Web-Authentisierung mit dem ePA

Christian J. Dietrich

dietrich [at] internet-sicherheit . de

2008-07-11

Inhalt

1. Einleitung
2. Der elektronische Personalausweis
3. Die Authentisierungsfunktion im Detail
4. Kurzvorstellung der Implementierung
5. Fazit und Ausblick

1. Einleitung

Einleitung

- International Civil Aviation Organization (ICAO) normt Machine Readable Travel Documents (MRTD) seit 1944
- ~190 Mitgliedstaaten
- Ziele von MRTDs
  - bessere Identifikation
  - starke Bindung zwischen Dokument und Inhaber

- Nov. 2005: Einführung des ePasses (Stufe 1)
- Nov. 2007: Einführung des ePasses (Stufe 2)

- ~2010: Einführung des ePA

2. Der elektronische Personalausweis

Brauchen wir einen neuen Personalausweis?

- Fälschungssicherheit? Nein!
  - Deutsche Ausweise gehören zu den am schwersten fälschbaren der Welt!
  - 2007: 62 Mio. Dokumente im Umlauf
    495 Urkundendelikte (<0,008‰)
    88 Totalfälschungen

- Elektronische Authentisierung
  - Im Offline-Bereich
    - Hotel Check-In
    - Jugendschutzfunktion
  - Im Online-Bereich
    - **Sichere Authentikation ist bisher nicht möglich!**

Sicherheitsmerkmale

- physikalisch (insgesamt 11)
  - holografische Bilder (1-7)
  - kinematische Bewegungsstrukturen (3)
  - Mikroschrift (4)
  - Guillochen (9)
  - Wasserzeichen (11)
  - Oberflächenstruktur (8, 10)
- elektronisch (künftig)
  - Biometrie
  - erweiterter Zugriffsschutz
- Funkschnittstelle ist kein Sicherheitsmerkmal

3. Die Authentisierungsfunktion im Detail

Die Authentikationsfunktion

- Definition

  Sichere Übertragung von Attributen des Personalausweises an einen Dritten

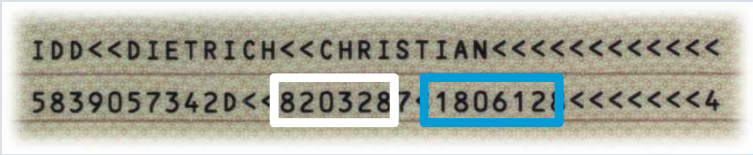
- *Sichere Übertragung*: Gewährleistung der Vertraulichkeit (Authentizität und Integrität)
  - sowohl der gespeicherten Daten
  - als auch während der Übertragung

- *Attribute*
  - (nicht notwendigerweise) explizit personenbezogene Daten
  - relative Aussagen (z.B. „ist älter als 18 Jahre“)

- Beispiele
  - Online-Anmeldung eines KFZ
  - Registrierung in einem Online-Shop
  - Altersverifikation

Authentisierung beim ePass (Basic Access Control)

1) Übergabe des Dokuments an Kontrolleur
2) Auflegen des Passes
3) Scan der maschinenlesbaren Zone (MRZ)
4) Ableitung eines Schlüssels
5) elektronisches Auslesen des ePasses
6) Vergleich der ausgelesenen Daten mit Dokumententräger

