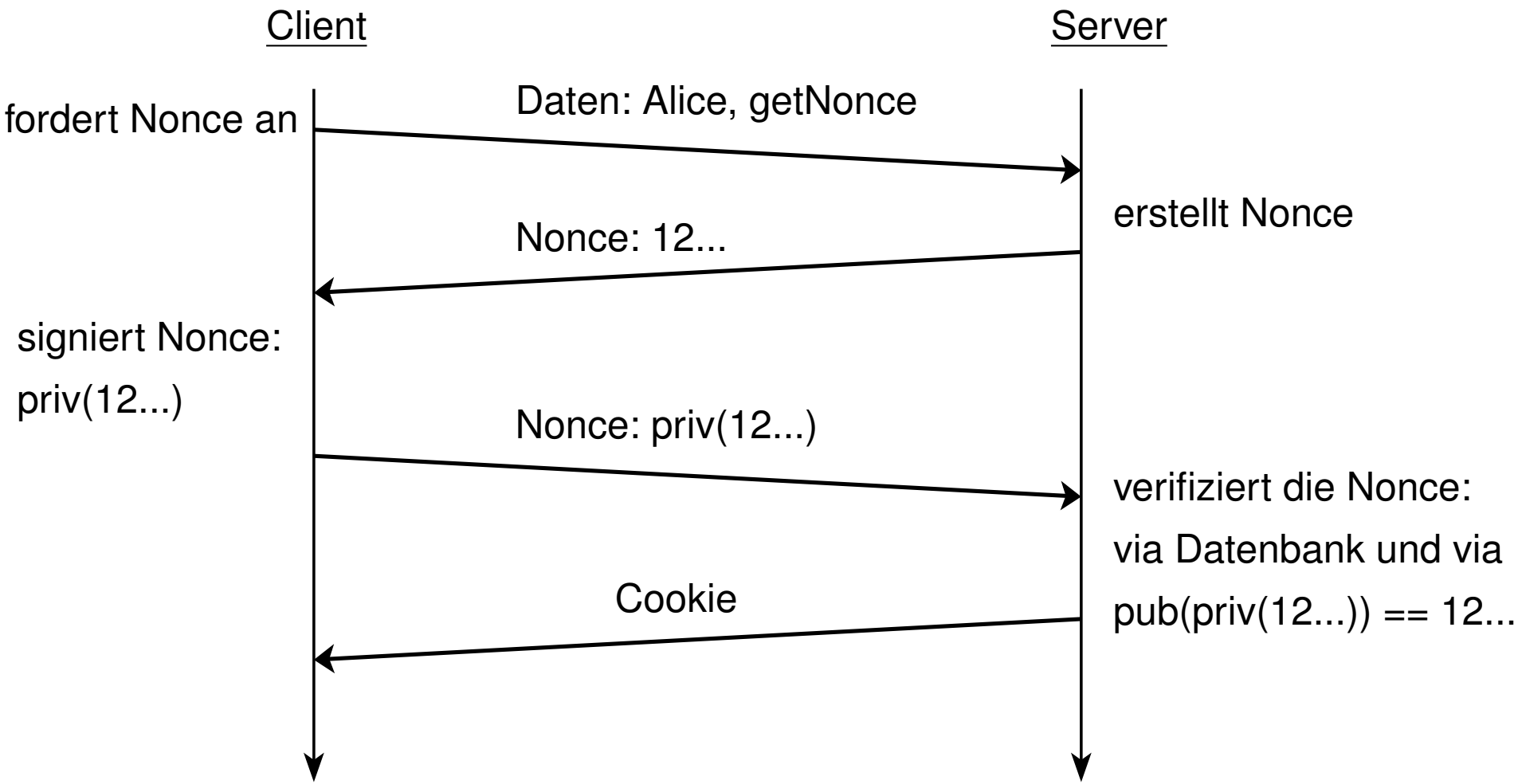
HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

PKWL 1.1 - Signierte Noncen



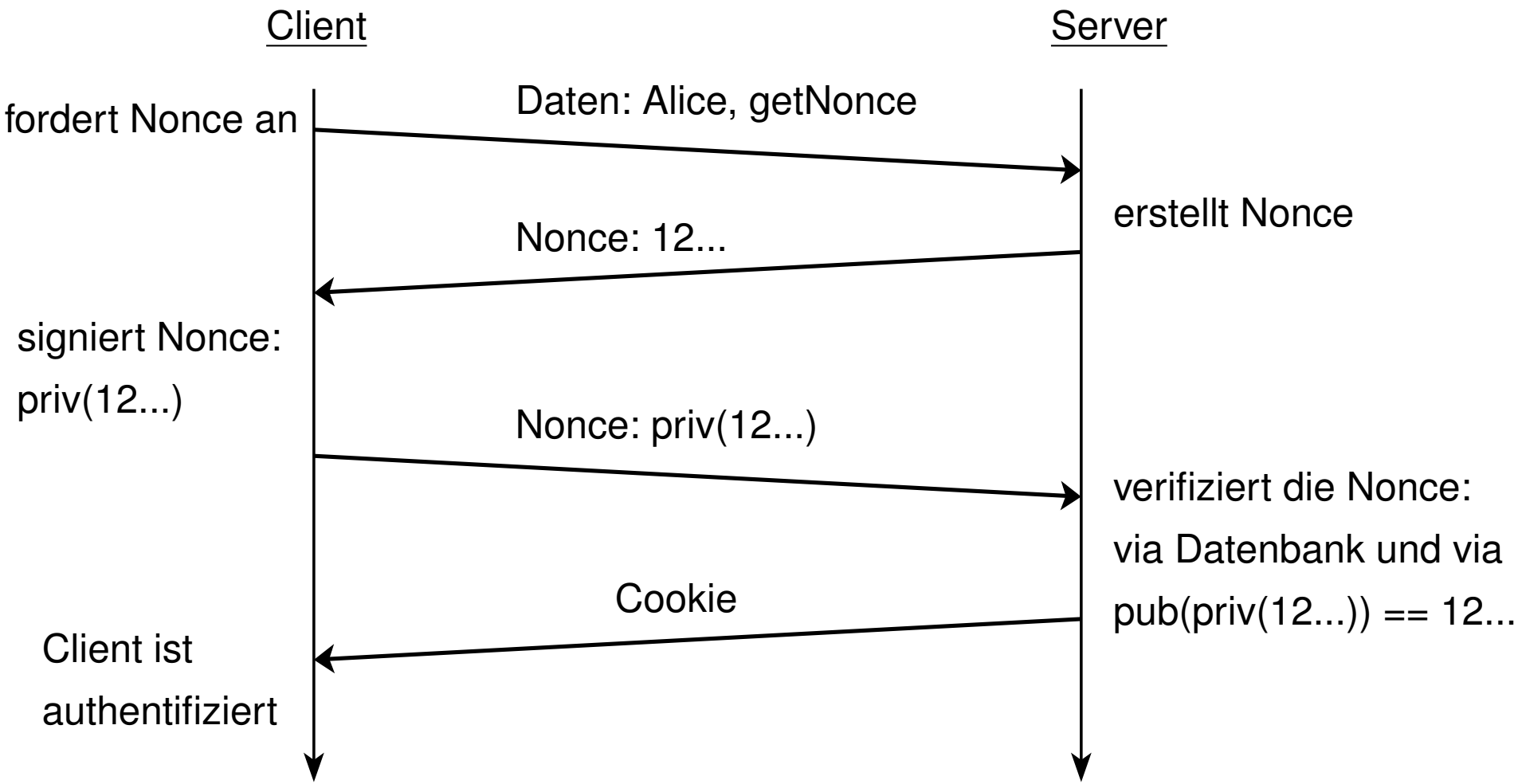
HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

PKWL 1.1 - Signierte Noncen



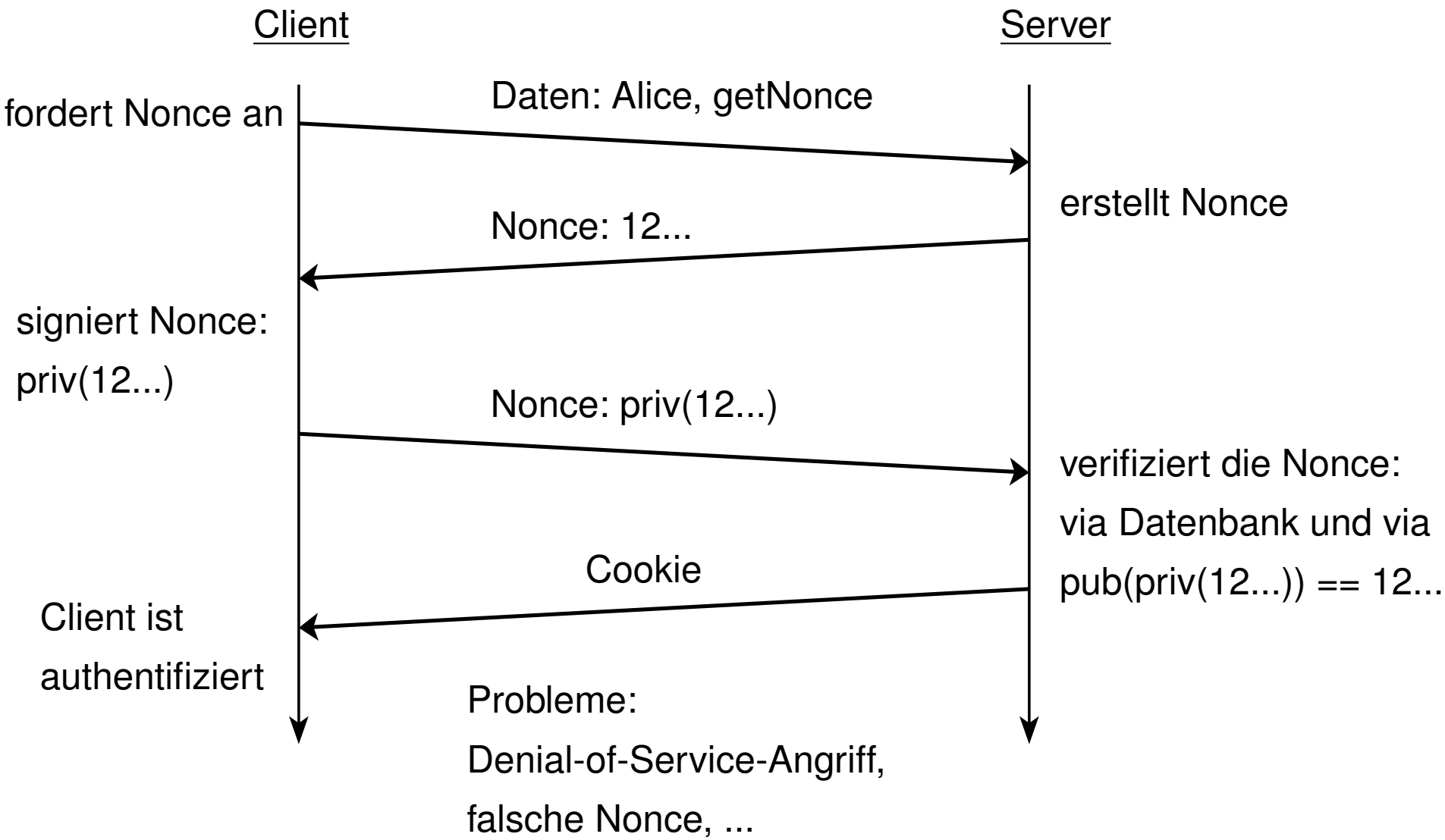
HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

