
C_12431_Anlage

In diesem Änderungseintrag werden die geänderten Anforderungen in gemSpec_ZETA Dokumentenrelease 25_3 zusammengefasst.

Inhaltsverzeichnis

1 Auslistung der neuen und geänderten Anforderungen.....	2
2 Auslistung der Anforderungen mit redaktionellen Änderungen..	8
3 Auslistung der Anforderungen mit geänderten Prüfverfahren....	9

1 Auslistung der neuen und geänderten Anforderungen

Afo-ID	Titel	Beschreibung	Prüfverfahren Anzeige
A_2579 7-01	ZETA Guard- Komponenten - Health Check Schnittstelle für gematik Monitoring	Der Anbieter des TI 2.0 Dienstes MUSS die Schnittstellen zu Health Checks des ZETA Guard dem gematik Monitoring zur Verfügung stellen.	organ./ betriebl. Eignung: Anbietererklär ung, funkt. Eignung: Anbietererklär ung
A_2843 4	ZETA Guard, Verwendung externer Ingress	Der vom Hersteller des TI2.0-Dienstes bereitgestellte externe Ingress MUSS alle Festlegungen erfüllen, die der ZETA Guard Komponente Ingress zugewiesen sind.	funkt. Eignung: Test Produkt/FA (Anwendung)
A_2842 1	ZETA Guard, Service Discovery - Unterstützung If- None-Match- Header	<p>Der ZETA Guard MUSS Client-Anfragen, die den If-None-Match-Header enthalten, korrekt verarbeiten. Die nachfolgende Fallunterscheidung ist zu beachten:</p> <p>* Keine Änderung des Well-known JSON Dokuments:</p> <p>Wenn der vom ZETA Client im If-None-Match -Header gesendete ETag mit dem aktuellen ETag des Dokuments auf dem Server übereinstimmt, MUSS der ZETA Guard mit einem HTTP-Statuscode 304 (Not Modified) antworten und darf keinen Nachrichtentext senden.</p> <p>* Änderung des Well-known JSON Dokuments:</p> <p>Wenn der vom ZETA Client im If-None-Match-Header gesendete ETag nicht mit dem aktuellen ETag des Dokuments auf dem Server übereinstimmt (oder wenn der Header fehlt), MUSS der ZETA Guard mit einem HTTP-Statuscode 200 OK antworten und das vollständige, aktuelle Well-known JSON-Dokument im Nachrichtentext sowie den aktuellen ETag-Header senden.</p>	funkt. Eignung: Test Produkt/FA
A_2842 0	ZETA Guard, Service Discovery - Bereitstellung	Der ZETA Guard MUSS für jedes Well-known JSON-Dokument einen eindeutigen ETag-Header generieren und diesen gemäß [RFC 9110] in der HTTP-Antwort bei jeder Anfrage	funkt. Eignung: Test Produkt/FA

