



# Eine transparente Open-Source-Lösung für eID

**Fachtagung Verwaltungsinformatik und Fachtagung Rechtsinformatik 2010**

**Koblenz, 25. März 2010**

**Andreas Kasten, [andreas.kasten@uni-koblenz.de](mailto:andreas.kasten@uni-koblenz.de)**

**Helge Hundacker, [helge.hundacker@uni-koblenz.de](mailto:helge.hundacker@uni-koblenz.de)**

**Universität Koblenz-Landau**

**IWVI**

**Professur IT-Risk-Management**

# Agenda

1. Grundlagen zum neuen Personalausweis & eID
2. Aspekte von Open Source
3. eID-Client „rosecat“

# Agenda

- 1. Grundlagen zum neuen Personalausweis & eID**
2. Aspekte von Open Source
3. eID-Client „rosecat“

# Allgemeines zum neuen Personalausweis

- Ausgabe ab 01. November 2010
- neue Funktionen
  - eSign
  - ePassport
  - eID



# Allgemeines zum neuen Personalausweis

- Ausgabe ab 01. November 2010
- neue Funktionen
  - **eSign: elektronische Signatur**
  - ePassport
  - eID



# Allgemeines zum neuen Personalausweis

- Ausgabe ab 01. November 2010
- neue Funktionen
  - eSign
  - **ePassport: hoheitliche Authentifikation**
  - eID

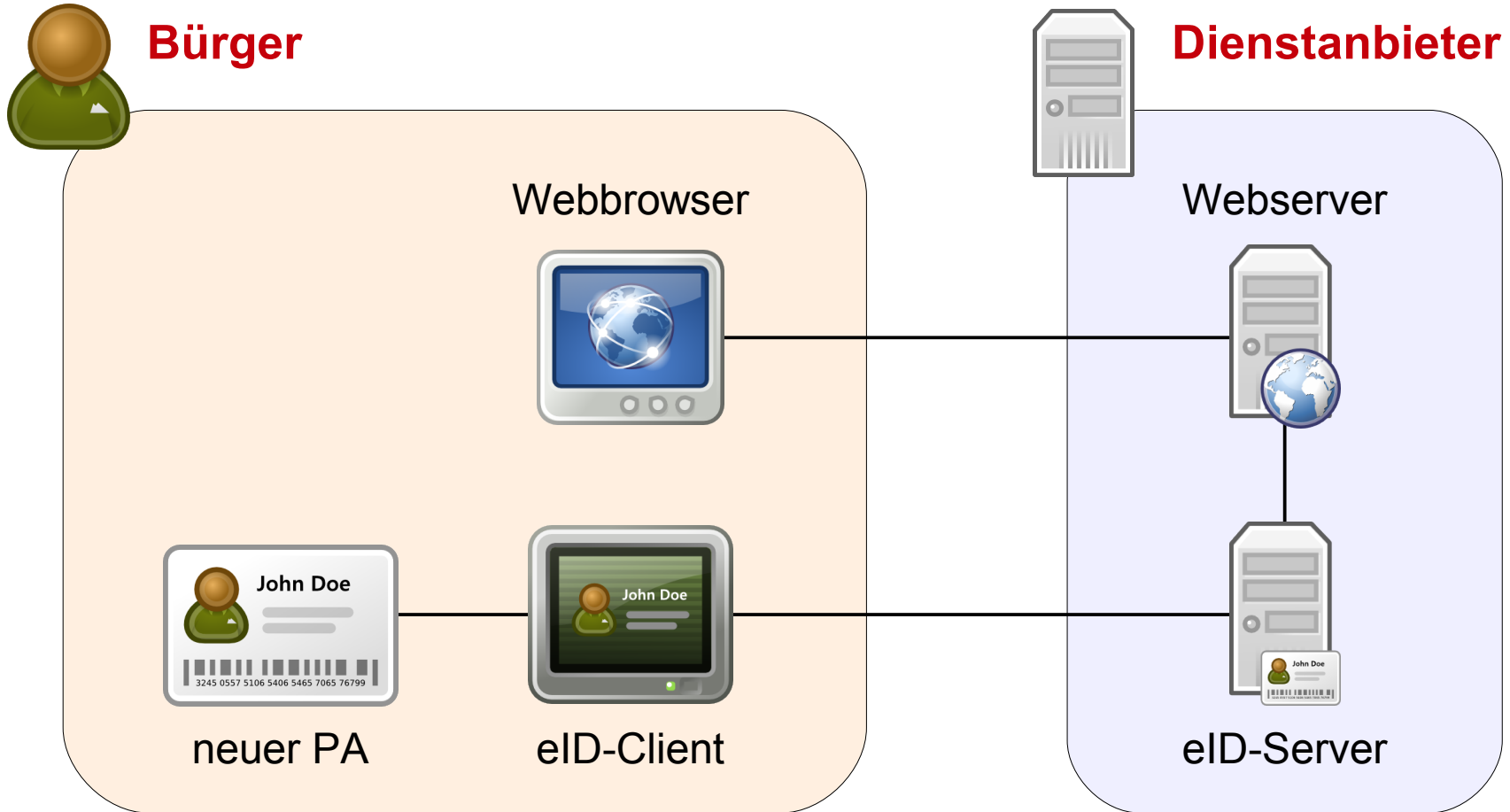


# Allgemeines zum neuen Personalausweis

- Ausgabe ab 01. November 2010
- neue Funktionen
  - eSign
  - ePassport
  - **eID: private Authentifikation**