PKWL 1.1 - Signierte Noncen



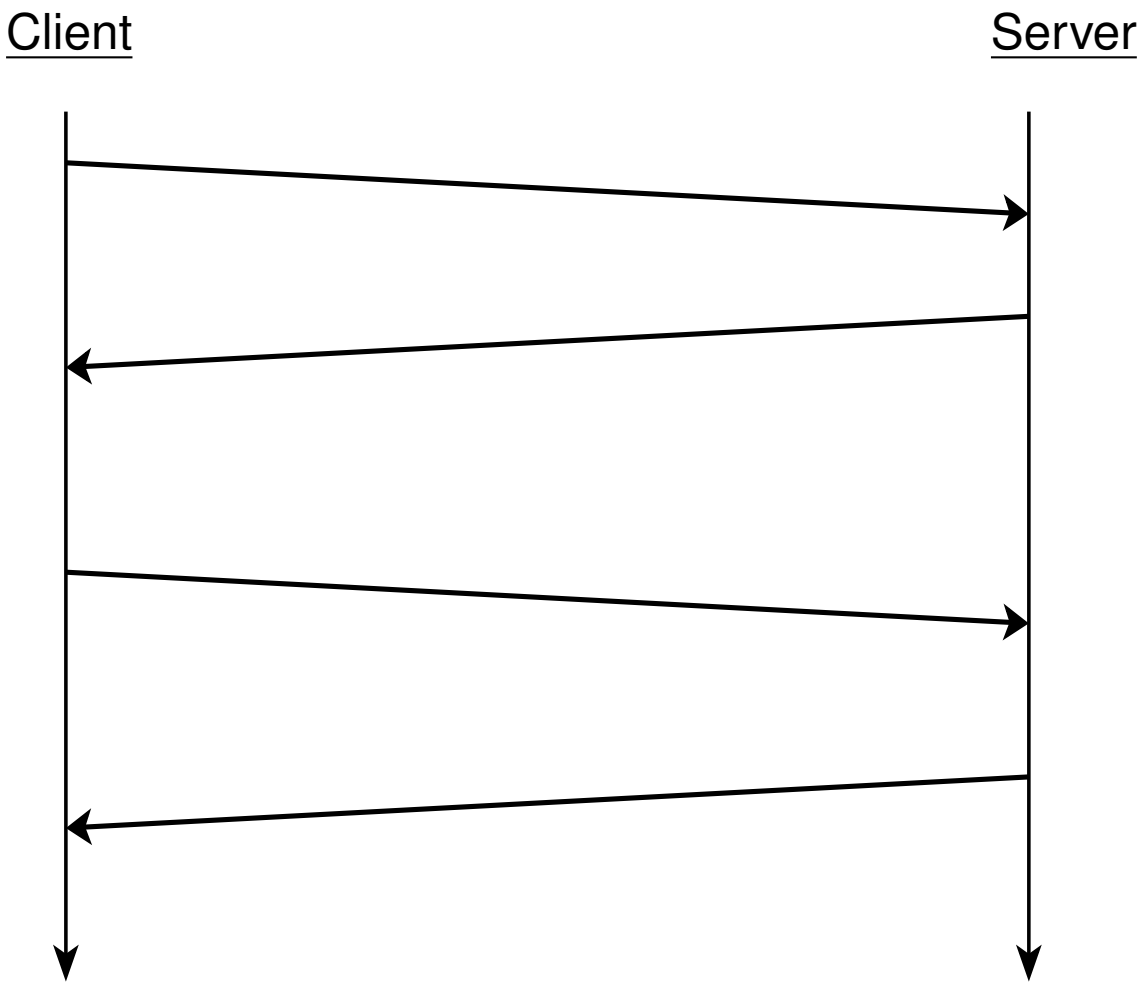
HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

PKWL 1.1 - Signierte Noncen



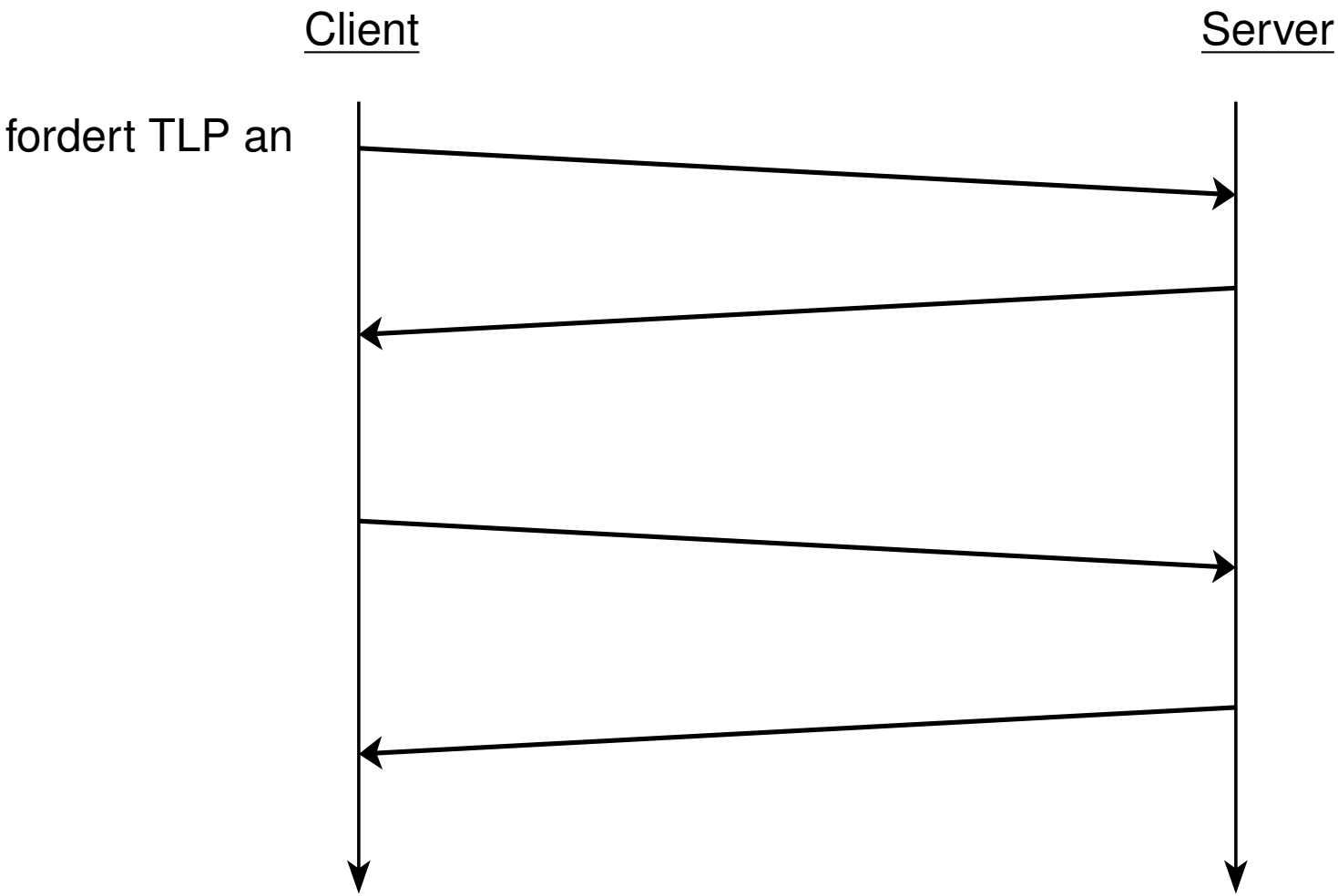
HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

PKWL 2.0 - Proof-of-Work-System



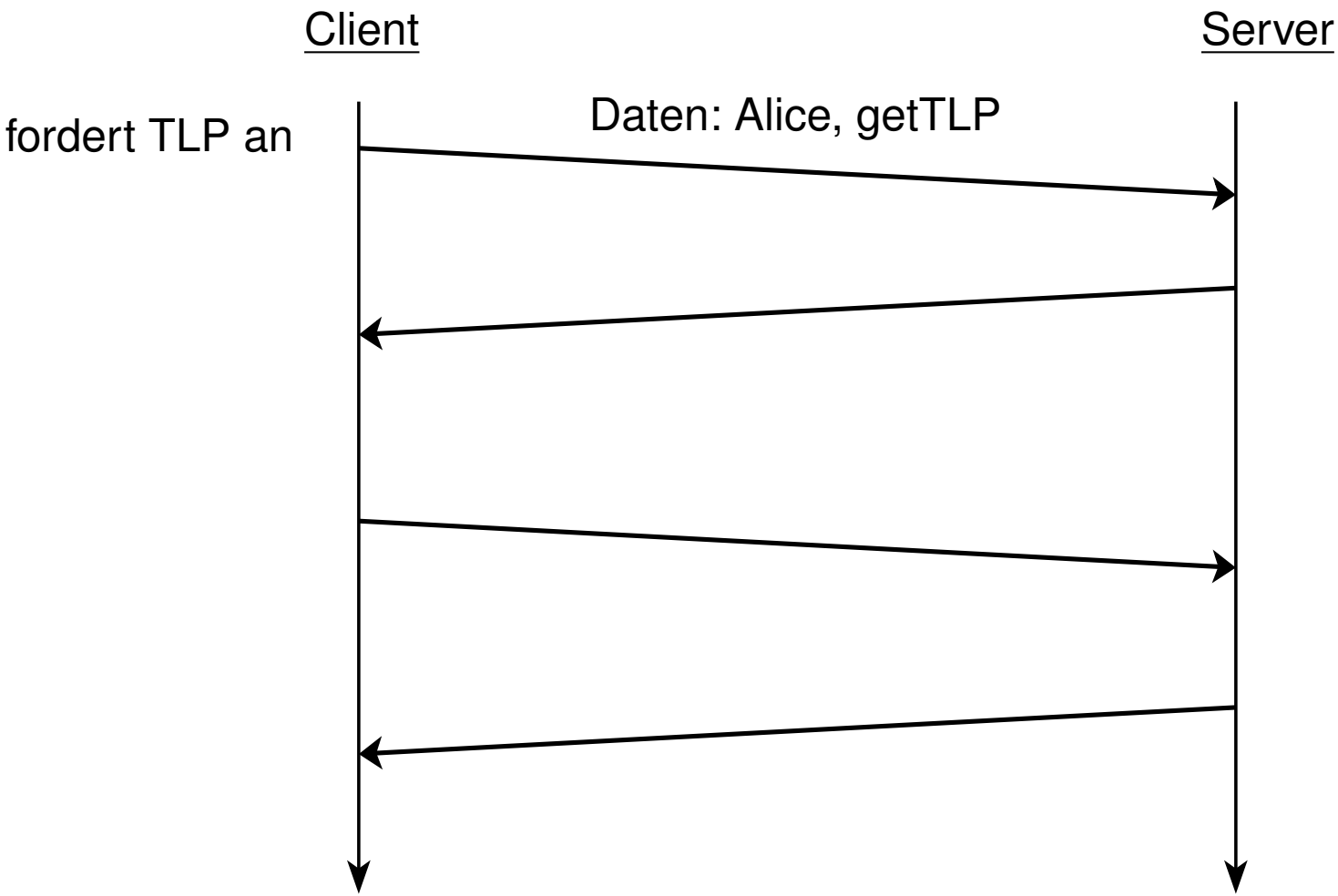
HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

PKWL 2.0 - Proof-of-Work-System



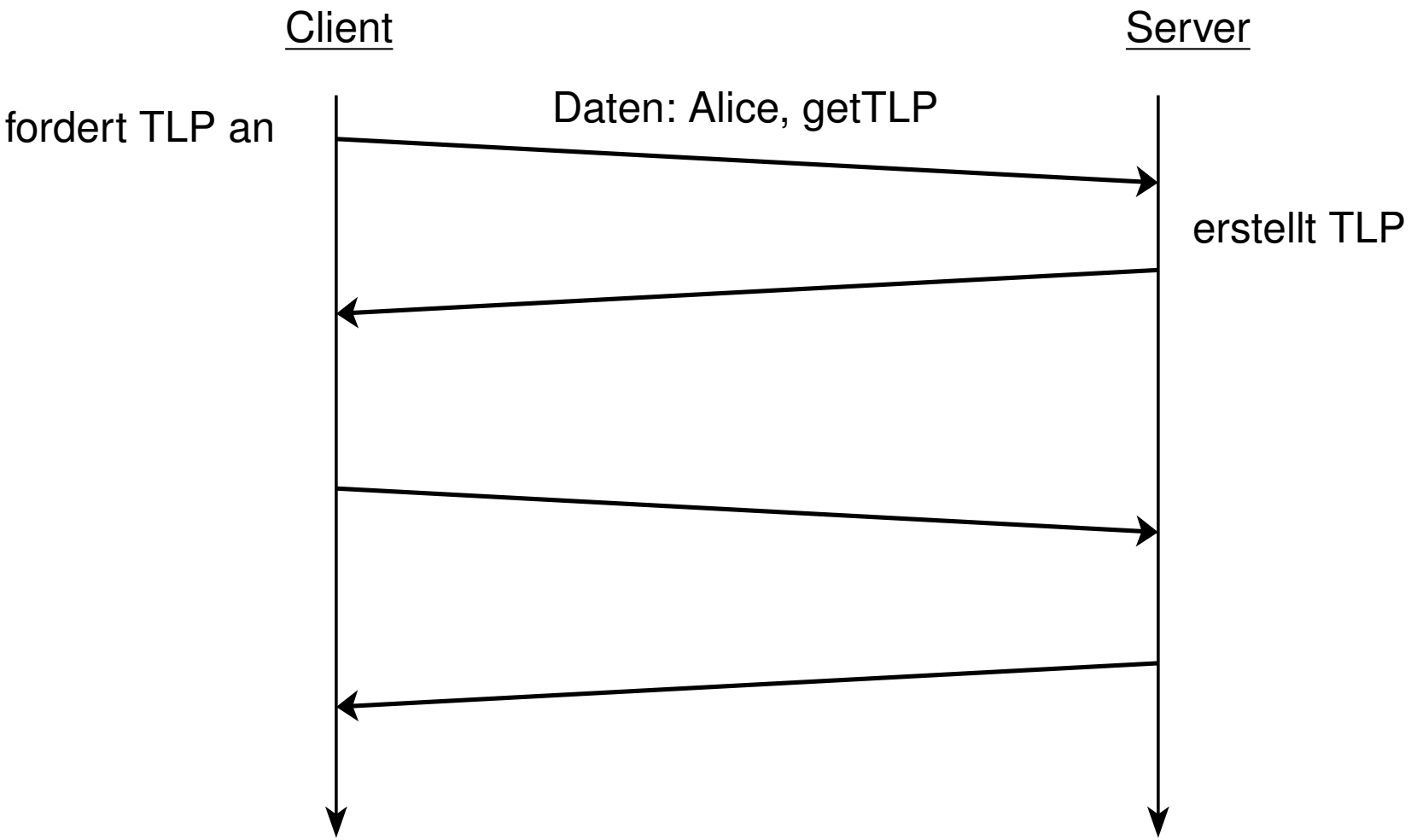
HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

