Christophe Andrey

Zertifikatbasierte Authentisierung für CORBA

Diplomarbeit

LABORATOIRE DE SYSTEMES D'EXPLOITATION

Ziel der Arbeit

- Authentisierung in JacORB mit Hilfe von SPKI-Zertifikaten implementieren.
- Die Zertifikate enthalten authentisierte Attribute eines Subjekts.

- Sekundäres Ziel: Zusammenfassung von existierenden Zertifikatinfrastrukturen.

LABORATOIRE DE SYSTEMES D'EXPLOITATION

Struktur

1. Theoretischer Hintergrund
   - JacORB
   - Authentisierung in CORBA: Credentials
   - SPKI
2. Protokoll:
   - Erlangung und Vermittlung von authentisierten Credentials
3. Implementierung: Schichtenarchitektur
4. Beispielanwendung:
   - Demonstration von *Access Control* für den Namensdienst
5. Beitrag der Arbeit

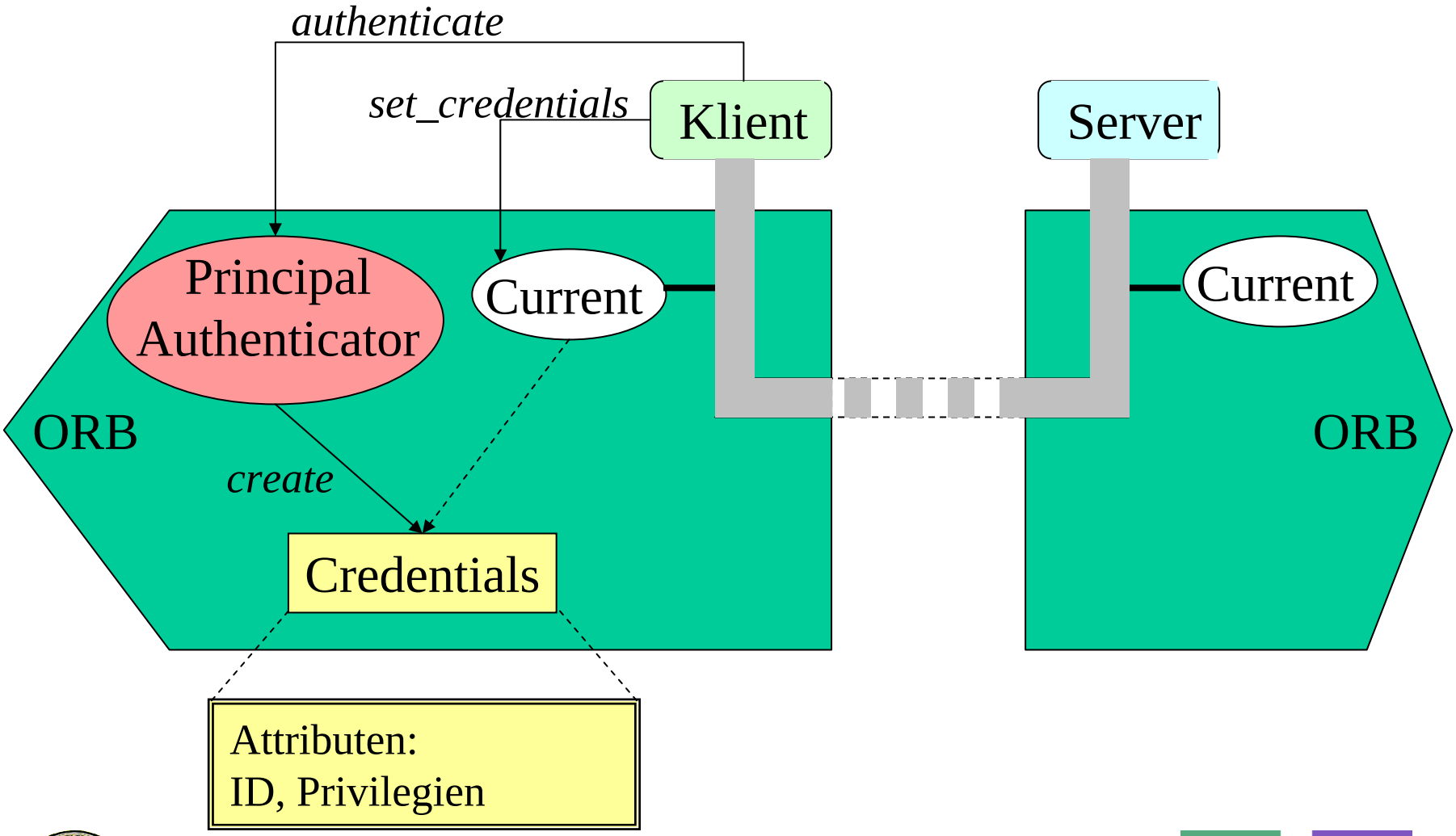
LABORATOIRE DE SYSTEMES D'EXPLOITATION

JacORB

- Freie und reine Java-Implementierung von CORBA
- Von Gerald Brose, FU-Berlin
- Verfügt über keinen Sicherheitsdienst (Version 0.9)

