Test specification WHO-DDCCG-Gateway (incl. regression test for the EU DCCG-GW)

Fix Version WHO_Rel_1.0 ▾

						Tests By Status						
Key	Summary	Version	Planned start date	Planned end date	Test Environments	#Test Executions	#Test runs	Total Tests	PASS	TODO	EXECUTING	FAIL
TXR-5912	WHO_DDCCG_TP_GW_API_Rel_1.0	WHO_Rel_1.0			DDCC_TST	1	32	32	0	32	0	0
TXR-4985	WHO_DDCCG_TP_Integration_GW_API_Unchanged_Part_Rel_1.0	WHO_Rel_1.0			DDCC_TST	1	50	51	0	51	0	0

Test specification DDCCG-Gateway-API

TC-ID	Testcase	Description	Manual test steps		
TXR-5843	WHO_GW_API_Certificate_Up_and_Download_from_Country	Subject: Certificate handling Situation: CountryA and CountryB are both authorized to use the gateway. CountryC is unauthorized. The test cases cover the handling of certificates from their national backends Test issue: upload certificate - CountryA creates a certificate and uploads it. It must appear in the trustlist. Steps: •"CountryA" creates a certificate •"CountryA" creates CMS message with certificate •"CountryA" uploads CMS certificate •check that the response had no error •"CountryA" downloads the certificate trustlist •check that the certificate is in the trustlist	Step	Input/Data	Expected Results
			1 Carry out the appropriated test script belong to the test case description		Script is carriet out witout error and with the scripted result expected.
TXR-5844	WHO_GW_API_Certificate_Data_Distribution_Between_Countries	Subject: Certificate handling Situation: CountryA and CountryB are both authorized to use the gateway. CountryC is unauthorized. The test cases cover the handling of certificates from their national backends Test issue: certificate data distribution - CountryA creates a certificate and CountryB can download it. Another (simulated) gateway can also download the certificate. Steps: •"CountryA" creates a certificate •"CountryA" creates CMS message with certificate •"CountryA" uploads CMS certificate •check that the response had no error •Reference "TXR-4994" •Secondary gateway downloads the certificate trustlist •check that the certificate is in the trustlist •Reference "TXR-4998" •"CountryB" downloads the certificate trustlist •check that the certificate is in the trustlist	Step	Input/Data	Expected Results
			1 Carry out the appropriated test script belong to the test case description above.		Script is carried out without error and with the scripted result expected.
TXR-5845	WHO_GW_API_Certificate_Delete_Uploaded_Trustlist_With_DELETE_API	Subject: Certificate handling Situation: CountryA and CountryB are both authorized to use the gateway. CountryC is unauthorized. The test cases cover the handling of certificates from their national backends Test issue: delete certificate - CountryA creates a certificate and deletes it using the defaulte endpoint Steps: •"CountryA" creates a certificate •"CountryA" creates CMS message with certificate •"CountryA" uploads CMS certificate •check that the response had no error •"CountryA" downloads the certificate trustlist •check that the certificate is in the trustlist •"CountryA" deletes uploaded certificate •check that the response had no error	Step	Input/Data	Expected Results
			1 Carry out the appropriated test script belong to the test case description above.		Script is carried out without error and with the scripted result expected.

		•"CountryA" downloads the certificate trustlist •check that the certificate is NOT in the trustlist			
TXR-5846	WHO_GW_API_Certificate_Delete_Uploaded_Trustlist_With_POST_API	Subject: Certificate handling Situation: CountryA and CountryB are both authorized to use the gateway. CountryC is unauthorized. The test cases cover the handling of certificates from their national backends Test issue: delete certificate alternate endpoint - CountryA creates a certificate and deletes it using the alternative endpoint (POST instead of DELETE) Steps: •"CountryA" creates a certificate •"CountryA" creates CMS message with certificate •"CountryA" uploads CMS certificate •check that the response had no error •"CountryA" downloads the certificate trustlist •check that the certificate is in the trustlist •"CountryA" deletes uploaded certificate with alternate endpoint "POST" •check that the response had no error •"CountryA" downloads the certificate trustlist •check that the certificate is NOT in the trustlist		Step	Input/Data	Expected Results
			1	Carry out the appropriated test script belong to the test case description above.		Script is carried out without error and with the scripted result expected.
TXR-5848	WHO_GW_API_Certificate_Unauthorized_Try_To_Delete_Trustlist	Subject: Certificate handling Situation: CountryA and CountryB are both authorized to use the gateway. CountryC is unauthorized. The test cases cover the handling of certificates from their national backends Test issue: unauthorized delete certificate - CountryB tries to delete a certificate of CountryA. The operation must not succeed. Steps: •"CountryA" creates a certificate •"CountryA" creates CMS message with certificate •"CountryA" uploads CMS certificate •check that the response had no error •"CountryA" downloads the certificate trustlist •check that the certificate is in the trustlist •"CountryB" deletes uploaded certificate •check that the response had an error •"CountryA" downloads the certificate trustlist •check that the certificate is in the trustlist		Step	Input/Data	Expected Results
			1	Carry out the appropriated test script belong to the test case description above.		Script is carried out without error and with the scripted result expected.
TXR-5849	WHO_GW_API_Certificate_Unauthorized_Try_To_Download_Trust	Subject: Certificate handling		Step	Input/Data	Expected Results