PKWL 2.0 - Proof-of-Work-System



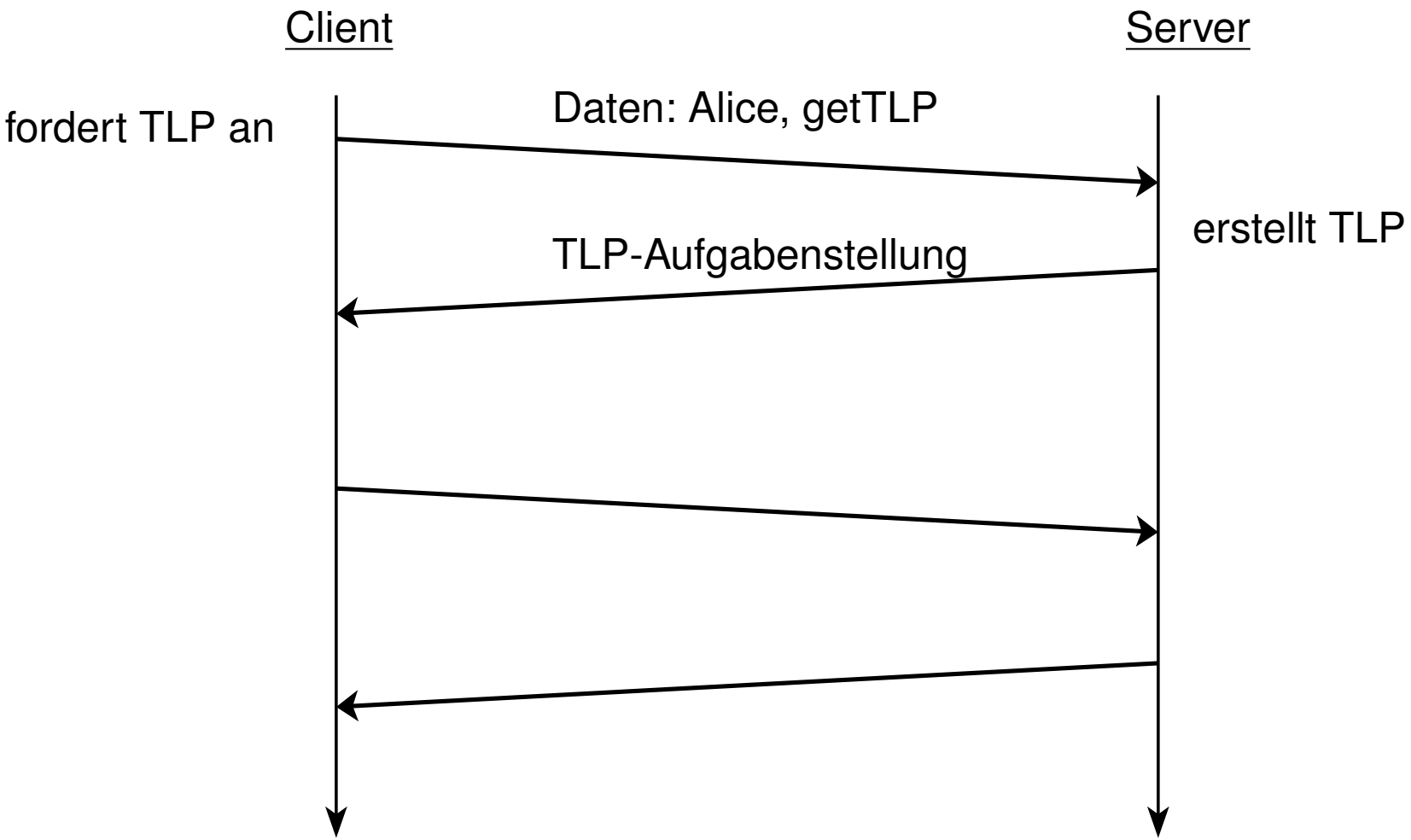
HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

PKWL 2.0 - Proof-of-Work-System



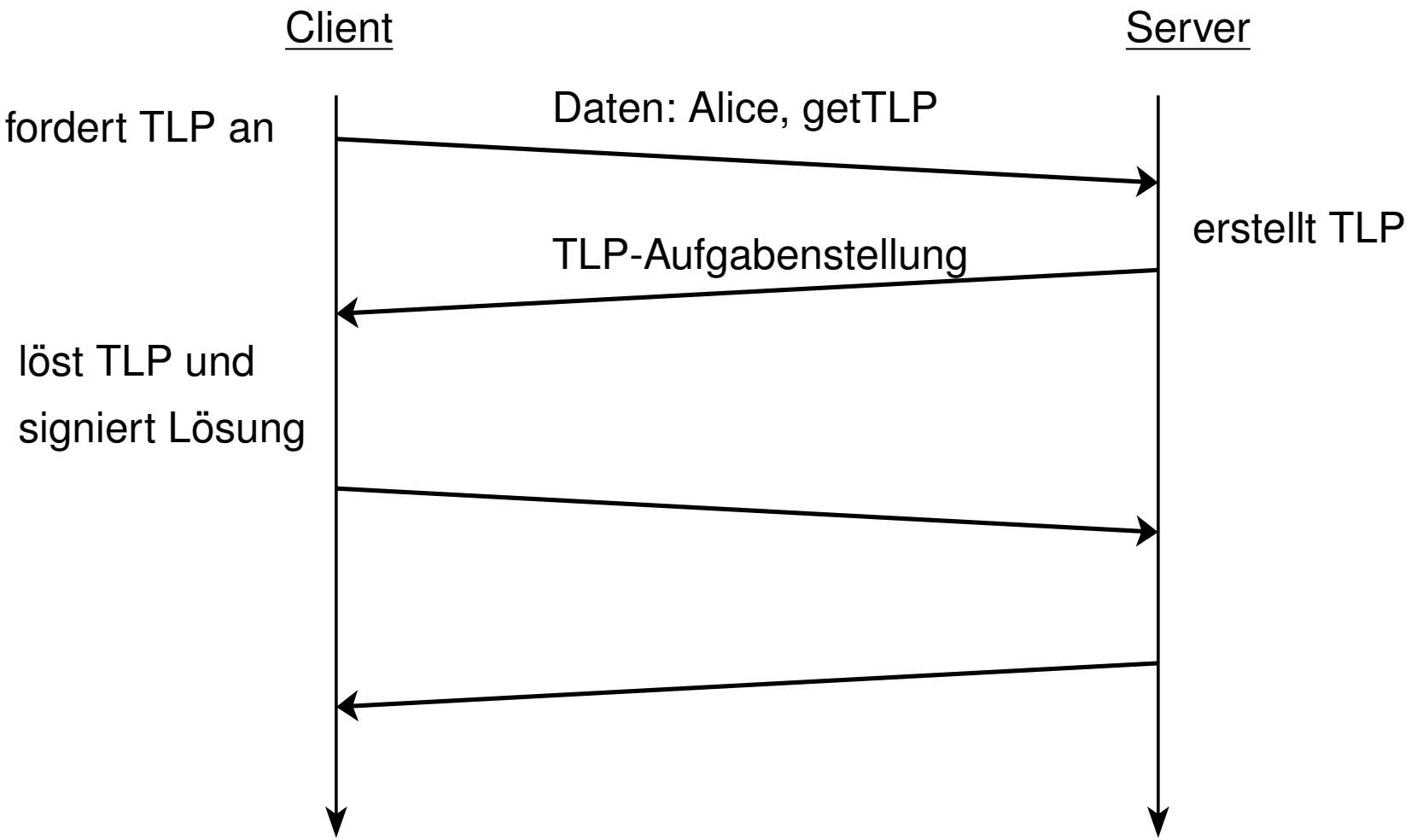
HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

PKWL 2.0 - Proof-of-Work-System



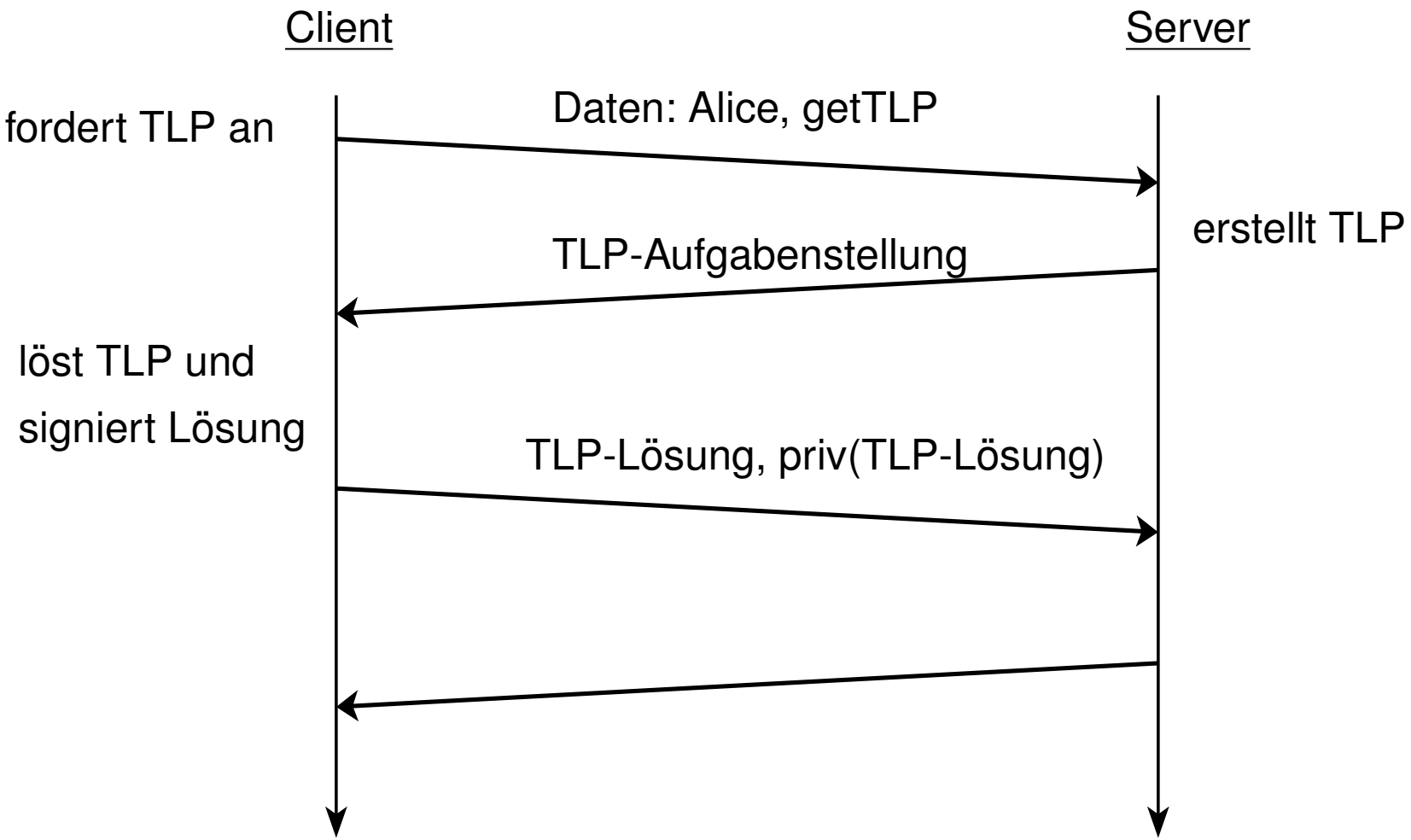
HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

