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.

Diese Anlage behandelt Änderungen am normativen gematik-Dokument [gemSpec_ServiceMon] im Bereich der Probe CRL Download.

5.3 Technische Use Cases – TUCs

Die hier beschriebenen TUCs werden in Probes für wiederkehrende Abläufe genutzt.

TIP1-A_7147 - Service Monitoring, TUC_SM_001_DNS_Name_Resolution
Das Service Monitoring MUSS TUC_SM_001_DNS_Name_Resolution entsprechend Tab_Service_Monitoring_TUC_SM_001_DNS_Name_Resolutionbereitstellen. Dieser TUC MUSS in allen Probes zur DNS-Namensauflösung genutzt werden.

Tabelle 6: Tab_Service_Monitoring_TUC_SM_001_DNS_Name_Resolution

Name	TUC_SM_001_DNS_Name_Resolution	
Beschreibung	Dieser TUC führt die Auflösung eines FQDN in eine IP-Adresse durch.	
Vorbedingungen	• Keine	
Eingangsdaten	• IP-Adresse Namensdienst • Aufzulösender FQDN • Bisher ermittelte Service Monitoring Daten • Ein Flag für die DNS-Record Validierung (DNSSEC). Ist es gesetzt wird die Validierung durchgeführt.	
Komponenten	• Service Monitoring Probe, DNS-Nameserver	
Ausgangsdaten	• Aufgelöste IP-Adresse • Ermittelte Service Monitoring Daten für die DNS Namensauflösung	
Standardablauf	**Aktion**	**Beschreibung**
	IP-Adresse der Schnittstelle ermitteln	Durch eine DNS-Anfrage (I_DNS_Name_Resolution:: get_IP_Address.) wird der FQDN in eine IP-Adresse aufgelöst.
	Falls bei der DNS-Anfrage keine Antwort (und kein DNS-Fehler) ermittelt wer-	Prüfung der Erreichbarkeit des DNS-Nameserver über TUC_SM_002_Erreichbarkeitsprüfung. Der Service Monitoring Datensatz für die DNS-Namensauflösung wird in diesem Fall in TUC_SM_002_Erreichbarkeitsprüfung erstellt.

	den konnte	
	Falls bei der DNS-Anfrage eine Antwort oder ein DNS-Fehler ermittelt werden konnte	Die Service Monitoring-Daten (aus den Eingangsdaten) werden entsprechend der durchgeführten Aktionen, Tab_Service_Monitoring_Probe_Daten und um die Performance-Kenngröße „Bearbeitungszeit“ ergänzt. Dabei wird das „Probe-Ergebnis“ dieses Datensatzes • auf OK gesetzt, falls der FQDN in eine IP-Adresse aufgelöst wurde. • auf 7102 gesetzt, falls der DNS-Server mit einem Fehler geantwortet hat. • Auf 7108 gesetzt, falls die DNS-Record Validierung (DNSSEC) fehlgeschlagen ist.
	Rückgabe der Daten	Rückgabe der Ausgangsdaten

[<=]

5.4.1 DNS Name Resolution

TIP1-A_7149 - Service Monitoring, Probe DNS_Name_Resolution
Das Service Monitoring MUSS die Probe DNS_Name_Resolution entsprechend Tab_Service_Monitoring_Probes_DNS_Name_Resolution bereitstellen.

Tabelle 8: Tab_Service_Monitoring_Probes_DNS_Name_Resolution

Element	Beschreibung
Benennung der Probe	DNS_Name_Resolution
Dienst	Namensdienst
Schnittstelle	I_DNS_Name_Resolution
Operation	get_IP_Address
Netzwerk	Internet zentrales Netz der TI
Beschreibung	Diese Probe wird ausgeführt für • die autoritativen Nameserver des Namensdienstes • alle Bestandsnetze (implizit I_Secure_Access_Bestandsnetz)
Vorbedingung	~~Die DNS-Nameserver und die aufzulösenden FQDN müssen in der Probe konfigurierbar sein.~~ Für die Probe müssen folgende Informationen konfigurierbar sein: • Die DNS-Nameserver, für die diese Probe ausgeführt wird.

	• Die aufzulösenden FQDN für jeden DNS-Nameserver. • Ein Flag für jeden DNS-Nameserver. Ist es gesetzt wird eine DNS-Record Validierung (DNSSEC) in der Probe durchgeführt.
Nachbedingung	Im Service Monitoring müssen für die Teilschritte des Probe-Ablaufs die dort definierten Daten für jeden DNS-Nameserver verfügbar sein.
Standardablauf	1. Die Probe ruft für jeden DNS-Nameserver TUC_SM_001_DNS_Name_Resolution mit der FQDN, dem Flag für die DNS-Record Validierung und den Service Monitoring Daten für diese Operation auf.
	2. Rückgabe der ermittelten Daten an das Service Monitoring. Alternativ können die Daten auch nach jeden Teilschritt an das Service Monitoring übergeben werden.

