Regressionstest specification E2E OAT Wallet-/Verifier App

TC-ID	Testcase	Description	Manual test steps			
TXR-2028	INT_WalletApp_Citizen_scans_QR-Code	scann the QR-code with the wallet app		Step	Input/Data	Expected Results
			1	open the (internal) QR-codescanner via "scan code"		QR-codescanner starts
			2	position the QR-Code under the camera		QR-code is displayed sharply
TXR-2029	INT_WalletApp_shows_the_certificate_on_mobile_device	show the saved certificate on mobile device within the details of the data		Step	Input/Data	Expected Results
			1	open the internal storage		all scanned QR-codes will be listed
			2	Choose one QR-code		QR-code will be displayed on screen
TXR-2032	INT_WalletApp_biometric_security	on Start the WalletApp a biometric request has to start. To be sure that a verified person get access to WalletApp Data		Step	Input/Data	Expected Results
			1	open WalletApp on Mobile Device		biometric data are requested
			2	scan your biometric data		WalletApp starts
TXR-2033	INT_WalletApp_negative_biometric_security	on Start the WalletApp a biometric request has to start. To be sure that a verified person get access to WalletApp Data		Step	Input/Data	Expected Results
			1	open WalletApp on Mobile Device		biometric data are requested
			2	scan wrong biometric data		Error: Access denied
TXR-2075	INT_VERIAPP_verify_qr_code_for_a_valid_dgc	A Digital Green Certificate with: 1) a valid QR Code; 2) valid Payload; 3) valid Attributes. is presented for offline verification. The Verifier App confirms that the DGC is valid. It also tests that the same DGC can be verified twice by the same VeriApp instance.		Step	Input/Data	Expected Results
			1	VeriApp scans QR-Code.		QR-Code is approved as verified.
			2	VeriApp scans the same QR-Code for a second time.		QR-Code is again approved as verified.
TXR-2077	INT_VERIAPP_neg_verify_qr_code_with_invalid_signature	A Digital Green Certificate (DGC) with invalidly signed QR-Code is presented for offline verification. The Verifier App evaluates the DGC as invalid.		Step	Input/Data	Expected Results
			1	VeriApp scans QR-Code.		The VeriApp evaluates the DGC as invalid.
TXR-2079	INT_VERIAPP_neg_verify_qr_code_with_invalid_payload_syntax	A Digital Green Certificate with correct signature but syntactically invalid payload (e.g. missing name etc.) is presented for verification. The signature is validated but the DGC is evaluated as invalid due to invalid Payload. An Error Code "Invalid Payload" is returned.		Step	Input/Data	Expected Results
			1	VeriApp scans QR-Code.		QR-Code signature is approved as valid.
			2	VeriApp reads payload.		The DGC is evaluated as invalid. An Error Code "Invalid Payload" is shown.
TXR-2084	INT_VERIAPP_render_dgc_for_type_PCRtest	A validly signed Digital Green Certificate of type (PCR) TEST is presented for verification. The testcase tests presentation of the DGC Data for the DGC of type test, independently of test result (postive or negative).		Step	Input/Data	Expected Results
			1	VeriApp scans QR-Code, registrated in IOS-WalletApp.		The DGC is approved as valid and the Contents Data is presented for type TEST. The content is preseneted as a positive or negative quick test.
			2	VeriApp scans QR-Code, registrated in Android-WalletApp.		The DGC is approved as valid and the Contents Data is presented for type TEST. The content is preseneted as a positive or negative quick test.
			3	VeriApp scans QR-Code, created from the Issuer Web Application (on paper or on the screen.)		The DGC is approved as valid and the Contents Data is presented for type TEST. The content is preseneted as a positive or negative quick test.
TXR-2085	INT_VERIAPP_render_dgc_for_type_vac	A valid Digital Green Certificate of type VAC (owner has been vaccinated) is presented for verification. The testcase tests presentation of the DGC Data.		Step	Input/Data	Expected Results
			1	VeriApp scans a created QR-Code from Issuer Web Application (on paper or on the screen).		The DGC is approved as valid and the Contents Data is presented for type VAC.
			2	VeriApp scans QR-Code in Android-Wallet App		The DGC is approved as valid and the Contents Data is presented for type VAC.
			3	VeriApp scans QR-Code in IOS-Wallet App		The DGC is approved as valid and the Contents Data is presented for type VAC.
TXR-2086	INT_VERIAPP_render_dgc_for_type_rec	A valid Digital Green Certificate of type REC (owner has recovered) is presented for verification. The testcase tests presentation of the DGC Data.		Step	Input/Data	Expected Results
			1	VeriApp scans QR-Code.		The DGC is approved as valid and the Contents Data is presented for type REC.
TXR-2087	INT_VERIAPP_fetch_an_use_manually_trigered	The Verifier App has to support the manual triggering of the synchronisation process.		Step	Input/Data	Expected Results
			1	The VerifierApp has been installed. Internet connection is available. It has been less than 24 hours since the last synchronisation. The user triggers the synchronisation manually.		A Synchronisation process has been triggered and the keys have been updated.
TXR-2088		This testcase examines the case where no synchronisation has		Step	Input/Data	Expected Results