	list	Situation: CountryA and CountryB are both authorized to use the gateway. CountryC is unauthorized. The test cases cover the handling of certificates from their national backends Test issue: unauthorized access to certificate trustlist - CountryC tries to download the certificate trustlist. Steps: •"CountryC" downloads the certificate trustlist •check that the response had an error	1	Carry out the appropriated test script belong to the test case description above.		Script is carried out without error and with the scripted result expected.
TXR-5850	WHO_GW_API_Certificate_Unauthorized_Try_To_Upload_Not_Own_Certificate	Subject: Certificate handling Situation: CountryA and CountryB are both authorized to use the gateway. CountryC is unauthorized. The test cases cover the handling of certificates from their national backends Test issue: unauthorized upload certificate - variant 1 - CountryB attempts to upload a certificate of CountryA; It must not appear in the trustlist. Steps: •"CountryA" creates a certificate •"CountryB" creates CMS message with certificate •"CountryB" uploads CMS certificate •check that the response had an error •"CountryA" downloads the certificate trustlist •check that the certificate is NOT in the trustlist		Step	Input/Data	Expected Results
			1	Carry out the appropriated test script belong to the test case description above.		Script is carried out without error and with the scripted result expected.
TXR-5851	WHO_GW_API_Certificate_Unauthorized_Try_To_Upload_Certificate_Of_Other_Country_But_With_Authorized_Access	Subject: Certificate handling Situation: CountryA and CountryB are both authorized to use the gateway. CountryC is unauthorized. The test cases cover the handling of certificates from their national backends Test issue: unauthorized upload certificate - variant 2 - CountryB attempts to upload a certificate of CountryA and has access to CountryA's upload keys; It must not appear in the trustlist. Steps: •"CountryA" creates a certificate •"CountryA" creates CMS message with certificate •"CountryB" uploads CMS certificate •check that the response had an error •"CountryA" downloads the certificate trustlist •check that the certificate is NOT in the trustlist		Step	Input/Data	Expected Results
			1	Carry out the appropriated test script belong to the test case description above.		Script is carried out without error and with the scripted result expected.

TXR-5852	WHO_GW_API_TrustIssuer_Up_And_Download_Trust_Issuer_Cert	Subject: Trusted issuer handling Situation: CountryA and CountryB are both authorized to use the gateway. CountryC is unauthorized. The test cases cover the handling of trusted issuer certificates from their national backends Test issue: upload trusted issuer - CountryA creates a trusted issuer certificate and uploads it. It must appear in the trustlist. Steps: •"CountryA" creates a trusted issuer certificate •"CountryA" creates CMS message with trusted issuer certificate •"CountryA" uploads CMS trusted issuer certificate •check that the response had no error •"CountryA" downloads the trusted issuer trustlist •check that the trusted issuer is in the trustlist		Step	Input/Data	Expected Results
			1	Carry out the appropriated test script belong to the test case description above.		Script is carriet out witout error and with the scripted result expected.
TXR-5853	WHO_GW_API_TrustIssuer_Distribution_TrustIssuerCert_To_Sec GW_AND_To_Countries	Subject: Trusted issuer handling Situation: CountryA and CountryB are both authorized to use the gateway. CountryC is unauthorized. The test cases cover the handling of trusted issuer certificates from their national backends Test issue: trusted issuer certificate data distribution - CountryA creates a trusted issuer certificate and CountryB can download it. Another (simulated) gateway can also download the trusted issuer certificate. Steps: •"CountryA" creates a trusted issuer certificate •"CountryA" creates CMS message with trusted issuer certificate •"CountryA" uploads CMS trusted issuer certificate •check that the response had no error •Secondary gateway downloads the trusted issuer trustlist •check that the trusted issuer is in the trustlist •"CountryB" downloads the trusted issuer trustlist •check that the trusted issuer is in the trustlist		Step	Input/Data	Expected Results
			1	Carry out the appropriated test script belong to the test case description above.		Script is carriet out witout error and with the scripted result expected.
TXR-5854	WHO_GW_API_TrustIssuer_Delete_Uploaded_TrustIssuerCert_Wi th_DELETE_API	Subject: Trusted issuer handling Situation: CountryA and CountryB are both authorized to use the gateway. CountryC is unauthorized. The test cases cover the handling of trusted issuer certificates from their national backends		Step	Input/Data	Expected Results
			1	Carry out the appropriated test script belong to the test case description above.		Script is carriet out witout error and with the scripted result expected.

		Test issue: delete trusted issuer certificate via Delete-API - CountryA creates a trusted issuer certificate and deletes it using the default endpoint Steps: •"CountryA" creates a trusted issuer certificate •"CountryA" creates CMS message with trusted issuer certificate •"CountryA" uploads CMS trusted issuer certificate •check that the response had no error •"CountryA" downloads the trusted issuer trustlist •check that the trusted issuer is in the trustlist •"CountryA" deletes uploaded trusted issuer certificate •check that the response had no error •"CountryA" downloads the trusted issuer trustlist •check that the trusted issuer is NOT in the trustlist	
TXR-5855	WHO_GW_API_TrustIssuer_Delete_Uploaded_TrustIssuerCert_With_POST_API	Subject: Trusted issuer handling Situation: CountryA and CountryB are both authorized to use the gateway. CountryC is unauthorized. The test cases cover the handling of trusted issuer certificates from their national backends Test issue: delete trusted issuer certificate via POST-API - CountryA creates a trusted issuer certificate and deletes it using the alternative endpoint (POST instead of DELETE). Steps: •"CountryA" creates a trusted issuer certificate •"CountryA" creates CMS message with trusted issuer certificate •"CountryA" uploads CMS trusted issuer certificate •check that the response had no error •"CountryA" downloads the trusted issuer trustlist •check that the trusted issuer is in the trustlist •"CountryA" deletes uploaded trusted issuer certificate with alternate endpoint "POST" •check that the response had no error •"CountryA" downloads the trusted issuer trustlist •check that the trusted issuer is NOT in the trustlist	Step: 1 — Carry out the appropriated test script belong to the test case description above. Input/Data: Expected Results: Script is carriet out witout error and with the scripted result expected.
TXR-5856	WHO_GW_API_TrustIssuer_Unauthorized_Try_To_Delete_TrustIssuerCert	Subject: Trusted issuer handling Situation: CountryA and CountryB are both authorized to use the gateway. CountryC is unauthorized. The test cases cover the handling of trusted issuer certificates from their national backends	Step: 1 — Carry out the appropriated test script belong to the test case description above. Input/Data: Expected Results: Script is carriet out witout error and with the scripted result expected.

		Test issue: unauthorized delete trusted issuer certificate - CountryB tries to delete a trusted issuer certificate of CountryA. The operation must not succeed. Steps: •"CountryA" creates a trusted issuer certificate •"CountryA" creates CMS message with trusted issuer certificate •"CountryA" uploads CMS trusted issuer certificate • check that the response had no error •"CountryA" downloads the trusted issuer trustlist •check that the trusted issuer is in the trustlist •"CountryB" deletes uploaded trusted issuer certificate •check that the response had an error •"CountryA" downloads the trusted issuer trustlist •check that the trusted issuer is in the trustlist	
TXR-5858	WHO_GW_API_TrustIssuer_Unauthorized_Try_To_Download_TrustIssuerCert	Subject: Trusted issuer handling Situation: CountryA and CountryB are both authorized to use the gateway. CountryC is unauthorized. The test cases cover the handling of trusted issuer certificates from their national backends Test issue: unauthorized access to trusted issuer trustlist - CountryC tries to downloads the trusted issuer trustlist. The operation must not succeed. Steps: •"CountryC" downloads the trusted issuer trustlist •check that the response had an error	

	Step	Input/Data	Expected Results
1	Carry out the appropriated test script belong to the test case description above.		Script is carriet out witout error and with the scripted result expected.