PKWL 2.0 - Proof-of-Work-System



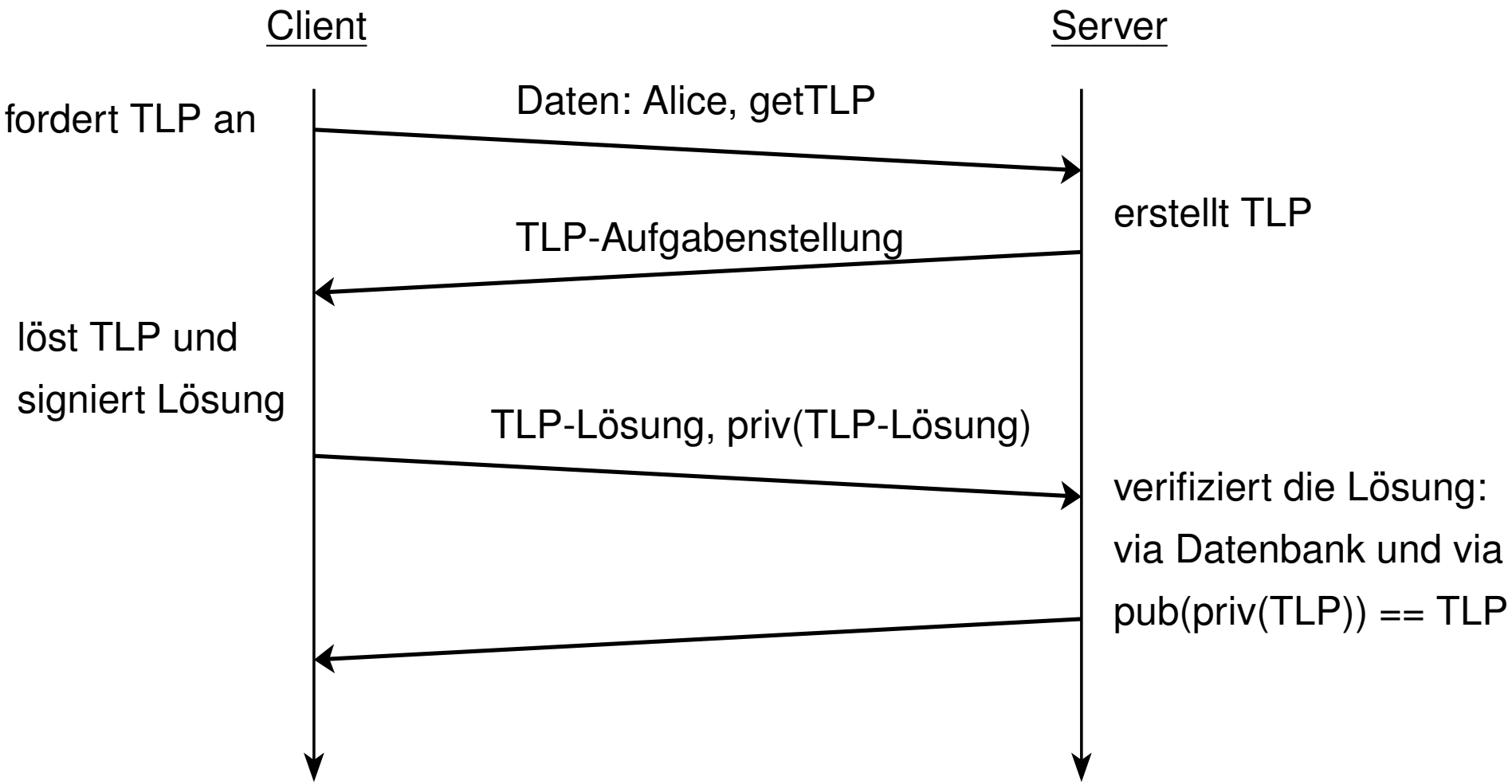
HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

PKWL 2.0 - Proof-of-Work-System



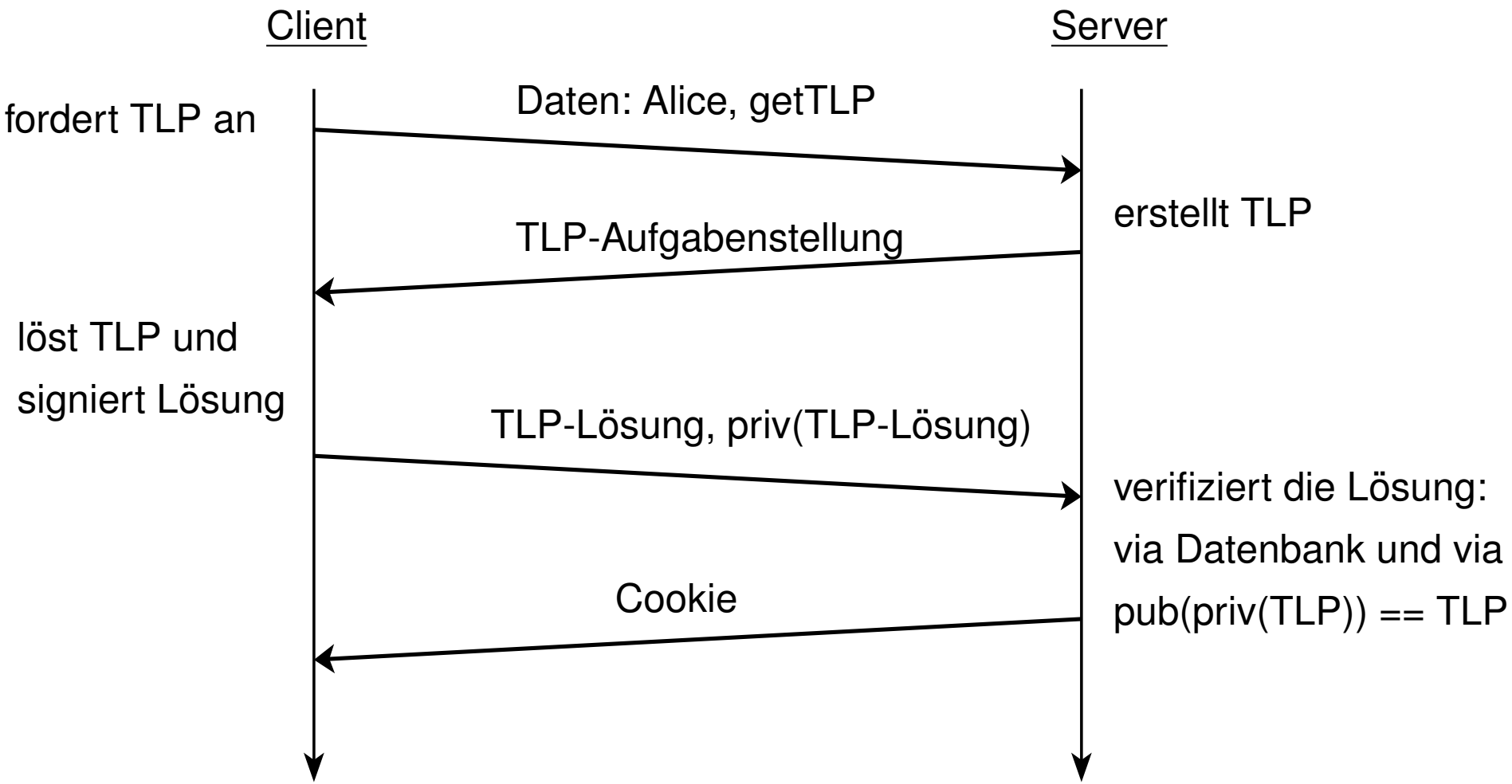
HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

PKWL 2.0 - Proof-of-Work-System



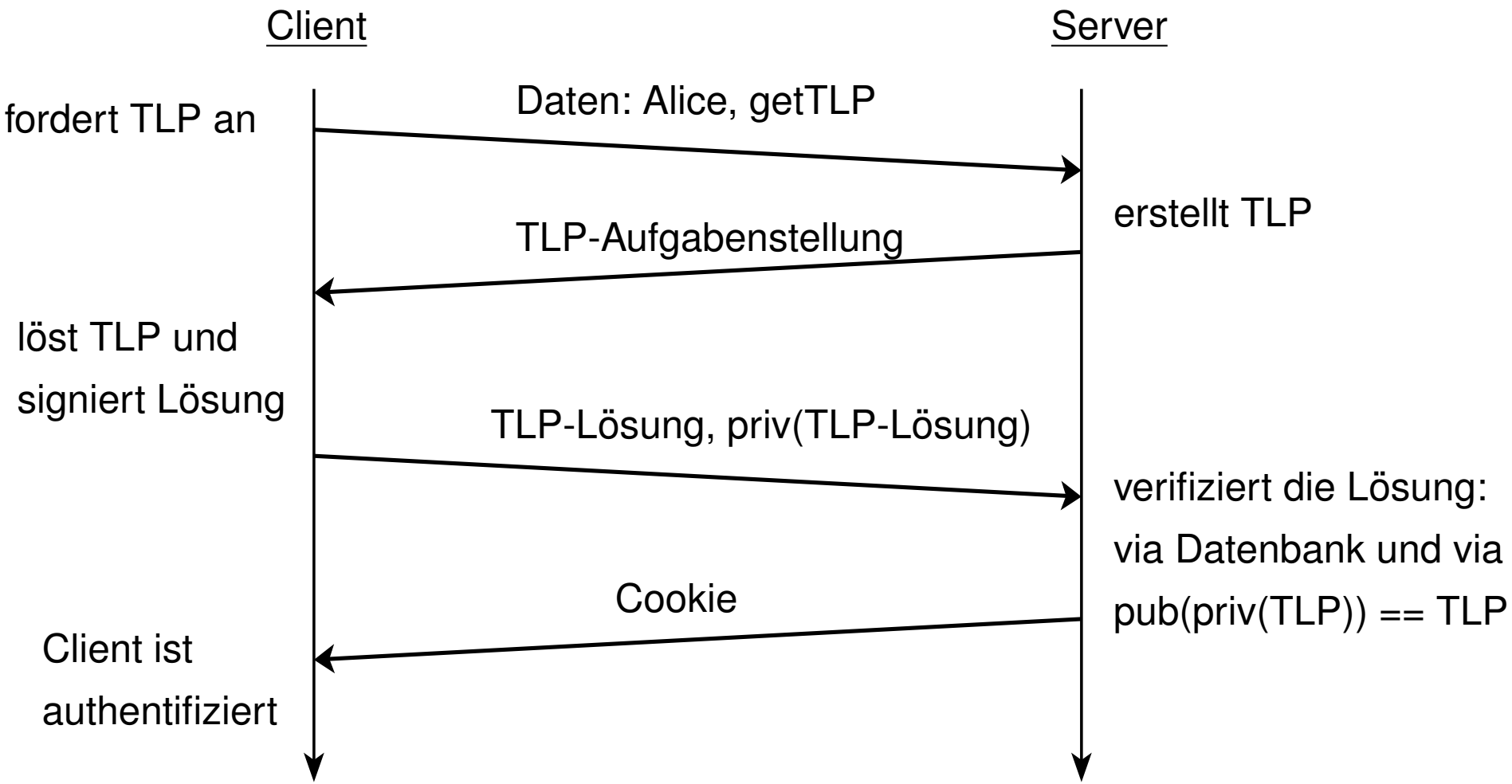
HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

PKWL 2.0 - Proof-of-Work-System



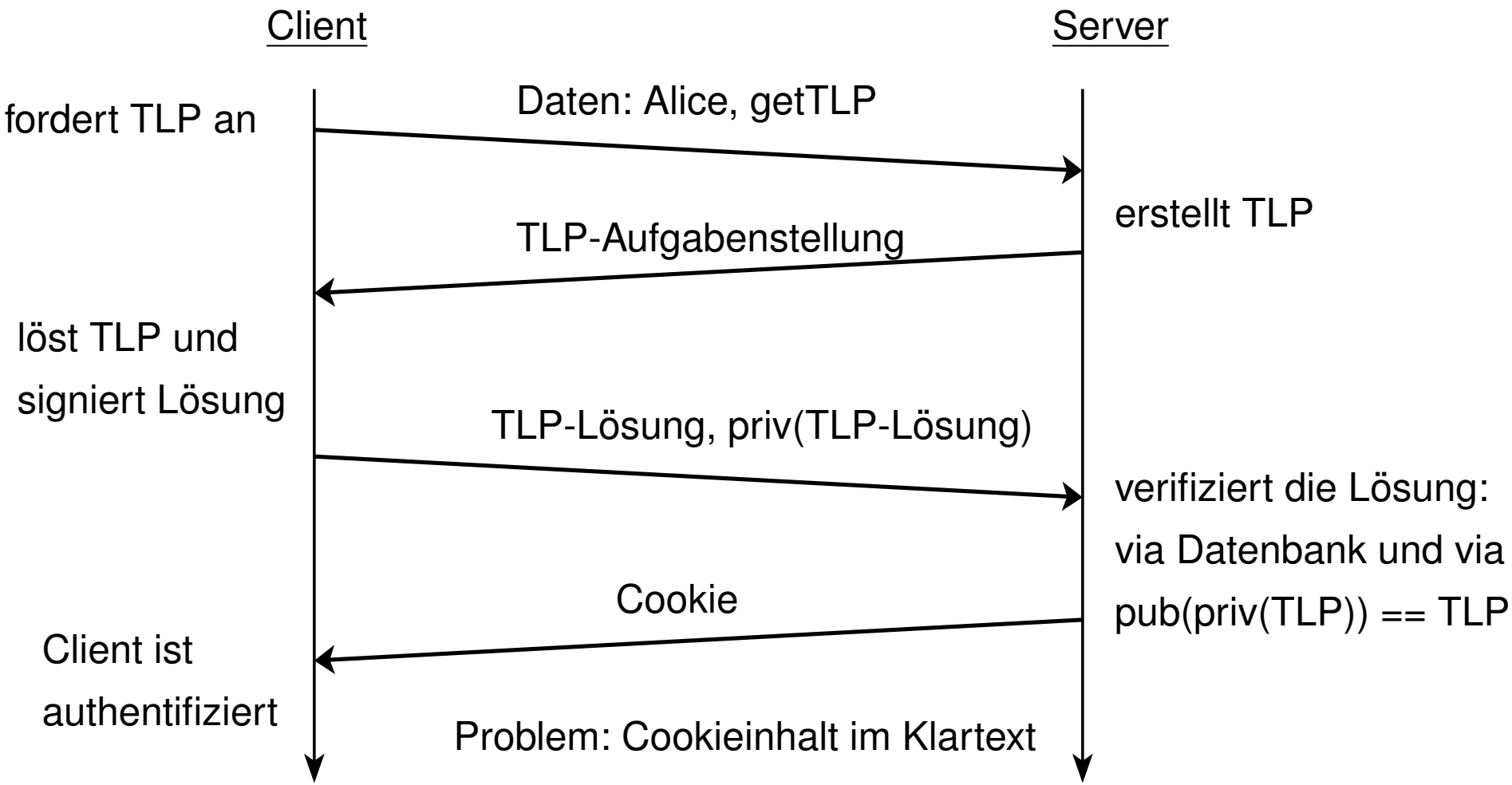
HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