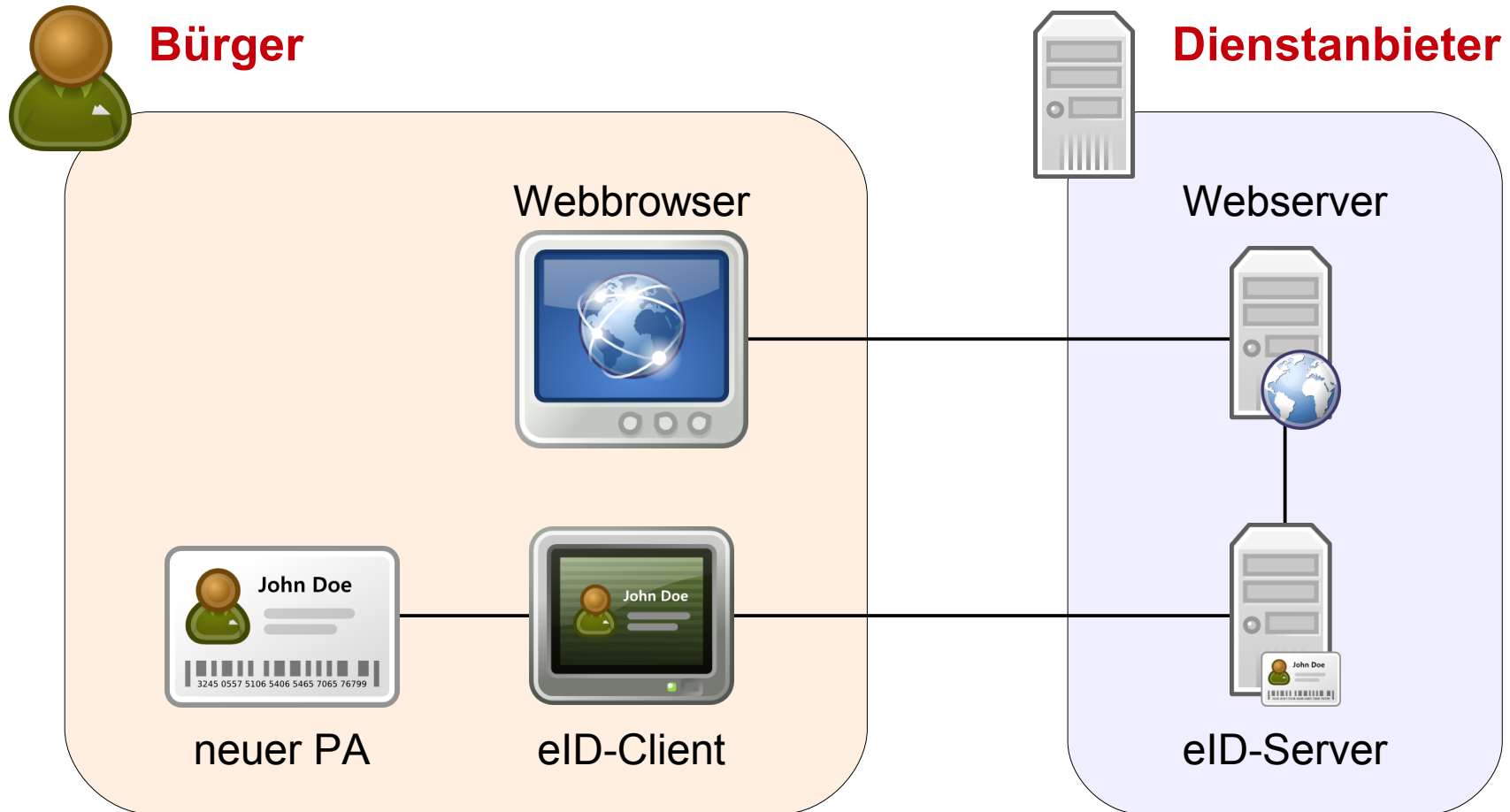


# Komponenten bei eID

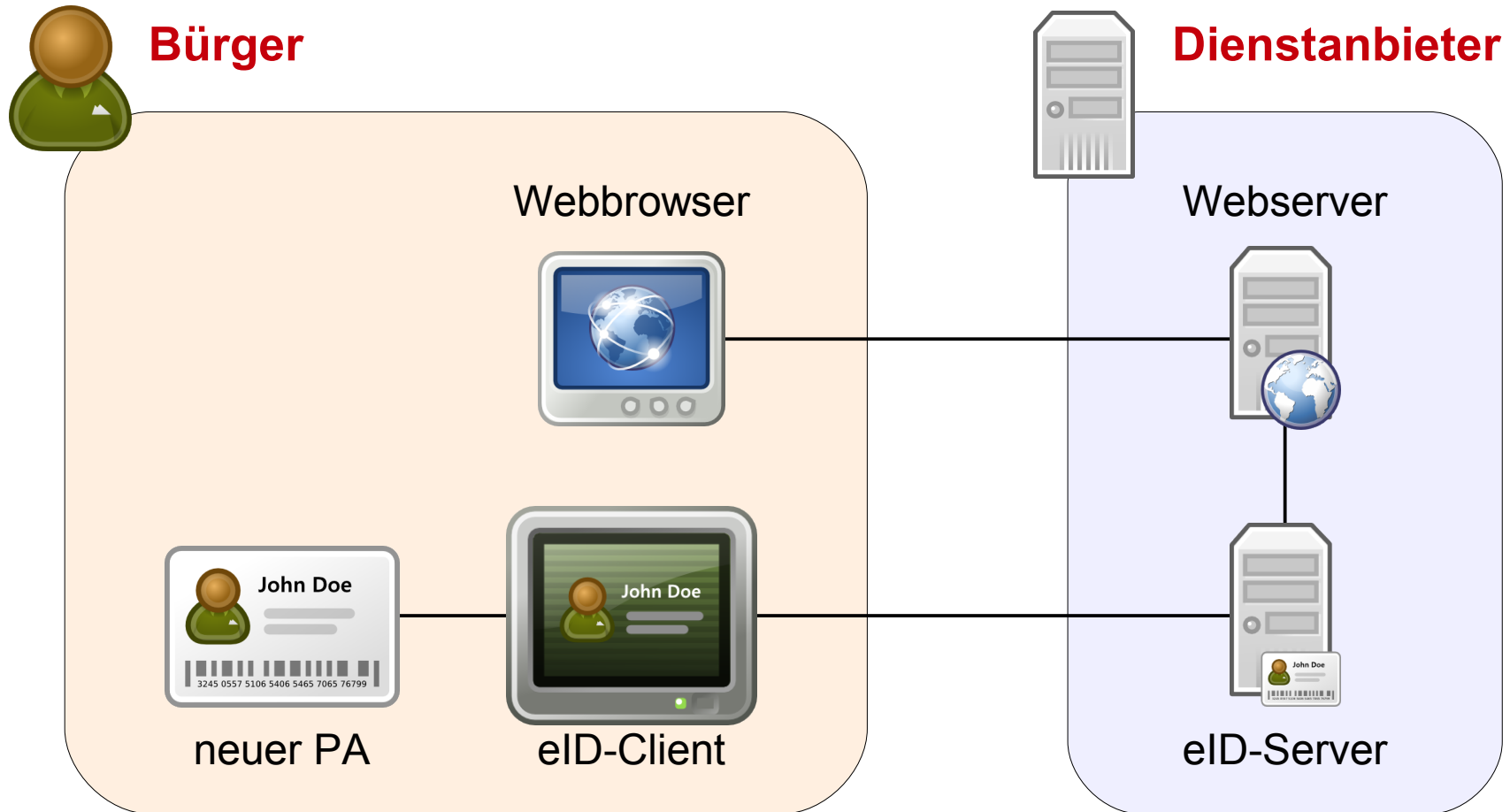




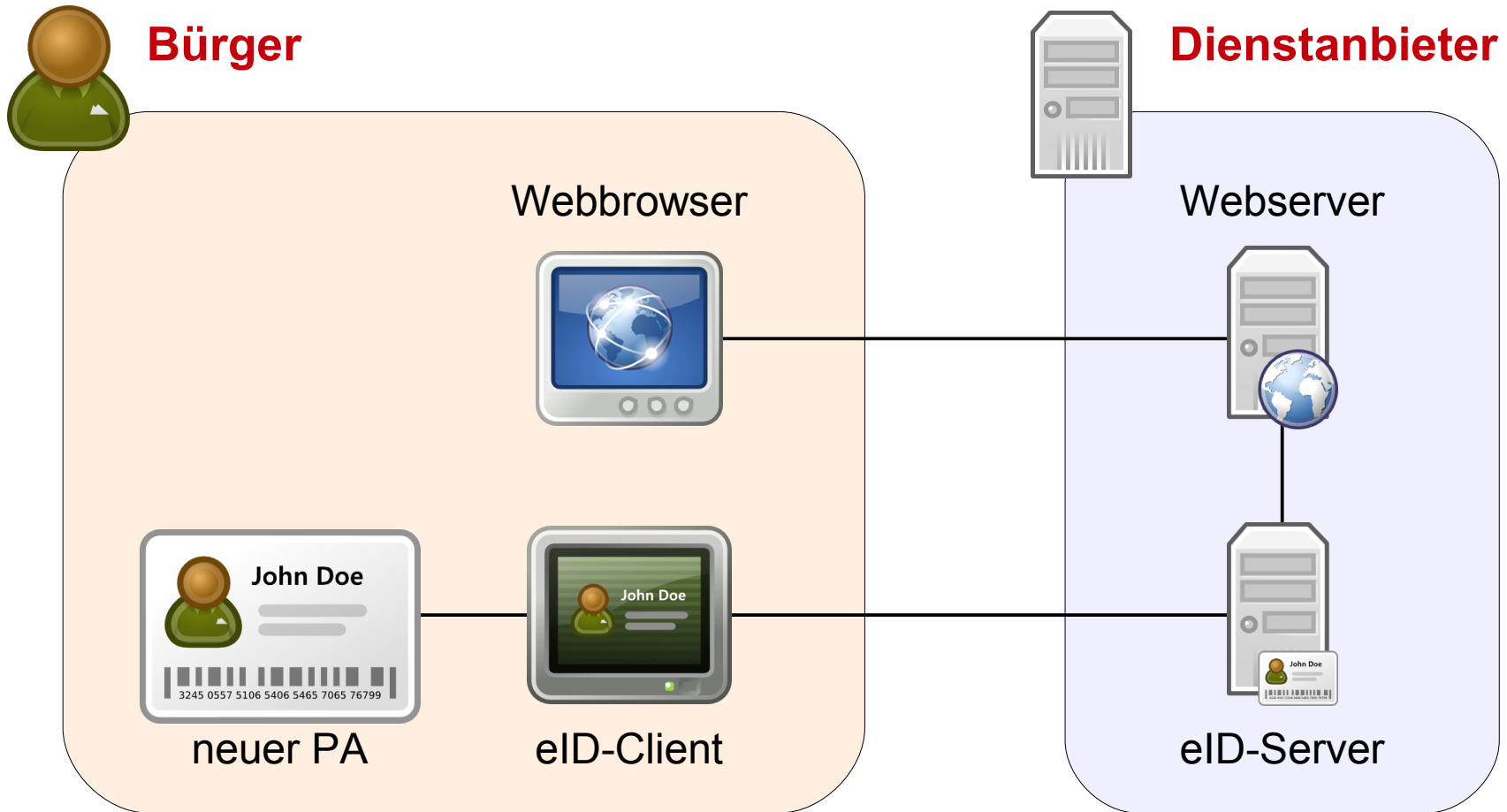
# Komponenten bei eID



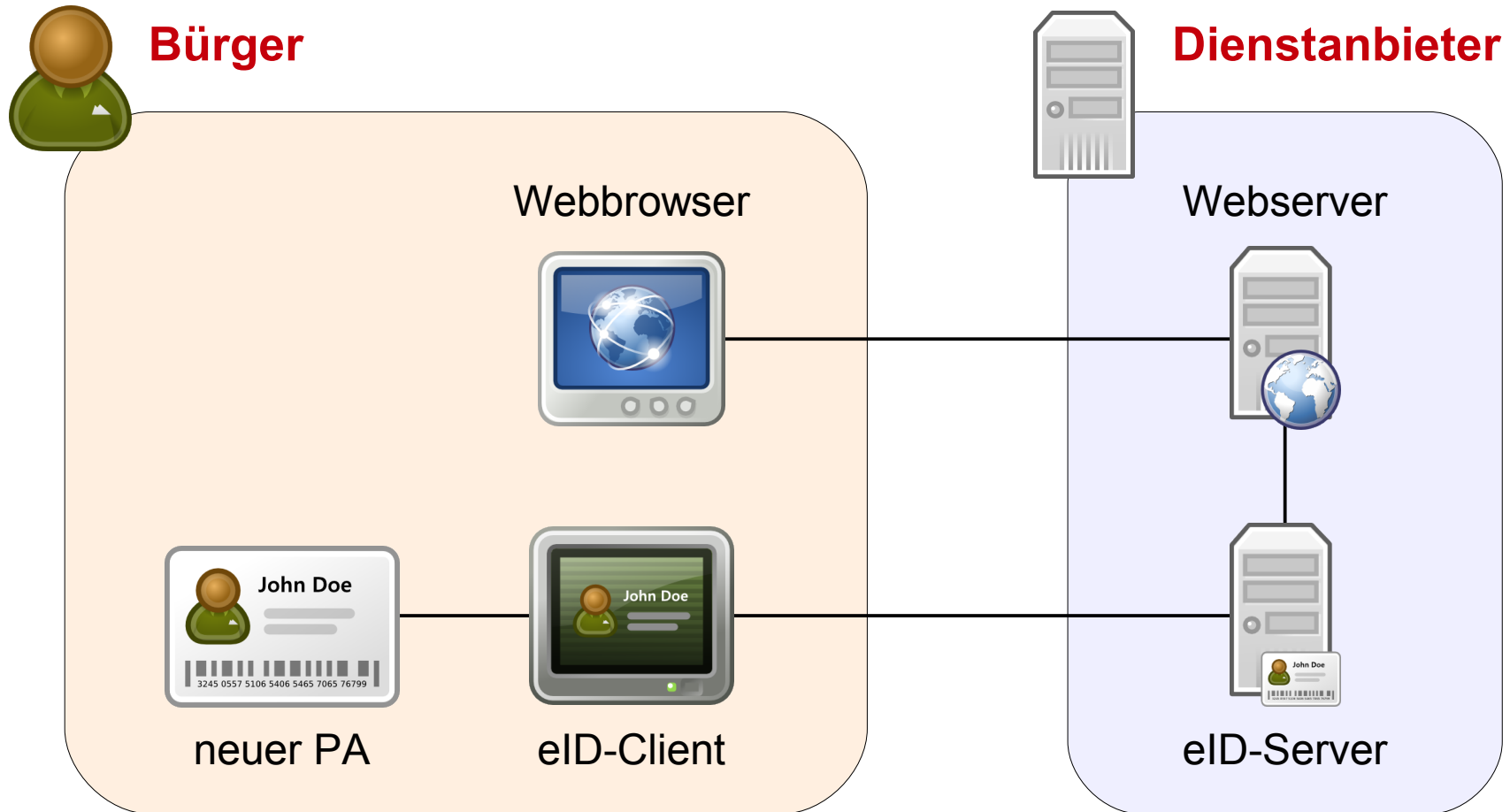
