Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Online-Ausweisfunktion anbinden – aber sicher!

AusweisApp2-Webinar: Best Practices für bestehende & zukünftige Anbieter der eID

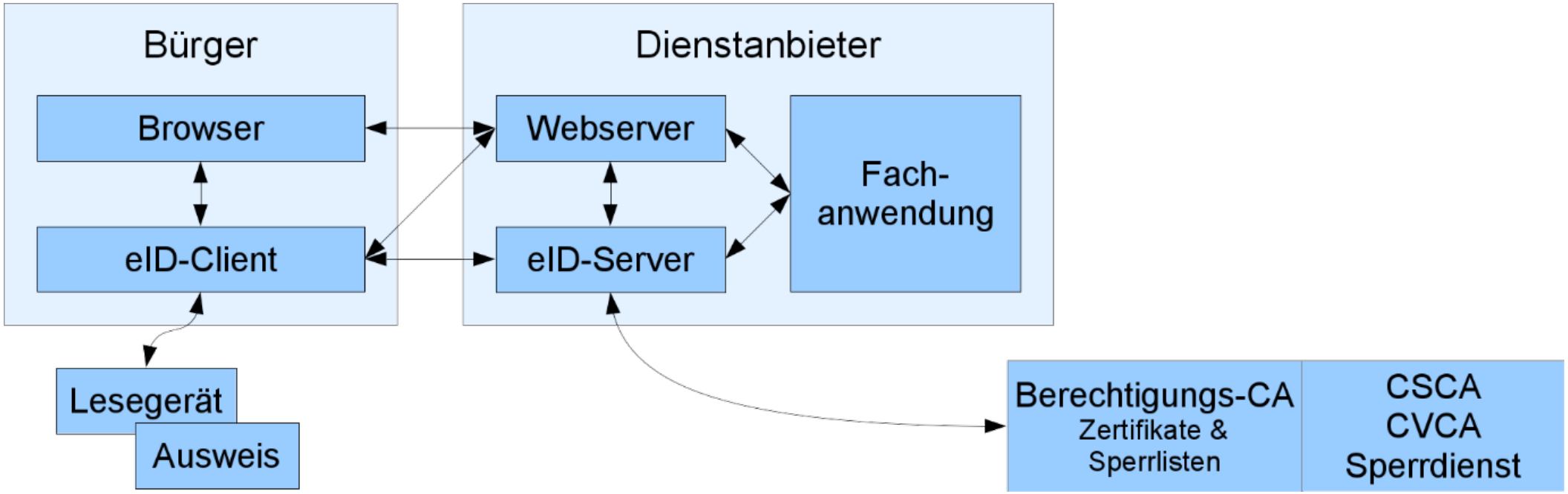
03. März 2022

Dr. Niels Räth
Bundesamt für Sicherheit in der Informationstechnik

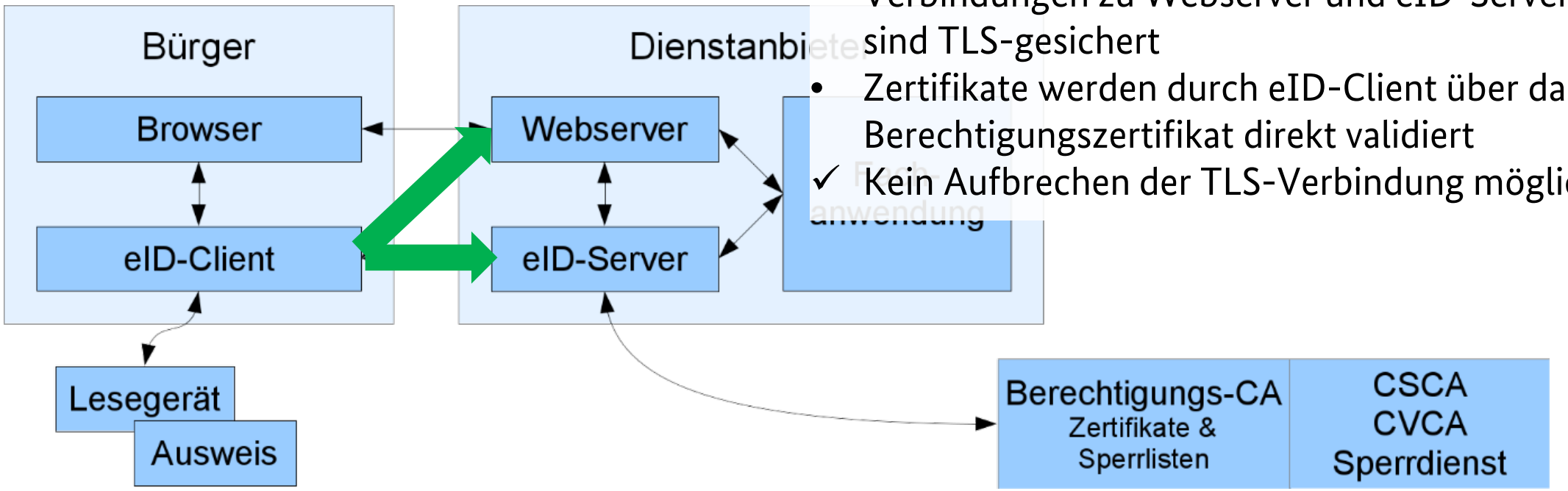
Wesentliche Sicherheitsmechanismen der Online-Ausweisfunktion