LABORATOIRE DE SYSTEMES D'EXPLOITATION

Authentisierung in CORBA



Credentials

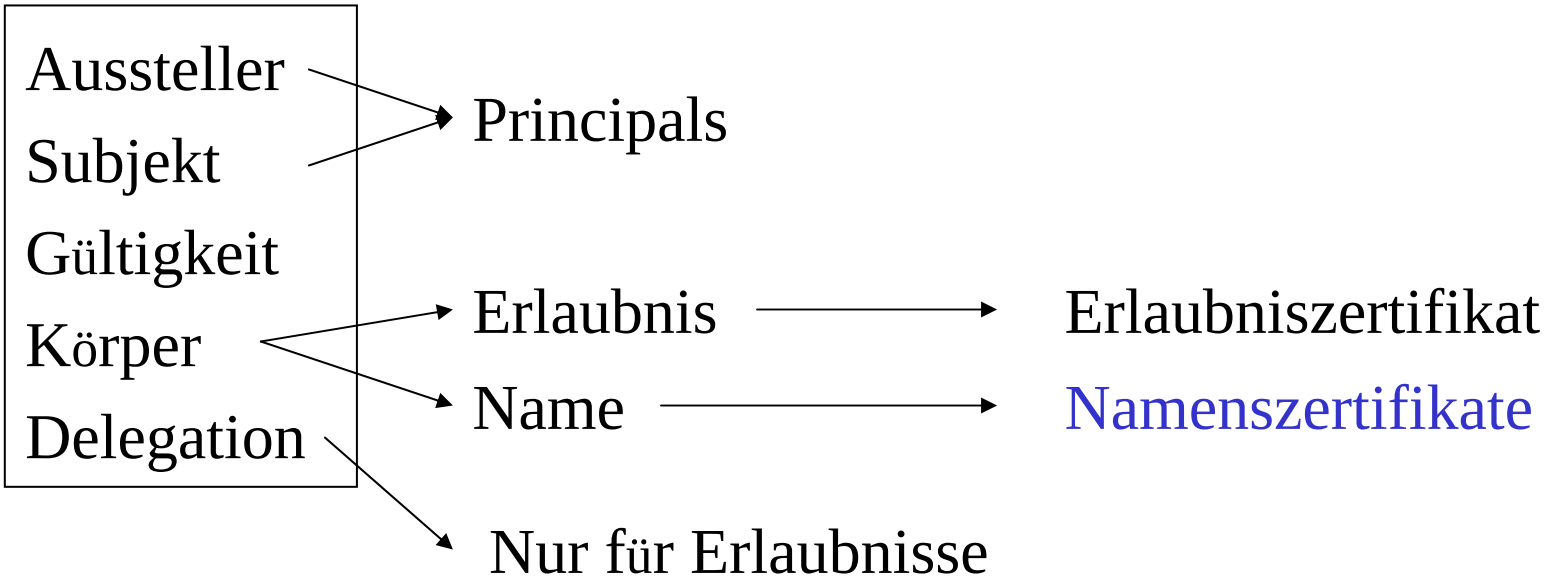
- Von CORBA nicht spezifiziert

- Bedeutung / Inhalt → ID-Attribut
- Format → SPKI-Zertifikat
- Herkunft → Protokoll

LABORATOIRE DE SYSTEMES D'EXPLOITATION

Struktur von SPKI

- Infrastruktur:
  - X.509 & PGP : 1 Principal = 1 Name
  - SPKI : 1 Principal = 1 öffentlicher Schlüssel
- Struktur eines Zertifikats:



LABORATOIRE DE SYSTEMES D'EXPLOITATION

Gründe für die Wahl von SPKI

- Neuheit
- Mehr Aussagekraft als X.509 oder PGP
- Flexibles Vertrauensmodell

LABORATOIRE DE SYSTEMES D'EXPLOITATION

SPKI-Grammatik

- Auf S-Expressions basiert
- 83 Produktionsregeln
- Unstabil

- Beispiel

- Vorteil: Interoperabilität
- Nachteile: beim Parsieren
  - Grosses *Lookahead* (bis 14)
  - Zwei Formen: fortgeschrittene und kanonisch

LABORATOIRE DE SYSTEMES D'EXPLOITATION

Beispiel von S-Expression

```
(sequence
    (cert
       (issuer
          (name
             (public-key rsa-pkcs1-md5
                    (n  ALH467KORQkeigyGhMRAwYfHxWyfLmO++tC3WJaasUp7becE0H7aWXay9jlunB8M
                        JixayaAxZKXmZ/pU17UuwMpLlxAeY3BAq2Mdjhcdwgqt25+CwGYOH0xyL8dGTePn
                        14OH4+cj5/rDNA/y2zWF6T6isXPHneEi1U23EU1WgeR7 )
                    (e AQAB ))
             AccessId/1 ))
       (subject
          (public-key rsa-pkcs1-md5
                    (n AI8RDzo1NkvlhvmGcQtUC6VPgVXFaYdap1pDZtfnHqE4avTPtRiw1QXqDrlpRQsp
                       M+h3xfZ7yFAxlK5MOFcRGlcdykhqbr7lshyyHcme3+9reJYhz7taik9OUDLjzNeg
                       WCkEPnhk2GrgT5h1JUz25yh97c7fyjiWraF8W2hDy0Vd )
                    (e AQAB )))
       (not-before 1999-03-08_11:52:31 )
       (not-after 1999-03-08_12:22:31 ))

    (signature
          (hash md5 Dt3V2QCqn0WT7/mfN0hAhA== )
          (public-key rsa-pkcs1-md5
              (n ALH467KORQkeigyGhMRAwYfHxWyfLmO++tC3WJaasUp7becE0H7aWXay9jlunB8M
                 JixayaAxZKXmZ/pU17UuwMpLlxAeY3BAq2Mdjhcdwgqt25+CwGYOH0xyL8dGTePn
                 14OH4+cj5/rDNA/y2zWF6T6isXPHneEi1U23EU1WgeR7 )
              (e AQAB ))
          XtIoC+RMtouXCv69Kq/tOcUTUqMDq+cf5wd1urkBQoZuvhwSVcHE6gv9wqY8FnCn
          o0Cyu+ZSY1PLVwUMQjvdZEwHieDRDWTeiyDinVUGwUKo0mlP9d9rJjUCnKh37P8J
          92oslUVy8kxjXtNZsIap3nOc9RTvKoh69gDcrW7QcuQ= )
)
```