	INT_VERIAPP_fetch_and_use_resynchronise_after_offline_state	taken place in the last 24 hours due to missing internet connection. As soon as the internet connection is available again, the verifier app should initiate synchronisation.	1	The VerifierApp has been installed and at it is has been 24 hours since the installation.		A Synchronisation process has been triggered and the keys have been updated within the last 24 hours.
			2	After the synchronisation has been done, the internet is switched off for at least 24 hours.		No synchronisation of the keys database could take place.
			3	The internet connection is available again.		The verifier app initiates synchronisation (fetch and use) within the next 24 hours.
TXR-2089	INT_VERIAPP_fetch_an_use_daily_synchronisation	The Verifier App has to synchronise its public key database daily with the backend. Internet Connection is available.		Step	Input/Data	Expected Results
			1	The VerifierApp has been installed and at it is has been 24 hours since the installation.		A Synchronisation process has been triggered and the keys have been updated within the last 24 hours.
TXR-2094	INT_VERIAPP_render_dgc_for_test_result_positive	A validly signed Digital Green Certificate of type POSITIVE TEST (owner has tested positive) is presented for verification.		Step	Input/Data	Expected Results
			1	VeriApp scans QR-Code.		The DGC is read and a positive test result is displayed.
TXR-2103	INT_WalletApp_register_QR-Code_with_TAN	The QR-code is only allowed to save on one device. Therefor the citizen gets a TAN which can be used only one time. After the registration, the TAN can't be used twice.		Step	Input/Data	Expected Results
			1	scann QR-code with integrated barcode-scanner		Barcode will be shown on screen
			2	push save button		TAN will be requested
			3	insert valid TAN		scanned QR-code will be saved
TXR-2105	INT_WalletApp_start_WalletApp_with_PIN	If the citizen has no biometric data on his mobile device it shoul be possible to start the device by PIN		Step	Input/Data	Expected Results
			1	start the WalletApp on mobile device		biometric data are requested
			2	user push cancel		a user PIN is requested
			3	insert the correct PIN		WalletApp starts
TXR-2106	INT_WalletApp_negative_register_QR-Code_with_TAN_-_TAN_expired	The QR-code is only allowed to save on one device. Therefor the citizen gets a TAN which can be used only once for a defined time after creation. (Expirationtime has to be defined) After this time, the TAN can't be used anymore.		Step	Input/Data	Expected Results
			1	scann QR-code with integrated barcode-scanner		Barcode will be shown on screen
			2	push save button		TAN will be requested
			3	insert expired TAN		An error occurred: TAN expired QR-code will not be saved
TXR-2107	INT_WalletApp_negative_register_QR-Code_with_TAN _twice	The QR-code is only allowed to save on one device. Therefor the citizen gets a TAN which can be used only one time. After the registration, the TAN can't be used twice.		Step	Input/Data	Expected Results
			1	scann QR-code with integrated barcode-scanner		Barcode will be shown on screen
			2	push save button		TAN will be requested
			3	insert valid TAN a seconed time		an error occurred: TAN can't be used twice
TXR-2182	INT_VERIAPP_render_dgc_for_test_result_negative	A validly signed Digital Green Certificate of type Negative TEST (owner has tested negative) is presented for verification. The		Step	Input/Data	Expected Results
			1	VeriApp scans QR-Code.		The DGC is read and a negative test result is displayed.
TXR-2187	INT_WalletApp_valid_TAN_which_does_not_belong_to_this_qr-code	Issuer has created two different QR-codes. Each with valid TAN. He gave citizen A qr-code A with valid TAN to qr-code B. He gave citizen B qr-code B with valid TAN to qr-code A. So, we have A valid TAN which belongs to an other valid QR-code.		Step	Input/Data	Expected Results
			1	scann QR-code with integrated barcode-scanner		Barcode A will be shown on screen
			2	push save button		TAN will be requested
			3	insert valid TAN B which does not belong to this qr-code (dgci)		TAN B will be accepted by wallet app
			4	send data to national backend		national backend will proof the data and returns an error to wallet app
			5	get error code from national backend		qr-code will not be saved
TXR-2205	INT_WalletApp_start_WalletApp_with_wrong_PIN	If the citizen has no biometric data on his mobile device it shoul be possible to start the device by PIN		Step	Input/Data	Expected Results
			1	start the WalletApp on mobile device		pin is requested instead of biometric data. Only works when no biometric data are saved
			2	insert the wrong PIN		WalletApp shows an error
TXR-2823	INT_VERIAPP_BR_choose_CoD	Precondition: The default ruleset (CoA) is the initial setting. Verifier has to choose the ruleset from CoD (Country of departure). The Verifier then switches back to the default ruleset (CoA).		Step	Input/Data	Expected Results
			1	Verifier starts VerifierApp		VerifierApp starts
			2	Verifier selects "settings"		Settings will open. The default ruleset (CoA) is initially loaded.
			3	Verifier selects the ruleset of CoD		Ruleset will be set to CoD.
			4	Verifier switches back to default ruleset CoA.		Default ruleset CoA is loaded.
TXR-2824	INT_VERIAPP_BR_choose_CoA	A user with a verifier app (“verifier”) in the country of arrival (CoA) wants to check whether a DCC holder fulfills all		Step	Input/Data	Expected Results
			1	Verifier starts VerifierApp		VerifierApp starts

	INT_VERIAPP_BR_choose_CoA	requirements of the CoA. The CoA is his default setting for scanning the provided DCCs.	2	Verifier selects "settings"		The default for ruleset CoA is set.
TXR-2825	INT_VERIAPP_BR_business_validation_QR-code_multiple_rules	Given a QR-Code which is technically valid, a business validation is to be run with respect to the QR-Code's Country of Issuance. There exist more than one available rules. The test checks the good case scenario where business validation is successful (i.e. positive test case).		Step	Input/Data	Expected Results
			1	Verifier scans a technically valid QR-Code. The QR-Code is created in a way that the business rules applied to the country of issuance are valid as well.		The QR-Code is scanned. Technical check is passed. Country of Issuance is read.
			2	Verifier sets the ruleset corresponding to the displayed Issuance Country, unless this is already the default value set.		The rules value set for the country of issuance is set.
			3	Verifier scans the QR-Code again, this time with the rules valueset being set.		VerifierApp shows green certificate, due to successful business validation.
TXR-2827	INT_WALLETAPP_BR_check_verificationDateTime_is_currentDateTime	The rules are checked against the Verification DateTime. If no Verification DateTime is provided, it will be filled with the current date and time. Precondition: The QR code contains information on 1 event with one entry: either a vaccination, a negative test, or a recovery statement (V, T or R). Create a valid PCR- or RAT test with the "time rule" (tbd) where verification DateTime is missing. Outcome: Wallet App will use the current date and time as verification DateTime.		Step	Input/Data	Expected Results
			1	Open a saved DCC in the wallet app and press "Check validity".		The current date is set in the field "Check the date" per default.
			2	Pess "I agree, check validity".		Validity is checked.
TXR-2828	INT_WALLETAPP_BR_negative_check_verificationDateTime_is_currentDateTime	The rules are checked against the Verification DateTime. If no Verification DateTime is provided, it will be filled with the current date and time. Precondition: The QR code contains information on 1 event with one entry: either a vaccination, a negative test, or a recovery statement (V, T or R). Create a valid PCR- or RAT test with the "time rule" (tbd) where verification DateTime is missing. Outcome: Wallet App will use the current date and time as verification DateTime.		Step	Input/Data	Expected Results
			1	Scan an expired PCR- or RAT test with the "time rule" (tbd) where verification DateTime is missing.		The "Verification Datetime" is automatically filled with the current date and time. The validation is carried out with a red validation result.
TXR-2829	INT_VERIAPP_BR_check_signingExpiration_supersedes_certificateExpiration	In this case, we want to check, that the signing certificate expiration datetime supersedes the expiration datetime in the Green certificate. Precondition: A qr-codes which is signed with a DSC-certificate which becomes invalid during testing but the green certificate will be valid longer. For example: green certificat validity: 31.12.2022 DSC validity: 01.08.2021		Step	Input/Data	Expected Results
			1	Scan green certificate wich is actually valid		verifier App shows green validation result
			2	wait a few hours	time has to be defined	Verifier App shows invalid certificate
TXR-2830	INT_VERIAPP_BR_check_issuer_timeZone_is_used	In this case, we check that the time zone specified in the QR code is taken into account when checking the period of validity. Precondition:		Step	Input/Data	Expected Results
			1	Set device time to Finnish time zone		the timezone of the device is set to Finnish timezone
			2	Scan qr-code generated within German device time		VerifierApp shows the correct UTC-time