- Verifizierung der TLS-Endpunkte
- Gegenseitige Authentisierung
- Ende-zu-Ende Verschlüsselungen der Personendaten
- Sicherer Rücksprung zum Dienst (Kanalbindung)

Komponenten der Online-Ausweisfunktion



Verifizierung der TLS-Endpunkte



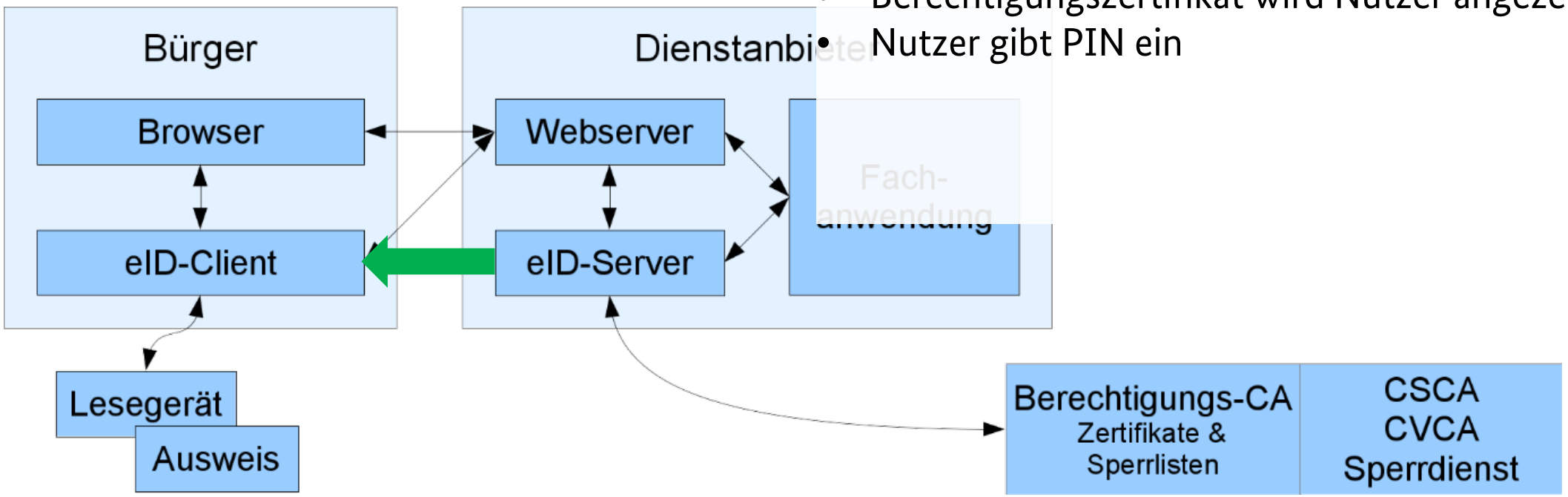
- Verbindungen zu Webserver und eID-Server sind TLS-gesichert
- Zertifikate werden durch eID-Client über das Berechtigungszertifikat direkt validiert