TXR-5859	WHO_GW_API_TrustIssuer_Unauthorized_Try_To_Upoad_Of_Not_Own_TrustIssuerCert	Subject: Trusted issuer handling Situation: CountryA and CountryB are both authorized to use the gateway. CountryC is unauthorized. The test cases cover the handling of trusted issuer certificates from their national backends Test issue: unauthorized upload trusted issuer - variant 1 - CountryB attempts to upload a trusted issuer certificate of CountryA. Steps: It must not appear in the trustlist. •"CountryA" creates a trusted issuer certificate •"CountryB" creates CMS message with trusted issuer certificate	

	Step	Input/Data	Expected Results
1	Carry out the appropriated test script belong to the test case description above.		Script is carriet out witout error and with the scripted result expected.

		•"CountryB" uploads CMS trusted issuer certificate •check that the response had an error •"CountryA" downloads the trusted issuer trustlist •check that the trusted issuer is NOT in the trustlist	
TXR-5860	WHO_GW_API_TrustIssuer_Unauthorized_Try_To_Upoad_TrustIssuerCert_Of_Other_Country_But_With_Authorized_Access	Subject: Trusted issuer handling Situation: CountryA and CountryB are both authorized to use the gateway. CountryC is unauthorized. The test cases cover the handling of trusted issuer certificates from their national backends Test issue: unauthorized upload trusted issuer - variant 2 - CountryB attempts to upload a trusted issuer certificate of CountryA and has access to CountryA's upload keys Steps: It must not appear in the trustlist. •"CountryA" creates a trusted issuer certificate •"CountryA" creates CMS message with trusted issuer certificate •"CountryB" uploads CMS trusted issuer certificate •check that the response had an error •"CountryA" downloads the trusted issuer trustlist •check that the trusted issuer is NOT in the trustlist	Step: 1 — Carry out the appropriated test script belong to the test case description above. Input/Data: Expected Results: Script is carriet out witout error and with the scripted result expected.
TXR-5861	WHO_GW_API_Reference_Up_And_Download_Reference	Subject: Reference handling Situation: CountryA and CountryB are both authorized to use the gateway. CountryC is unauthorized. The test cases cover the handling of references from their national backends Test issue: Up- and download reference - CountryA creates a reference and uploads it. It must appear in the trustlist. Steps: • "CountryA" creates a reference • "CountryA" creates CMS message with reference • "CountryA" uploads CMS reference	Step: 1 — Carry out the appropriated test script belong to the test case description above. Input/Data: Expected Results: Script is carriet out witout error and with the scripted result expected.

		• check that the response had no error • "CountryA" downloads the reference trustlist • check that the reference is in the trustlist	
TXR-5862	WHO_GW_API_Reference_Distribution_Reference_To_SecGW_And_To_Countries	Subject: Reference handling Situation: CountryA and CountryB are both authorized to use the gateway. CountryC is unauthorized. The test cases cover the handling of references from their national backends Test issue: reference data distribution - CountryA creates a reference and CountryB can download it. Another (simulated) gateway can also download the reference. Steps: • "CountryA" creates a reference • "CountryA" creates CMS message with reference • "CountryA" uploads CMS reference • check that the response had no error • Secondary gateway downloads the reference trustlist • check that the reference is in the trustlist • "CountryB" downloads the reference trustlist • check that the reference is in the trustlist	1 Carry out the appropriated test script belong to the test case description above. — Input/Data: — Expected Results: Script is carriet out witout error and with the scripted result expected.
TXR-5863	WHO_GW_API_Reference_Delete_Uploaded_Reference_with_DELETE_API	Subject: Reference handling Situation: CountryA and CountryB are both authorized to use the gateway. CountryC is unauthorized. The test cases cover the handling of references from their national backends Test issue: Delete reference - CountryA creates a reference and deletes it using the default endpoint with DELETE-API. Steps: • "CountryA" creates a reference • "CountryA" creates CMS message with reference • "CountryA" uploads CMS reference • check that the response had no error • "CountryA" downloads the reference trustlist • check that the reference is in the trustlist • "CountryA" deletes uploaded reference • check that the response had no error • "CountryA" downloads the reference trustlist • check that the reference is NOT in the trustlist	1 Carry out the appropriated test script belong to the test case description above. — Input/Data: — Expected Results: Script is carriet out witout error and with the scripted result expected.

TXR-5864	WHO_GW_API_Reference_Delete_Uploaded_Reference_with_POST_API	Subject: Reference handling Situation: CountryA and CountryB are both authorized to use the gateway. CountryC is unauthorized. The test cases cover the handling of references from their national backends Test issue: Delete reference alternate endpoint - CountryA creates a reference and deletes it using the alternative endpoint with POST-API. Steps: • "CountryA" creates a reference • "CountryA" creates CMS message with reference • "CountryA" uploads CMS reference • check that the response had no error • "CountryA" downloads the reference trustlist • check that the reference is in the trustlist • "CountryA" deletes uploaded reference with POST-API • check that the response had no error • "CountryA" downloads the reference trustlist • check that the reference is NOT in the trustlist	Step: 1 — Carry out the appropriated test script belong to the test case description above. Input/Data: Expected Results: Script is carriet out witout error and with the scripted result expected.
TXR-5865	WHO_GW_API_Reference_Unauthorized_Try_To_Delete_Reference	Subject: Reference handling Situation: CountryA and CountryB are both authorized to use the gateway. CountryC is unauthorized. The test cases cover the handling of references from their national backends Test issue: Unauthorized delete reference - CountryB tries to delete a reference of CountryA. The operation must not succeed Steps: • "CountryA" creates a reference • "CountryA" creates CMS message with reference • "CountryA" uploads CMS reference • check that the response had no error • "CountryA" downloads the reference trustlist • check that the reference is in the trustlist • "CountryB" deletes uploaded reference • check that the response had an error	Step: 1 — Carry out the appropriated test script belong to the test case description above. Input/Data: Expected Results: Script is carriet out witout error and with the scripted result expected.