PKWL 2.0 - Proof-of-Work-System



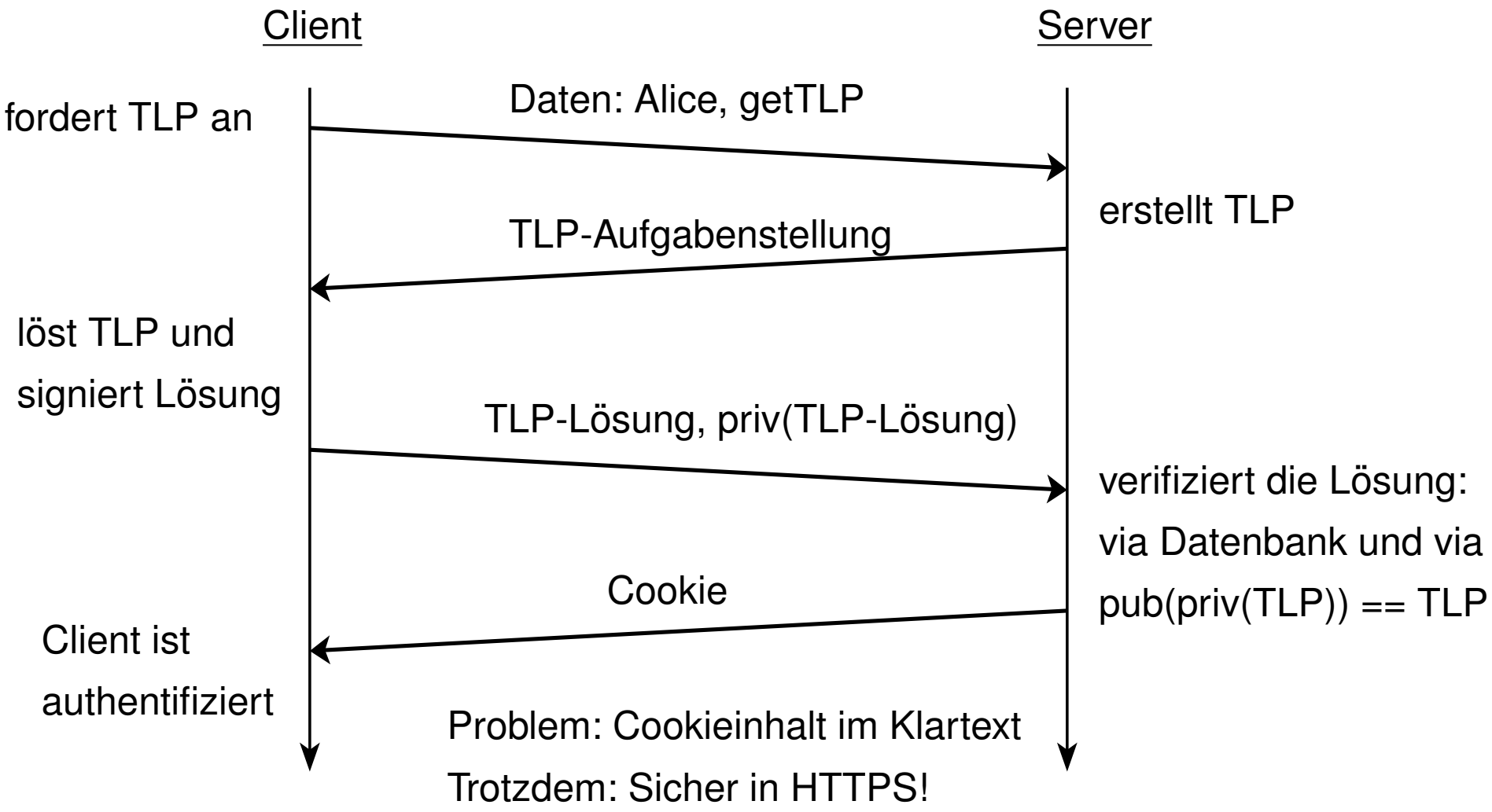
HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

PKWL 2.0 - Proof-of-Work-System



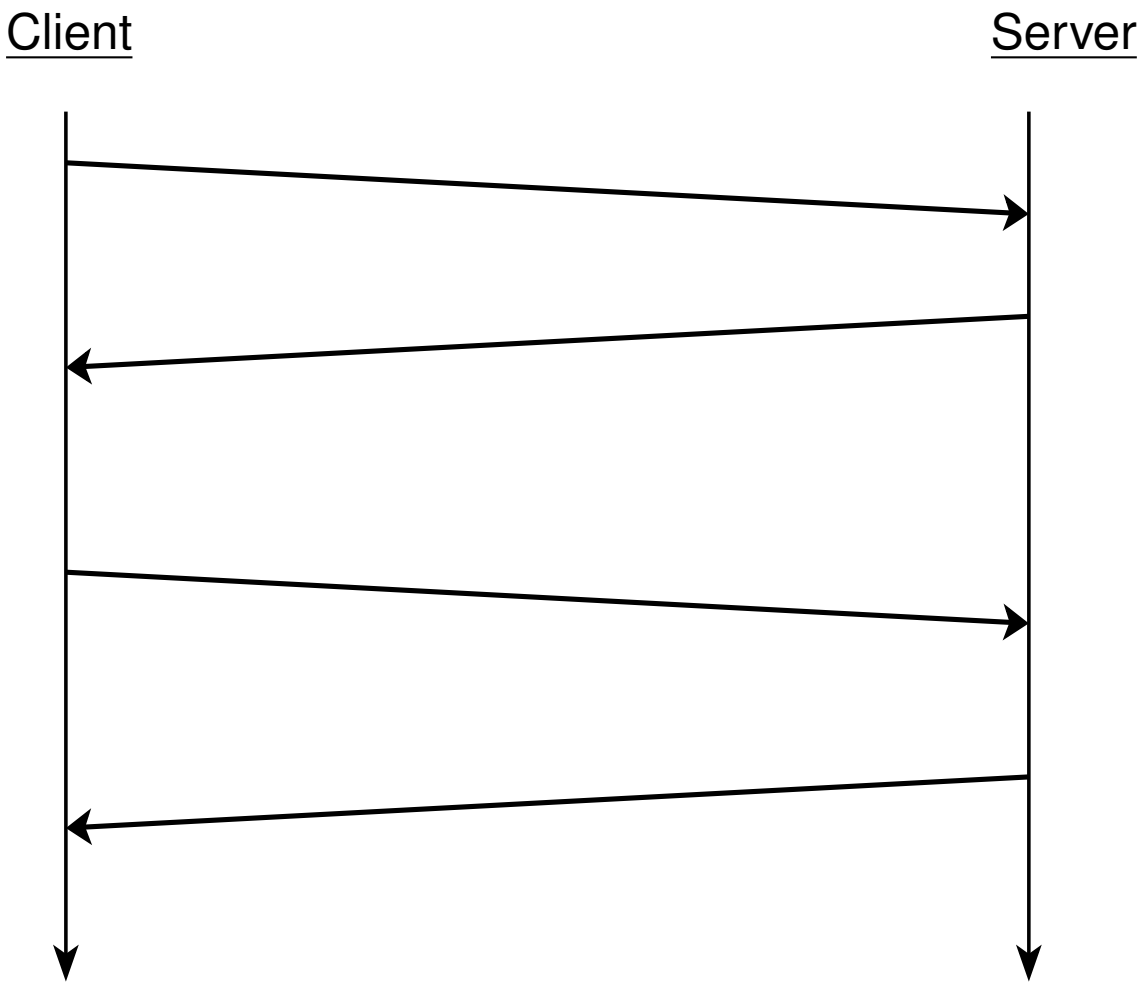
HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

PKWL 2.0 - Proof-of-Work-System



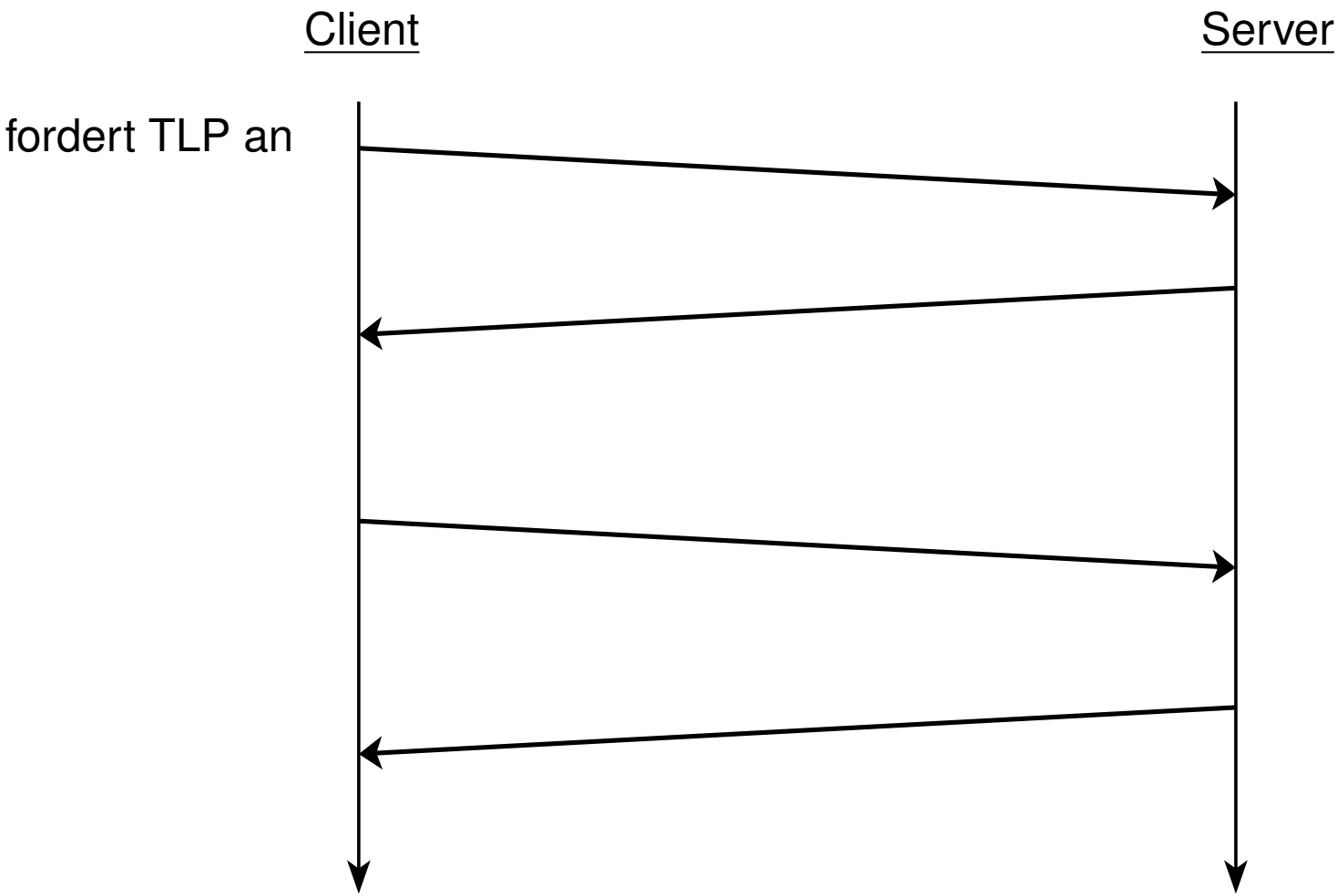
HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

