LEHRSTUHL 14
SOFTWARE ENGINEERING

Willkommen zur Vorlesung

Methodische Grundlagen des Software-Engineering

im Sommersemester 2011

Prof. Dr. Jan Jürjens

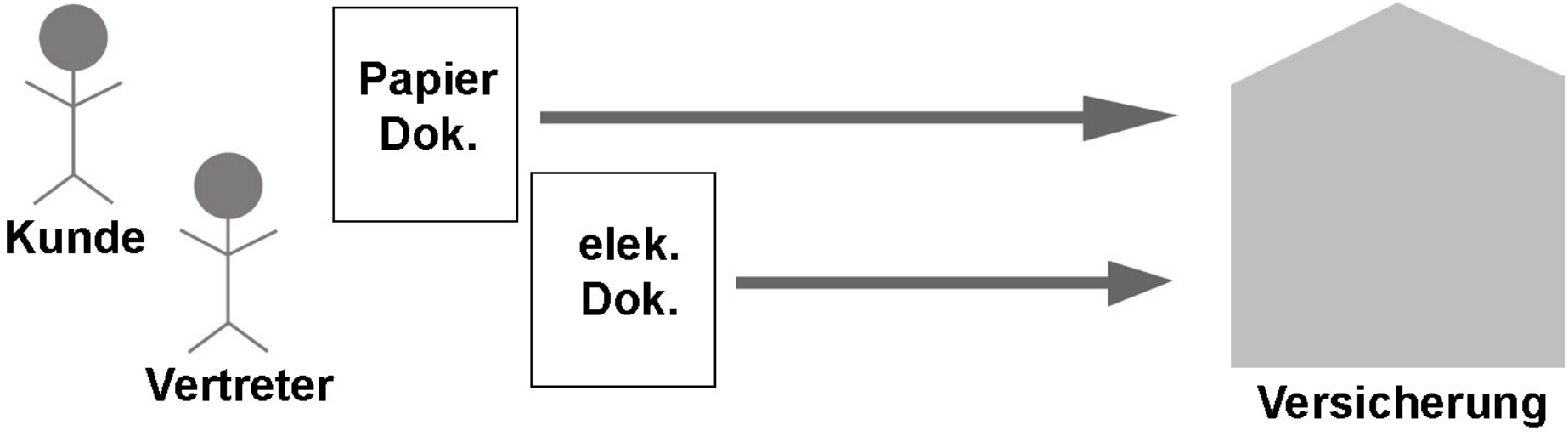
TU Dortmund, Fakultät Informatik, Lehrstuhl XIV

26. Software Architektur Anwendungsbeispiele

Sicherer Einsatz elektronischer Unterschriften im Versicherungswesen

Motivation

- 2 Versionen des Antrags wegen Unterschrift
- Zusammenführung notwendig
- Medienbruch verursacht Kosten



Lösungsmöglichkeit

- Kunde unterschreibt auf Pad
- Unterschrift ins digitale Dokument einbinden
- Archivierung und Weiterverarbeitung des elektronischen Antrags

Bedrohungen

- für den Kunden
  - seine Unterschrift wird missbraucht
  - sein Antrag wird verändert
- für die Gesellschaft
  - Kunde kann Antrag anzweifeln
  - Vertreter kann Antrag manipulieren