		A QR-Code created with respect to a different time zone than the time zone of the verifier app device.				
TXR-2831	INT_VERIAPP_BR_ruleset_is_used_for_validation	In this Testcase, we check that during the validation, all valid rules in the ruleset for selected country are actually checked against the qr-code. For this perpose we need a QR-Code which conforms to all but one the selected country's rules.		Step	Input/Data	Expected Results
			1	Given a QR-Code which conforms to all but one the selected country's rules, scan it with the verifier app.		A validation error occurs and the verifier app feedbacks the validation result to the user in a table format.
TXR-2848	INT_WalletAPP_BR_ruleset_is_used_for_validation	In this Testcase, we check that during the validation, all valid rules in the ruleset for selected country are actually checked against the qr-code. Precondition: Citizen has a valid certificate stored in the walletApp		Step	Input/Data	Expected Results
			1	Choose a certificate		Details of the certificate is shown
			2	choose a ruleset of a eu-country, where not the certificate was created		The ruleset is choosen to check and each rule is checked. The screen shows the validation result. (valid = green arrow, invalid = red cross)
TXR-2849	INT_WalletAPP_BR_negative_check_ruleengine_version	Check that in the event of an incompatible rule engine "Rule engine version> current version" (?), The human readable fallback case is used (Section 6.4.1 Incompatible Rule Engine Version) (In case of incompatible rule-engine, the verifierApp checks the qr-code with the old ruleset.(?))		Step	Input/Data	Expected Results
			1	Given incompatible rule engines, the wallet app scans a technically valid QR-Code.		The human readble fallback is presented as feedback in a table format.
TXR-2850	INT_WalletAPP_BR_check_issuer_timeZone_is_used	In this case, we check that the time zone specified in the QR code is taken into account when checking the period of validity. Precondition: a QR-code with another timezone than the tomezone of the mobile with the verifier app-- in this case the timezone for Finland - is created.		Step	Input/Data	Expected Results
			1	Set the Mobile to Finnish time zone		the timezone of the mobile is set to Finnish timezone
			2	scan qr-code generated with german time		walletApp request TAN
			3	Insert valid TAN		WalletApp shows certificate and the correct UTC-time
TXR-2852	INT_WalletApp_BR_compareCertificate_with_country_ruleset	The holder must be able to select each onboarded country from the complete EU country list (In order to be able to check its selected ruleset against a specific selected QR code). Precondition: List of all onboared countries is known a valid certificate is already scanned and successfully claimed		Step	Input/Data	Expected Results
			1	Choose a certificate		Details of the certificate is shown
			2	Check validity for ruleset of a EU-Country other than the issuer country itself.		The ruleset is choosen to check and each rule is checked. The screen shows the validation result. (valid = green arrow, invalid = red cross)
TXR-2914	INT_VERIAPP_BR_process_result_invalid	The scanned techniclally valid QR Code contains a rule, which evaluates to false. Scan a vaccination certificate with the Acceptance Rule for Belgium. Link to the Rules Specification: https://telekom.sharepoint.de/sites/DGCG/_layouts/OneNote.aspx?id=%2Fsites%2FDGCG%2FSiteAssets%2FNotizbuch%20f%C3%BCr%20DGCG&wd=target%28Aktionen.one%7CDE069537-8D0A-48C8-8E26-CFDAAB47D15C%2FTestdaten%7CAADE1931-F80E-4FBC-AED7-A26A1452BC11%2F%29		Step	Input/Data	Expected Results
			1	Verifier starts verifierApp		verifierApp starts successful
			2	Verifier choose the needed country ruleset		the needed ruleset will be loaded
			3	Verifier scans a technically valid but logically invalid qr-code.		VerifierApp shows red certificate and the details of result. The results are collected and presented in a table format.
TXR-2935	INT_VERIAPP_BR_rules_available_for_schema_version_less_than_48_hr_old	The technical validation of the received certificate for expiration and schema compatibility was successful. The process can continue with the rule engine checkup but all rules available for the schema are less than 48 hr old.		Step	Input/Data	Expected Results
			1	Scan QR Coide.		Rule is not yet applied.
TXR-2936		Given a QR-Code which is technically valid, a business validation is to be run with respect to the QR-Code's Country of Issuance. There exists only one available rule.		Step	Input/Data	Expected Results

	INT_VERIAPP_BR_business_validation_QR-code_single_rule	The test checks the good case scenario where business validation is successful (i.e. positive test case).	1	Verifier scans a technically valid QR-Code. The QR-Code is created in a way that the business rules applied to the country of issuance are valid as well.		The QR-Code is scanned. Technical check is passed. Country of Issuance is read.
			2	Verifier sets the ruleset corresponding to the displayed Issuance Country, unless this is already the default value set.		The rules value set for the country of issuance is set.
			3	Verifier scans the QR-Code again, this time with the rules valueset being set.		VerifierApp shows green certificate, due to successful business validation.
TXR-2937	INT_VERIAPP_BR_check_validationrules_of_CoA_and_invalidationRules_of_IssuerCountry_is_used	In case we check if the invalidation rules are used by set the certificate invalid by a rule of the invalidation rule. A Holder travels to another country. In this country the certificate is valid. By checking the invalidation Rules, the certificate is invalid. Testdata: a certificate which is valid in the CoA (France) but invalid in another Country (Germany) by invalidation rule or another rule.		Step	Input/Data	Expected Results
			1	Verifier starts VerifierApp		Verifier-App starts
			2	Verifier scans the certificate for the selected Country Germany		The Verifier-App shows an invalid certificate and the reason.
			3	Verifier scans the certificate for the selected Country France		The Verifier-App shows a valid certificate.
TXR-3374	INT_WalletApp_SavedData_After_Update	This test case tests whether all previously saved personal data in the wallet app (QR-Codes Test, VAC und REC, biometrric sec. password) remain unchanged after updating the app. Precondition: At least one certificate of each of the three types (VAC, TEST, REC) has been saved in the wallet app.		Step	Input/Data	Expected Results
			1	Update the wallet app to the latest version (without previously deleting the old app). Open the app.		Biometric login data remains unchanged. All previously saved certificate are still available.
TXR-4116	TB_ENHANCE_VERIAPP_DCC_exported_TST	Check if a exported TEST DCC is readable by the verifier app.		Step	Input/Data	Expected Results
			1	A DCC of type TEST has been already already exported from the wallet app. The user let it be read by the verifier app.		The DCC of type TEST can be read by the verifier.
TXR-4117	TB_ENHANCE_VERIAPP_DCC_exported_REC	Check if a exported REC DCC is readable by the verifier app.		Step	Input/Data	Expected Results
			1	A DCC of type REC has been already already exported from the wallet app. The user let it be read by the verifier app.		The DCC of type REC can be read by the verifier.
TXR-4118	TB_ENHANCE_VERIAPP_DCC_exported_VAC	Check if a exported VAC DCC is readable by the verifier app.		Step	Input/Data	Expected Results
			1	A DCC of type VAC has been already already exported from the wallet app. The user let it be read by the verifier app.		The DCC of type VAC can be read by the verifier.