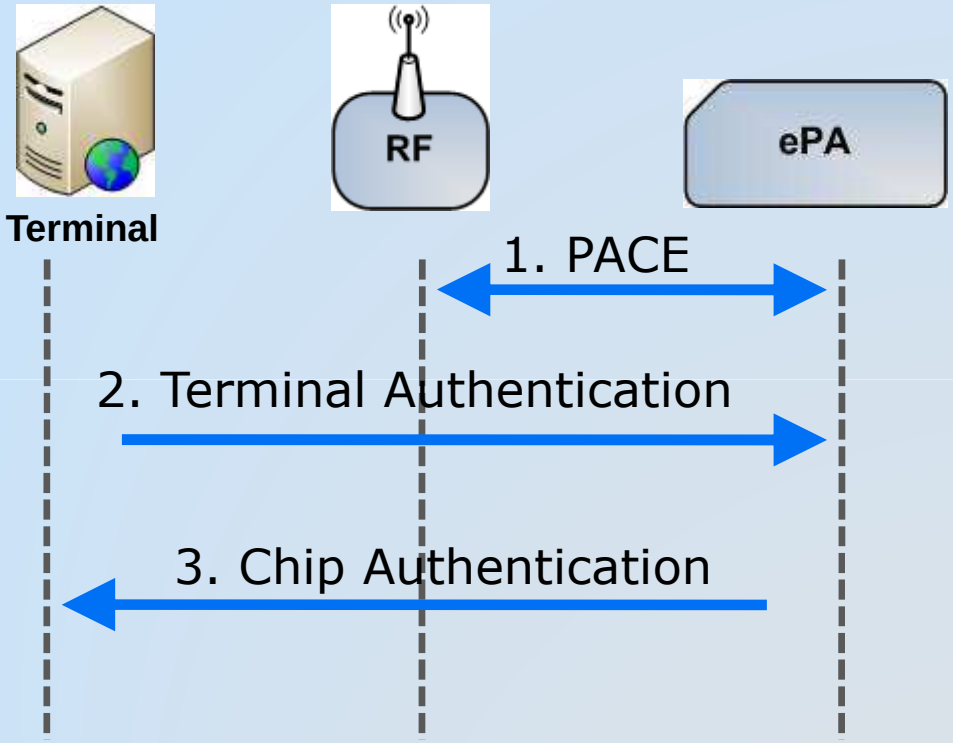


Extended Access Control

- in Deutschland entwickeltes Verfahren für den erweiterten Zugriffsschutz
- Kernbestandteile
  - asymmetrische Verschlüsselung
  - digital signierte gespeicherte Daten
  - (globale) Public Key Infrastruktur
  - Challenge-Response-Verfahren (abstreitbar)
- 3 Protokolle
  - Password Authenticated Connection Establishment
  - Terminal Authentication
  - Chip Authentication