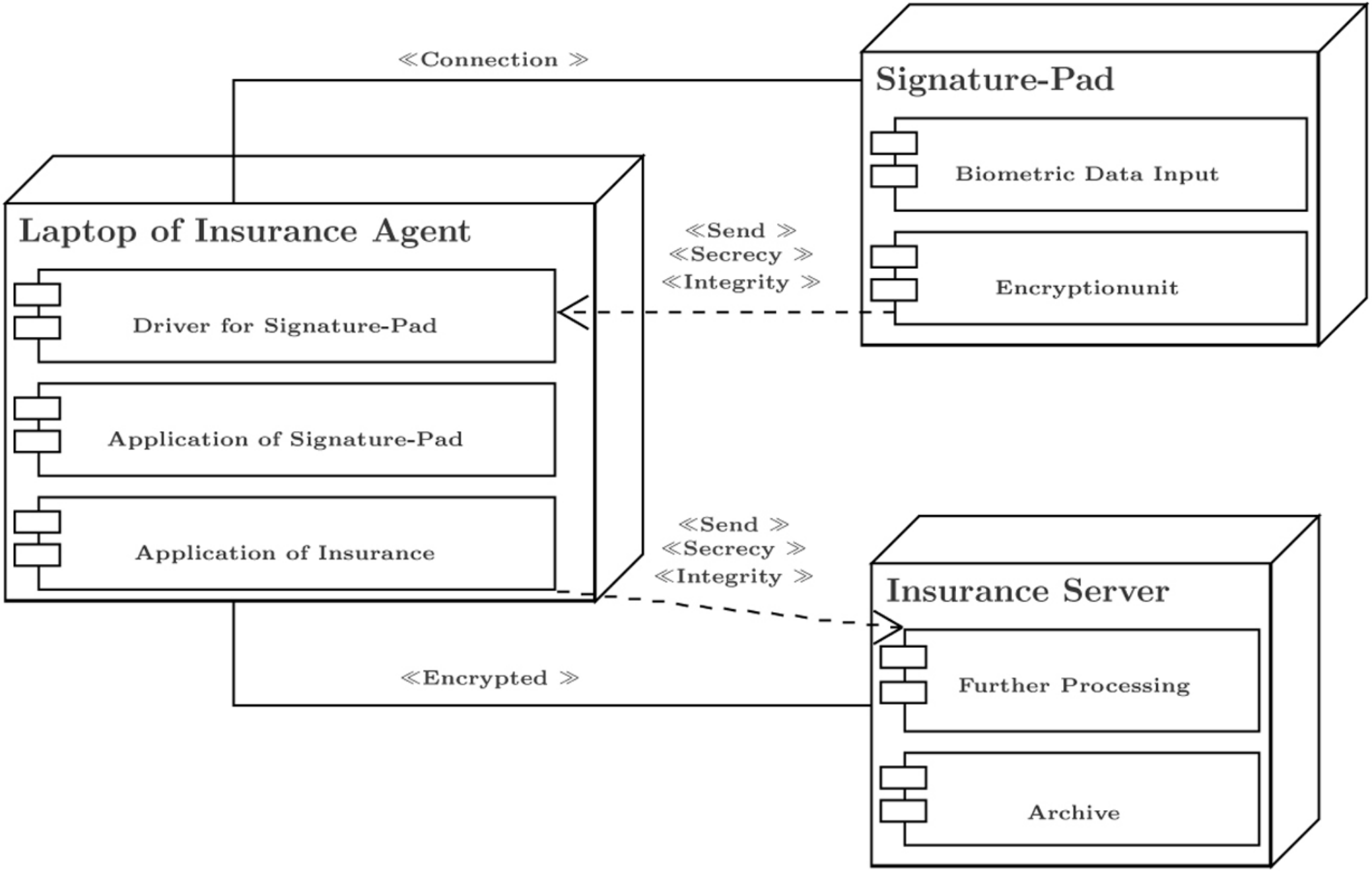
Sicherheitsziele

- Vertraulichkeit der biometrischen Daten
- Verbindlichkeit der Kunden-Unterschrift
- Integrität des Dokuments