Regressionstest specification E2E OAT_IssuerWeb

TC-ID	Testcase	Description		Manual test steps		
TXR-2013		Open the WebApp in Browser		Step	Input/Data	Expected Results
	INT_IssApp_Start_WebApp		1	Open Browser	https://issuance-dgca-test.cfapps.eu10.hana.ondemand.com/record/vac	WebApp is starting
			2	Teststep		Teststep
TXR-2017		Insert relevant Data in Issuer App. Send inserted Data to national backend. According to the document "EU eHealthNetwork: Value Sets for Digital Covid Certificates. version 1.0, 2021-04-16" the data elements are defined in detail, which will be included in digital implementations in Europe (see attachment). They serve to ensure interoperability on semantic level and will allow technical implementations for the DGC to address this issue uniformly.		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 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 2.2" Actual: 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: 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)
	INT_IssApp_Create_QR-Code		9			Organisations Management System is shown in textfield.

				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: 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.
TXR-2019	INT_IssApp_Request_signed_QR-Code	send unsigned QR-code to national Backend, which signs it and send it back to the Issuer App. The signed QR-code will be displayed on screen		Step	Input/Data	Expected Results
			1	Send created QR-Code from type TEST to national backend via "finish process" button		QR-Code will be sent - national backend returns signed QR-Code
			2	Repeat the test for the QR-Code of type VAC		QR-Code will be sent - national backend returns signed QR-Code
			3	Repeat the test for the QR-Code of type REC		QR-Code will be sent - national backend returns signed QR-Code
TXR-2020	INT_IssApp_Print_signed_QR-Code	print the QR-code/vaccination certificate with included print service(?)		Step	Input/Data	Expected Results
			1	Create signed QR-code from type TEST		signed QR-code TEST created
			2	Push the "Create PDF" Button		A PDF document is created with all dates filled in.
			3	Repeat the test for an QR-Code of type VAC		The signed QR-Code VAC is created. A PDF document of this QR-Code with all the filled in data is created correctly.
			4	Repeat the test for an QR-Code of type REC		The signed QR-Code REC is created. A PDF document of this QR-Code with all the filled in data is created correctly.
TXR-2113		Insert relevant Data in Issuer App with wrong birthdate. Start creation of QR-code. Get QR-code with wrong birthday. proof data in QR-code and find the misstake. correct birthday in Issuer App and create new QR-code.		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

	INT_IssApp_Create_corrected_QR-Code		3	insert given name in textfield "Given name"		"Given name" is shown in textfield
			4	insert date of birth in textfield with picker 'Date of Birth'		date is shown in textfield
			5	insert "Disease/Agent*" in textfield Disease/Agent*		"Disease/Agent*" is shown in textfield
			6	choose vaccination type in combo box 'Vaccine/Prophylaxis*'		vaccination type is shown textfield
			7	choose medical product in combo box 'Medicinal Product*'		medical product is shown in textfield
			8	choose Organisations Management System* in combo box 'Organisations Management System*'		Organisations Management System is shown in textfield
			9	insert dose number in Textfield "Dose Number*"		dose number is shown in textfield
			10	insert total series of doses in Textfield "Total Series of Doses*"		total series of doses is shown in textfield
			11	insert vaccination date in textfield with picker'vaccination date'		vaccination date is schown textfield
			12	choose Issuer country in combo box 'Issuer Country*'		issuer country is shown in textfield
			13	insert certificate issuer in textfield "Certificate Issuer*"		Certificate Issuer is shown in textfield
			14	push "next" button		QR-code cannot be generated and showed the field "Date of Birth*" as a mandatory-field, requires for fill in.
			15	fill in the correct value for the field "Date of Bith*" and push "next" button again		QR-code will be generated with inserted data
			16	push "correct patient data" button		inserted data will be shown in data entry mask
			17	Changed correctly all the values in the fields and push the button "Next" again.		The QR-Code with the changed values/datas is generated and shown correctly. A TAN for claiming this QR-Code in Wallet App is shown.
			18	push "Finish" button after scanning this QR-Code in the Wallet App with the generated TAN.		IssueWeb returns to start mask. The QR-Code is claimed correctly in the Wallet App.
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)
	INT_IssApp_Create_QR-Code_TEST_VAC_REC_Regression		9	choose Organisations Management System* in combo box 'Organisations Management System*'		Organisations Management System 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 2.4" 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/), that the extension-option "Valid-Until-Field" is at least a.)- used b.)- notused by one value set.		The result of the check can be confirmed as described in step 18.