✓ Kein Aufbrechen der TLS-Verbindung möglich*

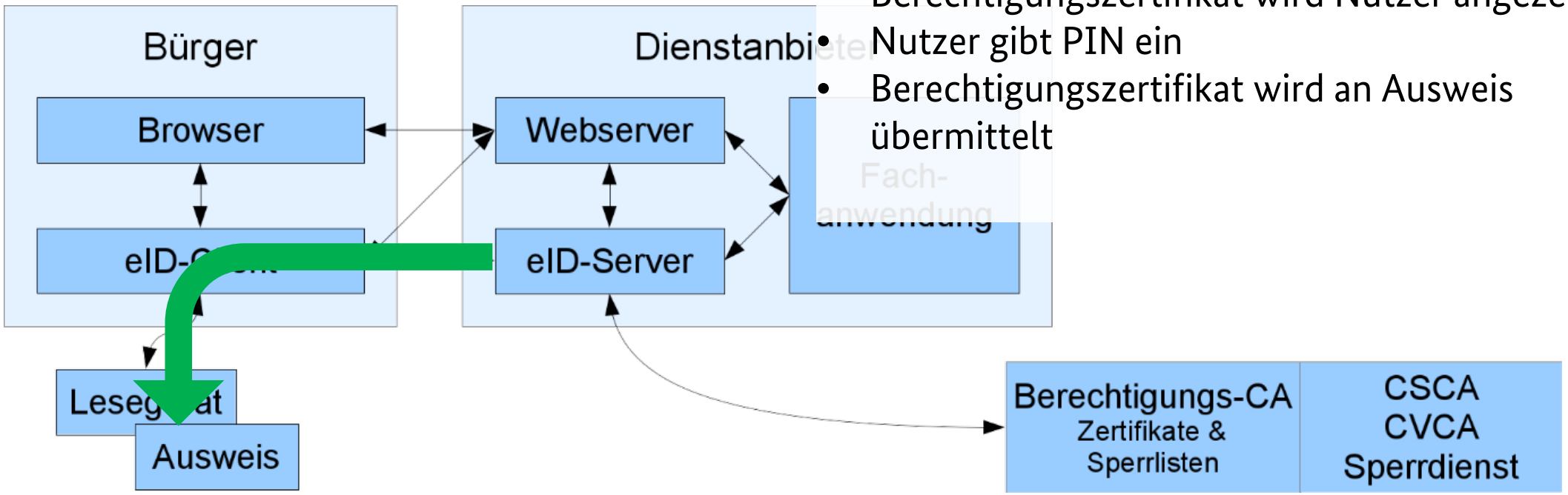
* z.B. durch Proxy, Virenschutz oder Angreifer