PKWL 3.0 - Verschlüsselte Cookies



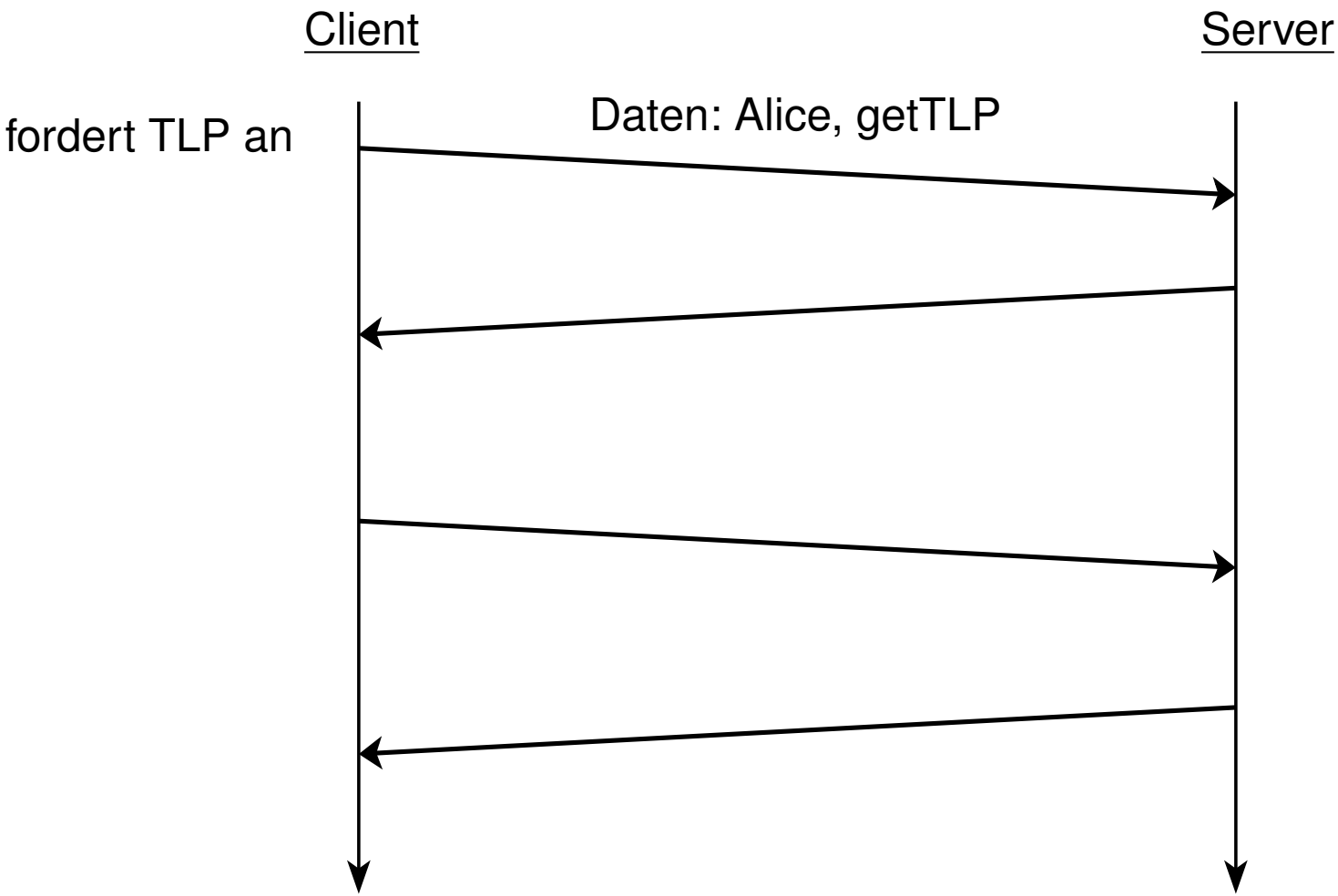
HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

PKWL 3.0 - Verschlüsselte Cookies



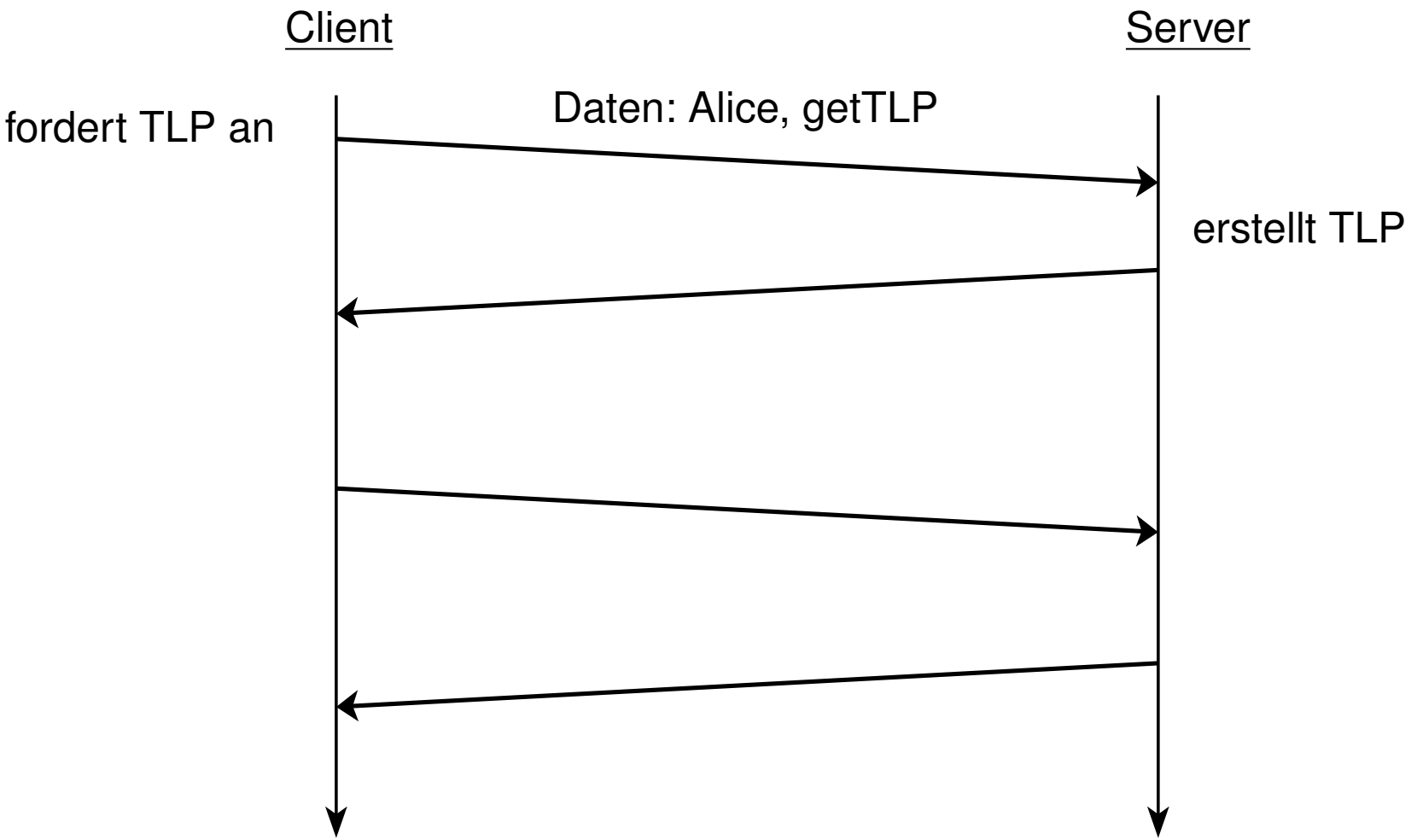
HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

PKWL 3.0 - Verschlüsselte Cookies



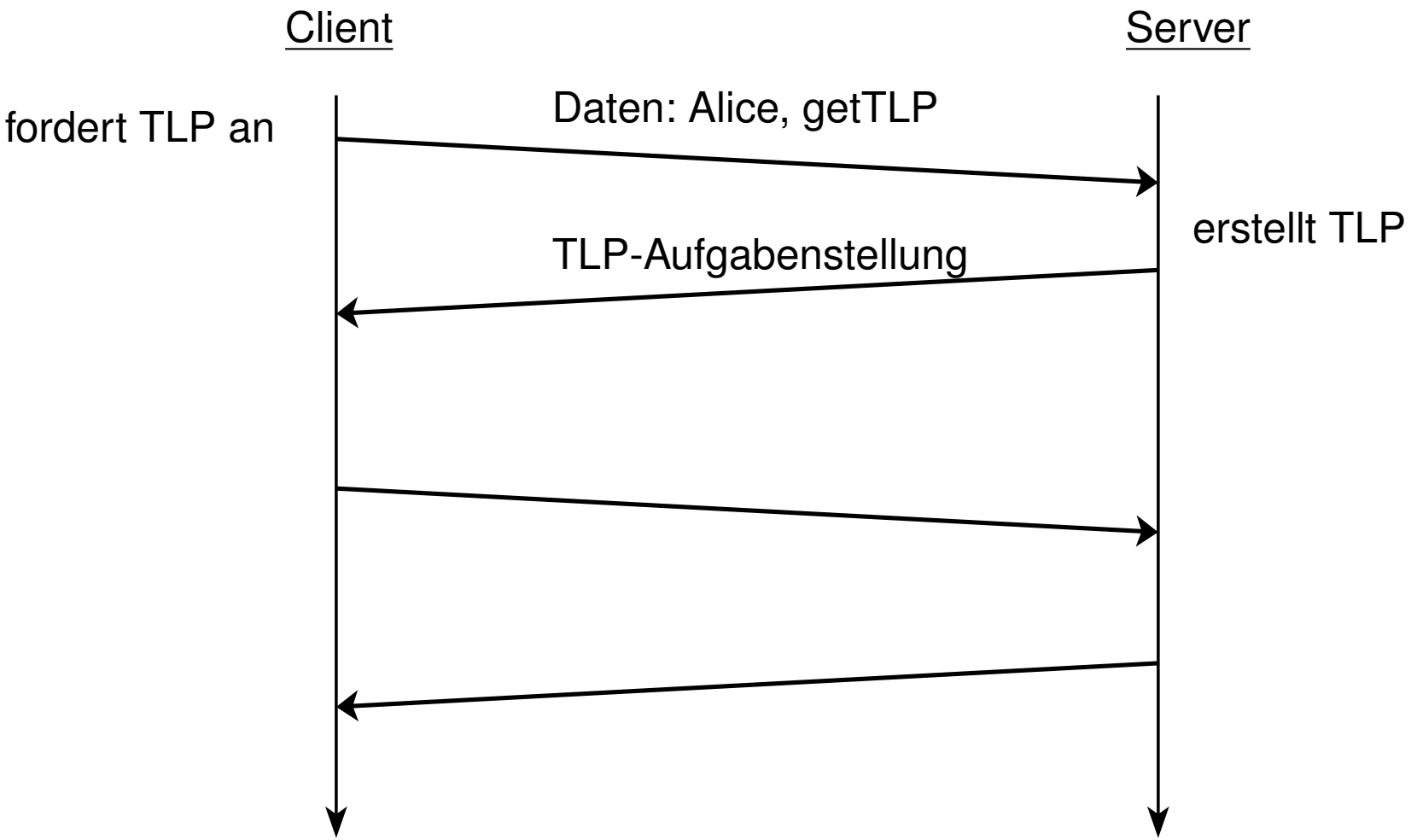
HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

PKWL 3.0 - Verschlüsselte Cookies



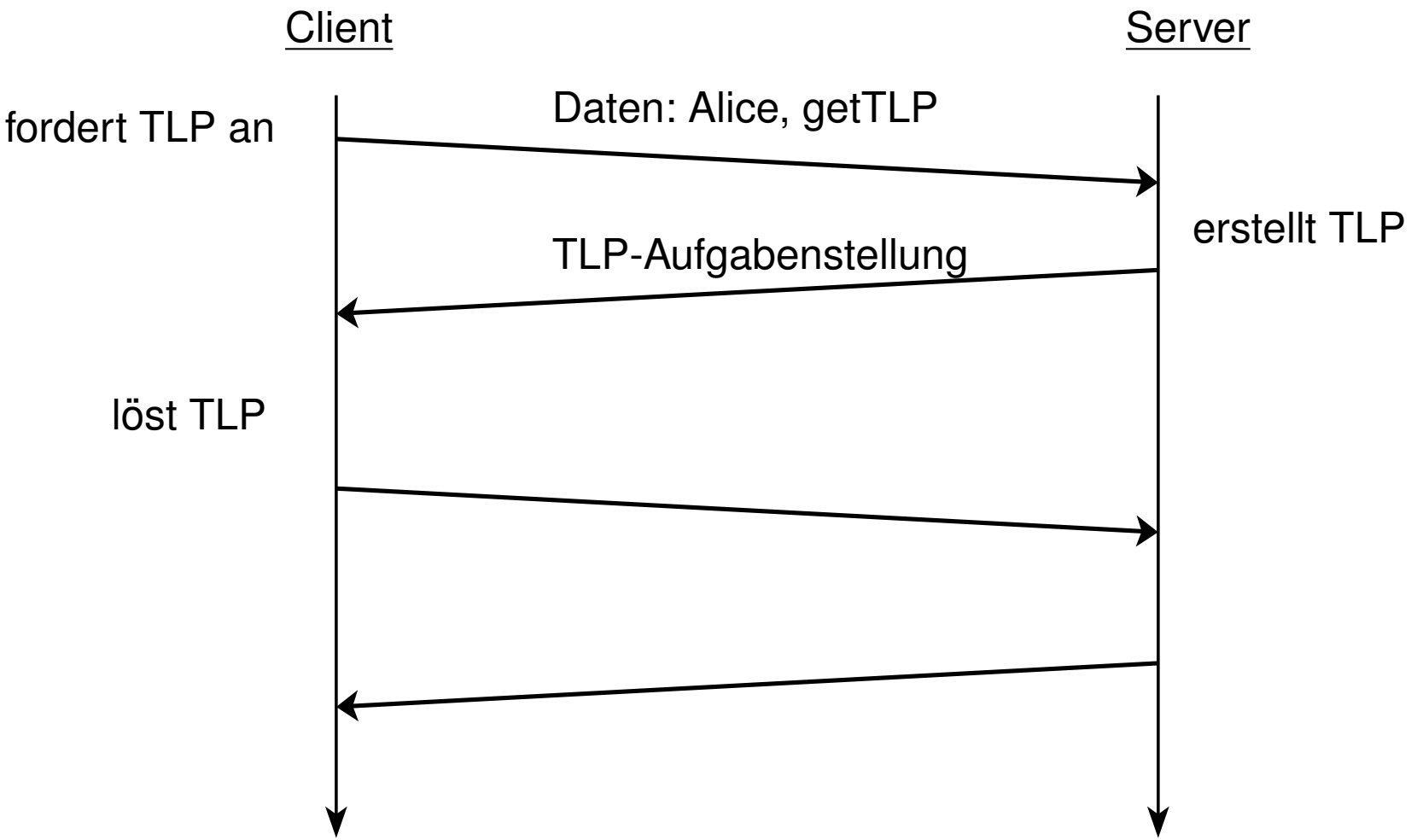
HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