Test specification E2E OAT Import_Export_ExchangeNFC

TC-ID	Testcase	Description	Manual test steps			
TXR-3860	TB_ENHANCE_WalletApp_DCC_TEST_Export_as_PDF_Export_via_Email	2.2 DCC Backup (Export) During travel the paper or the digital version of an DCC can be lost or damaged. To avoid this, it should be possible to generate a PDF/PNG to backup or print the DCC. A traveler is then able to generate a PDF/PNG/JPEG in the wallet which can be printed or stores as a picture of the DCC. Here: a DCC-Test will be shared via Email as a PDF-document.		Step	Input/Data	Expected Results
			1	A DCC-TEST has been already saved in the wallet app. User wants to share this DCC via email and press on SHARE-Button and select the medium email to share his/her DCC.		The selected DCC-Test is sent correctly via email.
TXR-3861	TB_ENHANCE_WalletApp_DCC_Test_Exchange_via_NFC_Android_2_Android	2.3 DCC Exchange A user wants to present the DCC TEST-QR code to NFC readers, to enable future use cases like faster and less error prone DCC verification and semi-automated entry control systems. This test case checks the exchange of items from wallet app to wallet app. Wallet App on Mobile Device A wants to exchange items with Wallet Appon Mobile Device B via NFC.		Step	Input/Data	Expected Results
			1	User with Mobile Device A (Source) transfers his/her TEST-DCC to wallet app on Mobile Device B (destination).		Wallet App on Mobile Device B (destination) contains item TEST-DCC from Wallet App on Mobile Device A (source). TEST-SCC in Wallet App on Mobile Device A (source) remain unchanged.
TXR-3874	TB_ENHANCE_WalletApp_DCC_TEST_Exchange_via_NFC_Android_2_NFC-Reader	To exchange data between devices for the purpose of verification and sharing, the NFC will be integrated into the wallet and the verifier app. This should allow to verify DCCs directly Smartphone to Smartphone, Smartphone to NFC Reader or exchange wallet items between smartphones. This test cases checks whether the DCC can be read from a smartphone (i.e. Wallet App) to NFC Reader.		Step	Input/Data	Expected Results
			1	User presents a DCC from his/her wallet app to be read by a NFC Reader.		DCC is successfully read.
TXR-3893	TB_ENHANCE_WalletApp_DCC_REC_Export_as_Image_to_PrinterApp	2.2 DCC Backup (Export) During travel the paper or the digital version of an DCC can be lost or damaged. To avoid this, it should be possible to generate a PDF/PNG to backup or print the DCC. A traveler is then able to generate a PDF/PNG/JPEG in the wallet which can be printed or stores as a picture of the DCC Here: A DCC-REC can be selected and sent as an Image to a PrinterApp for print.		Step	Input/Data	Expected Results
			1	A DCC-REC has been already saved in the wallet app. User wants to print this DCC. He/She press on SHARE-Image-Button and select his/her medium Printer-App to send his/her DCC to the Printer-App		The selected DCC-REC is correctly sent as a image to the printerApp for print.
TXR-3894	TB_ENHANCE_WalletApp_DCC_TEST_Export_as_Image_on_Smartphone_via_DataManagerApp	2.2 DCC Backup (Export) During travel the paper or the digital version of an DCC can be lost or damaged. To avoid this, it should be possible to generate a PDF/PNG to backup or print the DCC. A traveler is then able to generate a PDF/PNG/JPEG in the wallet which can be printed or stores as a picture of the DCC. Here: A DCC-TEST can be selected and stored as a image correctly on the smartphone via DataManagerApp		Step	Input/Data	Expected Results
			1	A DCC-TEST has been already saved in the wallet app. User wants to store this DCC on his smarthone as an image. He/She press on SHARE-Image-Button and select his/her medium DataManagerApp (as an example) to store his/her DCC.		The selected DCC-TEST is stored correctly as an image on his smartphone.
TXR-3898	TB_ENHANCE_WalletApp_DCC_VAC_Export_as_PDF_Export_via_Email	2.2 DCC Backup (Export) During travel the paper or the digital version of an DCC can be lost or damaged. To avoid this, it should be possible to generate a PDF/PNG to backup or print the DCC. A traveler is then able to generate a PDF/PNG/JPEG in the wallet which can be printed or stores as a picture of the DCC Here: A DCC_VAC is shared via Email as a PDF-document.		Step	Input/Data	Expected Results
			1	A DCC-VAC has been already saved in the wallet app. User wants to share this DCC via email and press on SHARE-Button and select the medium email to share his/her DCC-document.		DCC-VAC is sent correctly via email.
TXR-3899		2.2 DCC Backup (Export)		Step	Input/Data	Expected Results

	TB_ENHANCE_WalletApp_DCC_REC_Export_as_PDF_to_PrinterApp	During travel the paper or the digital version of an DCC can be lost or damaged. To avoid this, it should be possible to generate a PDF/PNG to backup or print the DCC. A traveler is then able to generate a PDF/PNG/JPEG in the wallet which can be printed or stores as a picture of the DCC Here: A DCC-REC can be selected and sent as a PDF-document to a PrinterApp for print.	1	A DCC-REC has been already saved in the wallet app. User wants to print this DCC. He/She press on SHARE-PDF-Button and select his/her medium Printer-App to send his/her DCC to the Printer-App		The selected DCC-REC is sent as a PDF-document correctly to the PrinterApp and can be printed from there.
TXR-3902	TB_ENHANCE_WalletApp_DCC_VAC_Export_as_Image_on_Smartphone_via_DataManagerApp	2.2 DCC Backup (Export) During travel the paper or the digital version of an DCC can be lost or damaged. To avoid this, it should be possible to generate a PDF/PNG to backup or print the DCC. A traveler is then able to generate a PDF/PNG/JPEG in the wallet which can be printed or stores as a picture of the DCC. Here: A DCC-VAC can be selected and stored correctly as an image on the smartphone.		Step	Input/Data	Expected Results
			1	A DCC-VAC has been already saved in the wallet app. User wants to store this DCC on his smarthone as an image. He/She press on SHARE-Image-Button and select his/her medium DataManagerApp (as an example) to store his/her DCC.		The selected DCC-VAC is stored correctly as an image on the smartphone.
TXR-3911	TB_ENHANCE_WalletApp_DCC_TEST_Exchange_via_NFC_Android_2_iOS	2.3 DCC Exchange A user wants to present the DCC TEST-QR code to NFC readers, to enable future use cases like faster and less error prone DCC verification and semi-automated entry control systems. This test case checks the exchange of items from wallet app to wallet app. Wallet App on Mobile Device A wants to exchange items with Wallet Appon Mobile Device B via NFC.		Step	Input/Data	Expected Results
			1	User with Mobile Device A (Source) transfers his/her DCC-TEST to wallet app on Mobile Device B (destination).		Wallet App on Mobile Device B (destination) contains DCC-TEST from Wallet App on Mobile Device A (source). DCC-TEST-ITEM in Wallet App on Mobile Device A (source) remain unchanged.
TXR-3924	TB_ENHANCE_WalletApp_DOC_Image_Export_on_Smartphone_via_Data Manager	2.2 DCC Backup (Export) A traveler is able to export external images (not DCC).		Step	Input/Data	Expected Results
			1	An image-document has been already saved in the wallet app. User wants to share this document via email and press on SHARE-Button and select the medium Data Manager (as an example)to to store his/her image-document.		The image is stored in the selected folder.
TXR-3925	TB_ENHANCE_WalletApp_ReImport_DCC_TEST_After_Export	2.2 DCC-TEST reimport. A traveler exports a DCC-Test certificate and then imports it again.		Step	Input/Data	Expected Results
			1	A DCC of type TEST has been already already exported from the wallet app. The user tries to import it again.		The DCC of type TEST can be successfully imported.
TXR-3928	TB_ENHANCE_WalletApp_Import_PDF	2.2 DCC Backup (Export) A traveler imports an external pdf-file (not a DCC).		Step	Input/Data	Expected Results
			1	User presses "Import PDF" and selects an external PDF File (Not a DCC) to import.		PDF file is correctly imported in the wallet app. It can be selected and shown thoroughly in the Wallet App.
TXR-3929	TB_ENHANCE_WalletApp_Import_Image_via_Camera	Image import taken by the camera. A traveler imports an image which has been taken by the camera into his wallet App.		Step	Input/Data	Expected Results
			1	The user presses "Add New", "Import Image" and then "Take Photo".		The user takes a photo.
			2	Checks in the "Certificate Wallet"-Display for the image, which has been taken before.		The expected image is there and can be selected to be shown.
TXR-3930	TB_ENHANCE_WalletApp_DOC_PDF_Export_Extern_OnDevice_via_Email	2.2 DCC Backup (Export) A traveler is able to send a PDF-document via e-mail.		Step	Input/Data	Expected Results
			1	A PDF-document has been already saved in the wallet app. User wants to share this document via email and press on SHARE-Button and select the medium email to share his/her PDF-document.		Selected PDF-Document is correctly shared.
TXR-3947	TB_ENHANCE_WalletApp_DCC_TEST_Import_via_Scan	2.2 DCC Backup (Import) The User imports a DCC of type TEST via QR Code Scan.		Step	Input/Data	Expected Results
			1	The user scans a DCC-TEST QR Code to be imported in the wallet app. The user presses "Add new" and then "Scan certificate".		The DCC is successfully imported.
TXR-3948		2.2 DCC Backup (Import)		Step	Input/Data	Expected Results