Gegenseitige Authentisierung

- Berechtigungszertifikat wird Nutzer angezeigt
- Nutzer gibt PIN ein

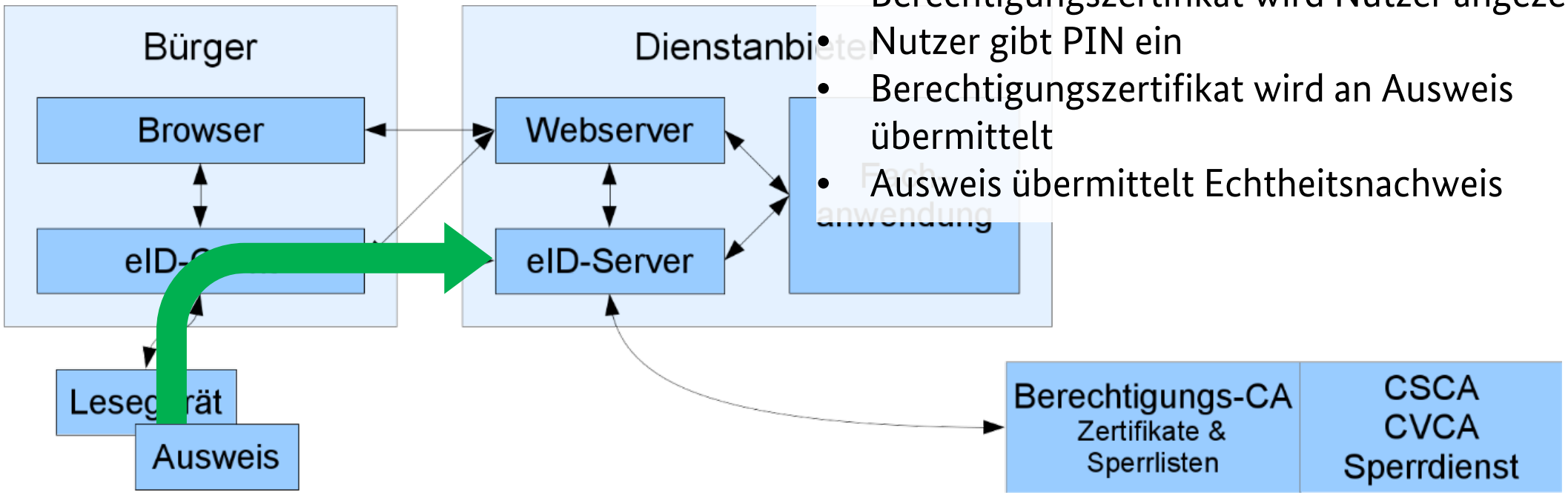


Gegenseitige Authentisierung



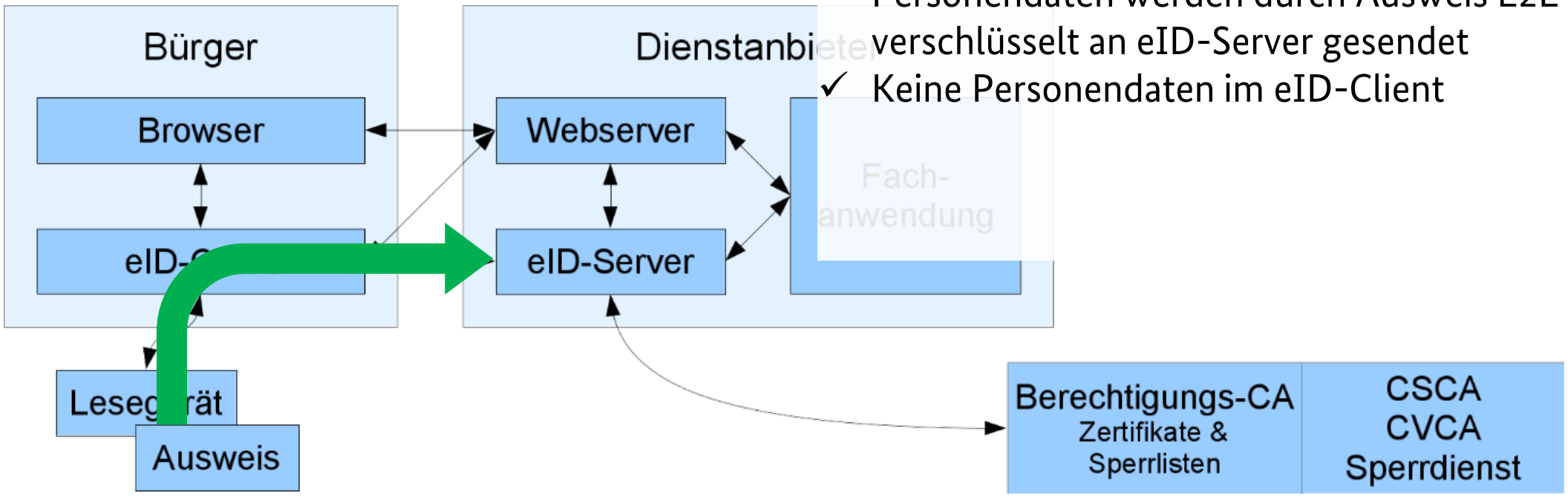
- Berechtigungszertifikat wird Nutzer angezeigt
- Nutzer gibt PIN ein
- Berechtigungszertifikat wird an Ausweis übermittelt