# Komponenten bei eID



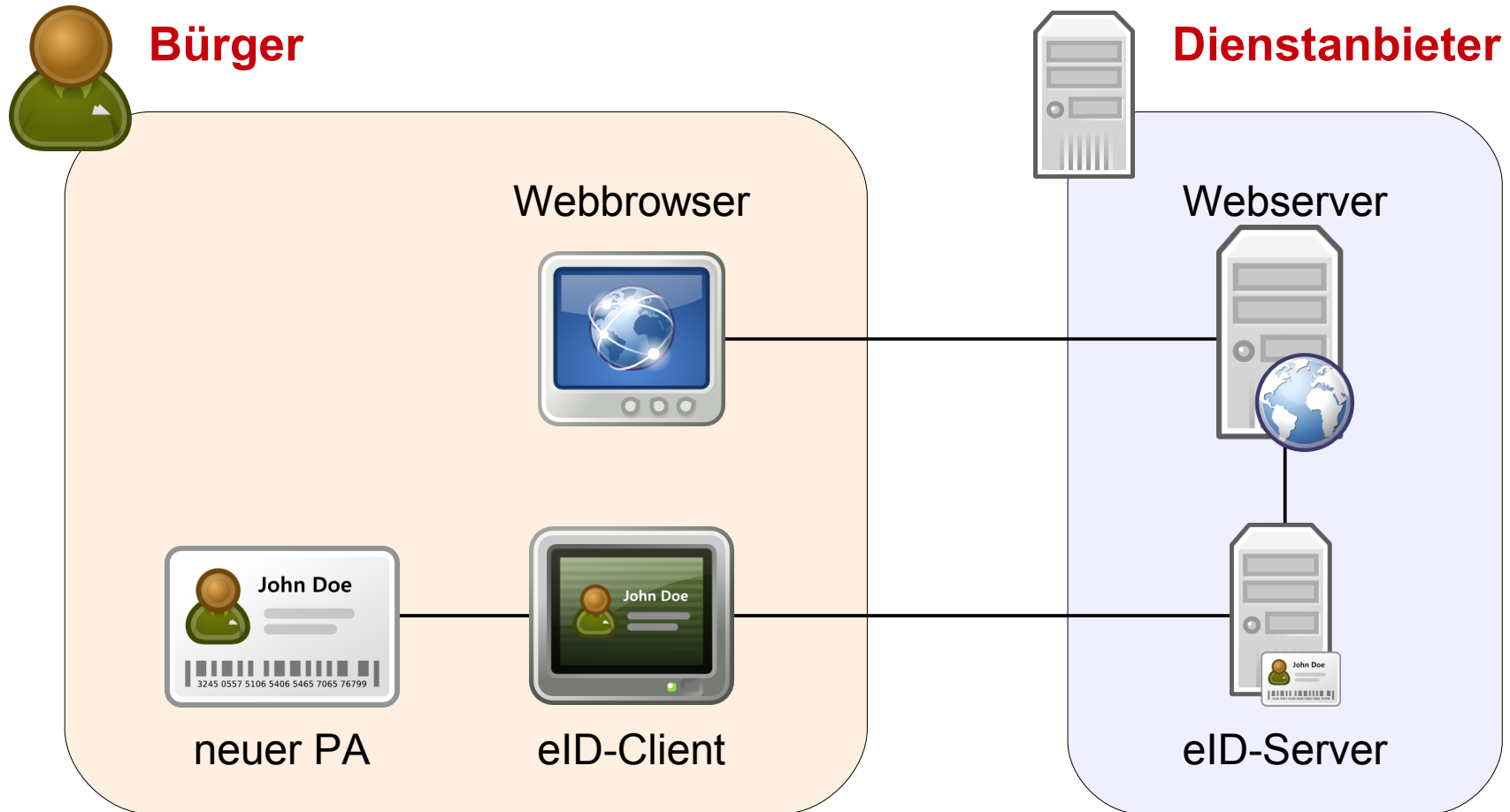
# Komponenten bei eID



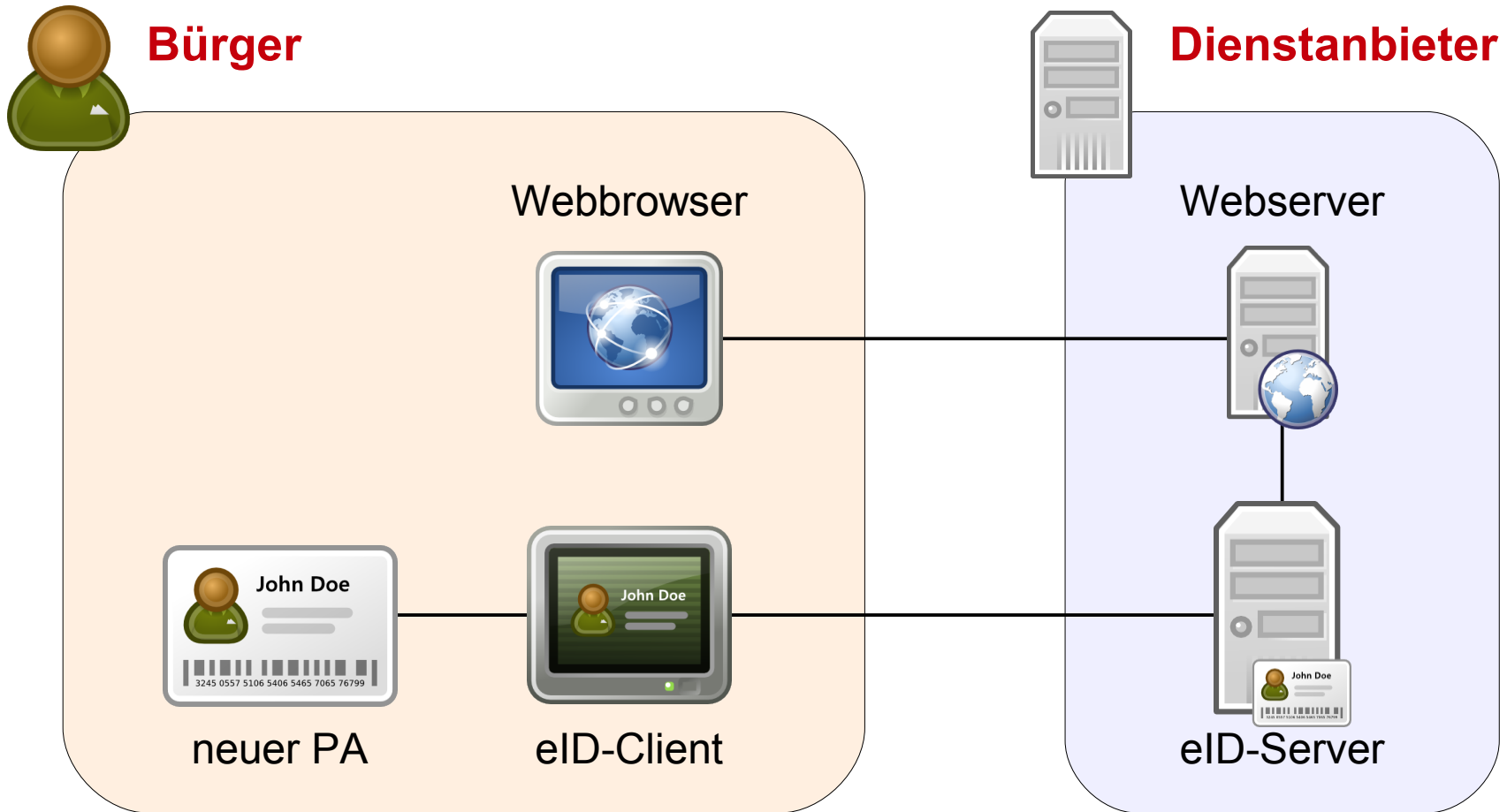
# Komponenten bei eID



# Komponenten bei eID



# Komponenten bei eID



# Berechtigungs-zertifikat