Bundesamt für Sicherheit in der Informationstechnik

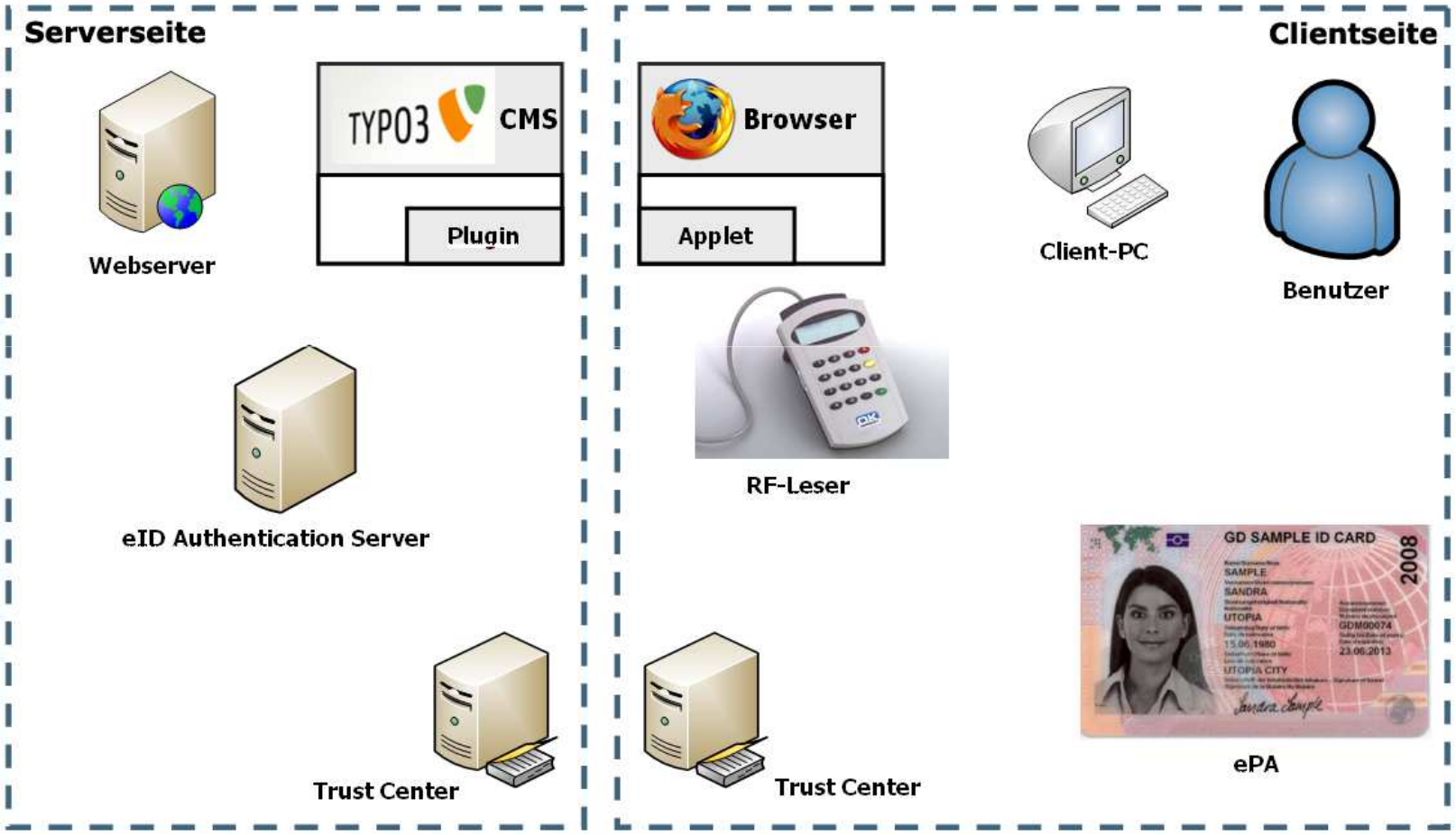
Extended Access Control



1. **PACE**
   Freischalten des ePA (Diffie-Hellman)
2. **Term. Authentication**
   Authentikation des Terminals gegenüber dem ePA mittels C/R und Terminal Certificate
3. **Chip Authentication**
   Authentikation des ePA gegenüber dem Terminal (Diffie-Hellman mit statischem Chip Key)