	ETag Header	bereitstellen. Bei jeder inhaltlichen Änderung oder der Repräsentation der Well-known JSON-Dokumente MUSS der ETag sich ändern.	
A_2842 2	ZETA Guard, Service Discovery - Cache-Control- Header Direktiven	Der ZETA Guard MUSS im HTTP-Response-Header zur Anfrage der Well-Known und JWKS JSON-Dokumente einen Cache-Control-Header einfügen, der die Direktiven max-age und public setzt. Die Dauer der Direktive max-age MUSS konfigurierbar sein (Default: 86400 s) .	funkt. Eignung: Test Produkt/FA
A_2843 7	ZETA Guard, Registrierung bei der gematik	Der Anbieter des TI 2.0 Dienstes MUSS den ZETA Guard Authorization Server und den Issuer des Kubernetes Cluster IDP bei der gematik registrieren.	organ./ betriebl. Eignung: Anbietererklär ung
A_2843 2	ZETA Guard, Komponenten Ingress optional	Der Ingress MUSS als optionale Komponente im ZETA Guard angeboten werden.	funkt. Eignung: Test Produkt/FA
A_2843 5	ZETA Guard, Ingress - Unterstützung Forwarded- Header	Die Komponente Ingress MUSS in jeder empfangene HTTP-Anfrage für die nachgelagerten Komponenten PDP Authorization Server und PEP HTTP Proxy den Forwarded-Header gemäß [RFC 7239] in der weitergeleiteten Anfrage hinzufügen oder aktualisieren.	funkt. Eignung: Test Produkt/FA (Anwendung)
A_2843 8	ZETA Guard, geo-redundanter Betrieb	Der Anbieter eines TI 2.0 Dienstes MUSS beim geo-redundanten Betrieb des ZETA Guard in einer Kubernetes Multi-Cluster-Umgebung folgende Bedingungen erfüllen: * Die PDP DB MUSS vom Anbieter des TI 2.0 Dienstes über alle Cluster synchronisiert bereitgestellt werden. * Die Authorization Server Instanzen müssen über einen globalen Load Balancer als ein logischer Authorization Server bereitgestellt werden.	organ./ betriebl. Eignung: Anbietererklär ung
A_2846 4	ZETA Guard, genau ein Authorization Server	Die Komponente PEP HTTP Proxy MUSS das OAuth Protected Resource Well-known so bereitstellen, dass für ZETA Clients der ZETA Guard Authorization Server als genau eine logische Komponente bereitgestellt wird (nur ein Eintrag authorization_servers im OAuth Protected Resource Well-known).	funkt. Eignung: Test Produkt/FA
A_2846 2	ZETA Guard, externer Ingress - TLS Terminierung	Der Hersteller des TI2.0-Dienstes MUSS TLS für eingehende Verbindungen von außerhalb Kubernetes für die Komponenten PEP HTTP Proxy und PDP Authorization Server an den jeweiligen Komponenten terminieren, wenn	funkt. Eignung: Test Produkt/FA (Anwendung), Sich.techn.

		ein externer Ingress zum Einsatz kommt und der ZETA Guard in einer VAU bereitgestellt wird.	Eignung: Gutachten (Anbieter)
A_2843 6	ZETA Guard, Endpunkte im Internet	Der Anbieter eines TI 2.0 Dienstes MUSS die ZETA Guard und Kubernetes Cluster Endpunkte gemäß Tab_gemSpec_ZETA_Schnittstellendefinition_ZETA_Guard im Internet bereitstellen.	funkt. Eignung: Anbietererklärung
A_2843 3	ZETA Guard, Bereitstellung externer Ingress	Der Hersteller des TI2.0-Dienstes MUSS entweder den Kubernetes Ingress des ZETA Guard oder einen eigenen Ingress verwenden.	funkt. Eignung: Test Produkt/FA (Anwendung)
A_2843 1	ZETA Guard, Ablauf Dienst- zu-Dienst Kommunikation	Der ZETA Guard MUSS den Ablauf gemäß Abbildung Abb_ZETA-Guard-Dienst-zu-Dienst-Kommunikation unterstützen.	funkt. Eignung: Test Produkt/FA
A_2840 6	ZETA Guard - Verification des ZETA-Images	Der Hersteller des TI2.0-Dienstes MUSS vor der Aktualisierung von ZETA Guard innerhalb seines Build-Systems die Authentizität und Aktualität der zu aktualisierenden Komponenten auf der Grundlage der gematik-Signatur und der Versionshistorie der Komponenten verifizieren und bei Fehlschlägen der Verifikation die Aktualisierung abbrechen und gematik umgehend informieren.	Sich.techn. Eignung: Gutachten
A_2840 5	ZETA Guard - Umwandlung für Ziel-VAU- Architektur	Falls der ZETA Guard in einer VAU umgesetzt wird, muss der Hersteller des TI2.0-Dienstes sicherstellen: * dass das ZETA Guard-Image in einer manipulationssicheren Build-Pipeline für die Ziel-VAU-Architektur erstellt und umgewandelt wird, und * dass der Build-Log sämtliche VAU-spezifischen Ergänzungen am ZETA Guard-Image protokolliert und für die gematik auditierbar ist.	Sich.techn. Eignung: Gutachten
A_2840 7	ZETA Guard - Nachweisbarkeit verwendete Version des ZETA-Images	Der Hersteller eines TI 2.0-Dienstes MUSS ein SBOM für sein Produkt erstellen, aus dem eindeutig hervorgeht, welches ursprüngliche ZETA Guard-Image verwendet wurde.	Sich.techn. Eignung: Herstellererklärung
A_2647 9-02	ZETA Guard - Ordnungsgemäße Änderung von Konfigurationen	Der Anbieter eines TI2.0 Dienstes MUSS durch technische und organisatorische Mittel sicherstellen, dass eine Änderung der Konfiguration des ZETA Guards nur unter 4-Augen erfolgen kann.	Sich.techn. Eignung: Produktgutachten, Sich.techn.