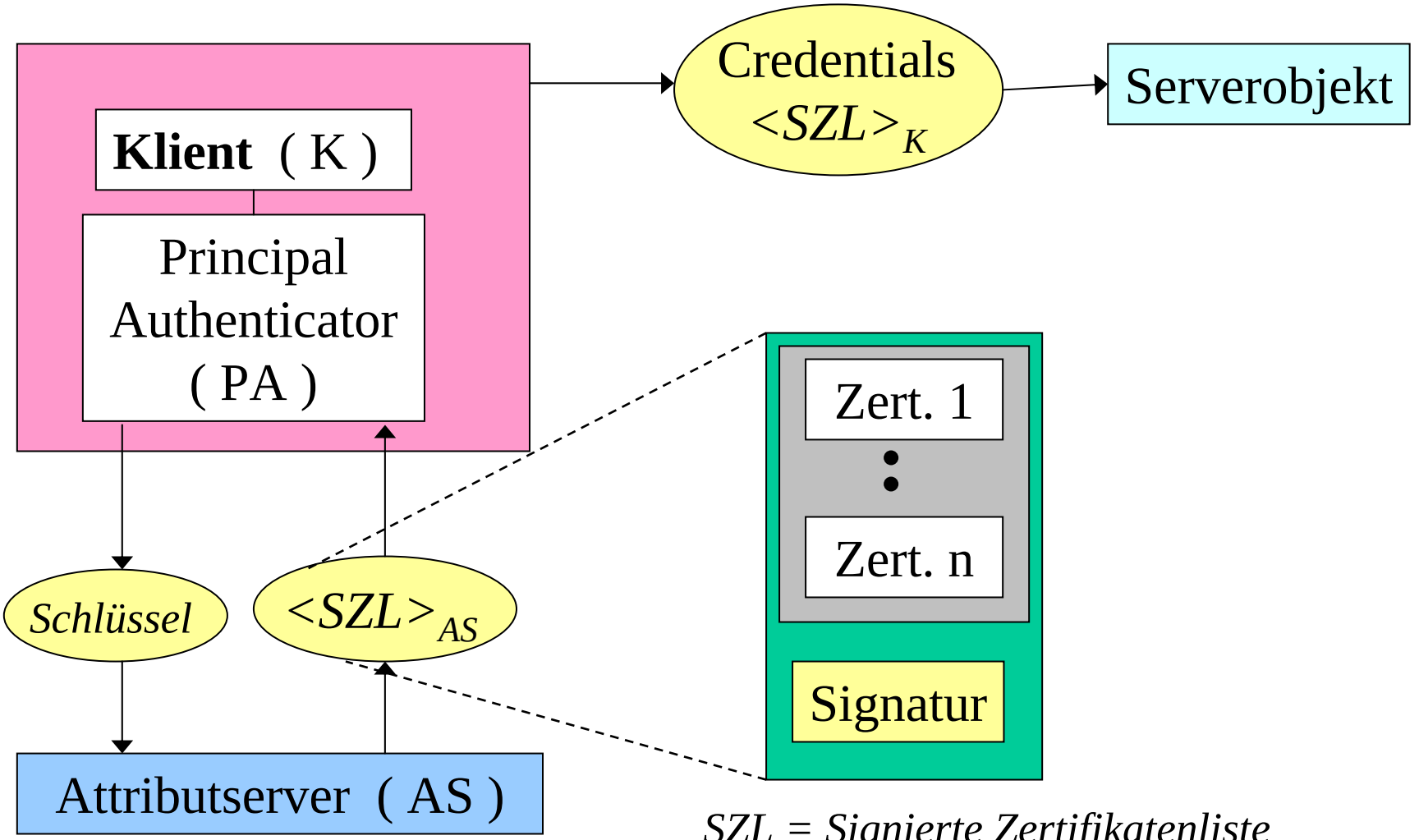
LABORATOIRE DE SYSTEMES D'EXPLOITATION

Struktur

1. Theoretischer Hintergrund
   - JacORB
   - Authentisierung in CORBA: Credentials
   - SPKI
2. Protokoll:
   - Erlangung und Vermittlung von authentisierten Credentials
3. Implementierung: Schichtenarchitektur
4. Beispielanwendung:
   - Demonstration von *Access Control* für den Namensdienst
5. Beitrag der Arbeit