- zweckgebunden für Dienstanbieter ausgestellt
- legitimiert zum Auslesen von Daten



# Ablauf von eID





# Ablauf von eID



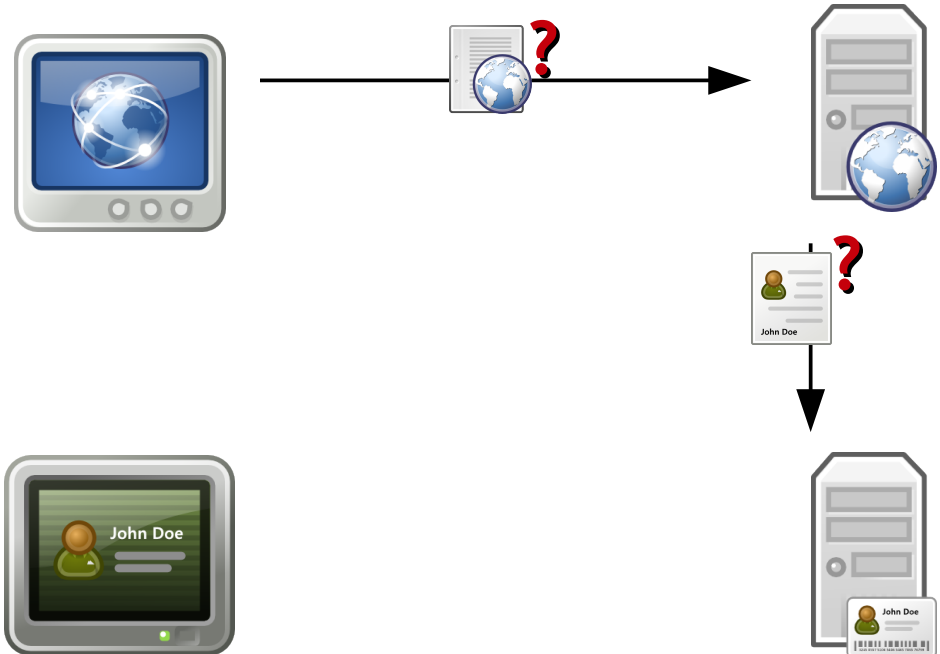
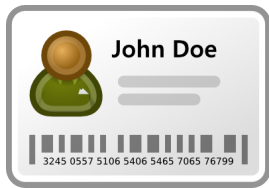
# Ablauf von eID