4. Kurzvorstellung der Implementierung

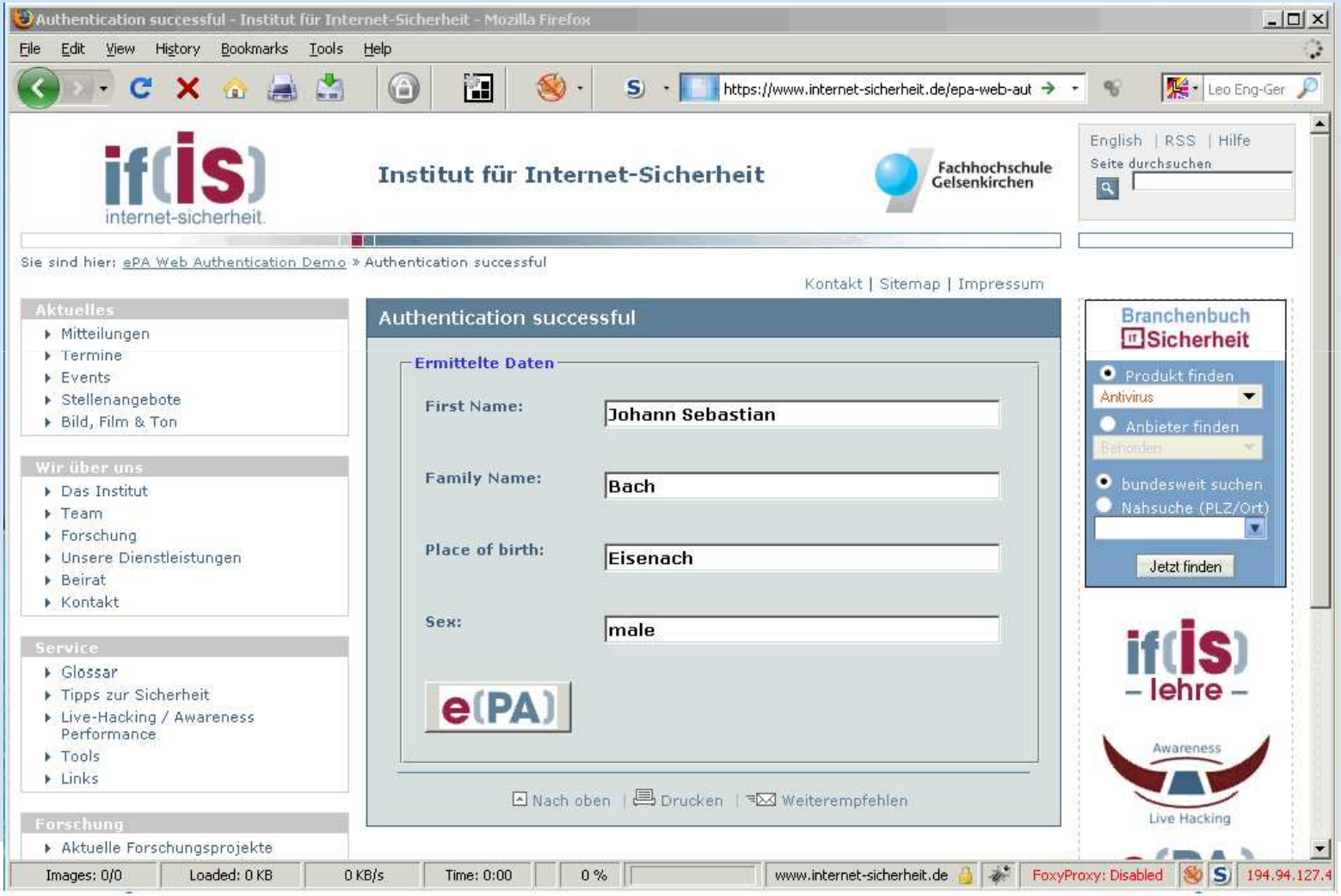
Szenario: Web-Authentisierung



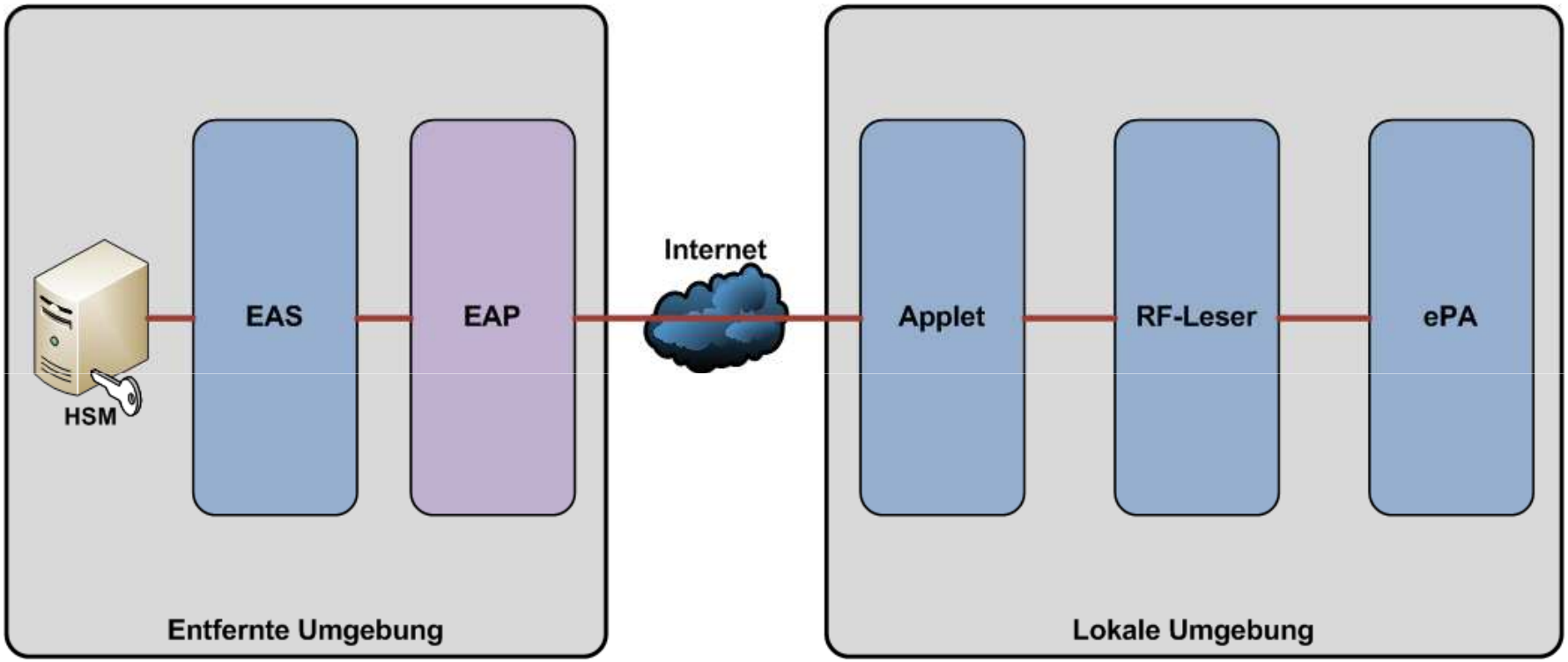
Berechtigungszertifikat / Terminal Certificate