Gegenseitige Authentisierung



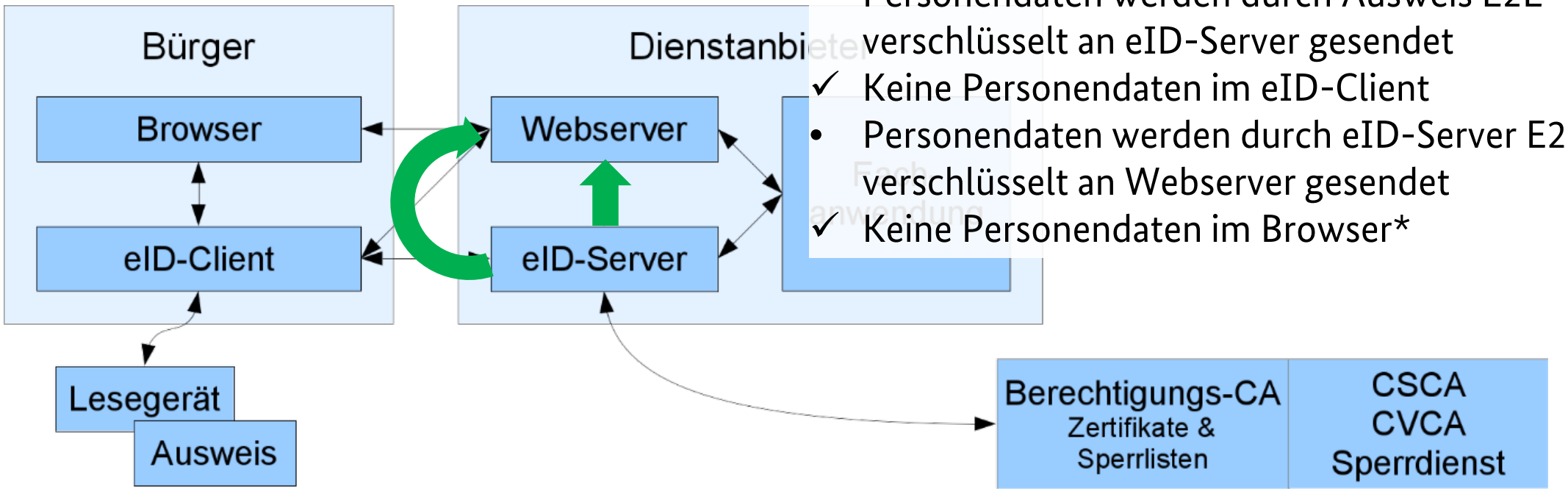
- Berechtigungszertifikat wird Nutzer angezeigt
- Nutzer gibt PIN ein
- Berechtigungszertifikat wird an Ausweis übermittelt
- Ausweis übermittelt Echtheitsnachweis

Ende-zu-Ende Verschlüsselungen der Personendaten



- Personendaten werden durch Ausweis E2E-verschlüsselt an eID-Server gesendet
- ✓ Keine Personendaten im eID-Client

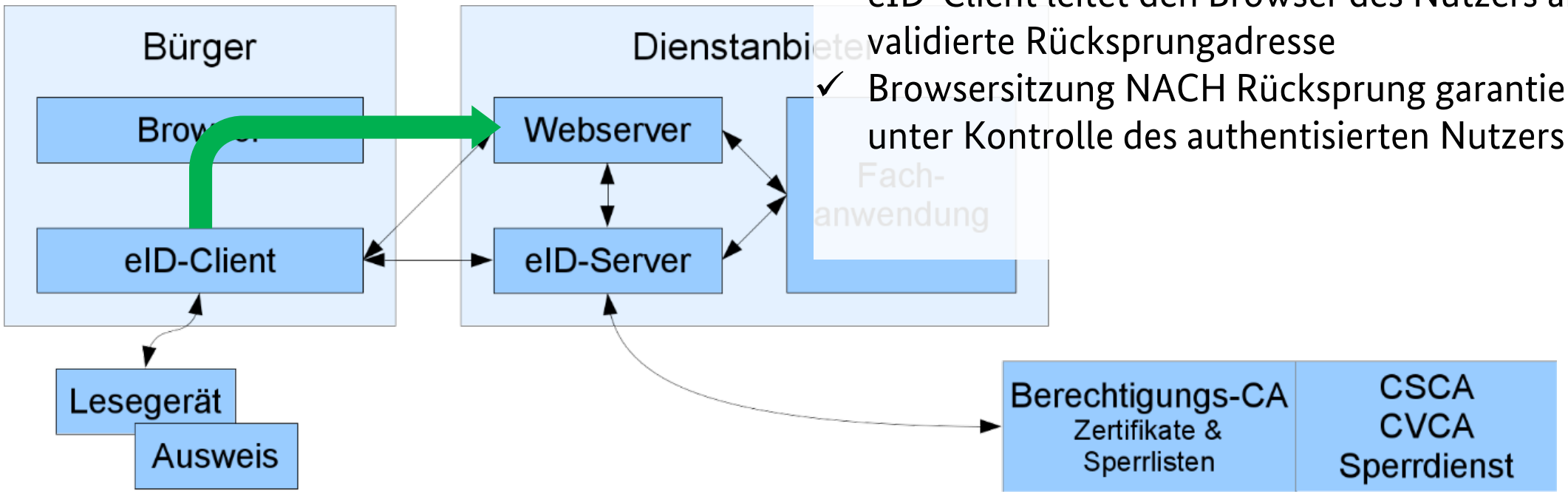
Ende-zu-Ende Verschlüsselungen der Personendaten



