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:

6.4 Identitäten der KTR-AdV

Die KTR-AdV benötigt zwei Rollen mit entsprechenden Identitäten zur Abbildung der oben genannten Anwendungsfälle. Als Kostenträgerorganisation soll sie dem Versicherten Zugriffsrechte auf seiner eGK zur Durchführung der AdV-Anwendungsfälle freischalten. Die Angaben zu dieser Kostenträgerorganisation werden auch zur Vervollständigung des obligatorischen eGK-Protokolleintrags verwendet.

Des Weiteren muss sich die KTR-AdV mit fachanwendungsspezifischen Fachdiensten verbinden können. Hierzu muss sie als Rechenzentrums-Consumer in einer passenden Rolle authentisiert werden.

Diese zwei Aspekte müssen in der KTR-AdV über Zertifikate abgebildet werden, deren zugehöriges kryptografisches, privates Schlüsselmaterial in der Realisierung der KTR-AdV integritätsgeschützt und zugriffsgesichert gespeichert werden muss.

⌦ **AdV-A_2513 Privates Schlüsselmaterial in HSM speichern**

Die KTR-AdV MUSS privates Schlüsselmaterial zu Zertifikaten der Rollenauthentisierung gegenüber einer eGK und des Verbindungsaufbaus zu Diensten der TI in einem HSM integritätsgeschützt und zugriffsgesichert speichern, dessen Eignung durch eine erfolgreiche Evaluierung nachgewiesen wurde. Als Evaluierungsschema kommen dabei Common Criteria, ITSEC oder Federal Information Processing Standard (FIPS) in Frage. Die Prüftiefe MUSS mindestens (a) FIPS 140-2 Level 3, (b) Common Criteria EAL 4+ mit hohem Angriffspotenzial oder (c) ITSEC E3 der Stärke „hoch“ entsprechen. ⌫

Die Anbindung an den AdV-Server in einem Rechenzentrum kann über eine herstellerspezifische Schnittstelle mit einer handelsüblichen HSM erfolgen, die die oben genannten Sicherheitsziele erfüllt. Eine Anbindung eines HSM-Bs via SICCT ist nicht zwingend erforderlich.

Falls keine SMC-B als HSM zum Einsatz kommt müssen die Zertifikate auf sichere Weise in das HSM eingebracht werden. An dieser Stelle werden keine konkreten Technologien oder Prozessschritte vorgegeben, damit der Betreiber der KTR-AdV mit einem TSP ein geeignetes Verfahren etablieren kann.

Tabelle 61: TAB_ADV_385 – Personalisierung eines HSM

Aspekt	Beschreibung
Schlüsselmaterial der KTR-AdV	Das Schlüsselmaterial wird sicher im HSM erzeugt.
	Das private Schlüsselmaterial verlässt das HSM nicht oder nur zum Zwecke eines Backups auf einem Backup-HSM, wobei die Übertragung hinsichtlich Vertraulichkeit geschützt sein muss.
Zertifikatsrequest	Die benötigten Zertifikatsrequests werden im HSM erzeugt und exportiert.
	Die Zertifikatsrequests werden unter Wahrung der Authentizität und Integrität dem TSP übermittelt.
Zertifikat	Das Zertifikat wird vom TSP zum Betreiber übermittelt.

⌦ Afo_Neu-152590 Personalisierung des HSMs

Falls der Betreiber der KTR-AdV keine SMC-B als HSM einsetzt MUSS er einen sicheren Prozess zur Personalisierung des HSMs definieren und etablieren, der die in TAB_ADV_385 genannten Aspekte beinhaltet.⌫

Falls für diesen Prozess nur eine geringe Anzahl an Instanzen erwartet wird, kann es sinnvoll sein, Teile dieses Prozesses rein organisatorisch umzusetzen. Anstelle einer technischen Schnittstelle kann dann ein papierbasiertes Verfahren eingesetzt werden.

⌦ AdV-A_2514 CV-Zertifikat für eGK-Freischaltung

Die KTR-AdV MUSS über ein CV-Zertifikat verfügen, mit dem auf einer eGK Zugriffsrechte für KTR-AdV-Anwendungsfälle in einem Authentisierungsverfahren freigeschaltet werden. ⌫

Abhängig von der Realisierung eines sicheren Zertifikatsspeichers in der KTR-AdV kann das Authentisierungsverfahren zur Freischaltung der eGK über ein Card-2-Card- oder auch Card-2-Server-Verfahren erfolgen.

⌦ AdV-A_2515 X.509-Zertifikat für TLS-gesicherte Verbindung

Die KTR-AdV MUSS über ein X.509-Zertifikat zum Zweck des TLS-Verbindungsaufbaus mit der Rolle `professionOID = OID <oid_adv_ktr>` gemäß [gemSpec_OID] verfügen, um sich gegenüber einem Fachdienst zu authentisieren, welches als C.HCI.AUT identifiziert wird. ⌫

⌦ AdV-A_2516 X.509-Zertifikat für eGK-Protokolleintrag

Die KTR-AdV MUSS über ein X.509-Zertifikat mit einem CommonName entsprechend den Vorgaben des verantwortlichen Zertifikat-Herausgebers verfügen, um einen für den Versicherten lesbaren, nachvollziehbaren Protokolleintrag auf der eGK über die Nutzung der KTR-AdV erzeugen zu können. ⌫

⌦ AdV-A_2556 nachvollziehbarer eGK-Protokolleintrag mit Bezug zum Anbieter

Der Anbieter der KTR-AdV MUSS sicherstellen, dass auf der eGK des Versicherten ein lesbarer, nachvollziehbarer Protokolleintrag mit Bezug zum Anbieter der KTR-AdV erzeugt werden kann.⌫

Der Anbieter ist in diesem Zusammenhang eine Krankenkasse, in deren Auftrag ein Betreiber die KTR-AdV eines spezifischen Herstellers den Versicherten zur Verfügung stellt. Da aus diesem Zertifikat lediglich der CommonName verwendet und kein privates Schlüsselmaterial zur Authentisierung verwendet wird, kann auf die Nutzung dieses Zertifikats verzichtet werden. Es muss jedoch sichergestellt werden, dass auf der eGK des Versicherten ein lesbarer, nachvollziehbarer Protokolleintrag mit Bezug zum Anbieter der KTR-AdV erzeugt wird.

 © gematik – öffentlich_Entwurf