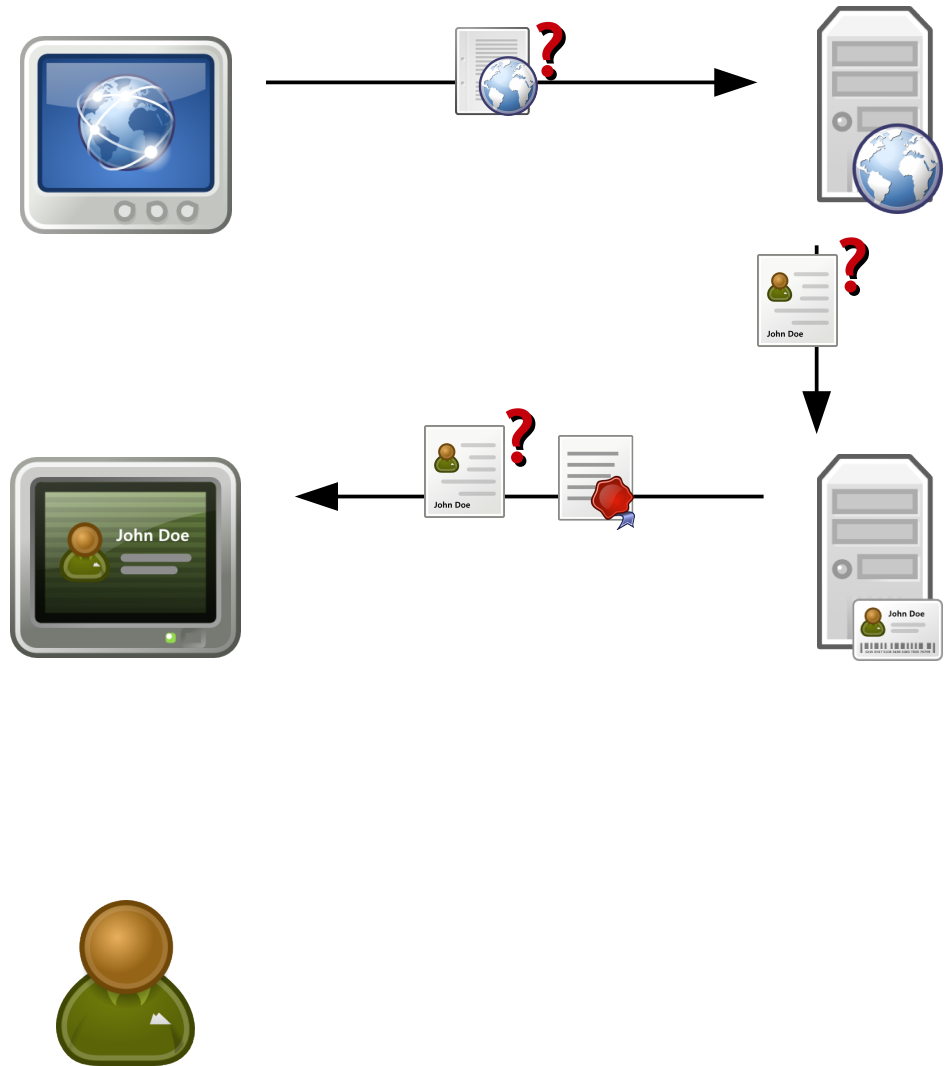
# Ablauf von eID



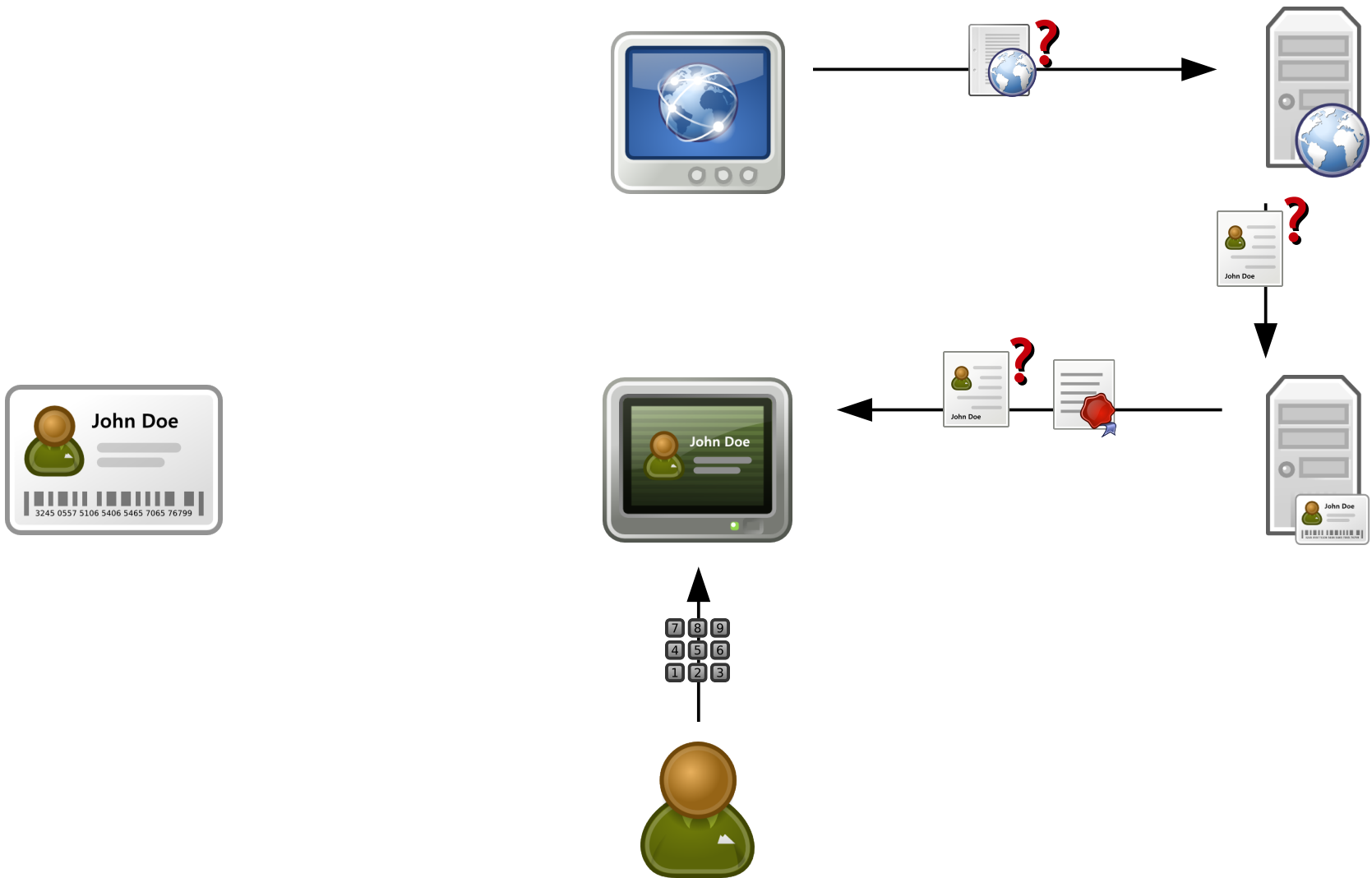
# Ablauf von eID



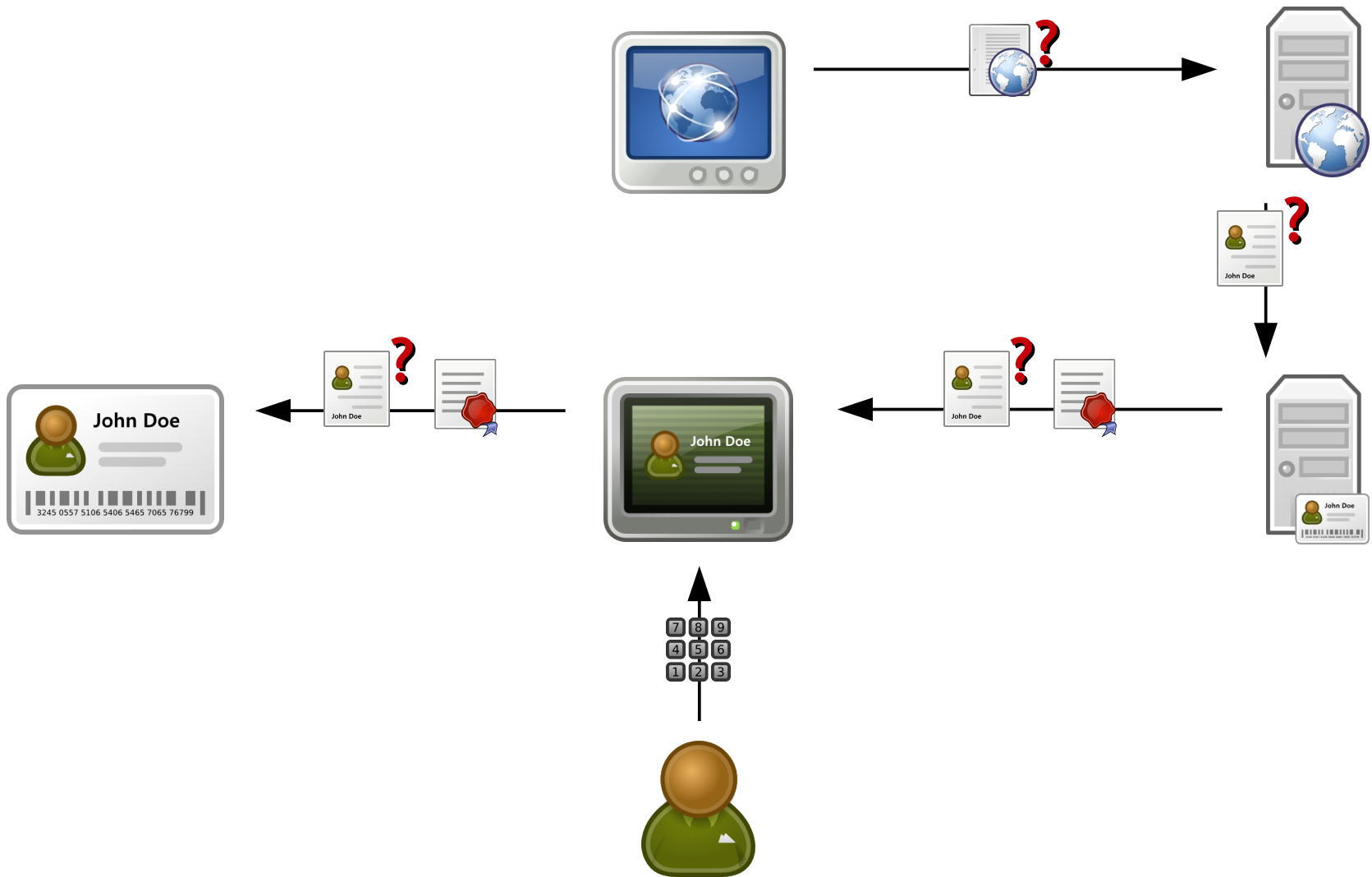
# Ablauf von eID



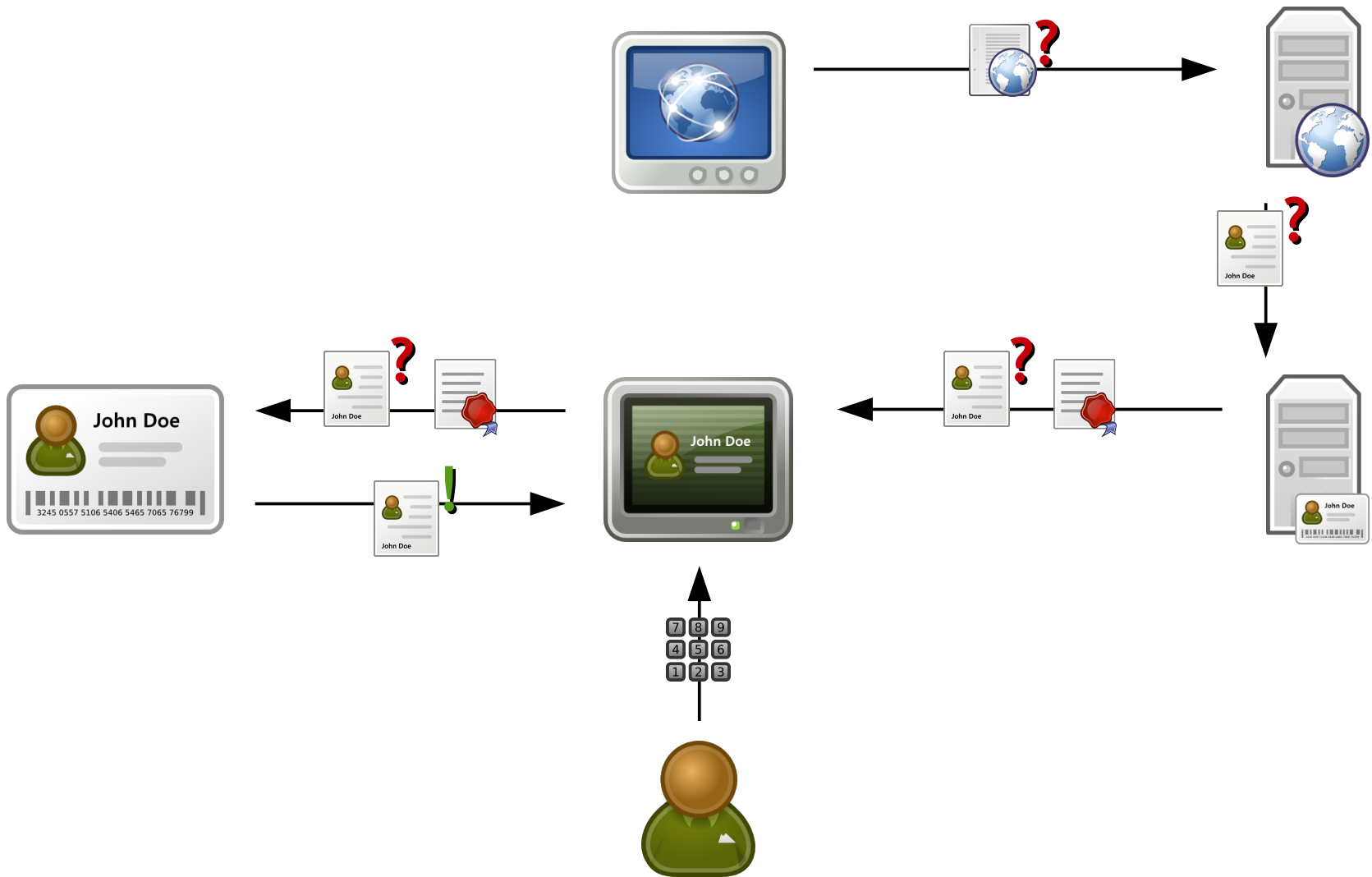
# Ablauf von eID



# Ablauf von eID

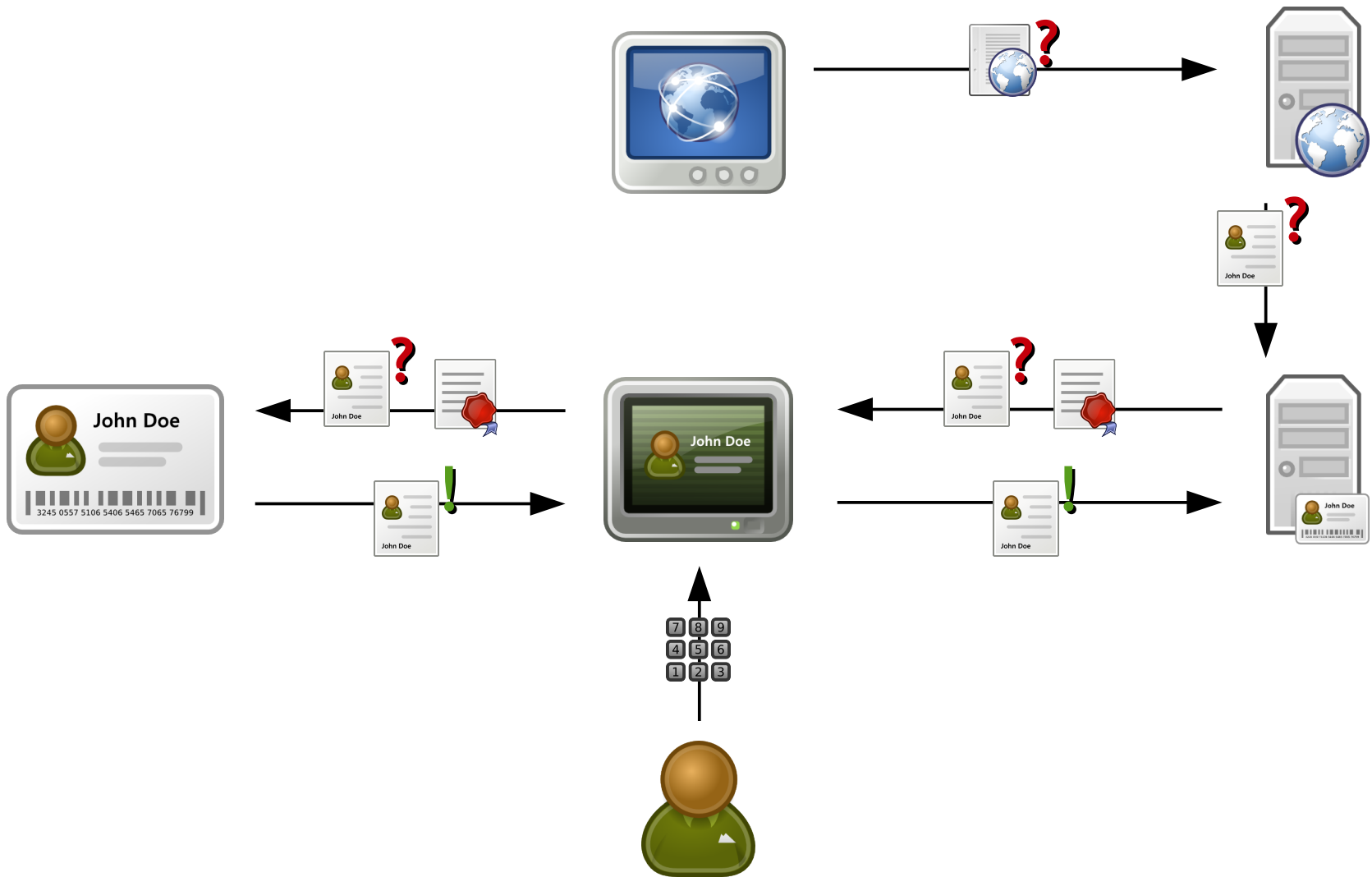


# Ablauf von eID

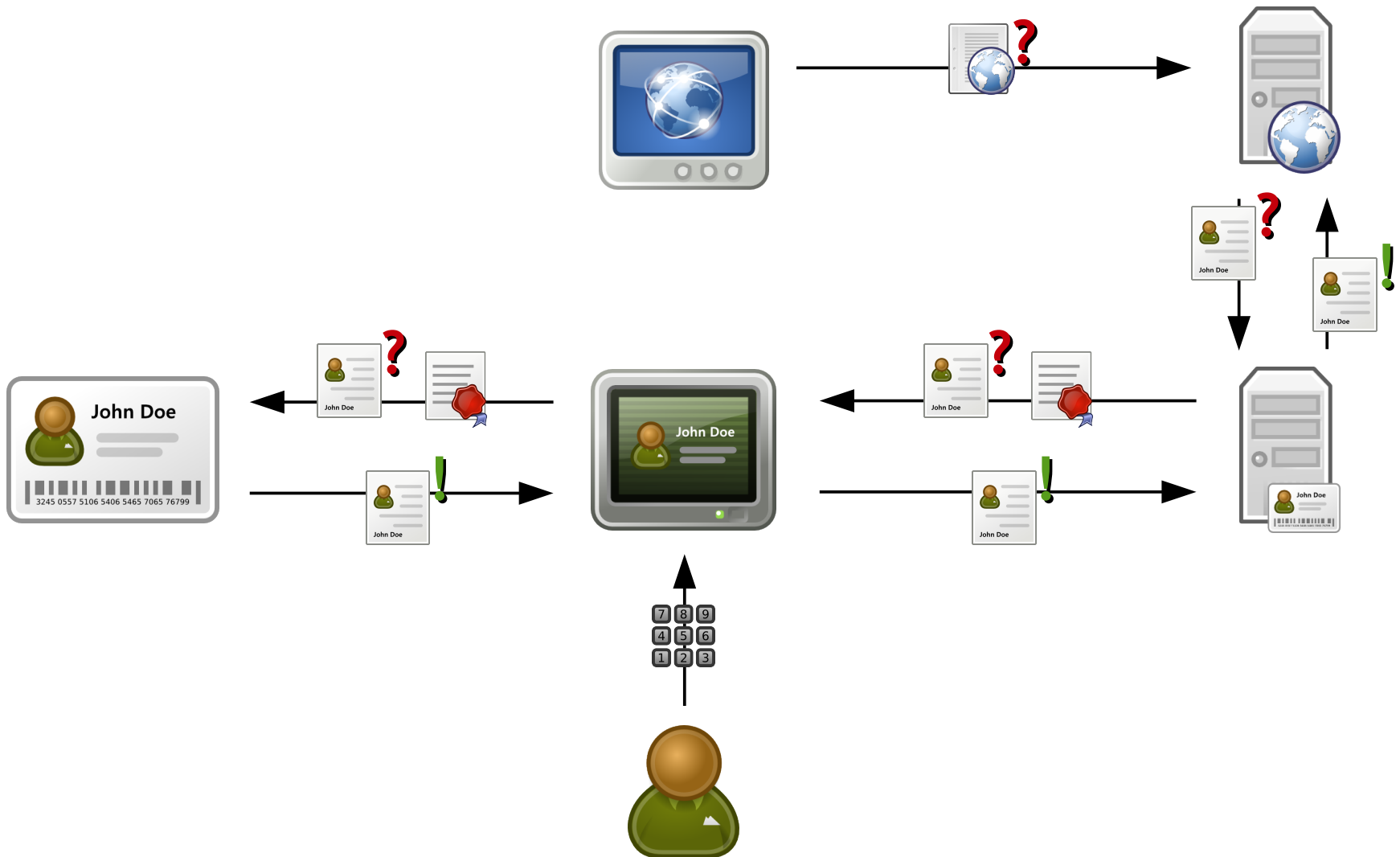




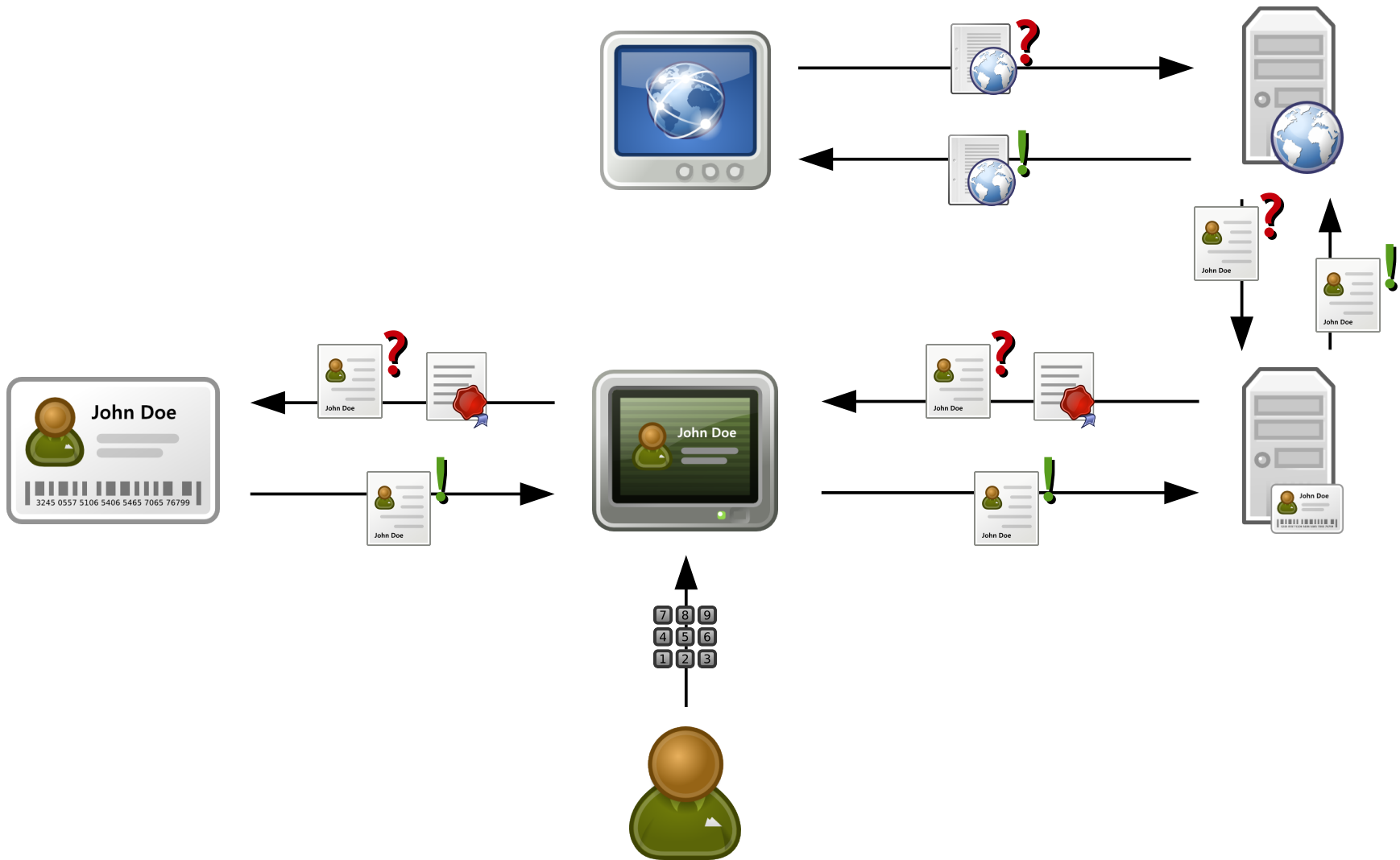
# Ablauf von eID



# Ablauf von eID



# Ablauf von eID



# Agenda

1. Grundlagen zum neuen Personalausweis & eID
- 2. Aspekte von Open Source**
3. eID-Client „rosecat“

# Open Source nach der Open Source Initiative

- Quellcode für jeden frei
  - zugänglich
  - nachvollziehbar
  - modifizierbar
  - verteilbar



# Technische Vorteile

- Aspekt
  - Testen als Teil der Softwareentwicklung
- Open Source ermöglicht
  - intensives Testen und Untersuchen für alle
- Voraussetzung
  - gute Dokumentation der Software



# Rechtliche Vorteile

- Aspekt
  - Recht auf informationelle Selbstbestimmung
- Open Source ermöglicht