		• "CountryA" downloads the reference trustlist • check that the reference is in the trustlist	
TXR-5866	WHO_GW_API_Reference_Unauthorized_Try_To_Download_Reference	Subject: Reference handling Situation: CountryA and CountryB are both authorized to use the gateway. CountryC is unauthorized. The test cases cover the handling of references from their national backends Test issue: Unauthorized access to reference trustlist - CountryC tries to download the reference trustlist. Steps: • "CountryC" downloads the reference trustlist • check that the response had an error	Step / Input/Data / Expected Results 1 Carry out the appropriated test script belong to the test case description above. / / Script is carriet out witout error and with the scripted result expected.
TXR-5867	WHO_GW_API_Reference_Unauthorized_Try_To_Upload_Of_Not_Own_Reference	Subject: Reference handling Situation: CountryA and CountryB are both authorized to use the gateway. CountryC is unauthorized. The test cases cover the handling of references from their national backends Test issue: Unauthorized upload reference - variant 1 - CountryB attempts to upload a reference of CountryA. It must not appear in the trustlist. Steps: • "CountryA" creates a reference • "CountryB" creates CMS message with reference • "CountryB" uploads CMS reference • check that the response had an error • "CountryA" downloads the reference trustlist •check that the reference is NOT in the trustlist	Step / Input/Data / Expected Results 1 Carry out the appropriated test script belong to the test case description above. / / Script is carriet out witout error and with the scripted result expected.

TXR-5868	WHO_GW_API_Reference_Unauthorized_Try_To_Upload_Reference_Of_Other_Country_But_With_Authorized_Access	Subject: Reference handling Situation: CountryA and CountryB are both authorized to use the gateway. CountryC is unauthorized. The test cases cover the handling of references from their national backends Test issue: Unauthorized upload reference - variant 2 - CountryB attempts to upload a reference of CountryA and has access to CountryA's upload keys. It must not appear in the trustlist. Steps: • "CountryA" creates a reference • "CountryA" creates CMS message with reference • "CountryB" uploads CMS reference • check that the response had an error • "CountryA" downloads the reference trustlist • check that the reference is NOT in the trustlist	

	Step	Input/Data	Expected Results
1	Carry out the appropriated test script belong to the test case description above.		Script is carriet out witout error and with the scripted result expected.

TXR-5888	WHO_GW_API_Federation_Certificate_Up_and_Download_Certificates_Between_Federations	Subject: Certificate handling between federations Situation: CountryA is authorized to use the primary gateway. CountryC is authorized to use the secondary gateway. The test cases cover the handling of references from their national backends Test issue: Certificate federation - CountryA creates a certificate on the primary gateway and CountryC can download it from the secondary gateway. Steps: • "CountryA" creates a certificate • "CountryA" creates CMS message with certificate • "CountryA" uploads CMS certificate • check that the response had no error • "CountryA" downloads the certificate trustlist • check that the certificate is in the trustlist • wait synchronization time (means the Workflow of the process for the request and download of the certificate trustlist from primary gateway by secondary gateway is completed)	

	Step	Input/Data	Expected Results
1	Carry out the appropriated test script belong to the test case description		Script is carriet out witout error and with the scripted result expected.

		• "CountryC" downloads the federated certificate trustlist • check that the certificate is in the trustlist			
TXR-5892	WHO_GW_API_Federation_TrustIssuer_Up_and_Download_TrustIssuerCert_Between_Federations	Subject: Certificate handling between federations Situation: CountryA is authorized to use the first gateway. CountryC is authorized to use the second gateway. The test cases cover the handling of the trusted issuer entries from their national backends Test issue: Trusted issuer between two federations - CountryA creates a trusted issuer on the primary gateway and CountryC can download it from the secondary gateway. Steps: • "CountryA" creates a trusted issuer entry • "CountryA" creates CMS message with trusted issuer • "CountryA" uploads CMS with trusted issuer • check that the response had no error • "CountryA" downloads the trusted issuer trustlist • check that the trusted issuer is in the trustlist • wait synchronization time (means the Workflow of the process for the request and download of the Trusted Issuer Trustlist from primary gateway by secondary gateway is completed) • "CountryC" downloads the federated issuer trustlist • check that the trusted issuer is in the trustlist	1	Step: Carry out the appropriated test script belong to the test case description	Input/Data:	Expected Results: Script is carriet out witout error and with the scripted result expected.
TXR-5893	WHO_GW_API_Federation_Reference_Up_and_Download_References_Between_Federations	Subject: Reference handling between federations Situation: CountryA is authorized to use the first gateway. CountryC is authorized to use the second gateway. The test cases cover the handling of references from their national backends Test issue: trusted reference between federations - CountryA creates a trusted issuer on the primary gateway and CountryC can download it from the secondary gateway. Steps: • "CountryA" creates a reference • "CountryA" creates CMS message with trusted reference • "CountryA" uploads CMS reference • check that the response had no error • "CountryA" downloads the reference trustlist • check that the reference is in the trustlist • wait synchronization time (means the Workflow of the process for the request and download of the references from primary gateway by secondary gateway is completed) • "CountryC" downloads the federated reference trustlist • check that the reference is in the trustlist	1	Step: Carry out the appropriated test script belong to the test case description	Input/Data:	Expected Results: Script is carriet out witout error and with the scripted result expected.
TXR-5894	WHO_GW_API_MetaData_Download_Of_Federated_Signatures	Subject: Meta data handling between federations Situation: CountryA is authorized to use the first gateway. CountryC is authorized to use the second gateway. Test issue: Federated signatures can be download	1	Step: Carry out the appropriated test script belong to the test case description above.	Input/Data:	Expected Results: Script is carried out without error and with the scripted result expected.