Geräte zur Unterschriftenerfassung

- Statische Informationen
  - Bild
- Dynamische Informationen
  - Druck
  - Zeit

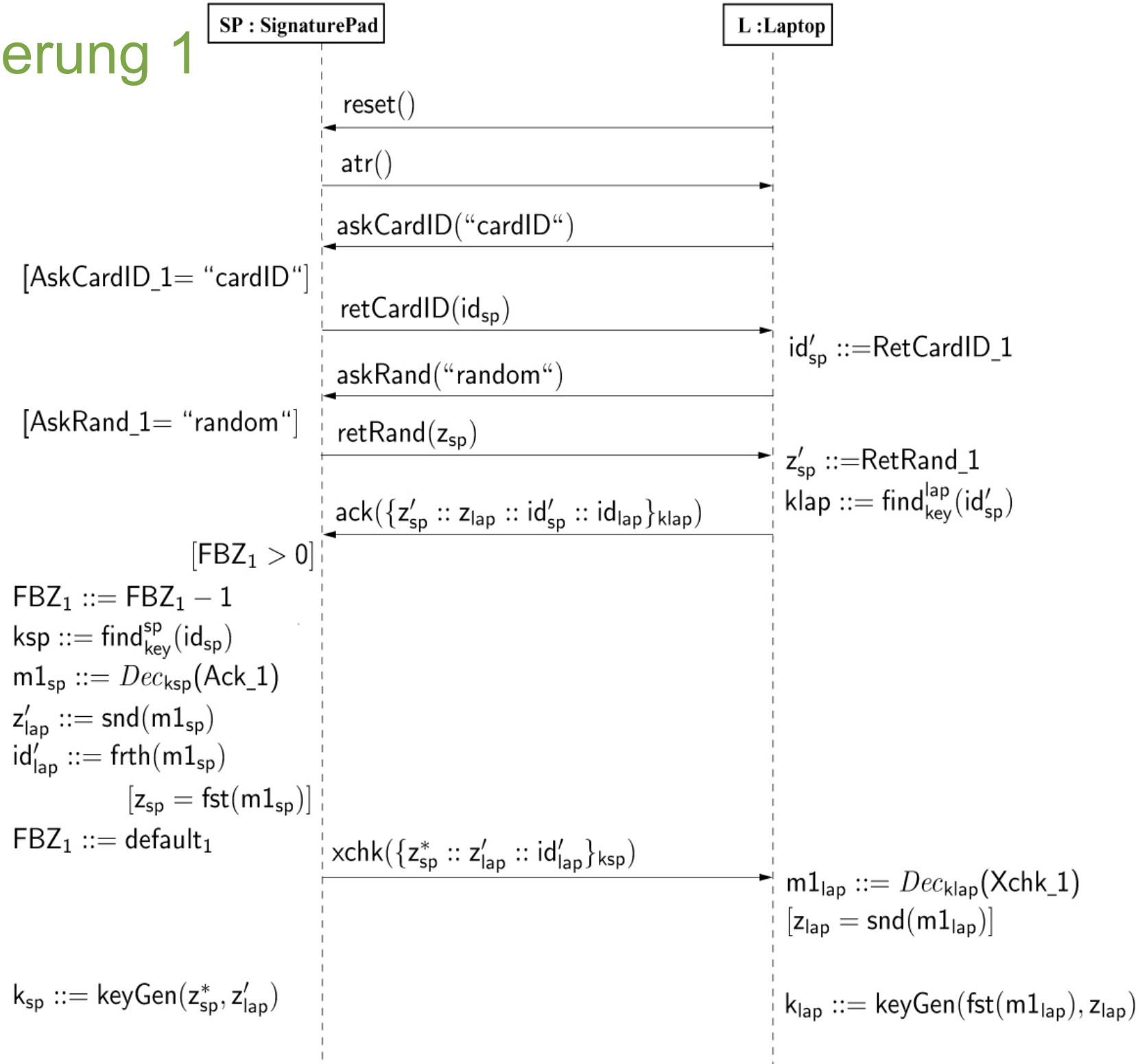
Kommunikationspartner



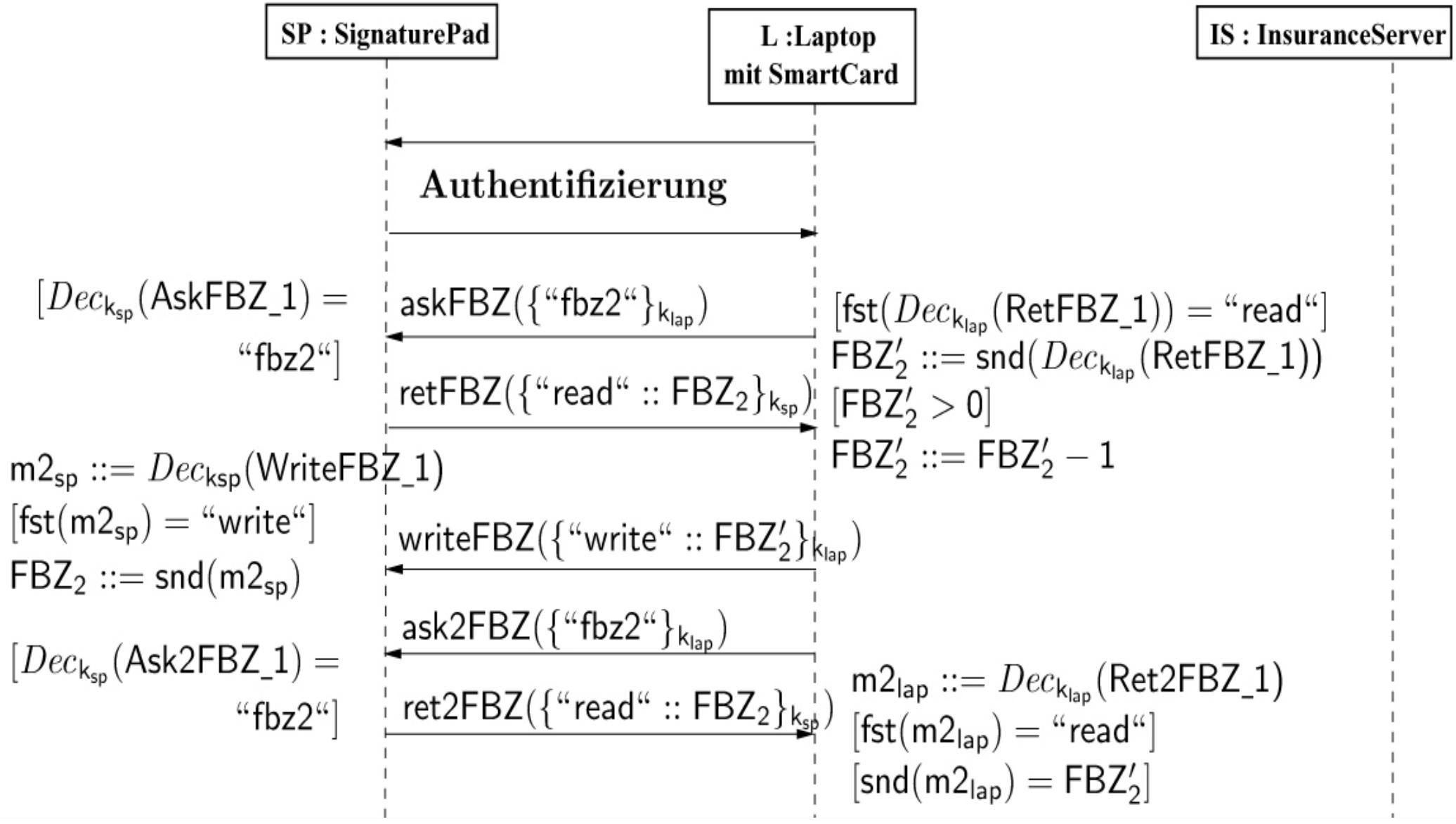
Protokoll mit SmartCard

- Orientierung am biom. Zugangsverfahren
- Authentifizierung zwischen Laptop und Pad
- SmartCard im Laptop des Vertreters
- Kontrolle der Signatur auf der SmartCard
- Anforderung der Referenzdaten zum Vergleich von der Gesellschaft