PKWL 3.0 - Verschlüsselte Cookies



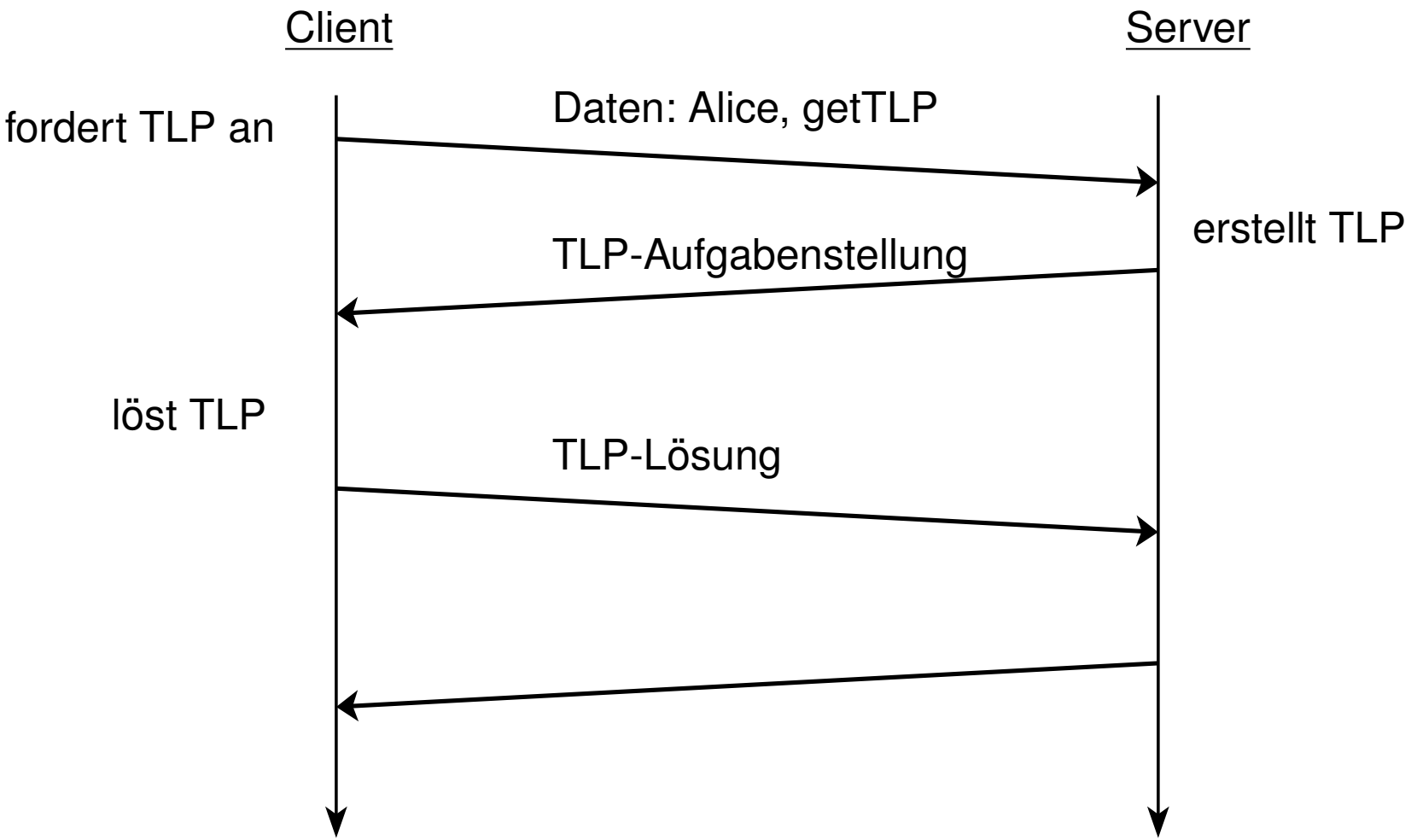
HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

PKWL 3.0 - Verschlüsselte Cookies



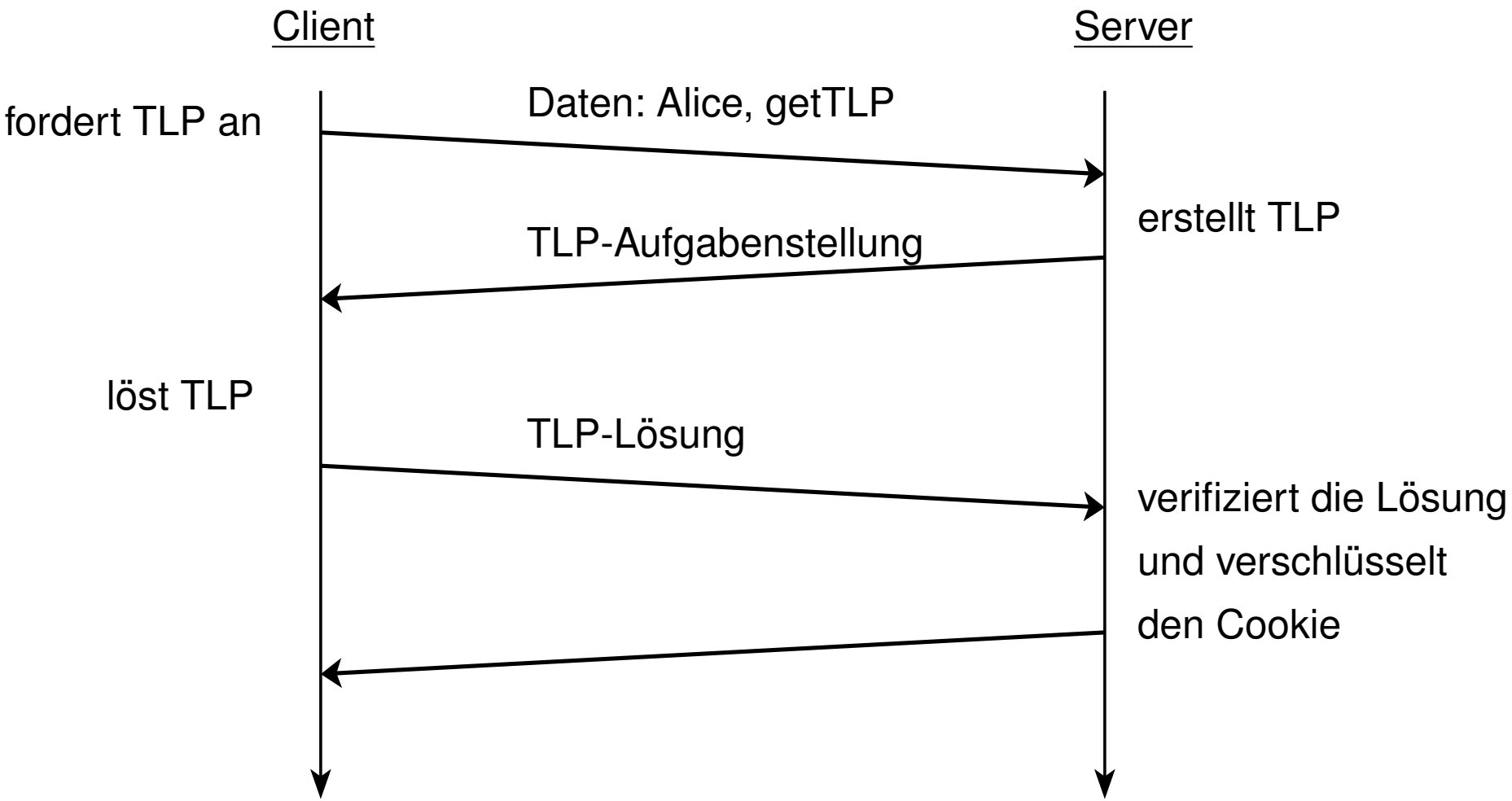
HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

PKWL 3.0 - Verschlüsselte Cookies



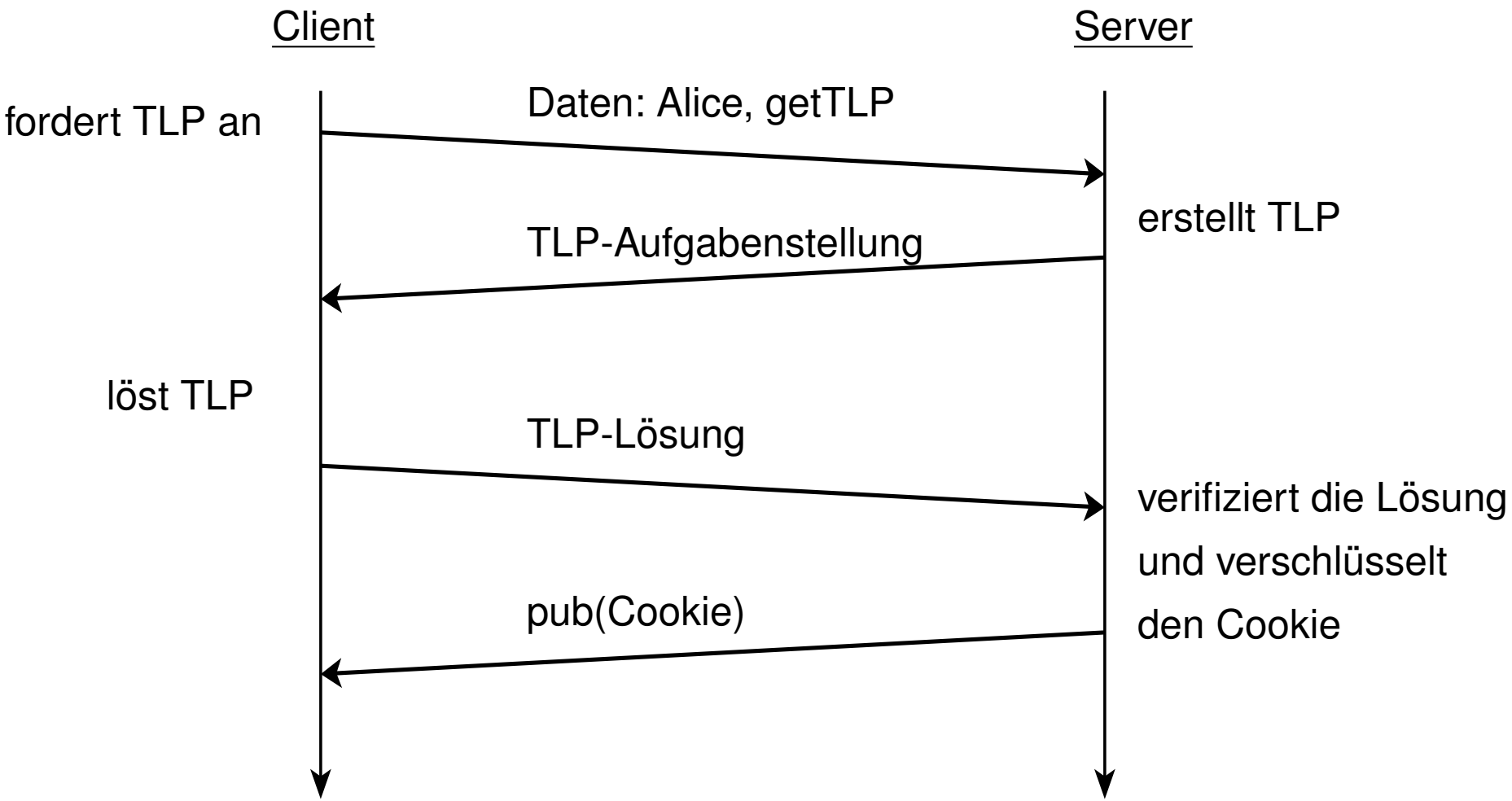
HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