		- CountryA downloads federated signatures Steps: • "CountryA" downloads federated signatures • check that the response had no error				
TXR-5895	WHO_GW_API_MetaData_Download_Of_Federated_Gateway_List_Between_Federations	Subject: Meta data handling between federations Situation: CountryA is authorized to use the first gateway. CountryC is authorized to use the second gateway. Test issue: Federated gateways can be download and appear in downloaded gateway list Steps: • "CountryA" downloads the federated gateway list on "firstGateway" • check that the response had no error • check that "secondGateway" is in the gateway list • "CountryC" downloads the federated gateway list on "secondGateway" • check that the response had no error • check that "firstGateway" is in the gateway list		Step	Input/Data	Expected Results
			1	Carry out the appropriated test script belong to the test case description above.		Script is carried out without error and with the scripted result expected.
TXR-5896	WHO_GW_API_MetaData_Download_Of_Federated_Federator_List_Between_Federations	Subject: Meta data handling between federations Situation: CountryA is authorized to use the first gateway. CountryC is authorized to use the second gateway. Test issue: Federated federators can be download and appear in downloaded list of federators Steps: • "CountryA" downloads the federated federator list on "firstGateway" • check that the response had no error • check that the federator of the "secondGateway" is in the federator list • "CountryC" downloads the federated federator list on "secondGateway" • check that the response had no error • check that the federator of the "firstGateway" is in the federator list		Step	Input/Data	Expected Results
			1	Carry out the appropriated test script belong to the test case description above.		Script is carried out without error and with the scripted result expected.
TXR-5897	WHO_GW_API_MetaData_Unauthorized_Try_To_Download_Of_F	Subject: Meta data handling between federations		Step	Input/Data	Expected Results

	ederated_Data_Between_Federations	Situation: CountryA is authorized to use the first gateway. CountryC is authorized to use the second gateway. Test issue: Federated endpoints are protected and cannot downloaded by unauthorized countries Steps: • "CountryA" downloads the federated gateway list on "secondGateway" • check that the response had an error • "CountryC" downloads the federated gateway list on "firstGateway" • check that the response had an error • "CountryA" downloads the federated federator list on "secondGateway" • check that the response had an error • "CountryC" downloads the federated federator list on "firstGateway" • check that the response had an error	1	Carry out the appropriated test script belong to the test case description above.		Script is carried out without error and with the scripted result expected.
TXR-5898	WHO_GW_API_MetaData_Authorized_Download_Of_Federated_MetaData	Subject: Meta data handling between federations Situation: CountryA is authorized to use the first gateway. CountryC is authorized to use the second gateway. Test issue: Federated meta data is accessible for authorized countries Steps: • "CountryA" downloads the federation metadata on "firstGateway" • check that the response had no error • check that meta data structure is OK • "CountryC" downloads the federation metadata on "secondGateway" • check that the response had no error • check that meta data structure is OK		Step	Input/Data	Expected Results
			1	Carry out the appropriated test script belong to the test case description above.		Script is carried out without error and with the scripted result expected.

Test specification EU-DCCG-Gateway-API-Regression test

TC-ID	Testcase	Description	Manual test steps			
TXR-2059	INT_DGCG_upload_dsc	Upload a DSC of a country		Step	Input/Data	Expected Results
			1	create a valid dsc		
			2	upload dsc		dsc is in trustlist
TXR-2060	INT_DGCG_neg_upload_dsc_with_unauthorized_client_certificate	Upload a DSC of a country with an unauthorized client certificate. The response should be with the status code 401 Unauthorized		Step	Input/Data	Expected Results
			1	create a valid DSC		
			2	create custom authentication certificate		
			3	upload DSC with custom client certificate		Error 401 Unauthorized
TXR-2061	INT_DGCG_neg_upload_dsc_with_mismatched_Certificates	Upload a DSC signed with CSCA certificate of a different country. The response code should be 400		Step	Input/Data	Expected Results
			1	create a valid DSC for another country		
			2	upload DSC		Error 400 Bad Request
TXR-2062	INT_DGCG_neg_upload_dsc_wrong_format	Upload a DSC of a country with the wrong format to trigger Error Code 406		Step	Input/Data	Expected Results
			1	upload text instead of DSC		Error 406 Content is not acceptable
TXR-2063	INT_DGCG_neg_upload_dublicate_dsc	Upload a DSC of a country with a UUID which is already in the database. The API should respond with the error Code 409		Step	Input/Data	Expected Results
			1	create DSC		
			2	upload DSC		DSC is in trustlist
			3	upload DSC (again)		Error 409 Conflict
TXR-2065	INT_DGCG_delete_a_dsc	delete DSC of a country		Step	Input/Data	Expected Results
			1	create a valid DSC		
			2	upload DSC		DSC is in trustlist
			3	delete public key created		public key is deleted in trustlist
TXR-2066	INT_DGCG_neg_delete_a_dsc_not_in_database	delete a dsc of a country which is not in the database		Step	Input/Data	Expected Results
			1	create a valid DSC		
			2	sign DSC with UPLOAD certificate		
			3	delete DSC created		error 400
TXR-2069	INT_DGCG_neg_delete_a_dsc_with_unauthorized_client_certificate	delete a dscof a country with a client certificate which is not authorized. The Error code should be 401 "unauthorized"		Step	Input/Data	Expected Results
			1	get trustlist of DSCs		
			2	delete dsc of the own country		Http Error 401 Unauthorized
TXR-2070	INT_DGCG_neg_delete_a_dsc_with_client_certificate_of_another_country	delete a DSC of another country with the client certificate not authorized to change DSCs of that country. The error Code should be 403 "Forbidden"		Step	Input/Data	Expected Results
			1	get trustlist of type "DSC"		trustlist with all DSCs
			2	get random dsc from trustlist from another country		
			3	delete dsc from another country		http error 403 forbidden
TXR-2071	INT_DGCG_get_trustlist	Get all trusted certificates		Step	Input/Data	Expected Results
			1	create a valid DSC		
			2	sign DSC with UPLOAD certificate		
			3	check that DSC is not in trustlist		DSC is not in trustlist
			4	upload DSC		
			5	check stat DSC is in trustlist		DSC is in trustlist
			6	delete DSC created		
			7	check that DSC is not in trustlist		DSC is not in trustlist
TXR-2072	INT_DGCG_get_trustlist_with_specific_type	Get all trusted public keys of a specific type		Step	Input/Data	Expected Results
			1	get the trustList just with a specific type	type = CSCA or type = UPLOAD or type = DSC	only certificates with that type should be present
TXR-2073	INT_DGCG_get_trustlist_with_specific_type_and_country	Get trusted public keys with a specific type (for example CSCA) and country.		Step	Input/Data	Expected Results
			1	get trustList with spedific type and country	type=csca country=de	only the trustList data with the type and country is present
TXR-2860		Upload a valid Rule		Step	Input/Data	Expected Results