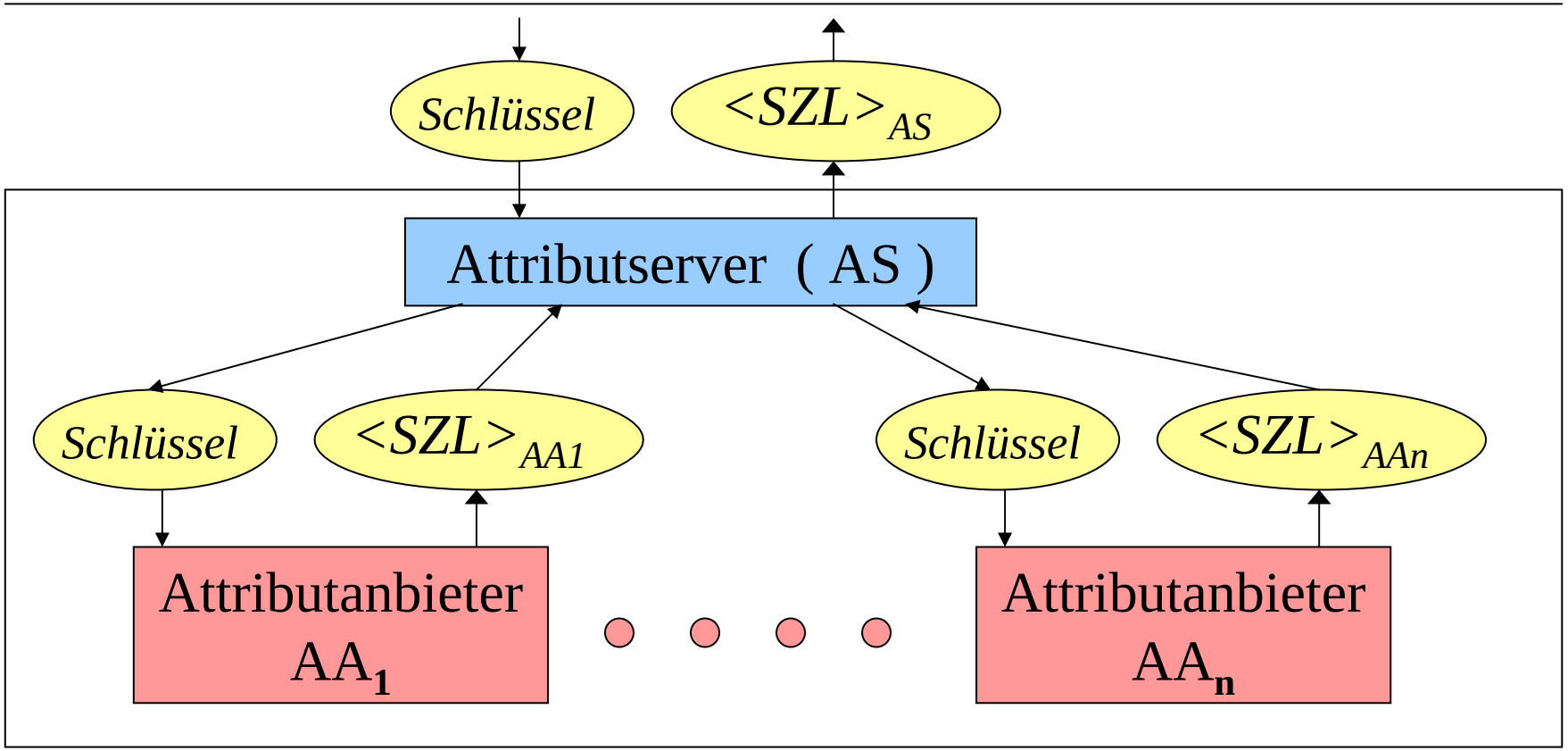
LABORATOIRE DE SYSTEMES D'EXPLOITATION

Protokoll: Übersicht

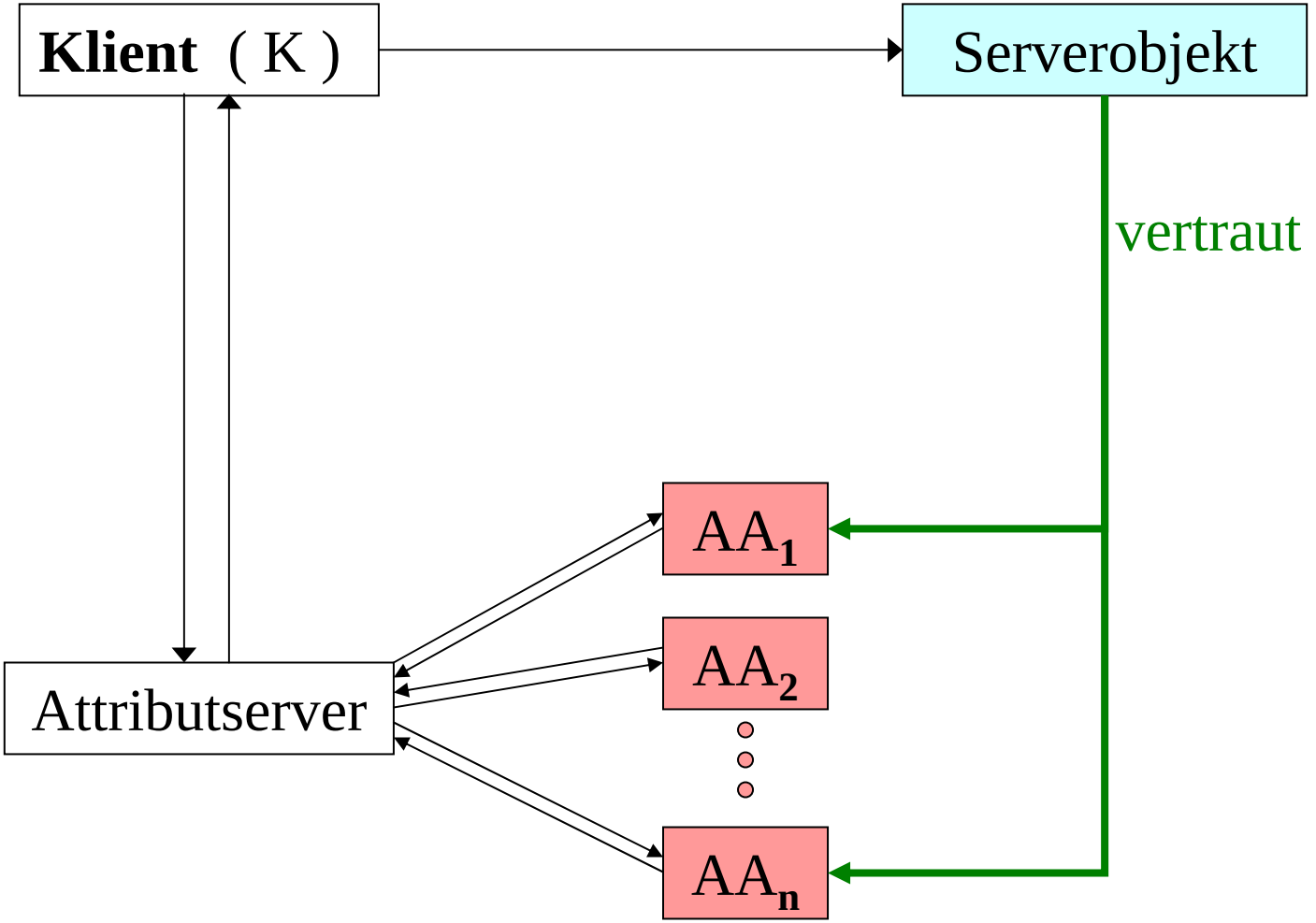


SZL = Signierte Zertifikatenliste

Protokoll: Struktur des Attributservers



Protokoll: Vertrauen des Servers



Struktur

1. Theoretischer Hintergrund
   - JacORB
   - Authentisierung in CORBA: Credentials
   - SPKI
2. Protokoll:
   - Erlangung und Vermittlung von authentisierten Credentials
3. Implementierung: Schichtenarchitektur
4. Beispielanwendung:
   - Demonstration von *Access Control* für den Namensdienst
5. Beitrag der Arbeit