			Eignung: Gutachten (Anbieter)
A_2577 3-02	ZETA Guard - Nutzung der von der gematik bereitgestellten Container Images	Der Anbieter eines Dienstes der TI 2.0 MUSS die von der gematik bereitgestellten Container Images im ZETA Guard verwenden, um den Zugang zum TI 2.0 Dienst zu kontrollieren.	funkt. Eignung: Anbietererklä- rung
A_2845 9	ZETA Guard - Informationsobje- kte im Produkthandbuc h	Der Hersteller des ZETA Guards MUSS alle vom ZETA Guard verarbeiteten Informationsobjekte in seinem Produkthandbuch vollständig auflisten.	Sich.techn. Eignung: Herstellererklä- rung
A_2846 3	ZETA Guard - Informationsobje- kte des ZETA Clients im Produkthandbuc h	Der Hersteller des ZETA Guards MUSS alle vom ZETA Client verarbeiteten Informationsobjekte im Produkthandbuch des ZETA Guard vollständig auflisten.	Sich.techn. Eignung: Herstellererklä- rung
A_2846 0	ZETA Guard - Datenschutzrech- tliche Bewertung durch den Diensteanbieter	Der Anbieter eines TI 2.0 Dienstes MUSS sich über die Informationsobjekte, die im ZETA Guard verarbeitet werden, aus dem Produkthandbuch informieren und als Datenschutzverantwortlicher für sein Dienst bewerten.	Sich.techn. Eignung: Herstellererklä- rung (Betrieb)
A_2842 5	ZETA Client, Service Discovery - If- None-Match und ETag	Der ZETA Client MUSS bei der Abfrage der Well-known JSON-Dokumente die HTTP-Header If-None-Match und ETag verwenden.	funkt. Eignung: Test Produkt/FA
A_2842 6	ZETA Client, Service Discovery	Der ZETA Client MUSS die Well-known und JWKS JSON-Dokumente regelmäßig einmal alle 24 Stunden neu laden, wenn im HTTP-Response-Header kein Cache-Control-Header vom ZETA Guard eingefügt wurde. Der ZETA Client MUSS die Service Discovery erneut durchführen, wenn beim Kommunikationsaufbau zu den geschützten Ressourcen der HTTP-Statuscodes 404 (Not Found) empfangen wird.	funkt. Eignung: Test Produkt/FA
A_2846 5	ZETA Client, Registrierung mit mehreren ZETA Guard	Der ZETA Client MUSS in der Lage sein sich an jedem ZETA Guard zu registrieren, über den eine Kommunikation mit einem TI 2.0 Dienst erfolgen soll. Durch die Registrierung erhält der ZETA Client von jedem ZETA Guard eine spezifische client_id. Der ZETA Client MUSS die Registrierungs-Daten und Konfigurationsdaten pro TI 2.0 Dienst verwalten.	funkt. Eignung: Test Produkt/FA
A_2649	PEP HTTP Proxy	Die Komponente HTTP Proxy MUSS so	funkt.