	TB_ENHANCE_WalletApp_DCC_VAC_Import_via_Scan	The traveller imports a DCC of type VAC via "scan certificate" QR Code.	1	The user scans a DCC-VAC QR Code to be imported in the wallet app. The user presses "Add new" and then "Scan certificate".		The new DCC has been successfully imported. The previously available DCC is still there.
TXR-3949	TB_ENHANCE_WalletApp_DCC_REC_Import_via_Scan	2.2 DCC Backup (Import) The traveller wants to import a DCC certificate of type REC via "scan certificate".		Step	Input/Data	Expected Results
			1	The user scans a DCC-REC QR Code to be imported in the wallet app. The user presses "Add New" and "Scan certificate".		The new DCC has been successfully imported. The previously available DCC is still there.
TXR-3958	TB_ENHANCE_WalletApp_DCC_VAC_Exchange_via_NFC_Android_2_Android	2.3 DCC Exchange A user wants to present the DCC VAC-QR code to NFC readers, to enable future use cases like faster and less error prone DCC verification and semi-automated entry control systems. This test case checks the exchange of items from wallet app to wallet app. Wallet App on Mobile Device A wants to exchange items with Wallet Appon Mobile Device B via NFC.		Step	Input/Data	Expected Results
			1	User with Mobile Device A (Source) transfers his/her VAC-DCC to wallet app on Mobile Device B (destination).		Wallet App on Mobile Device B (destination) contains item VAC-DCC from Wallet App on Mobile Device A (source). VAC-SCC in Wallet App on Mobile Device A (source) remain unchanged.
TXR-3959	TB_ENHANCE_WalletApp_DCC_REC_Exchange_via_NFC_Android_2_Android	2.3 DCC Exchange A user wants to present the DCC REC-QR code to NFC readers, to enable future use cases like faster and less error prone DCC verification and semi-automated entry control systems. This test case checks the exchange of items from wallet app to wallet app. Wallet App on Mobile Device A wants to exchange items with Wallet Appon Mobile Device B via NFC.		Step	Input/Data	Expected Results
			1	User with Mobile Device A (Source) transfers his/her REC-DCC to wallet app on Mobile Device B (destination).		Wallet App on Mobile Device B (destination) contains item REC-DCC from Wallet App on Mobile Device A (source). VAC-SCC in Wallet App on Mobile Device A (source) remain unchanged.
TXR-3960	TB_ENHANCE_WalletApp_DCC_VAC_Exchange_via_NFC_Android_2_iOS	2.3 DCC Exchange A user wants to present the DCC VAC-QR code to NFC readers, to enable future use cases like faster and less error prone DCC verification and semi-automated entry control systems. This test case checks the exchange of items from wallet app to wallet app. Wallet App on Mobile Device A wants to exchange items with Wallet Appon Mobile Device B via NFC.		Step	Input/Data	Expected Results
			1	User with Mobile Device A (Source) transfers his/her DCC-VAC to wallet app on Mobile Device B (destination).		Wallet App on Mobile Device B (destination) contains DCC-VAC from Wallet App on Mobile Device A (source). DCC-VAC-ITEM in Wallet App on Mobile Device A (source) remain unchanged.
TXR-3961	TB_ENHANCE_WalletApp_DCC_REC_Exchange_via_NFC_Android_2_iOS	2.3 DCC Exchange A user wants to present the DCC REC-QR code to NFC readers, to enable future use cases like faster and less error prone DCC verification and semi-automated entry control systems. This test case checks the exchange of items from wallet app to wallet app. Wallet App on Mobile Device A wants to exchange items with Wallet Appon Mobile Device B via NFC.		Step	Input/Data	Expected Results
			1	User with Mobile Device A (Source) transfers his/her DCC-REC to wallet app on Mobile Device B (destination).		Wallet App on Mobile Device B (destination) contains DCC-REC from Wallet App on Mobile Device A (source). DCC-REC-ITEM in Wallet App on Mobile Device A (source) remain unchanged.
TXR-3962	TB_ENHANCE_WalletApp_Import_Image_via_Selection_From_Gallery	Image Import from the gallery A traveler imports a image selected from his gallery in to his wallet App.		Step	Input/Data	Expected Results
			1	The user presses "Add New", "Import Image" and then "Pick from Gallery".		The user select a photo from his gallery, which has to be Importes to this Wallet App.

	[illegible]		2	Checks in the "Certificate Wallet"-Display for the image, which has been selected from the gallery before.		The expected image is there and can be selected to be shown.
TXR-3963	TB_ENHANCE_WalletApp_ReImport_DCC_VAC_After_Export	2.2 DCC-VAC Reimport A traveler exports a DCC-VAC certificate and then imports it again.		Step	Input/Data	Expected Results
			1	A DCC of type VAC has been already already exported from the wallet app. The user tries to import it again.		The DCC of type VAC can be successfully imported.
TXR-3964	TB_ENHANCE_WalletApp_ReImport_DCC_REC_After_Export	2.2 DCC-REC Reimport A traveler exports a DCC-REC certificate and then imports it again.		Step	Input/Data	Expected Results
			1	A DCC of type REC has been already already exported from the wallet app. The user tries to import it again.		The DCC of type REC can be successfully imported.
TXR-4116	TB_ENHANCE_VERIAPP_DCC_exported_TST	Check if a exported TEST DCC is readable by the verifier app.		Step	Input/Data	Expected Results
			1	A DCC of type TEST has been already already exported from the wallet app. The user let it be read by the verifier app.		The DCC of type TEST can be read by the verifier.
TXR-4117	TB_ENHANCE_VERIAPP_DCC_exported_REC	Check if a exported REC DCC is readable by the verifier app.		Step	Input/Data	Expected Results
			1	A DCC of type REC has been already already exported from the wallet app. The user let it be read by the verifier app.		The DCC of type REC can be read by the verifier.
TXR-4118	TB_ENHANCE_VERIAPP_DCC_exported_VAC	Check if a exported VAC DCC is readable by the verifier app.		Step	Input/Data	Expected Results
			1	A DCC of type VAC has been already already exported from the wallet app. The user let it be read by the verifier app.		The DCC of type VAC can be read by the verifier.