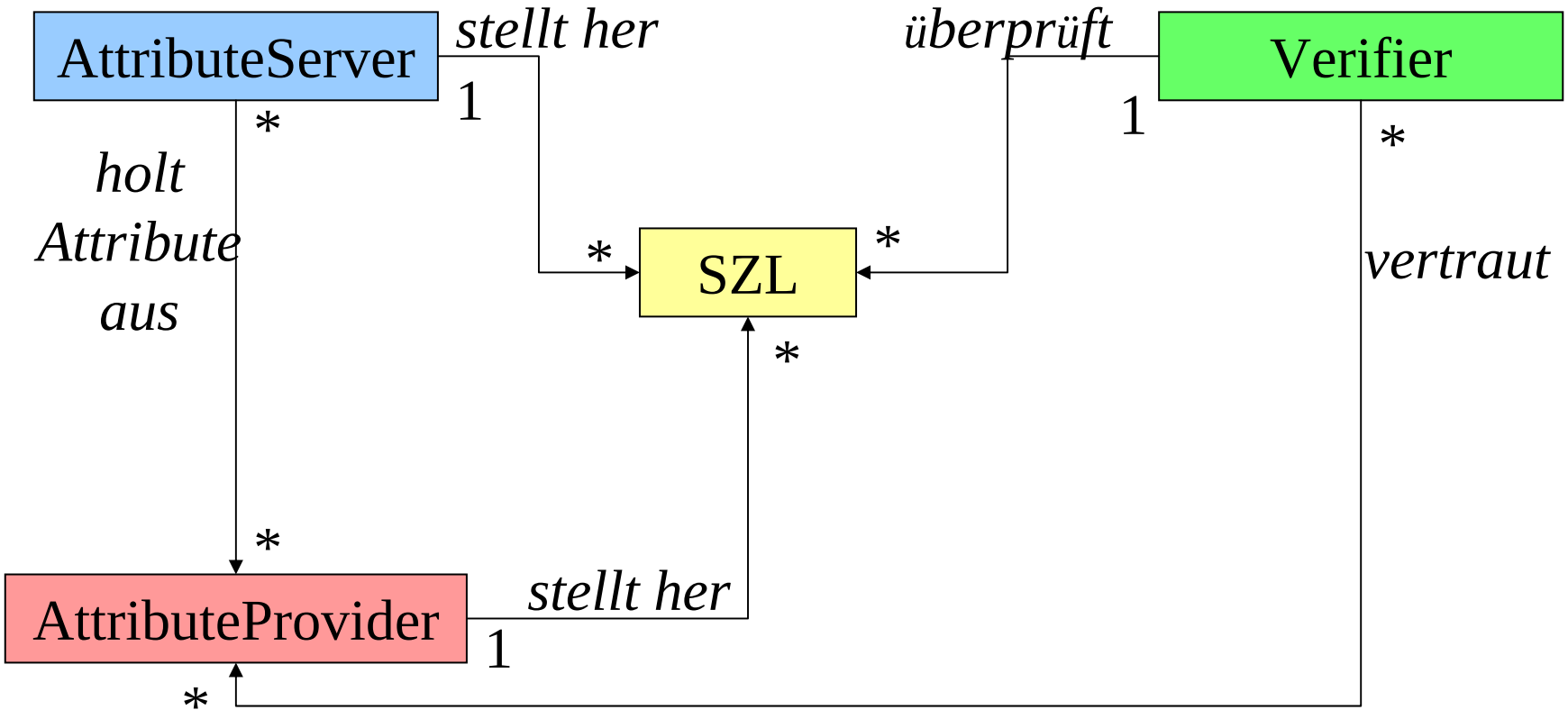
LABORATOIRE DE SYSTEMES D'EXPLOITATION

Architektur der Implementierung

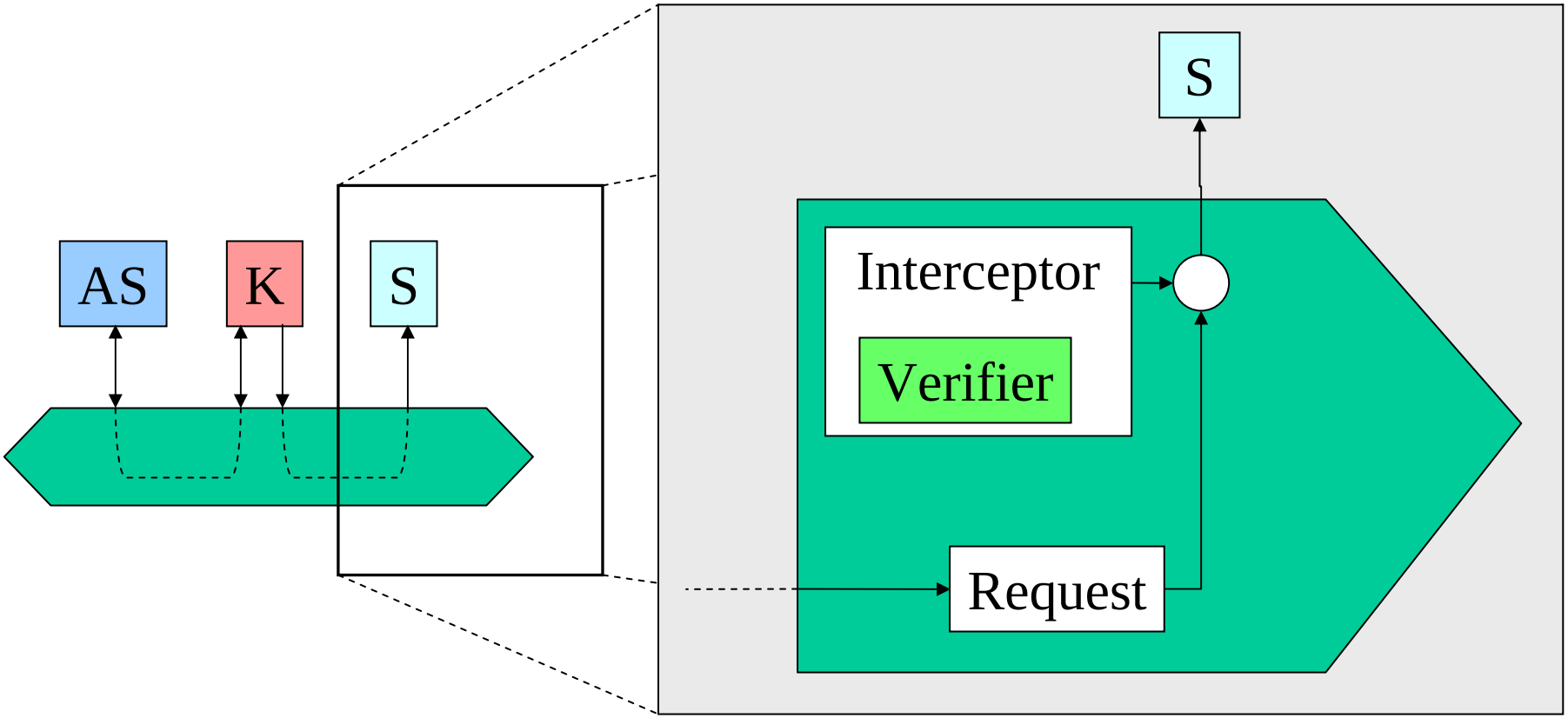
5	**JacORB** Principal Authenticator, Current, Credentials	`jacorb.*`
4	**Authentisierung** Attributserver und -anbieter Credentialserzeugung und -vermittlung	`spki.auth`
3	**SPKI Zertifikate** Unterschriften S-Expressions ↔ Zertifikate Schlüsselgenerierung	`spki.certificate`
2	**S-Expression-Objekte** Serialisierung in kanonischer / fortgeschrittener Form Lektüre von ASTs	`spki.sexp`

1	**Parsieren**
	Syntaxbaum
	Visitoren
		`spki.parsing`
		`spki.syntaxtree`
		`spki.visitor`

Schicht 4: Beziehungsmodell



Schicht 5: Mechanismus auf der Serverseite



Schicht 3: Funktionalität

1. Notationsunabhängige Darstellung von Zertifikaten

2. Signatur- und Hashverfahren

3. Generierung von Schlüsseln für Principals

4. Integration mit der Java 2 API

LABORATOIRE DE SYSTEMES D'EXPLOITATION

Schicht 3: Hauptklassen

- Zertifikate
  - 2 Kategorien: Namens- und Erlaubniszertifikate
  - Keine Integration mit Java 2
  - Jeder Zertifikat entspricht 2 Principals: Subjekt & Aussteller
- Principals:
  - Name
  - Hashwert
  - öffentlicher Schlüssel
- Öffentlicher Schlüssel
  - 3 Typen : RSA-SHA1, RSA-MD5, DSA-SHA1