2-01	- Weiterleitung von Client-Daten	konfiguriert werden können, dass pro Endpunkt des Resource Servers die Weiterleitung der Client-Daten durch den HTTP Proxy ein- und ausgeschaltet werden kann. Die default-Einstellung ist keine Weiterleitung der Client-Daten. Wenn die Weiterleitung der Client-Daten eingeschaltet ist, dann fragt der HTTP Proxy die Client-Daten anhand des client_id claims aus dem Access Token von der PDP-Datenbank ab und fügt sie als zusätzlichen Header in den Request ein.	Eignung: Test Produkt/FA
A_28439	PEP HTTP Proxy - Unterstützung Forwarded-Header	Die Komponente PEP HTTP Proxy MUSS in jeder empfangene HTTP-Anfrage den Forwarded-Header gemäß [RFC 7239] in der weitergeleiteten Anfragen aktualisieren.	funkt. Eignung: Test Produkt/FA
A_28440	PDP Authorization Server - Auswertung Forwarded-Header	Die Komponenten PDP Authorization Server MUSS HTTP-Anfragen mit einem vorhandenen Forwarded-Header auswerten, um die Client-IP Adresse zu ermitteln. Bei der Auswertung ist die Semantik gemäß [RFC 7239] und die* Reihenfolge der Parameter zu beachten.	funkt. Eignung: Test Produkt/FA
A_25775-01	PDP - Kontrolle des Audit-Logs	Der Anbieter des TI 2.0 Dienstes MUSS das Audit-Log des ZETA Guards mindestens alle 3 Monate im Vieraugenprinzip kontrollieren. Diese Rollen DÜRFEN NICHT an der Administration des ZETA Guards teilnehmen. Bei der Kontrolle ist insbesondere auf ungewöhnliche, nicht nachvollziehbare oder maliziöse Administratoraktivitäten zu achten.	Sich.techn. Eignung: Gutachten (Anbieter)
A_28461	Informationspflicht des Client-Herstellers gegenüber Nutzern	Der Hersteller eines TI 2.0-Clients MUSS die seine Anwendung betreffenden Informationsobjekte aus dem Produkthandbuch des ZETA Guard informieren und seine Nutzer datenschutzkonform über deren Verarbeitung informieren.	Sich.techn. Eignung: Herstellererklärung
A_27800-01	ZETA Guard, Authentifizierung und Autorisierung für stationäre Clients	Der ZETA Guard MUSS die Client-Registrierung für stationäre Clients gemäß Abbildung <i>Abb_Authentifizierung_und_Autorisierung</i> bereitstellen.	Sich.techn. Eignung: Produktgutachten
A_28480	ZETA Guard, Integration optionaler Komponenten	Der Anbieter des TI 2.0-Dienstes MUSS sicherstellen und nachweisen, dass alle Anforderungen an die optionalen ZETA Guard Komponenten erfüllt sind, wenn er eigene Lösungen dieser Komponenten anstelle der standardmäßigen ZETA Guard Installation verwendet.	organ./betriebl. Eignung: Test

2 Auslistung der Anforderungen mit redaktionellen Änderungen

- A_25401 - ZETA Guard - Darstellung der Voraussetzungen für sicheren Betrieb des Produkts im Produkthandbuch
- A_25718 - ZETA Guard - Bereitstellung Security-KPIs
- A_25762 - ZETA Client - Nutzerauthentifizierung - Unterstützung etablierter Identitäten und Dienste
- A_25338 - ZETA Client - Identifikation mittels product_id
- A_25484-01 - Security Monitoring - Security KPIs
- A_25606-01 - Security Monitoring - Fehlermeldung bei Aktualisierung von PIP-Daten oder PDP-Policies
- A_26590 - PEP HTTP Proxy - Client-Daten
- A_25644 - PDP Client-Registrierung mit Attestation
- A_25645 - PDP Authentifizierung mittels TI-Smartcard
- A_27379 - ZETA Client -OCSP Stapling Unterstützung
- A_27798 - ZETA Guard, Service Discovery