PKWL 3.0 - Verschlüsselte Cookies



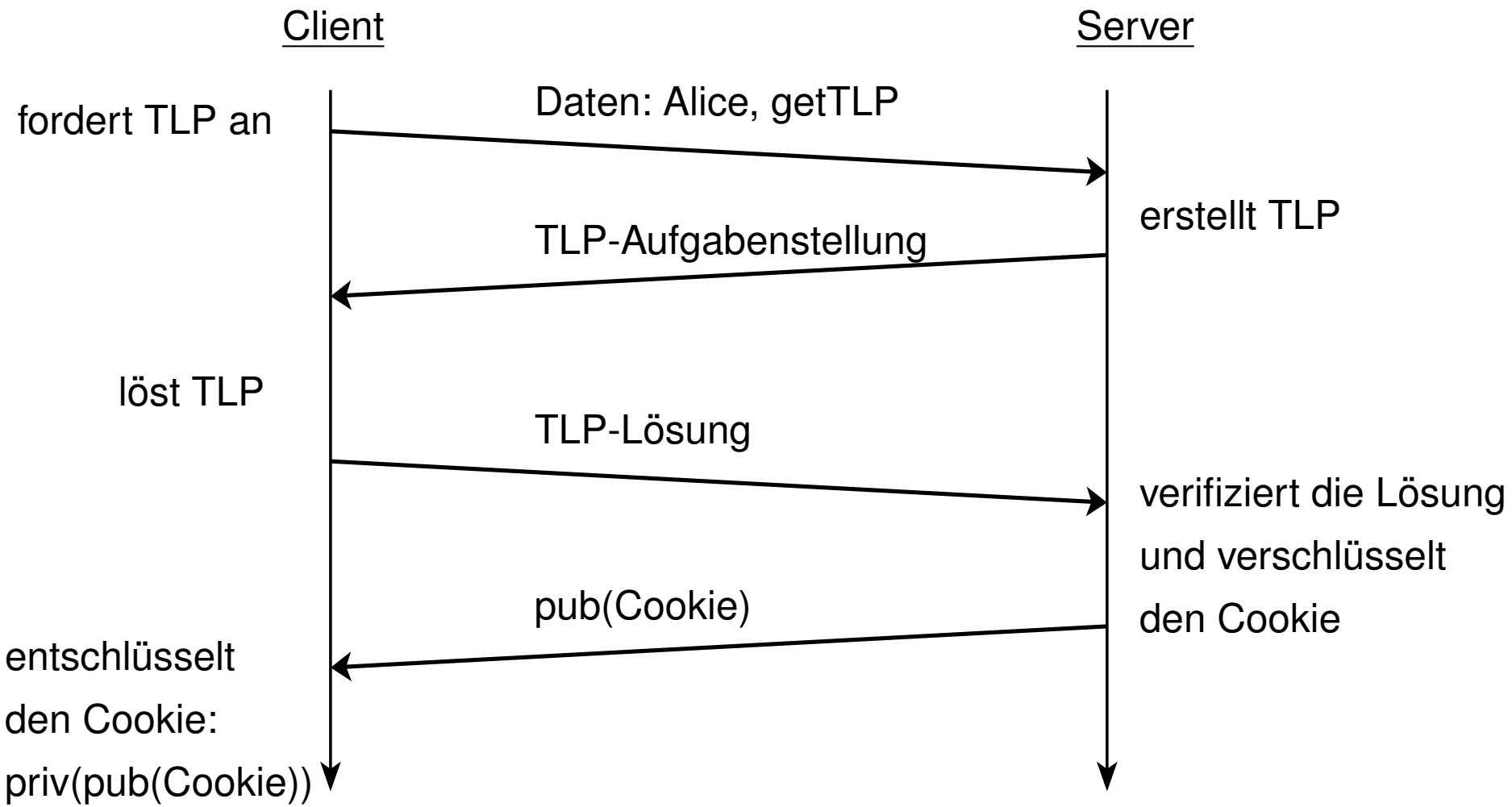
HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

PKWL 3.0 - Verschlüsselte Cookies



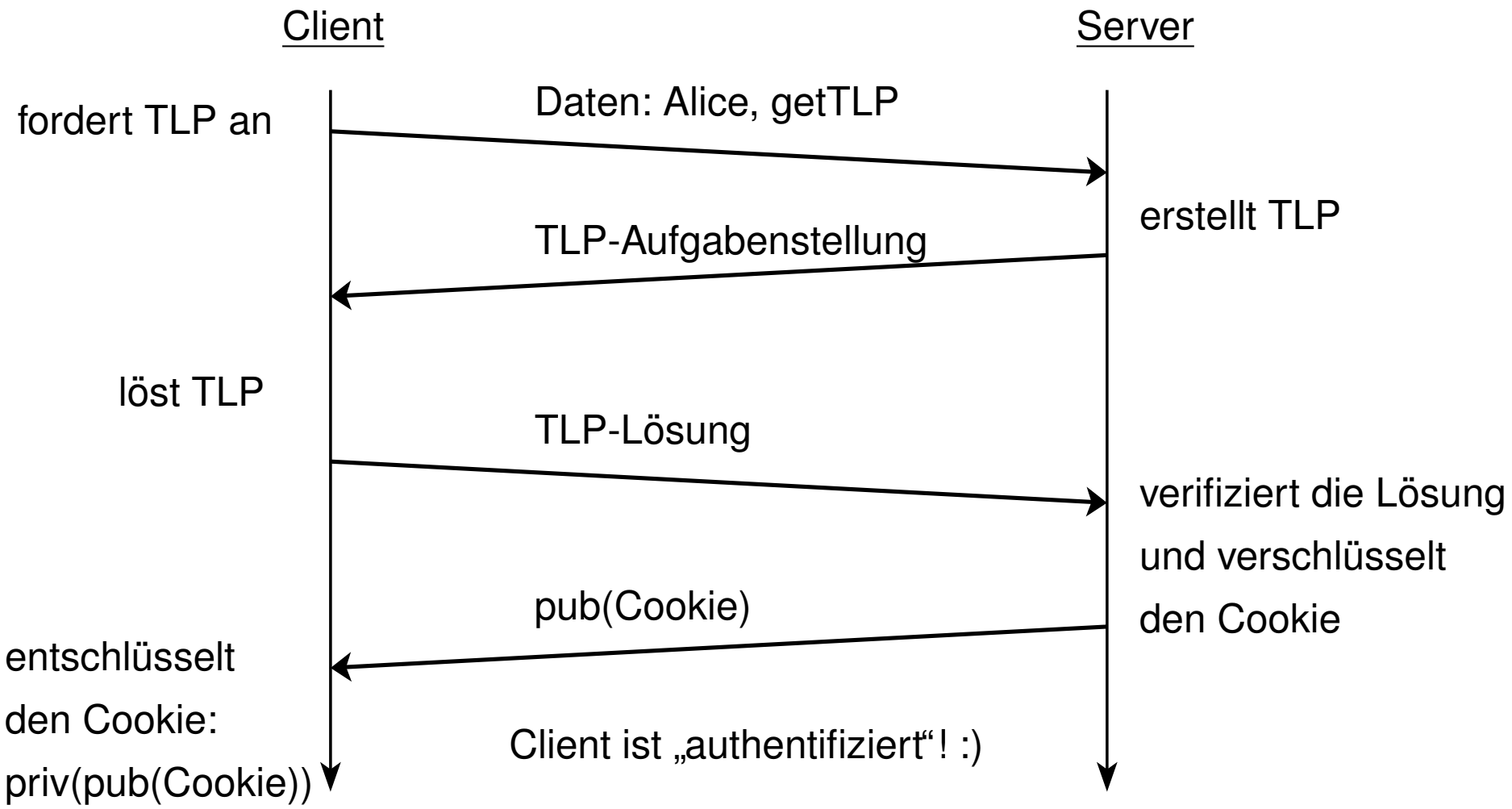
HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

PKWL 3.0 - Verschlüsselte Cookies



HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

PKWL 3.0 - Verschlüsselte Cookies

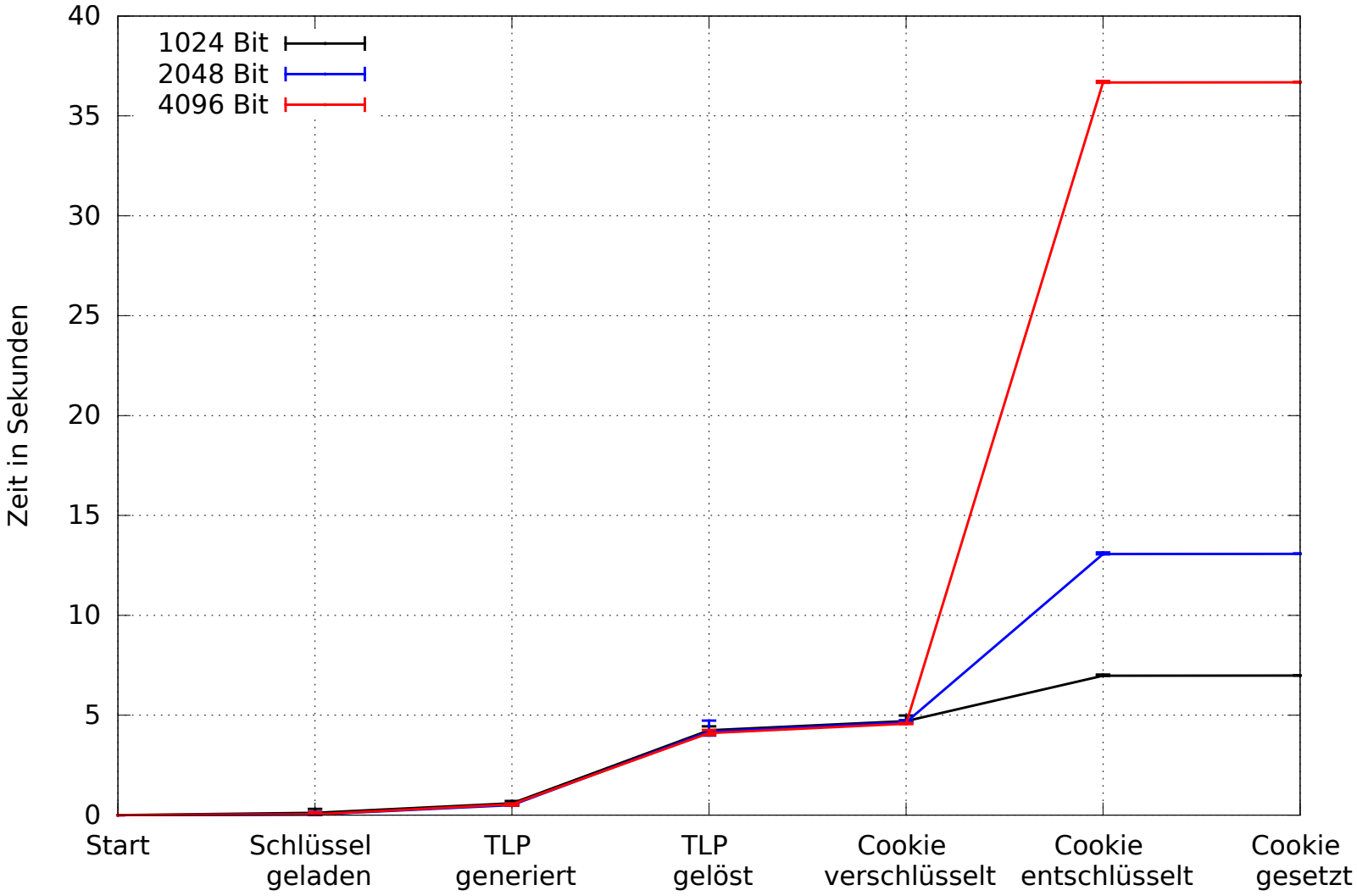


HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

Demo

HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

Evaluation



HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

Evaluation

HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

Evaluation

- Sicherheit per Design
  - Proof-of-Work-System
  - RSA-Kryptosystem

HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

Evaluation

- Sicherheit per Design
  - Proof-of-Work-System
  - RSA-Kryptosystem
- Performance
  - 2048 Bit-Schlüssellänge - ca. 13 Sekunden

HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

Evaluation

- Sicherheit per Design
  - Proof-of-Work-System
  - RSA-Kryptosystem
- Performance
  - 2048 Bit-Schlüssellänge - ca. 13 Sekunden
- Komfort
  - keine Konfiguration beim Server und Client nötig
  - vollständige Bedienung über die graphische Oberfläche
  - im Alltag: Zwei Mausklicks für die Authentifizierung

HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

Fazit

- Passwörter gehören der Vergangenheit an

HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

Fazit

- Passwörter gehören der Vergangenheit an
- PKWL bietet Sicherheit, Performance und Komfort

HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

Fazit

- Passwörter gehören der Vergangenheit an
- PKWL bietet Sicherheit, Performance und Komfort
- passwortlose Authentifizierung funktioniert!

HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

Fazit

- Passwörter gehören der Vergangenheit an
- PKWL bietet Sicherheit, Performance und Komfort
- passwortlose Authentifizierung funktioniert!

- Ausblick in die Zukunft

HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

Fazit

- Passwörter gehören der Vergangenheit an
- PKWL bietet Sicherheit, Performance und Komfort
- passwortlose Authentifizierung funktioniert!

- Ausblick in die Zukunft
  - dynamische Zeit-Anpassung des Proof-of-Work-Systems

HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

Fazit

- Passwörter gehören der Vergangenheit an
- PKWL bietet Sicherheit, Performance und Komfort
- passwortlose Authentifizierung funktioniert!

- Ausblick in die Zukunft
  - dynamische Zeit-Anpassung des Proof-of-Work-Systems
  - automatische Authentifizierung im Hintergrund

HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

Fazit

- Passwörter gehören der Vergangenheit an
- PKWL bietet Sicherheit, Performance und Komfort
- passwortlose Authentifizierung funktioniert!

- Ausblick in die Zukunft
  - dynamische Zeit-Anpassung des Proof-of-Work-Systems
  - automatische Authentifizierung im Hintergrund
  - W3C plant eine Web Cryptography API

HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

Fragen?

- Source-Code: `https://github.com/mirkoole/PKWL`