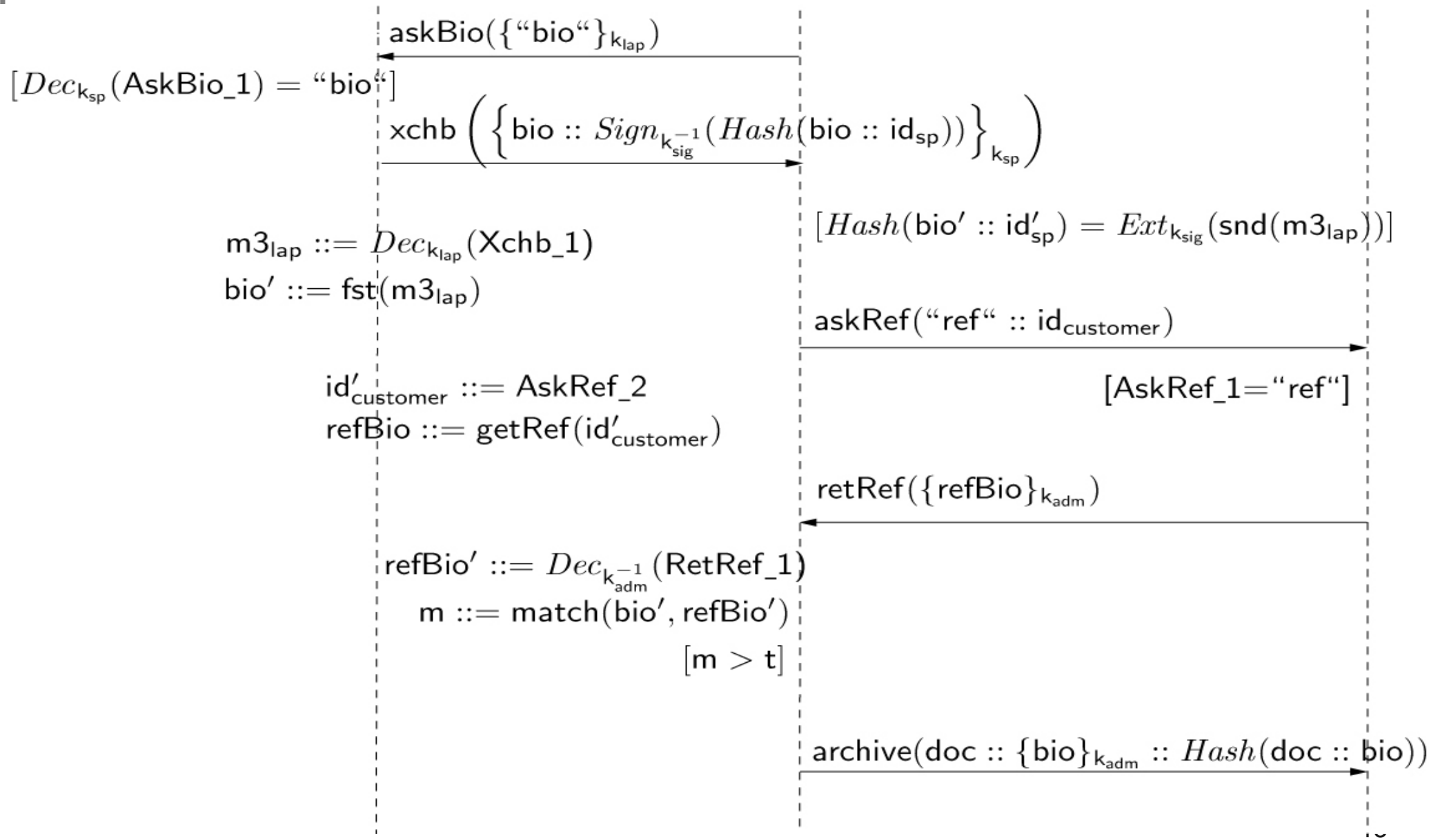
Authentifizierung 1



Authentifizierung 2



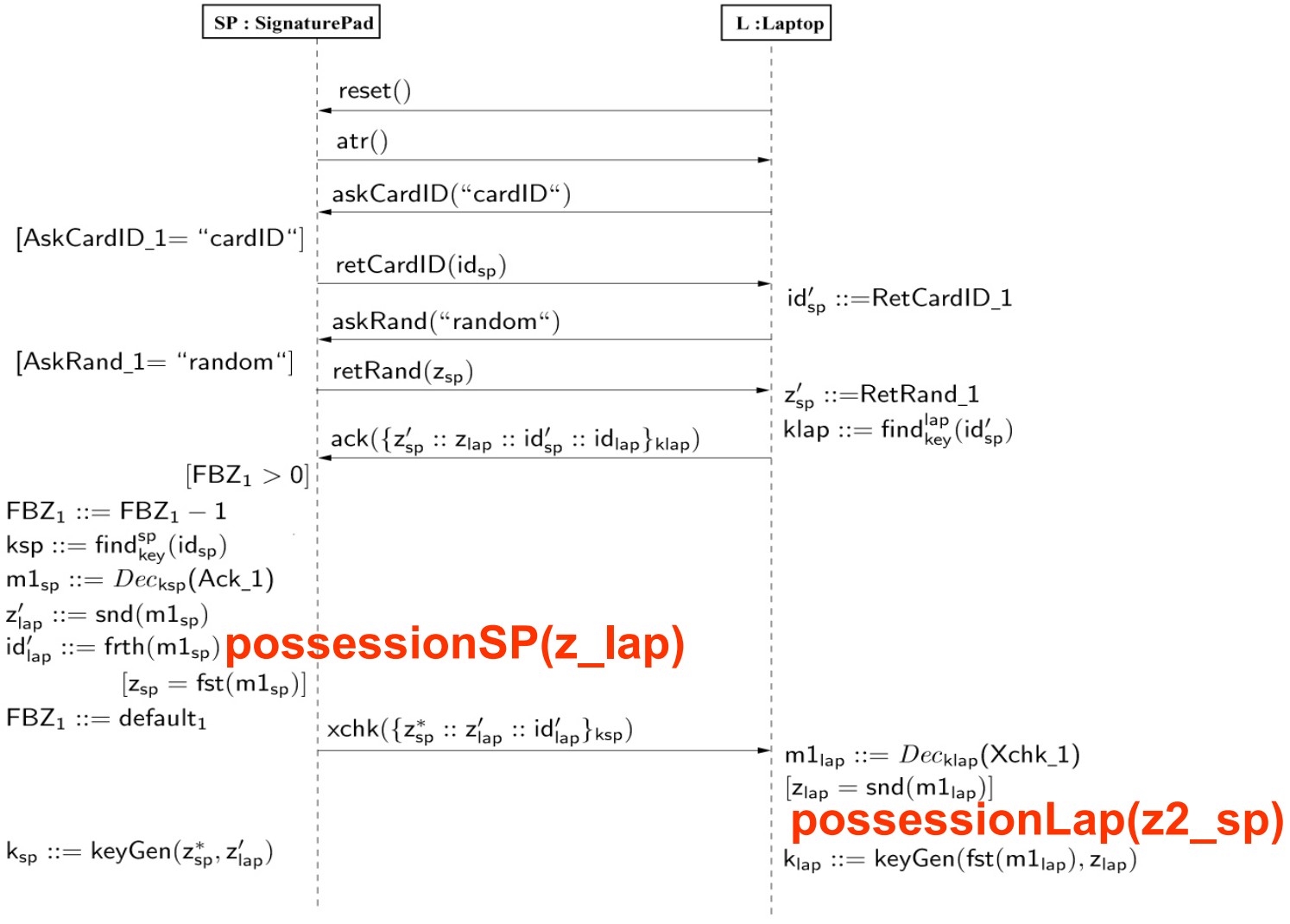
Authentifizierung 3



Authentizitätsprüfung

- Ist erfolgreich, falls Sitzungsschlüssel korrekt berechnet wird.
- Notwendig dazu
  - Zufallszahlen von Laptop und Pad
  - initialer sym. Schlüssel
- Überprüfung mit possession-Prädikat

Authentizitätsprüfung



Setzen der Prädikate

- Komponenten kennen eigene Zufallszahlen
- Authentifizierungsschlüssel beiden bekannt

```
Input_formula(attack, conjecture, (
   ( possessionLap(findKey)
   & possessionLap(z2_sp)
   & possessionLap(z_lap) )
)).
```

- Prüfung erfolgreich

Fazit

- Elekt. Unterschrift flexibel einsetzbar
  - für firmeninterne Dokumente
  - für Angebote von Zulieferern
- Protokoll notwendig, um Verbindlichkeit zu sichern