<=

5.4.7 CRL Download

TIP1-A_7155 - Service Monitoring, Probe CRL Download
Das Service Monitoring MUSS die Probe CRL Download entsprechend Tab_Service_Monitoring_Probes_CRL_Download bereitstellen.

Tabelle 12: Tab_Service_Monitoring_Probes_CRL_Download

Element	Beschreibung
Benennung der Probe	CRL Download
Dienst	Trust Service Provider X.509 nonQES
Schnittstelle	I_CRL_Download
Operation	download_CRL
Netzwerk	Internet
Beschreibung	Diese Probe wird ausgeführt für alle CRL Distribution Points (CDP).
Vorbedingung	Die CRL Distribution Points (CDP) müssen für die Probe konfigurierbar sein. Die minimale zeitliche Gültigkeit der CRL (KONF_ZG_CRL) muss konfigurierbar sein (in Minuten oder Sekunden).
Nachbedingung	Im Service Monitoring müssen für die Teilschritte des Probe-Ablaufs die dort definierten Daten für jeden CRL Distribution Point (CDP) verfügbar sein.
Standardablauf	1. Die Probe führt für jeden CRL Distribution Point (CDP) die folgenden Schritte durch:
	1.1. Ermittlung der IP-Adresse des CRL Distribution Points durch TUC_SM_001_DNS_Name_Resolution ohne DNS-Record Validierung (DNSSEC).

	1.2. Die Probe lädt die CRL vom CRL Distribution Point (siehe auch TIP1-A_4248 [gemSpec_X.509_TSP]). Falls die CRL nicht auf dem CRL Distribution Point vorliegt wird der gelieferte Fehlercode in den Service Monitoring Daten erfasst.
	1.3 Prüfung der CRL-Signatur • Prüfung auf zeitliche Gültigkeit des CRL-Signer-Zertifikats mittels TUC_PKI_002 "Gültigkeitsprüfung des Zertifikats" mit Referenzzeitpunkt = aktuelle Systemzeit. • Auswahl des öffentlichen Schlüssels des CRL-Signer-Zertifikats • Die Signatur und der verwendete Algorithmus werden aus der CRL ausgelesen • Verifikation der Signatur und Hashwert-Vergleich (Verfahren siehe [RFC5280]). • Prüfung ob die aktuelle Systemzeit + Konfigurationsparameter KONF_ZG_CRL den Wert NextUpdate aus der CRL erreicht oder überschritten hat.
	~~1.3~~ 1.4. Ermittlung der Service Monitoring-Daten für den CRL Distribution Point entsprechend Tab_Service_Monitoring_Probe_Daten und Erfassung der Performance-Kenngröße „Bearbeitungszeit“.
	2. Rückgabe der ermittelten Daten an das Service Monitoring. Alternativ können die Daten auch nach jeden Teilschritt an das Service Monitoring übergeben werden.
Ursachen-Analyse im Fehlerfall	Falls im Standardablauf (Punkt 1.2) beim Laden der CRL Fehler auftreten (es wird keine erwartete Antwort und keine Fehlermeldung geliefert), muss die Erreichbarkeit des Dienstes mit TUC_SM_002_Erreichbarkeitsprüfung geprüft und die Probe mit dem nächsten CRL Distribution Point fortgesetzt werden. Das „Probe-Ergebnis“ für diesen CRL Distribution Point wird auf • 7100 CRL Distribution Point nicht erreichbar oder • 7101 Ports vom CRL Distribution Point geschlossen oder • 7103 Aufruf mit Fehler beendet gesetzt. Falls im Standardablauf (Punkt 1.3) bei der CRL-Signaturprüfung Fehler auftreten, muss das „Probe-Ergebnis“ für diesen CRL Distribution Point auf • 7109 Minimale zeitliche Gültigkeit der CRL unterschritten oder • 7110 CRL Signaturprüfung fehlgeschlagen. gesetzt werden.

[<=]

6.6 Fehlercodes

Tabelle 25 - Tab_Service_Monitoring_Fehlercodes

Fehlercode	ErrorType	Severity	Fehlertext
7100	Technical	Fatal	Dienst ist nicht erreichbar
7101	Technical	Fatal	Ein oder mehrere Port(s) vom Dienst sind geschlossen
7102	Technical	Fatal	Zu einem DNS Namen konnte keine IP-Adresse gefunden werden
7103	Technical	Fatal	Aufruf mit Fehler beendet
7104	Technical	Fatal	Werte können nicht über DNS Service Discovery ermittelt werden
7105	Technical	Fatal	Fehler beim Aufruf des Registrierungsservers
7106	Technical	Fatal	TSL nicht valide
7107	Technical	Fatal	In der Probe ist ein Fehler aufgetreten
7108	Technical	Fatal	DNS-Record Validierung fehlgeschlagen (DNSSEC)
7109	Technical	Fatal	Minimale zeitliche Gültigkeit der CRL unterschritten
7110	Technical	Fatal	CRL Signaturprüfung fehlgeschlagen