3 Auslistung der Anforderungen mit geänderten Prüfverfahren

Afo-ID	Titel	Änderung
A_25762	ZETA Client - Nutzerauthentifizierung - Unterstützung etablierter Identitäten und Dienste	Neue Zuordnung zu funkt. Eignung: Herstellererklärung
A_25338	ZETA Client - Identifikation mittels product_id	Neue Zuordnung zu funkt. Eignung: Herstellererklärung
A_25340	ZETA Client- Zertifikatsprüfung	Neue Zuordnung zu funkt. Eignung: Test Produkt/FA(PS-Schnittstelle für ZETA und ZETA Guard)
A_25734	ZETA Client - Zugriffsprotokoll Clientregistrierung	Neue Zuordnung zu funkt. Eignung: Herstellererklärung (ZETA - Anforderungen an Hersteller eines FdV, ZETA Guard, PS-Schnittstelle für ZETA) und zu Sich.techn. Eignung: Produktgutachten (ZETA Guard)
A_25732	ZETA Client - Unterstützung des Nutzers bei der Registrierung	Neue Zuordnung zu funkt. Eignung: Herstellererklärung (ZETA - Anforderungen an Hersteller eines FdV, ZETA Guard, PS-Schnittstelle für ZETA)
A_26681	ZETA Client - Umsetzen eines ZETA/ASL-Kanals	Neue Zuordnung zu Sich.techn. Eignung: Herstellererklärung (PS-Schnittstelle für ZETA) und zu Sich.techn. Eignung: Produktgutachten (ZETA Guard)
A_27378	ZETA Client - TLS	Neue Zuordnung zu Sich.techn. Eignung: Herstellererklärung (PS-Schnittstelle für ZETA, ZETA - Anforderungen an Hersteller eines FdV)
A_27379	ZETA Client - OCSP Stapling Unterstützung	Neue Zuordnung zu funkt. Eignung: Test Produkt/FA(ZETA - Anforderungen an Hersteller eines FdV, ZETA Guard, PS-Schnittstelle für ZETA)
A_25782	ZETA Client - OAuth2 Session Management	Neue Zuordnung zu unkt. Eignung: Test Produkt/FA (ZETA Guard)

A_25761	ZETA Client - Nutzerauthentifizierung mittels etablierter Standards	Neue Zuordnung zu funkt. Eignung: Herstellererklärung (ZETA - Anforderungen an Hersteller eines FdV, ZETA Guard, PS-Schnittstelle für ZETA)
A_25339	ZETA Client - Exponential Backoff	Neue Zuordnung zu funkt. Eignung: Herstellererklärung (ZETA - Anforderungen an Hersteller eines FdV, ZETA Guard, PS-Schnittstelle für ZETA)
A_25758	ZETA Client - Erfassung Kontaktinformation für Offband-Verifikation	Neue Zuordnung zu funkt. Eignung: Herstellererklärung (ZETA - Anforderungen an Hersteller eines FdV, PS-Schnittstelle für ZETA) und funkt. Eignung: Test Produkt/FA (ZETA Guard)
A_25802	ZETA Client - Einhaltung der BSI [TR-03161-1]	Neue Zuordnung zu Sich.techn. Eignung: Herstellererklärung (PS-Schnittstelle für ZETA), Entfernung Zuordnung zu Sich.techn. Eignung: Produktgutachten, Sich.techn. Eignung: Herstellererklärung (ZETA Guard)
A_25733	ZETA Client - Clientverwaltung und manuelle De-Registrierung	Neue Zuordnung zu funkt. Eignung: Herstellererklärung (ZETA - Anforderungen an Hersteller eines FdV, PS-Schnittstelle für ZETA) und funkt. Eignung: Test Produkt/FA (ZETA Guard)
A_25768	ZETA Client - Clientregistrierung mit bestätigten Umgebungseigenschaften Apple	Neue Zuordnung zu funkt. Eignung: Herstellererklärung (ZETA - Anforderungen an Hersteller eines FdV, PS-Schnittstelle für ZETA) und funkt. Eignung: Test Produkt/FA (ZETA Guard)
A_25434	ZETA Client - Clientregistrierung mit bestätigten Umgebungseigenschaften Android	Neue Zuordnung zu funkt. Eignung: Herstellererklärung (ZETA - Anforderungen an Hersteller eines FdV, PS-Schnittstelle für ZETA) und funkt. Eignung: Test Produkt/FA (ZETA Guard)
A_25767	ZETA Client - Clientkey in JWT	Neue Zuordnung zu funkt. Eignung: Herstellererklärung (ZETA - Anforderungen an Hersteller eines FdV, PS-Schnittstelle für ZETA) und funkt. Eignung: Test Produkt/FA (ZETA Guard)