Test specification E2E OAT Emegency Mode

TC-ID	Testcase	Description	Manual test steps			
TXR-3954	TB_ENHANCE_VerifierApp_DebugMode_Level_1_DCC_TEST	The idea behind the feature is to provide ability to show extended data and provide ability to share it for not successful verification results, by turning intended feature switcher on, selecting data transparency, and selecting countries what extended data mode should be applied for. In this test case a DCC-TEST which fails at the technical verification is scanned. The datas of the verification collected for level 1 are shown correctly.		Step	Input/Data	Expected Results
			1	User opens the app and navigates to the settings screen.		Debug Mode is initially OFF.
			2	User scans a failing DCC-TEST.		A yellow screen with text "Limited Validity" is shown as well as the payload of the certificate.
			3	User enables debug mode from the settings screen and selects the country that corresponds to the certificate's issuance country.		The debug mode switch is ON (toggle pulled to the right) and issuance country has been selected.
			4	Then user scans the failing certificate a second time.		This time a detailed debug view, described for level 1, of the failing certificate's data is shown. A "share button" is available.
			5	User shares the certificate data via the "Share button" and select a media (f.e.email) to share the data collected in Emergency MOde.		The certificate data is shared correctly via Email.
TXR-3965	TB_ENHANCE_VerifierApp_DebugMode_Level_2_DCC_TEST	The idea behind the feature is to provide ability to show extended data and provide ability to share it for not successful verification results, by turning intended feature switcher on, selecting data transparency, and selecting countries what extended data mode should be applied for. In this test case a DCC-TEST which fails at the technical verification is scanned. The datas of the verification collected for level 2 are shown correctly.		Step	Input/Data	Expected Results
			1	User opens the app and navigates to the settings screen.		Debug Mode is initially OFF.
			2	User scans a failing DCC-TEST.		A yellow screen with text "Limited Validity" is shown as well as the payload of the certificate.
			3	User enables debug mode from the settings screen and selects the country that corresponds to the certificate's issuance country.		The debug mode switch is ON (toggle pulled to the right) and issuance country has been selected.
			4	Then user scans the failing certificate a second time.		This time a detailed debug view, described for level 2, of the failing certificate's data is shown. A "share button" is available.
			5	User shares the certificate data via the "Share button" and select a media (f.e.email) to share the data collected in Emergency MOde.		The certificate data is shared correctly via Email.

TXR-3966	TB_ENHANCE_VerifierApp_DebugMode_Level_3_DCC_TEST	The idea behind the feature is to provide ability to show extended data and provide ability to share it for not successful verification results, by turning intended feature switcher on, selecting data transparency, and selecting countries what extended data mode should be applied for. In this test case a DCC-TEST which fails at the technical verification is scanned. The datas of the verification collected for level 3 are shown correctly.		Step	Input/Data	Expected Results
			1	User opens the app and navigates to the settings screen.		Debug Mode is initially OFF.
			2	User scans a failing DCC-TEST.		A yellow screen with text "Limited Validity" is shown as well as the payload of the certificate.
			3	User enables debug mode from the settings screen and selects the country that corresponds to the certificate's issuance country.		The debug mode switch is ON (toggle pulled to the right) and issuance country has been selected.
			4	Then user scans the failing certificate a second time.		This time a detailed debug view, described for level 3, of the failing certificate's data is shown. A "share button" is available.
			5	User shares the certificate data via the "Share button" and select a media (f.e.email) to share the data collected in Emergency MOde.		The certificate data is shared correctly via Email.
TXR-3967	TB_ENHANCE_VerifierApp_DebugMode_Level_3_DCC_VAC	The idea behind the feature is to provide ability to show extended data and provide ability to share it for not successful verification results, by turning intended feature switcher on, selecting data transparency, and selecting countries what extended data mode should be applied for. In this test case a DCC-VAC which fails at the technical verification is scanned. The datas of the verification collected for level 3 are shown correctly.		Step	Input/Data	Expected Results
			1	User opens the app and navigates to the settings screen.		Debug Mode is initially OFF.
			2	User scans a failing DCC-VAC.		A yellow screen with text "Limited Validity" is shown as well as the payload of the certificate.
			3	User enables debug mode from the settings screen and selects the country that corresponds to the certificate's issuance country.		The debug mode switch is ON (toggle pulled to the right) and issuance country has been selected.
			4	Then user scans the failing certificate a second time.		This time a detailed debug view, described for level 3, of the failing certificate's data is shown. A "share button" is available.
			5	User shares the certificate data via the "Share button" and select a media (f.e.email) to share the data collected in Emergency MOde.		The certificate data is shared correctly via Email.
TXR-3968	TB_ENHANCE_VerifierApp_DebugMode_Level_3_DCC_VAC	The idea behind the feature is to provide ability to show extended data and provide ability to share it for not successful verification results, by turning intended feature switcher on, selecting data transparency, and selecting countries what extended data mode should be applied for. In this test case a DCC-VAC which fails at the technical verification is scanned. The datas of the verification collected for level 2 are shown correctly.		Step	Input/Data	Expected Results
			1	User opens the app and navigates to the settings screen.		Debug Mode is initially OFF.
			2	User scans a failing DCC-VAC.		A yellow screen with text "Limited Validity" is shown as well as the payload of the certificate.