- ist Kernelement der Terminal Authentication
- enthält Zertifikatsinhaber
- enthält den öffentlichen Schlüssel des EAS
- beinhaltet die Zugriffsberechtigungen für die Attribute eines ePA
- trägt die Signatur einer ausstellenden Behörde
- enthält Verweis auf die zuständige Aufsichtsbehörde
- gibt den Verwendungszweck der zu erhebenden Daten an
- hat eine sehr kurze Gültigkeit (24 Stunden)

Demo


Authentication successful - Institut für Internet-Sicherheit - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://www.internet-sicherheit.de/epa-web-aut
Leo Eng-Ger
if(is) internet-sicherheit.
Institut für Internet-Sicherheit
Fachhochschule Gelsenkirchen
English | RSS | Hilfe
Seite durchsuchen
Sie sind hier: ePA Web Authentication Demo » Authentication successful
Kontakt | Sitemap | Impressum
Aktuelles
Mitteilungen
Termine
Events
Stellenangebote
Bild, Film & Ton
Wir über uns
Das Institut
Team
Forschung
Unsere Dienstleistungen
Beirat
Kontakt
Service
Glossar
Tipps zur Sicherheit
Live-Hacking / Awareness Performance
Tools
Links
Forschung
Aktuelle Forschungsprojekte
Authentication successful
Ermittelte Daten
First Name: Johann Sebastian
Family Name: Bach
Place of birth: Eisenach
Sex: male
e(PA)
Nach oben | Drucken | Weiterempfehlen
Branchenbuch Sicherheit
Produkt finden
Antivirus
Anbieter finden
Behörden
bundesweit suchen
Nahsuche (PLZ/Ort)
Jetzt finden
if(is) – lehre –
Awareness
Live Hacking
Images: 0/0
Loaded: 0 KB
0 KB/s
Time: 0:00
0 %
www.internet-sicherheit.de
FoxyProxy: Disabled
194.94.127.4