	INT_DGCG_upload_valid_Rule		1	create a valid Invalidation/Acceptance Rule		
			2	upload Rule		Status Code 200
			3	check that Rule is in Rulelist		Rule is in Rulelist
			4	delete Rule created		
TXR-2861	INT_DGCG_neg_upload_rule_with_unauthenticated_certificate	Upload a Rule with an unauthenticated certificate. There should be an error and the Response Code should be 401.		Step	Input/Data	Expected Results
			1	create a valid Invalidation Rule		
			2	upload Rule with unauthenticated certificate		Response should have status code 401
			3	check that Rule is not in Rulelist		Rule should not be in Rulelist
TXR-2862	INT_DGCG_neg_upload_rule_with_authentication_certificate_of_another_country	Upload a Rule with a NBTLS certificate of another country. There should be an error and the status code should be 400.		Step	Input/Data	Expected Results
			1	create a valid Invalidation Rule		
			2	upload Rule with certificate from another country		Error with status Code 400
			3	check that Rule is not in Rulelist		Rule is not in Rulelist
TXR-2863	INT_DGCG_update_Rule_to_a_new_version	Update a Rule created to a new version.		Step	Input/Data	Expected Results
			1	create a valid Invalidation Rule		
			2	upload Rule		
			3	update Rule to new version		Status Code 200
			4	get Rules of own Country		
			5	check that Rule has the new version		rule has the new Version
			6	delete rule created		
TXR-2864	INT_DGCG_neg_update_Rule_with_lower_version_than_the_old_rule	Update a Rule with a Rule lower than the current version. There should be an error.		Step	Input/Data	Expected Results
			1	create a valid Invalidation Rule		
			2	upload Rule		
			3	update Rule to new version with lower version number		Response Status Code 400
			4	delete Rule created		
TXR-2865	INT_DGCG_neg_update_Rule_with_version_not_using_semver	Update a Rule without following the semantic versioning scheme (e.g. 1.3 instead of 1.3.0)		Step	Input/Data	Expected Results
			1	create a valid Invalidation Rule		
			2	upload Rule		
			3	update Rule with version in wrong format		Response Status Code 400
			4	delete Rule created		
TXR-2866	INT_DGCG_get_list_of_onboarded_countries	Get all onboarded countries. Should have at least the own country in the list.		Step	Input/Data	Expected Results
			1	get all onboarded countries		Response Status Code 200
			2	check that own country is in onboared countries list		Own Country is in the list
TXR-2867	INT_DGCG_download_all_Rules	Download Rules of all Countries.		Step	Input/Data	Expected Results
			1	get all onboarded countries		
			2	download rules of all countries		All Responses have status code 200
TXR-2868	INT_DGCG_neg_get_list_of_onboarded_countries_with_unauthenticated_certificate	Get all onboarded countries with unauthenticated certificate. Should lead to an error.		Step	Input/Data	Expected Results
			1	create custom authentication certificate		
			2	get all onboarded countries with custom certificate		Response Status Code 400
TXR-2869	INT_DGCG_download_Rules_with_unauthenticated_certificate	Get Rules from any country with an unauthenticated NBTLS. Should lead to an error.		Step	Input/Data	Expected Results
			1	get all onboarded countries		
			2	create custom authentication certificate		
			3	download rules of all countries with custom certificate		all Responses had the status code 400
TXR-2870	INT_DGCG_delete_Rule	Delete a Rule. This should be no problem as Invalidation Rules can be deleted.		Step	Input/Data	Expected Results
			1	create a valid Invalidation/Acceptance Rule		
			2	upload Rule		

			3	check that Rule is in Rulelist		Rule is in Rulelist
			4	delete Rule created		Response had no errors
			5	check that Rule is not in Rulelist		Rule is not in Rulelist
TXR-2872	INT_DGCG_neg_delete_Rule_of_another_country	Delete a Rule of another country. This should not be possible.		Step	Input/Data	Expected Results
			1	create a valid Invalidation/Acceptance Rule		
			2	upload Rule		
			3	check that Rule is in Rulelist		Rule is in Rulelist
			4	delete Rule created with certificate of another country		Response should have an error status code
			5	check that Rule is in Rulelist		Rule is in Rulelist
			6	delete Rule		
TXR-2873	INT_DGCG_neg_delete_Rule_with_unauthenticated_NBTLS	Delete a Rule with unauthenticated certificate. This should not be possible.		Step	Input/Data	Expected Results
			1	create a valid Invalidation/Acceptance Rule		
			2	upload Rule		
			3	check that Rule is in Rulelist		rule is in Rulelist
			4	create custom authentication certificate		
			5	delete Rule created with custom client certificate		response status code should be an error status code
			6	check that Rule is in Rulelist		Rule is in Rulelist
			7	delete Rule created		
TXR-2874	INT_DGCG_delete_Rule_not_in_database			Step	Input/Data	Expected Results
			1	delete Rule not in rulelist		Response status code should be an error status code
TXR-2875	INT_DGCG_neg_upload_Rule_with_uploader_country_in_wrong_format	Country attribute in a Rule should be like "en". Otherwise there should be an error		Step	Input/Data	Expected Results
			1	create a valid Invalidation/Acceptance Rule		
			2	change countrycode to a wrong format		
			3	upload Rule		response Code should be 400
			4	check that Rule is not in Rulelist		Rule is not in Rulelist
TXR-2876	INT_DGCG_neg_upload_rule_with_wrong_uploader_country	Upload a Rule from another country. There should be an error.		Step	Input/Data	Expected Results
			1	create a valid Invalidation/Acceptance Rule		
			2	change countrycode to a wrong country		
			3	upload Rule		Response Code should be 403
			4	check that Rule is not in Rulelist		
TXR-2877	INT_DGCG_neg_upload_acceptance_rule_with_ValidFrom_less_than_48h_in_the_future	Upload an Acceptance Rule which is valid ealier than 48h. There should be an error.		Step	Input/Data	Expected Results
			1	create a valid Acceptance Rule		
			2	change ValidFrom less than "48"h		
			3	upload Rule		Error with the http status code "400"
			4	check that Rule is not in Rulelist		
TXR-2878	INT_DGCG_neg_upload_rule_with_ValidTo_less_than_120h_in_the_future	Upload a Rule which is valid less than 72h. There should be an error.		Step	Input/Data	Expected Results
			1	create a valid Acceptance Rule		
			2	change ValidTo less than "120"h		
			3	upload Rule		Error with http status code "400"
			4	check that Rule is not in Rulelist		Rule is not in Rulelist
TXR-2879	INT_DGCG_neg_upload_rule_with_description_not_available	A Rule must have a description. An empty description should be an error.		Step	Input/Data	Expected Results
			1	create a valid Invalidation/Acceptance Rule		
			2	remove description of the Rule		
			3	upload Rule		Response http status code should be "400"
			4	check that Rule is not in Rulelist		Rule is not in Rulelist