LABORATOIRE DE SYSTEMES D'EXPLOITATION

Schicht 3: Funktionen von Schlüsseln

		Java	Cryptix	meine Impl.
Darstellung	öff. Schlüssel	●		●
	DSA-privat	●		●
	RSA-privat	●	●	
Signaturverfahren	DSA	●		
	RSA		●	
Schlüsselgenerierung	DSA	●		
	RSA		●	

- Persistenz:
  - Datei, die die S-Expression der Schlüssel enthält
  - Der private Schlüssel ist mit einem Pass-Satz verschlüsselt

LABORATOIRE DE SYSTEMES D'EXPLOITATION

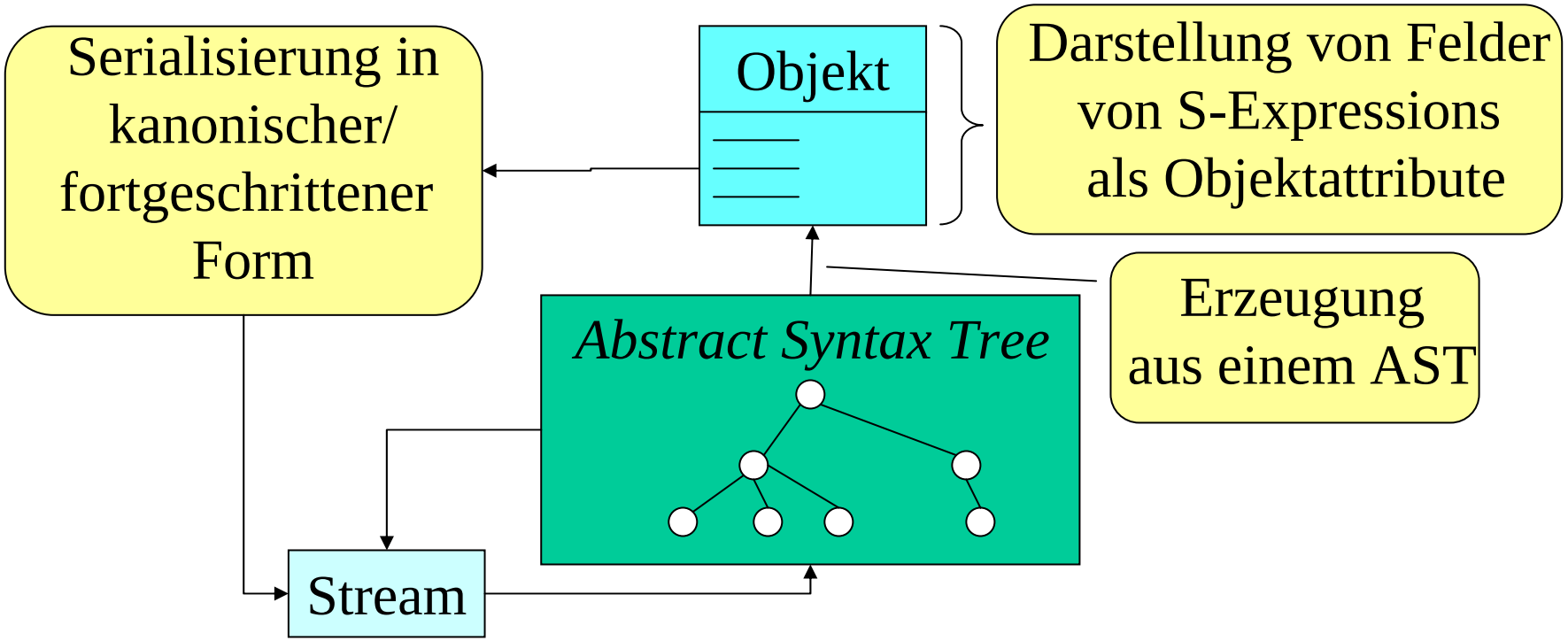
Schicht 1

- Funktionalität: Parsieren von S-Expressions
- Parsergenerator: JavaCC und Java Tree Builder (JTB)
  - hat alle Klassen der Schicht 1 generiert
- 3 Packages: spki.parsing, spki.syntaxtree, spki.visitor
- Visitoren:
  - Vorteil: Implementierte Funktionalität bleibt trotz Änderung der Grammatik
  - Nachteil: An lokale Operationen nicht angepasst
- Problem: Syntaxbäume sind mühsam zu untersuchen
- Lösung: Zwischenschicht, die strukturierte S-Expressions als Objekte darstellt.