  - transparentere Datenverarbeitung
- Voraussetzung
  - gute Dokumentation der Software



# Vorteile im E-Government

- Aspekt
  - sicherheitskritische Datenverarbeitung
- Open Source ermöglicht
  - mehr Vertrauen durch besseres Verständnis
- Voraussetzung
  - gute Dokumentation der Software





# Agenda

1. Grundlagen zum neuen Personalausweis & eID
2. Aspekte von Open Source
- 3. eID-Client „rosecat“**

# Forschungsprojekt

- Ziel
  - mehr Transparenz bei eID
- erster Schritt
  - eID-Client als Open Source



# rosecat

**rosecat Open Source eID Client attains transparency**

- Open-Source-eID-Client
- aktuell in Entwicklung

# Prototypische GUI

**Simulator Client (Chip + Local Terminal)**

Datei Einstellungen Ansicht Hilfe

Chip

Ausweis auf Lesegerät

**PACE**

**TA**

**CA**

Wissen des Chip

eID-Request	eID-Request: Alter >= 18 Jahre?	
eID-Pin	123456	Dpicc 89-43-4B-5B-18-7A-57-
s	1650577885546851132	eDpicc 97-1D-A8-B9-53-E0-00-
z	8943444628097641276	eSKpicc 48-5A-3F-4B-D9-09-64-