TXR-2880	INT_DGCG_neg_upload_rule_with_description_filled_with_one_language_without_english	A Rule must have a description in english. Only having a description in another language should be an error		Step	Input/Data	Expected Results
			1	create a valid Invalidation/Acceptance Rule		
			2	use only german in the description of the Rule		
			3	upload Rule		Response should have status code "400"
			4	check that Rule is not in Rulelist		Rule should not be in Rulelist
TXR-2881	INT_DGCG_neg_upload_rule_with_description_having_an_invalid_language	Languages of a Rule should have the formatting like "en" or "en-uk". Otherwise there should be an error.		Step	Input/Data	Expected Results
			1	create a valid Invalidation/Acceptance Rule		
			2	add language "en-" in description		
			3	upload Rule		Response http status code should be "400"
			4	check that Rule is not in Rulelist		Rule is not in Rulelist
TXR-2882	INT_DGCG_neg_upload_rule_which_version_doesn't_follow_semVer	Rule Version should be created with semantic versioning (like "1.2.3" and not like "1.2"). Otherwise there should be an error.		Step	Input/Data	Expected Results
			1	create a valid Invalidation/Acceptance Rule		
			2	set version of the Rule to "10"		
			3	upload Rule		Response status code should be "400"
			4	check that Rule is not in Rulelist		Rule should not be in Rulelist
TXR-2883	INT_DGCG_neg_upload_rule_which_schema_version_doesn't_follow_semVer	Rule Schema Version should be created with semantic versioning (like "1.2.3" and not like "1.2"). Otherwise there should be an error.		Step	Input/Data	Expected Results
			1	create a valid Invalidation/Acceptance Rule		
			2	set version of the schema to "10"		
			3	Upload Rule		Response http status code should be "400"
			4	check that Rule is not in Rulelist		Rule is not in Rulelist
TXR-2884	INT_DGCG_Updating_a_rule_automatically_removes_the_old_version	After a rule is updated and valid the old rule should not be in the downloaded list.		Step	Input/Data	Expected Results
			1	create a valid Invalidation Rule		
			2	upload Rule		Response doesn't have errors
			3	Update Rule with new Version with ValidFrom 10 Seconds in the future		Both Versions should be in Rulelist
			4	Wait for 10 Seconds		Only the new Version should be in Rulelist
TXR-2885	INT_DGCG_get_all_valuesets	Get All Valuesets. Response code should be 200.		Step	Input/Data	Expected Results
			1	get all valuesets		Check that Response is not Empty and has Response Code 200
TXR-2886	INT_DGCG_get_specifig_Valueset	Get data of a specific Valueset. The test first downloads all Valuesets and then checks if it can download the specirif Valueset.		Step	Input/Data	Expected Results
			1	get all valuesets		
			2	get details of first Valueset in list		Response is not empty and has no errors
TXR-2887	INT_DGCG_get_valueset_with_unauthenticated_NBTLS			Step	Input/Data	Expected Results
			1	create custom authentication certificate		
			2	get all valuesets with custom certificate		Response http status code should be "401"
TXR-3004	INT_DGCG_neg_upload_rule_with_the_Identifier_of_another_Country	Upload a Rule with the Identifier of another Country		Step	Input/Data	Expected Results
			1	create a valid Invalidation/Acceptance Rule		
			2	change countrycode in Identifier to a wrong country		
			3	upload Rule		Response should have Status Code 403
TXR-3005	INT_DGCG_neg_Value_of_ValidFrom_must_be_before_value_of_ValidTo	Value of ValidFrom must be before value of ValidTo		Step	Input/Data	Expected Results
			1	create a valid Invalidation/Acceptance Rule		
			2	set ValidFrom after ValidTo value		
			3	upload Rule		Response Status Code should be 400
TXR-3006		Value of ValidFrom must be within 2 weeks from today		Step	Input/Data	Expected Results

	INT_DGCG_neg_Value_of_ValidFrom_must_be_within_2_weeks_from_today		1	create a valid Invalidation/Acceptance Rule		
			2	set ValidFrom more than "14" days in the future		
			3	upload Rule		Response Code should be 400
TXR-3007	INT_DGCG_neg_Value_of_ValidFrom_must_be_in_future_of_today	Test that the Gateway responds with an error message if the ValidFrom Value is not in the Future		Step	Input/Data	Expected Results
			1	create a valid Invalidation Rule		
			2	change ValidFrom less than "0"h		
			3	upload Rule		Response Status Code should be 400
TXR-3031	INT_DGCG_neg_upload_rule_with_description_text_length_smaller_than_20_characters	A Rule must have a description. Those descriptions must have a length of at least 20 characters.		Step	Input/Data	Expected Results
			1	create a valid Invalidation/Acceptance Rule		
			2	change description to have less than "20" characters		
			3	upload Rule		Response Code should be 400
TXR-3032	INT_DGCG_update_Rule_to_a_new_version_and_ValidFrom_later_than_old_rule	Update a Rule created to a new version and ValidFrom value later than old rule. In the end both Versions of the rule should be downloaded.		Step	Input/Data	Expected Results
			1	create a valid Invalidation/Acceptance Rule		
			2	upload Rule		
			3	change Rule to new version		
			4	upload Rule		Response Code should be "201"
			5	check that Rule has the new version		Rule has the new Version
			6	check that both versions of the rule exist		both versions of the rule exist
TXR-3090	INT_DGCG_neg_upload_rule_with_CertificateType_not_matching_Rule_Identifier	Upload a Acceptance Rule where the CertificateType is not matching the Rule Identifier of the Rule. The Response code should be 400		Step	Input/Data	Expected Results
			1	Create a valid Acceptance Rule		
			2	change CertificateType to be invalid	If Rule Identifier is like "VR-..." the CertificateType should be changed to "General" and else to "Vaccination"	
			3	upload Rule		Response Code should be 400
TXR-3199	INT_DGCG_delete_Rule_with_alias_endpoint	Delete a Rule by using the POST endpoint. This is used so that a body can be used in a POST request instead of a DELETE request.		Step	Input/Data	Expected Results
			1	create a valid Invalidation/Acceptance Rule		
			2	upload Rule		
			3	check that Rule is in Rulelist		Rule is in Rulelist
			4	delete Rule using alias Endpoint		Response had no errors
			5	check that Rule is not in Rulelist		Rule is not in Rulelist
TXR-3200	INT_DGCG_delete_a_dsc_with_alias_endpoint	Delete a DSC certificate of a country by using the POST endpoint. This is used so that a body can be used in a POST request instead of a DELETE request.		Step	Input/Data	Expected Results
			1	create a valid DSC		
			2	upload DSC		DSC is in trustlist
			3	delete public key created using alias Endpoint		public key is deleted in trustlist
TXR-3209	INT_DGCG_upload_valid_Rule_with_cms_header	The content type header of rules normally in the test is "application/cms-text" but it can also be "application/cms" like for the certificates		Step	Input/Data	Expected Results
			1	create a valid Invalidation/Acceptance Rule		
			2	upload Rule with cms header		Status Code 200
			3	check that Rule is in Rulelist		Rule is in Rulelist
			4	delete Rule created		