LABORATOIRE DE SYSTEMES D'EXPLOITATION

Schicht 2: S-Expression-Objekte

- Funktionalität:

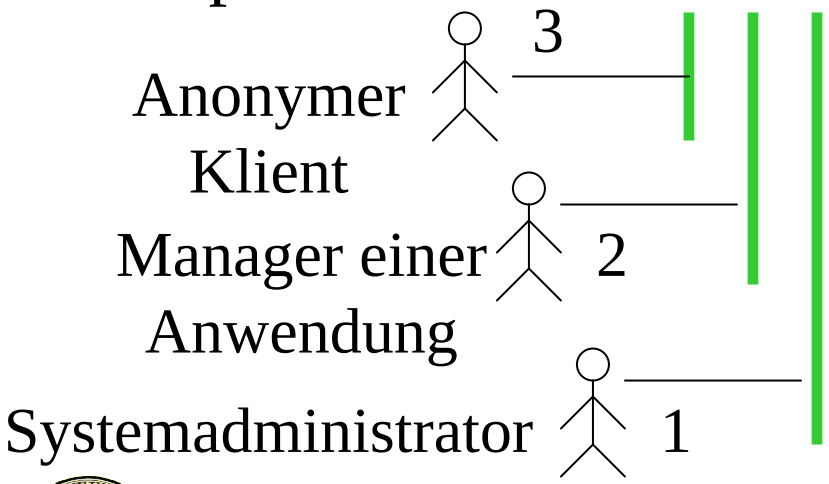


- Untermenge von S-Expressions unterstützt.
- Disjunktion in der Grammatik → Java Schnittstelle

LABORATOIRE DE SYSTEMES D'EXPLOITATION

Beispielanwendung: Prinzip

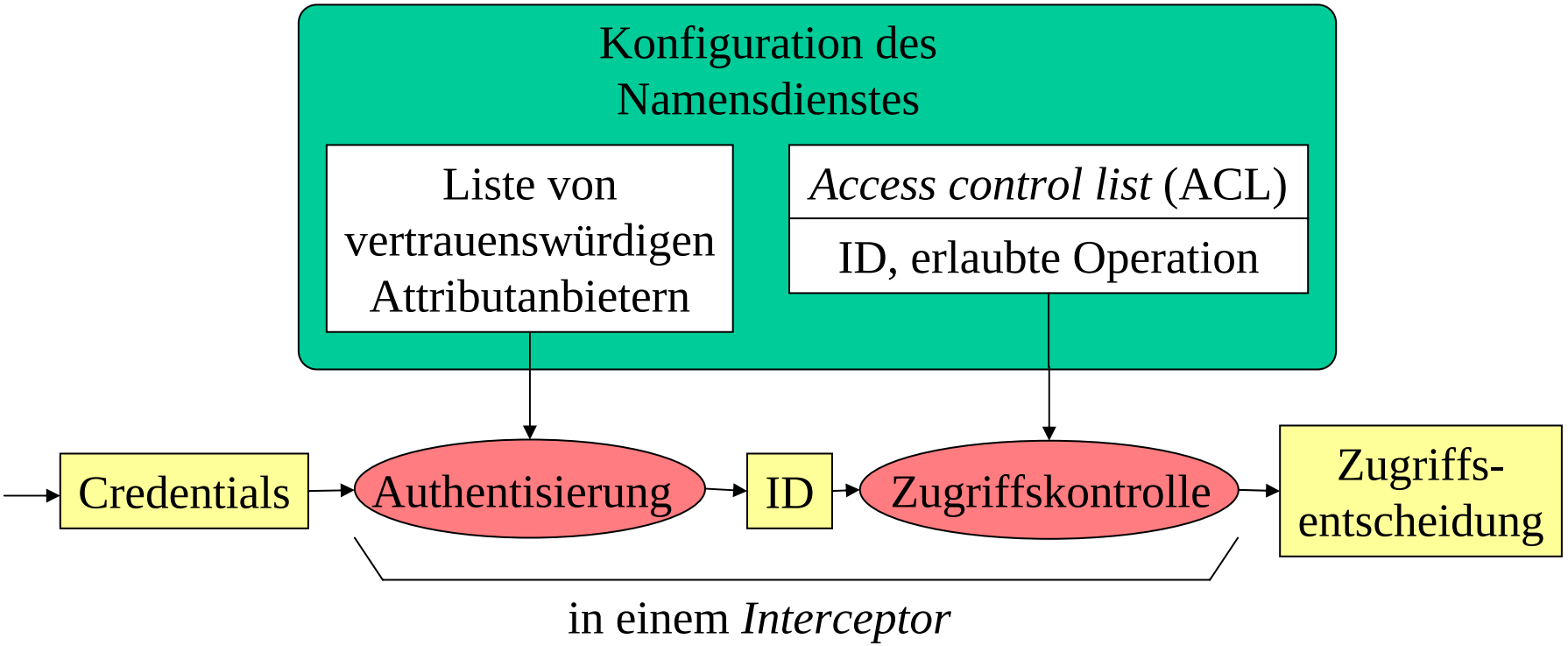
- Ziel: Auf Authentisierung basierter Zugrifsschutz des Namensdienstes von JacORB.
- Grund: Namensdienst ist sicherheitskritisch.
- Jeder Klient hat 1 Attribut: ein ID
- Grobkörnige Zugriffskontrolle
- Beispiel:



Operationen auf dem Namensdienst
resolve (Name) : Objekt
list ( )
bind (Name, Objekt)
rebind (Name, Objekt)
unbind (Name)
destroy()

Beispielanwendung: Mechanismus

- Prozess auf der Serverseite:



Beitrag der Arbeit

- Kenntnisse
  - Eine „real-world“ Anwendung von SPKI-Zertifikaten
  - Beweis, dass sie für eine sicherheitskritische Anwendung wie Authentisierung in CORBA angepaßt sind.
- Produkte
  - Eine Java-Bibliothek für die Serialisierung von SPKI-Zertifikaten.
  - Authentisierung in JacORB

LABORATOIRE DE SYSTEMES D'EXPLOITATION