- Personendaten werden durch Ausweis E2E-verschlüsselt an eID-Server gesendet
- ✓ Keine Personendaten im eID-Client
- Personendaten werden durch eID-Server E2E-verschlüsselt an Webserver gesendet
- ✓ Keine Personendaten im Browser*

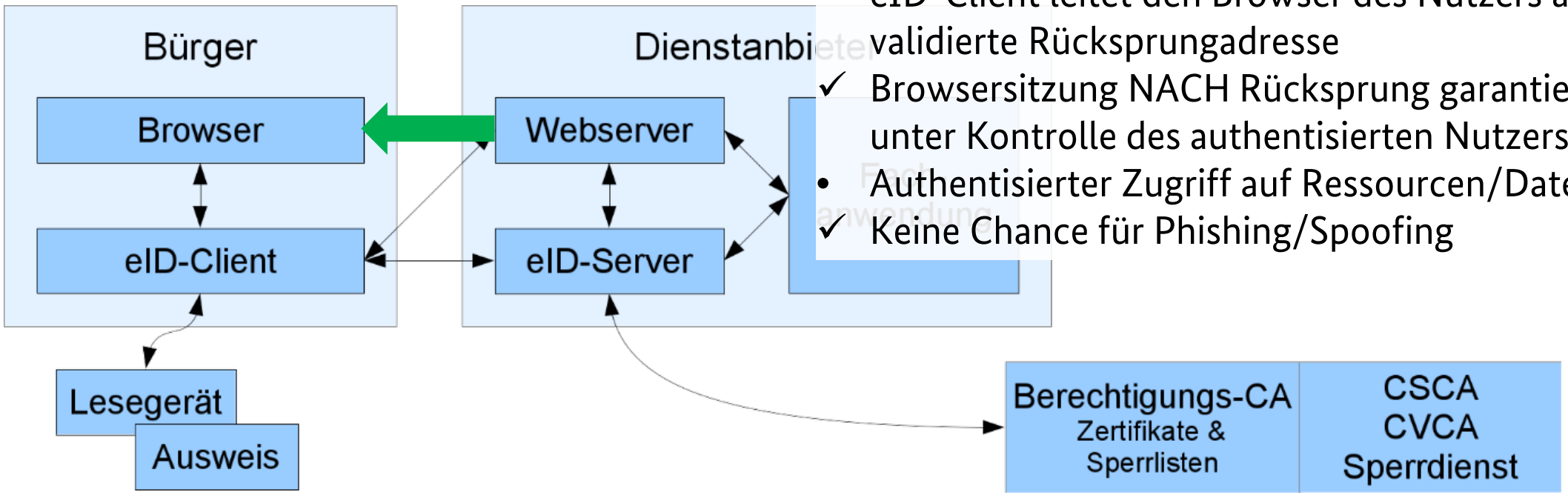
* abhängig von der Implementierung des Webdienstes

Sicherer Rücksprung zum Dienst (Kanalbindung)



- eID-Client leitet den Browser des Nutzers an validierte Rücksprungadresse
- ✓ Browsersitzung NACH Rücksprung garantiert unter Kontrolle des authentisierten Nutzers

Sicherer Rücksprung zum Dienst (Kanalbindung)



- eID-Client leitet den Browser des Nutzers an validierte Rücksprungadresse
- ✓ Browsersitzung NACH Rücksprung garantiert unter Kontrolle des authentisierten Nutzers
- Authentisierter Zugriff auf Ressourcen/Daten*
- ✓ Keine Chance für Phishing/Spoofing

*darf NUR für die durch den Rücksprung aufgebaute Verbindung gelten

Fazit

- Online-Ausweisfunktion in sich praktisch „bullet-proof“
- Bei Anbindung und Gestaltung der daran anknüpfenden Systeme jedoch darauf achten, die inhärenten Sicherheitsfunktionen nicht zu unterlaufen
- Insbesondere die sichere Rücksprungsfunktionalität nicht „umgehen“, sondern mit Mehrwert nutzen
- Sicherheitsempfehlungen aus den BSI TR und Best Practices der Protokolle umsetzen
  - BSI TR-03128-1
  - BSI TR-03124-1
  - BSI TR-03130-1
  - BSI TR-03116-4
  - SOAP/SAML/OIDC

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt

Niels Räth

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189
53175 Bonn
Tel. +49 (0) 22899 9582-0
www.bsi.bund.de
niels.raeth@bsi.bund.de

Bundesamt
für Sicherheit in der
Informationstechnik