TXR-3213	INT_DGCG_RAT_valueset_equal_to_JRE_database	The National Backend should update the RAT Valuesets from the JRC database.		Step	Input/Data	Expected Results
			1	get RAT Valuesets from JRC database		
			2	get RAT Valuesets from Gateway		
			3	check that RAT Valuesets from JRC database and Gateway match		all Values of JRE Database are in Gateway and are marked active if they are in the common List
TXR-4524		Regression test of the creation of the QR-codes for TEST-, VAC- and REC-certificates with the available value-sets . This test includes the visible check of the value-sets on the distribution-service on TST-Environment (https://dgca-businessrule-service-eu-test.cfapps.eu10.hana.ondemand.com/valuesets/) too: Visible check, that the extension-option "Valid-Until-Field" is at least a.)- used b.)- notused by one value set.		Step	Input/Data	Expected Results
			1	open the data entry mask		Data Entry Mask is shown
			2	insert Family name in textfield "Family name"		"Family name" is shown in textfield
			3	insert given name in textfield "Given name"		"Given name" is shown in textfield
			4	Choose Date of Birth Format		The textfield of DOB changes its format according to the choosen format
			5	insert date of birth in textfield with picker 'Date of Birth'		date is shown in textfield
			6	insert "Disease/Agent*" in textfield Disease/Agent*		"Disease/Agent*" is shown in textfield. All entries/values correspond to the actual version of the document "EU eHealthNetwork: Value Sets for Digital Covid Certificates. version 1.0, 2021-04-16, section 2.1" Actual: "COVID-19"
			7	choose vaccination type in combo box 'Vaccine/Prophylaxis*'		vaccination type is shown textfield. All actual entries/values: SARS-CoV-2 antigen vaccine SARS-CoV-2 mRNA vaccine covid-19 vaccines
			8	choose medical product in combo box 'Medicinal Product*'		medical product is shown in textfield. All entries/values correspond to the actual version of the document "EU eHealthNetwork: Value Sets for Digital Covid Certificates. version 1.0, 2021-04-16, section 2.3" Actual at least: Comirnaty COVID-19 Vaccine Moderna Vaxzevria COVID-19 Vaccine Janssen CVnCoV NVX-CoV2373 Sputnik V Convidecia EpiVacCorona BBIBP-CorV Inactivated SARS-CoV-2 (Vero Cell) CoronaVac Covaxin (also known as BBV152 A, B, C)
			9			Organisations Management System is shown in textfield.

	INT_IssApp_Create_QR-Code_TEST_VAC_REC_Regression			choose Organisations Management System* in combo box 'Organisations Management System*'		All entries/values correspond to the actual version of the document "EU eHealthNetwork: Value Sets for Digital Covid Certificates. version 1.0, 2021-04-16, section 2.4" Actual at least: AstraZeneca AB Biontech Manufacturing GmbH Janssen-Cilag International Moderna Biotech Spain S.L. Curevac AG CanSino Biologics China Sinopharm International Corp. - Beijing location Sinopharm Weiqida Europe Pharmaceutical s.r.o. - Prague location Sinopharm Zhijun (Shenzhen) Pharmaceutical Co. Ltd. - Shenzhen location Novavax CZ AS Gamaleya Research Institute Vector Institute Sinovac Biotech Bharat Biotech
			10	insert dose number in Textfield "Dose Number*"		dose number is shown in textfield. All entries/values corresponds to the actual version of the document "EU eHealthNetwork: Value Sets for Digital Covid Certificates. version 1.0, 2021-04-16, section 2.5". The value has to be less or equal to the total series of doses.
			11	insert total series of doses in Textfield "Total Series of Doses*"		total series of doses is shown in textfield. All entries/values corresponds to the actual version of the document "EU eHealthNetwork: Value Sets for Digital Covid Certificates. version 1.0, 2021-04-16, section 2.5"
			12	insert vaccination date in textfield with picker'vaccination date'		vaccination date is schown textfield
			13	choose Issuer country in combo box 'Issuer Country*'		issuer country is shown in textfield. All entries/values should correspond to ISO 3166 Country Codes (2-letter codes).
			14	insert certificate issuer in textfield "Certificate Issuer*"		Certificate Issuer is shown in textfield
			15	push "next" button		QR-code will be generated with inserted data
			16	Repeat the test with all fields to fill in for the certificate of type "TEST"		QR-Code for the type TEST is generated correctly with all data filled in.
			17	Repeat the test with all fields to fill in for the certificate of type "RECOVERY"		QR-Code for the type RECOVERY is generated correctly with all data filled in.
			18	Visible check on TST-Environment (here for TST-environment: https://dgca-businessrule-service-eu-test.cfapps.eu10.hana.ondemand.com/valuesets/),		The result of the check can be confirmed as described in step 18

			that the extension-option "Valid-Until-Field" is at least a.)- used b.)- notused by one value set.		described in step 18.