Beim vorliegenden Dokument handelt es sich um einen Entwurf der gematik in Vorbereitung auf zukünftige normative Festlegungen als Grundlage entsprechender Zulassungs- und Bestätigungsverfahren. Die gematik veröffentlicht diesen Entwurf mit dem Ziel, dass sich Interessierte bereits frühzeitig einen Überblick über die mögliche Weiterentwicklung der Telematikinfrastruktur verschaffen können. Die gematik übernimmt keine Gewähr für die Aktualität, Richtigkeit und Vollständigkeit dieses Entwurfes und behält sich das Recht vor, ohne vorherige Ankündigung Änderungen oder Ergänzungen vorzunehmen oder von den Regelungen insgesamt bzw. teilweise Abstand zu nehmen.

Änderungsbedarf in gemSpec_Kon

3.5.3 Unterstützung von Webanwendungen

Damit die für die Clientsystemschnittstelle definierten Web-Services auch von einer Webanwendung aus einem Webbrowser heraus genutzt werden können, unterstützt der Konnektor den Cross-Origin Resource Sharing (CORS) Mechanismus. Hierbei signalisiert der Konnektor einem auf die für die Clientsystemschnittstelle definierten Web-Services zugreifenden Browser, dass für Webanwendungen aus im Konnektor festgelegten Quellen (ORIGINs) der Browser Zugriffe auf den Konnektor zulassen soll, die a priori durch die Same-Origin-Policy des Browsers untersagt wären.

⌦ TIP1-A_6727 Cross-Origin Resource Sharing

Der Konnektor MUSS Cross-Origin Resource Sharing gemäß [CORS] für sämtliche für die Clientsystemschnittstelle definierten Web-Services unterstützen.

Dabei MUSS der Konnektor über den Access-Controll-Allow-Origin HTTP-Header ausschließlich explizit zugelassenen ORIGINs den Zugriff auf explizit zugelassene Operationen erlauben. Der Konnektor DARF NICHT über den Eintrag `"*"` im Access-Controll-Allow-Origin HTTP-Header den Zugriff über jede ORIGIN ermöglichen.

Explizit zugelassene ORIGINs sind alle ORIGINS, die sämtliche der folgenden Bedingungen erfüllen:

- ORIGIN, wie vom Aufrufer angegeben
- ORIGIN ist gemäß [RFC3986] wie folgt definiert: „https://<host>[:<port>]“
- <host> ist ein FQDN aus dem Namensraum der TI, d.h. er hat die Top Level Domain DNS_TOP_LEVEL_DOMAIN_TI

Explizit zugelassene Operationen sind alle in TAB_KON_803 aufgeführten Operationen.

Tabelle 1: TAB_KON_803 Erlaubte Operationen beim CORS-Zugriff

Name des Service	Operation
`ConnectorServiceDirectory`	`GET /connector.sds`
`EventService`	`GetLeCards`
`AuthSignatureService`	`ExternalAuthenticate`
`CertificateService`	`ReadCardCertificate`
`CardService`	`GetPinStatus`
`CardService`	`VerifyPin`

Der Konnektor MUSS bei Responses auf Cross-Origin Requests den HTTP-Header so zurückgeben, dass kein Caching der Antwort beim Browser erfolgt (z.B. Cache-Control: no-cache).

Der Konnektor MUSS bei Responses auf Cross-Origin Requests den HTTP-Header `Access-Control-Allow-Credentials: true` setzen, wenn im Konnektor `ANCL_CAUT_MANDATORY=Enabled` konfiguriert ist.⌫

Hinweis: CORS hat keinen Einfluss auf den HTTP-Body der Request-, Reply- und Fault-Nachrichten. CORS hat lediglich Einfluss auf die Header der bestehenden Nachrichten. Im Rahmen von [CORS] müssen außerdem CORS-spezifische Preflight-Requests bearbeitet werden.

3.5.5 Betriebsaspekte

⌦ **TIP1-A_7223 Aktivieren/Deaktivieren von CORS**

Die Managementschnittstelle MUSS es einem Administrator ermöglichen, die Funktionalität Cross-Origin Resource Sharing [CORS] zu aktivieren bzw. zu deaktivieren gemäß TAB_KON_847 Konfigurationswerte CORS.

Tabelle 2: TAB_KON_847 Konfigurationswerte CORS

ReferenzID	Belegung	Bedeutung und Administrator-Interaktion
`CORS_Mode`	`Enabled/Disabled`	Der Administrator MUSS CORS aktivieren bzw. deaktivieren können. ~~`En`~~`Disabled`: Cross-Origin Resource Sharing gemäß [CORS] ist für die Web-Services der Clientsystemschnittstelle NICHT erlaubt. ~~`Dis`~~`Enabled`: Cross-Origin Resource Sharing gemäß [CORS] ist für die erlaubten Operationen der Clientsystemschnittstelle gemäß TAB_KON_803 erlaubt. Default-Wert: ~~En~~Disabled

⌫