A_25769	ZETA Client - Client Credentials sicher generieren und schützen	Neue Zuordnung zu funkt. Eignung: Herstellererklärung (ZETA - Anforderungen an Hersteller eines FdV, PS-Schnittstelle für ZETA) und zur Sich.techn. Eignung: Produktgutachten (ZETA Guard)
A_25770	ZETA Client - Client Credentials Rotation	Neue Zuordnung zu funkt. Eignung: Herstellererklärung (ZETA - Anforderungen an Hersteller eines FdV, PS-Schnittstelle für ZETA) und zur Sich.techn. Eignung: Produktgutachten (ZETA Guard)
A_25766	ZETA Client - Client Credentials in TI Qualität	Neue Zuordnung zu funkt. Eignung: Herstellererklärung (ZETA - Anforderungen an Hersteller eines FdV, PS-Schnittstelle für ZETA) und funkt. Eignung: Test Produkt/FA (ZETA Guard)
A_25783	ZETA Client - Anweisungen aus HTTP Response Status Codes und Header folgen	Neue Zuordnung zu funkt. Eignung: Herstellererklärung (ZETA - Anforderungen an Hersteller eines FdV)
A_25432	ZETA Client - Ablauf Clientregistrierung	Neue Zuordnung zu funkt. Eignung: Herstellererklärung (ZETA - Anforderungen an Hersteller eines FdV) und funkt. Eignung: Test Produkt/FA (PS-Schnittstelle für ZETA, ZETA Guard)
A_25427	Hersteller Clientsystem Android - Google Cloud Projekt	Neue Zuordnung zu funkt. Eignung: Herstellererklärung (ZETA Guard) und zur Sich.techn. Eignung: Herstellererklärung (PS-Schnittstelle für ZETA, ZETA - Anforderungen an Hersteller eines FdV)
A_25337	Hersteller Clientsystem - Registrierung für product_id	Neue Zuordnung zu funkt. Eignung: Herstellererklärung (PS-Schnittstelle für ZETA) und funkt. Eignung: Test Produkt/FA (ZETA Guard)
A_25336	Hersteller Clientsystem - Regelmäßige Updates	Entfernung Zuordnung funkt. Eignung: Herstellererklärung (ZETA - Anforderungen an Hersteller eines FdV, PS-Schnittstelle für ZETA, ZETA Guard)
A_25335	Hersteller Clientsystem - Hinweise und Maßnahmen sicherer Betrieb	Entfernung Zuordnung funkt. Eignung: Herstellererklärung (ZETA - Anforderungen an Hersteller eines FdV, PS-Schnittstelle für ZETA, ZETA

		Guard)
--	--	--------