Die fünf Kernkomponenten

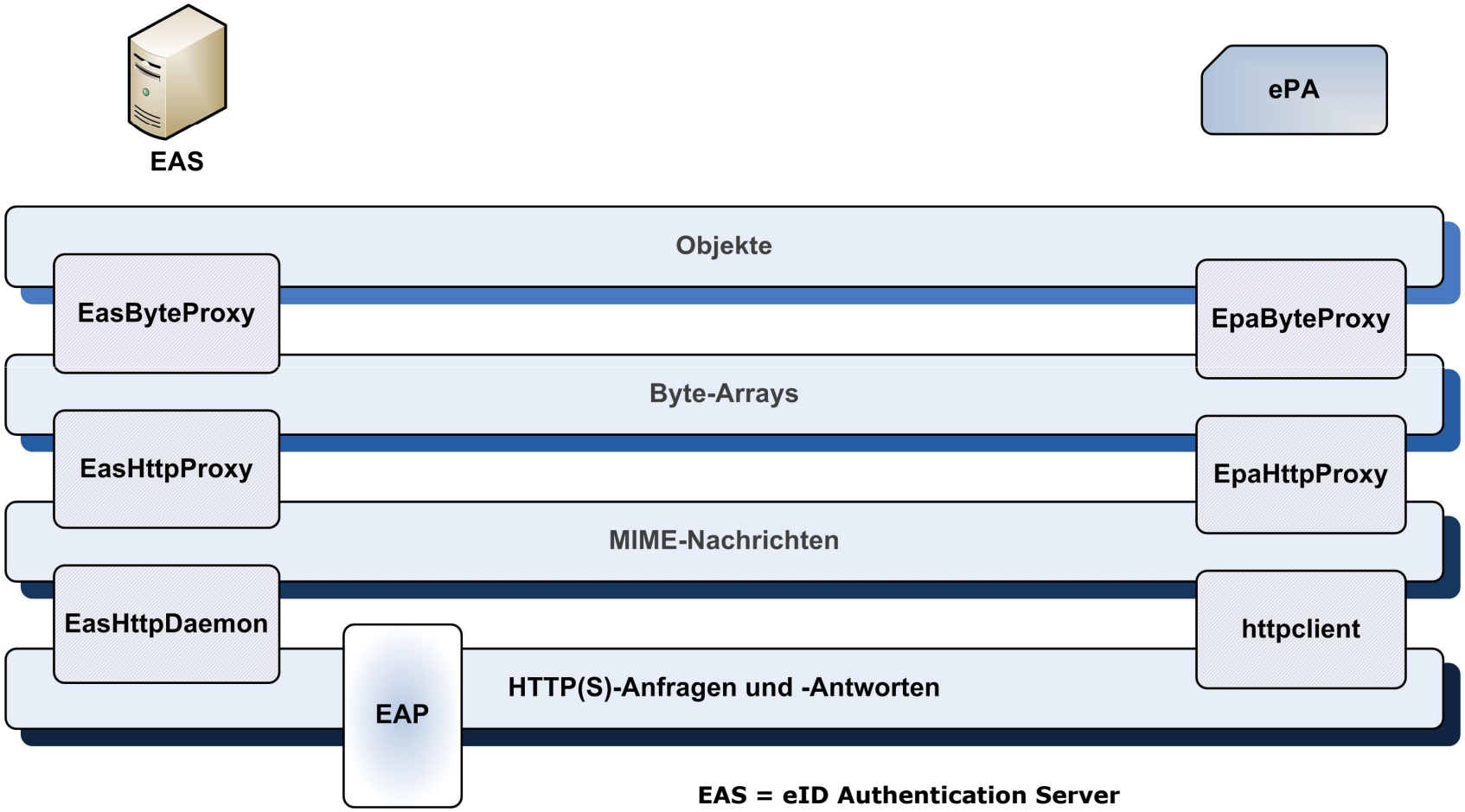


EAS = eID Authentication Server
EAP = eID Authentication Proxy
RF = Radio Frequency
ePA = elektronischer Personalausweis
HSM = Hochsicherheitsmodul

violett: **Implementierung in PHP (Extension von Typo3)**

blau: **Implementierung in Java**

Schichtenmodell



EAS = eID Authentication Server
EAP = eID Authentication Proxy
ePA = elektronischer Personalausweis
MIME = Multipurpose Internet Mail Extensions

5. Fazit und Ausblick

Fazit und Ausblick

- ePA ist sehr weit verbreitet
- ePA bringt Authentisierungsfunktion für das Internet
- Extended Access Control (EAC) ist ein bedeutender Meilenstein (ähnlich SSL/TLS)
- Teil dieser Arbeit: die erste Implementierung von EAC für den ePA

- Spezifikation erweitern
- Ausbau des Piloten mit realen Komponenten
- Kombination mit der Ausführung in sicheren Umgebungen, z.B. Trusted Computing

Vielen Dank für Ihre Aufmerksamkeit.

Fragen?