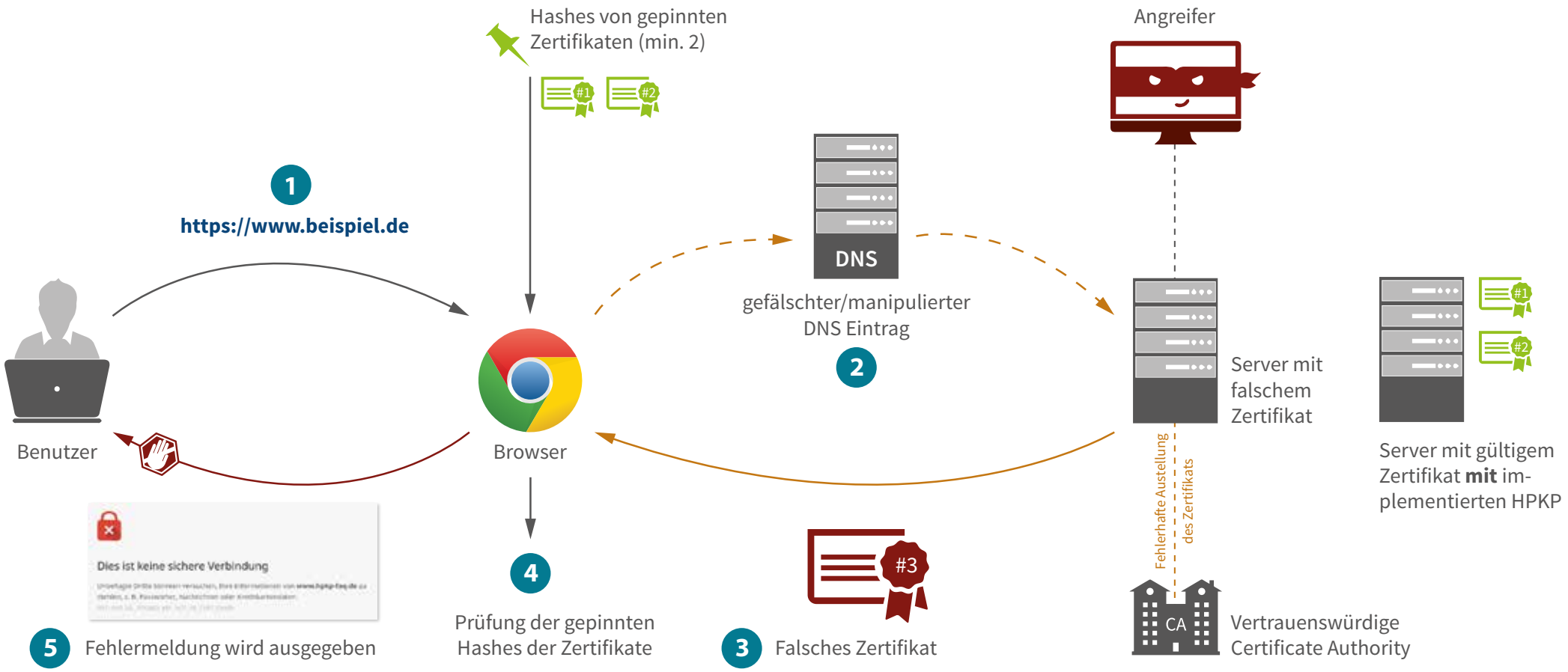
PSW GROUP



Puplic-Key-Pinning

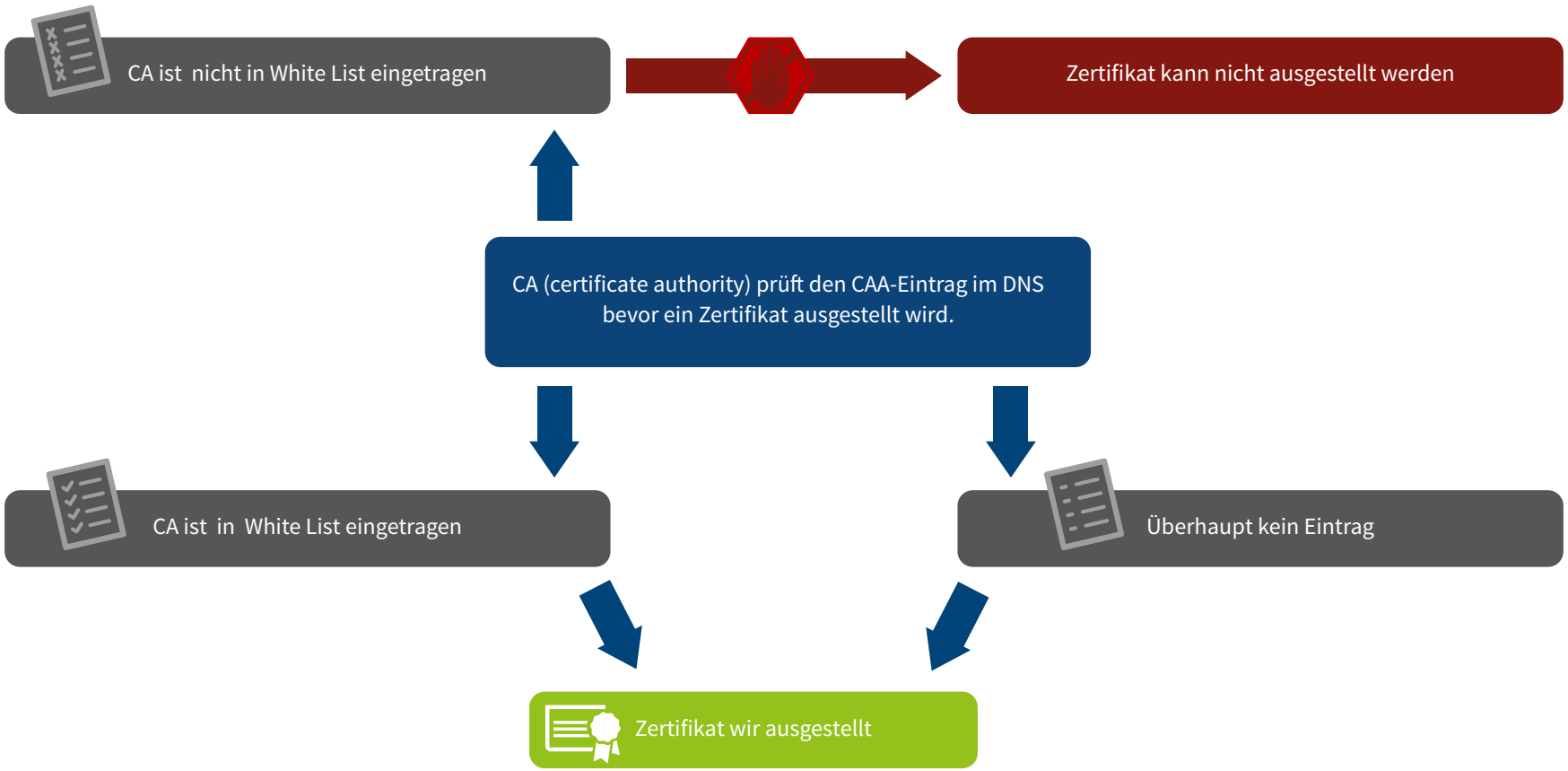
Pro

- Zertifikat kann nicht einfach unbemerkt durch ein anderes Zertifikat ausgetauscht werden, da es lokal gespeichert wird
- Erschwert das Abhören von sicheren SSL/TLS-Verbindungen

Kontra

- kein einheitliches Verfahren
- unterschiedliche Funktionsweise je nach Browser oder Betriebssystem, teilweise gar keine Unterstützung

PSW GROUP



Certification Authority Authorization

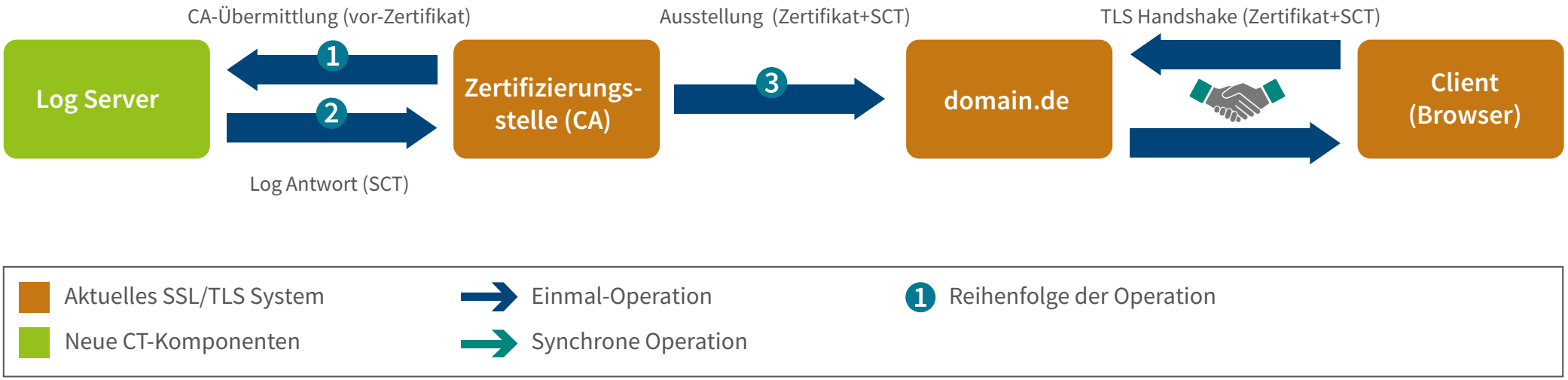
Pro

- Meldemechanismen können Websitebesitzer warnen, wenn ein falsches Zertifikat ausgestellt wird
- Verhindert Ausgabe von falschen Zertifikaten
- Erfordert keine Änderungen im Browser
- Keine hohen Implementierungskosten

Kontra

- Koordinationsprobleme durch mehrere Administratoren
- Nicht jede CA unterstützt DNS-Implementierung

PSW GROUP



Certificate Transparency

Pro

- Überprüfungs- und Überwachungssystem auf frei zugängliche und öffentlichen CT-Logs
- Keine nachträgliche Veränderung, Ergänzung oder sonstige Manipulation möglich
- Keine Ausstellung eines Zertifikats, ohne dass es für den Eigentümer der Domain sichtbar ist
- Identifizierung von fehlerhaft arbeitenden CAs

Kontra

- Problem der Sicherstellung des Datenschutzes
- Löst nicht die Problematik der falsch ausgestellten Zertifikate, ermittelt diese aber wesentlich einfacher
- Auch selbst signierte Zertifikate werden ausgegeben
- Nur für Google´s Browser Chrome
- Verhindert keine MITM-Angriffe