ePKpcd	8B-8E-22-BF-80-6B-C9-BF-	ePKpicc 8D-44-AE-D6-A2-A2-07-
geheimer Schlüssel K	64-04-F0-29-BE-5A-9E-00-1E-12-0F-3	
Kenc	5C-47-10-7F-C1-85-B1-A4-	Kmac 3C-2F-88-FA-7C-AD-E2-
Tpicc	70-37-47-BF-A8-9A-06-1E-	Tpcd AD-11-43-46-51-0F-DD-
Authentication Token Tpcd erfolgreich verifiziert		
PKpcd	7C-47-C1-D6-8A-94-22-	Terminal-Zertifikat 7C-47-C1-D6-8A-94-22-2B-C7-00-0D-C8-B6-13-
RT-Zertifikat verifiziert		
H(ePKpcd)	5D-7F-01-C2-23-D9-52-	Chall. r 56-89-06-7D-E9-16-42-
Signatur TA erfolgreich verifiziert		
PKpicc	B9-1F-88-55-F4-C6-0C-71-	ePKpcd CA E4-5F-AD-1E-CA-B9-16-
geheimer Schlüssel K CA	0C-84-E0-E5-37-DC-4F-82-52-65-EA-	
Kenc CA	EF-EC-B4-2C-9A-28-04-F5-	Kmac CA 6F-E2-23-9F-64-D7-51-
Chip-Authentication-Token	4D-14-C1-C5-DE-95-F0-89-09-17-9F-7	

Client zurücksetzen

Local Terminal

mit Server verbinden Serveradresse: 127.0.0.1 Port: 13000

Statusmeldungen

...mit Server verbunden  
PIN 123456 eingegeben.  
..PACE hergestellt  
..PACE hergestellt  
TA gestartet.  
TA erfolgreich beendet.  
CA gestartet.  
CA erfolgreich beendet.

Pinpad

\*\*\*\*\*

1 2 3 Abbruch

4 5 6 Korrektur

7 8 9

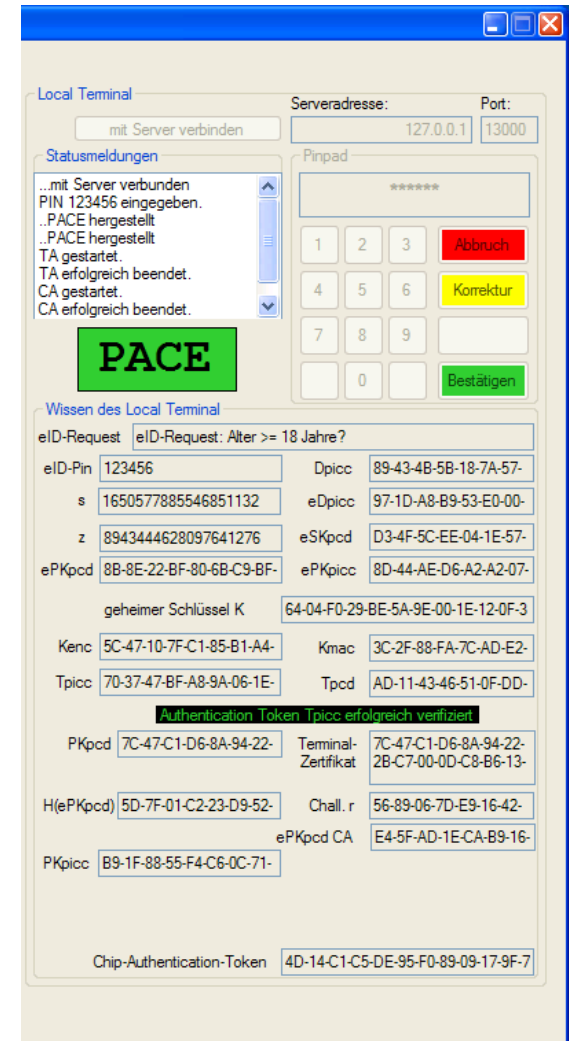
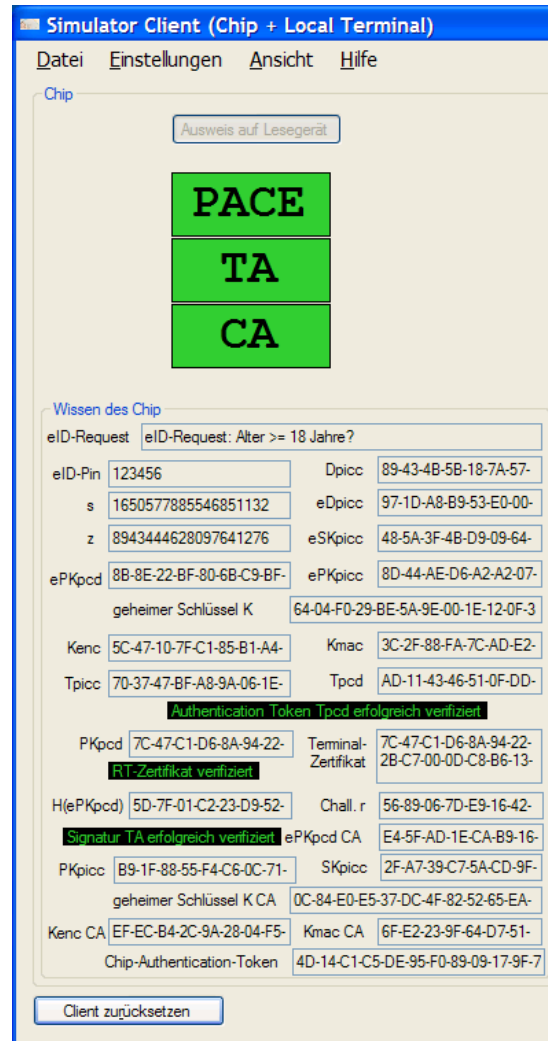
0 Bestätigen

**PACE**

Wissen des Local Terminal

eID-Request	eID-Request: Alter >= 18 Jahre?	
eID-Pin	123456	Dpicc 89-43-4B-5B-18-7A-57-
s	1650577885546851132	eDpicc 97-1D-A8-B9-53-E0-00-
z	8943444628097641276	eSKpcd D3-4F-5C-EE-04-1E-57-
ePKpcd	8B-8E-22-BF-80-6B-C9-BF-	ePKpicc 8D-44-AE-D6-A2-A2-07-
geheimer Schlüssel K	64-04-F0-29-BE-5A-9E-00-1E-12-0F-3	
Kenc	5C-47-10-7F-C1-85-B1-A4-	Kmac 3C-2F-88-FA-7C-AD-E2-
Tpicc	70-37-47-BF-A8-9A-06-1E-	Tpcd AD-11-43-46-51-0F-DD-
Authentication Token Tpicc erfolgreich verifiziert		
PKpcd	7C-47-C1-D6-8A-94-22-	Terminal-Zertifikat 7C-47-C1-D6-8A-94-22-2B-C7-00-0D-C8-B6-13-
H(ePKpcd)	5D-7F-01-C2-23-D9-52-	Chall. r 56-89-06-7D-E9-16-42-
PKpicc	B9-1F-88-55-F4-C6-0C-71-	ePKpcd CA E4-5F-AD-1E-CA-B9-16-
Chip-Authentication-Token	4D-14-C1-C5-DE-95-F0-89-09-17-9F-7	

# Prototypische GUI



# Ausblick

- Usability?
- E-Learning?
- Privacy Manager?

Danke, Ende.

# Literaturhinweise

Open Source Initiative (OSI): The Open Source Definition.

<http://www.opensource.org/docs/osd>; zuletzt abgerufen am 22.03.2010

Bundesamt für Sicherheit in der Informationstechnik: Technische Richtlinie TR-03127 – Architektur Elektronischer Personalausweis. Bonn, 2009.

Hansen, M.; Köhntopp, K.; Pfitzmann, A.: The Open Source approach – opportunities and limitations with respect to security and privacy. In: Computers & Security, Vol 21, No 5. Elsevier, München, 2002; S. 461-471.

McGaley, M.; McCarthy, J.: Transparency and e-Voting: Democratic vs. commercial interests. In (Prosser, A.; Krimmer, R. Hrsg.): Proc. of the 1st International Workshop on Electronic Voting, Bregenz 2004. Gesellschaft für Informatik, Bonn, 2004; S. 153-163.

Riedl, R.: Rethinking Trust and Confidence in European E-Government. In: Building the E-Service Society. Springer-Verlag, Boston, 2004; S. 89-108.



# Bildnachweise

Folien 4-7 (neuer PA)

[http://www.cio.bund.de/cae/servlet/contentblob/366776/poster/17408/cebit\\_2009\\_epa\\_leporello.jpg](http://www.cio.bund.de/cae/servlet/contentblob/366776/poster/17408/cebit_2009_epa_leporello.jpg)

Folien 8-27, 30, 34 (sämtliche Abbildungen)

Icons aus der freien Tango-Bibliothek, Version 0.8.90, stellenweise mit eigenen Nachbearbeitungen

[http://tango.freedesktop.org/Tango\\_Icon\\_Library](http://tango.freedesktop.org/Tango_Icon_Library)

Folie 29 (OSI-Logo)

<http://www.opensource.org/trademarks/opensource/OSI-logo-300x352.png>

Folie 31 (Waage)

eigener Entwurf

Folie 32 (Gebäude)

modifizierte Fassung eines Public-Domain-Icons

<http://www.clker.com/clipart-3828.html>

Folien 36, 37 (GUI)

selbsterstellter Screenshot der entwickelten GUI