	TB_ENHANCE_VerifierApp_DebugMode_Level_2_DCC_VAC		3	User enables debug mode from the settings screen and selects the country that corresponds to the certificate's issuance country.		The debug mode switch is ON (toggle pulled to the right) and issuance country has been selected.
			4	Then user scans the failing certificate a second time.		This time a detailed debug view, described for level 2, of the failing certificate's data is shown. A "share button" is available.
			5	User shares the certificate data via the "Share button" and select a media (f.e.email) to share the data collected in Emergency MOde.		The certificate data is shared correctly via Email.
TXR-3969	TB_ENHANCE_VerifierApp_DebugMode_Level_1_DCC_VAC	The idea behind the feature is to provide ability to show extended data and provide ability to share it for not successful verification results, by turning intended feature switcher on, selecting data transparency, and selecting countries what extended data mode should be applied for. In this test case a DCC-VAC which fails at the technical verification is scanned. The datas of the verification collected for level 1 are shown correctly.		Step	Input/Data	Expected Results
			1	User opens the app and navigates to the settings screen.		Debug Mode is initially OFF.
			2	User scans a failing DCC-VAC.		A yellow screen with text "Limited Validity" is shown as well as the payload of the certificate.
			3	User enables debug mode from the settings screen and selects the country that corresponds to the certificate's issuance country.		The debug mode switch is ON (toggle pulled to the right) and issuance country has been selected.
			4	Then user scans the failing certificate a second time.		This time a detailed debug view, described for level 1, of the failing certificate's data is shown. A "share button" is available.
			5	User shares the certificate data via the "Share button" and select a media (f.e.email) to share the data collected in Emergency MOde.		The certificate data is shared correctly via Email.
TXR-3970	TB_ENHANCE_VerifierApp_DebugMode_Level_1_DCC_REC	The idea behind the feature is to provide ability to show extended data and provide ability to share it for not successful verification results, by turning intended feature switcher on, selecting data transparency, and selecting countries what extended data mode should be applied for. In this test case a DCC-REC which fails at the technical verification is scanned. The datas of the verification collected for level 1 are shown correctly.		Step	Input/Data	Expected Results
			1	User opens the app and navigates to the settings screen.		Debug Mode is initially OFF.
			2	User scans a failing DCC-REC.		A yellow screen with text "Limited Validity" is shown as well as the payload of the certificate.
			3	User enables debug mode from the settings screen and selects the country that corresponds to the certificate's issuance country.		The debug mode switch is ON (toggle pulled to the right) and issuance country has been selected.
			4	Then user scans the failing certificate a second time.		This time a detailed debug view, described for level 1, of the failing certificate's data is shown. A "share button" is available.

			5	User shares the certificate data via the "Share button" and select a media (f.e.email) to share the data collected in Emergency MOde.		The certificate data is shared correctly via Email.
TXR-3971	TB_ENHANCE_VerifierApp_DebugMode_Level_2_DCC_REC	The idea behind the feature is to provide ability to show extended data and provide ability to share it for not successful verification results, by turning intended feature switcher on, selecting data transparency, and selecting countries what extended data mode should be applied for. In this test case a DCC-REC which fails at the technical verification is scanned. The datas of the verification collected for level 2 are shown correctly.		Step	Input/Data	Expected Results
			1	User opens the app and navigates to the settings screen.		Debug Mode is initially OFF.
			2	User scans a failing DCC-REC.		A yellow screen with text "Limited Validity" is shown as well as the payload of the certificate.
			3	User enables debug mode from the settings screen and selects the country that corresponds to the certificate's issuance country.		The debug mode switch is ON (toggle pulled to the right) and issuance country has been selected.
			4	Then user scans the failing certificate a second time.		This time a detailed debug view, described for level 2, of the failing certificate's data is shown. A "share button" is available.
			5	User shares the certificate data via the "Share button" and select a media (f.e.email) to share the data collected in Emergency MOde.		The certificate data is shared correctly via Email.
TXR-3972	TB_ENHANCE_VerifierApp_DebugMode_Level_3_DCC_REC	The idea behind the feature is to provide ability to show extended data and provide ability to share it for not successful verification results, by turning intended feature switcher on, selecting data transparency, and selecting countries what extended data mode should be applied for. In this test case a DCC-REC which fails at the technical verification is scanned. The datas of the verification collected for level 3 are shown correctly.		Step	Input/Data	Expected Results
			1	User opens the app and navigates to the settings screen.		Debug Mode is initially OFF.
			2	User scans a failing DCC-REC.		A yellow screen with text "Limited Validity" is shown as well as the payload of the certificate.
			3	User enables debug mode from the settings screen and selects the country that corresponds to the certificate's issuance country.		The debug mode switch is ON (toggle pulled to the right) and issuance country has been selected.
			4	Then user scans the failing certificate a second time.		This time a detailed debug view, described for level 3, of the failing certificate's data is shown. A "share button" is available.
			5	User shares the certificate data via the "Share button" and select a media (f.e.email) to share the data collected in Emergency MOde.		The certificate data is shared correctly via Email.
TXR-3973		The anonymization of the personal data in the qr code should be selectable by the user of the app and must follow the rules of the DCC Anomaly Capture Process		Step	Input/Data	Expected Results

	TB_ENHANCE_VerifierApp_Anonymization_DCC_TEST_for_DebugMode_Level_3	In this test case a user of the Verifer App must be able to select the configuration option for anonymization of the personal data in the DCC for the Emergency Mode (level 3) and all of the personal data of the DCC-TEST shared after a failed verification are anonymized.	1	User opens the app and navigates to the settings screen. He/she selects the option for anonymization of personal data in DeBug Mode.		Debug Mode is initially OFF. The anonymization-option is set.
			2	User scans a failing DCC-TEST.		A yellow screen with text "Limited Validity" is shown as well as the payload of the certificate.
			3	User enables debug mode for level 3 from the settings screen and selects the country that corresponds to the certificate's issuance country.		The debug mode switch is ON (toggle pulled to the right) and issuance country has been selected. Level 3 is selected.
			4	Then user scans the failing certificate a second time.		This time a detailed debug view of the failing certificate's data is shown for level 3. A "share button" is available.
			5	User shares the certificate data via the "Share button"		The certificate data is shared and all of the personal data are anonymized.
TXR-3974	TB_ENHANCE_VerifierApp_Anonymization_DCC_VAC_for_DebugMode_Level_3	The anonymization of the personal data in the qr code should be selectable by the user of the app and must follow the rules of the DCC Anomaly Capture Process In this test case a user of the Verifer App must be able to select the configuration option for anonymization of the personal data in the DCC for the Emergency Mode (level 3) and all of the personal data of the DCC-VAC shared after a failed verification are anonymized.		Step	Input/Data	Expected Results
			1	User opens the app and navigates to the settings screen. He/she selects the option for anonymization of personal data in DeBug Mode.		Debug Mode is initially OFF. The anonymization-option is set.
			2	User scans a failing DCC-VAC.		A yellow screen with text "Limited Validity" is shown as well as the payload of the certificate.
			3	User enables debug mode for level 3 from the settings screen and selects the country that corresponds to the certificate's issuance country.		The debug mode switch is ON (toggle pulled to the right) and issuance country has been selected. Level 3 is selected.
			4	Then user scans the failing certificate a second time.		This time a detailed debug view of the failing certificate's data is shown for level 3. A "share button" is available.
			5	User shares the certificate data via the "Share button"		The certificate data is shared and all of the personal data are anonymized.
TXR-3975		The anonymization of the personal data in the qr code should be selectable by the user of the app and must follow the rules of the DCC Anomaly Capture Process		Step	Input/Data	Expected Results

	TB_ENHANCE_VerifierApp_Anonymization_DCC_VAC_for_DebugMode_Level_1&2	In this test case a user of the Verifer App must be able to select the configuration option for anonymization of the personal data in the DCC for the Emergency Mode (level 2) and all of the personal data of the DCC-VAC shared after a failed verification are anonymized.	1	User opens the app and navigates to the settings screen. He/she selects the option for anonymization of personal data in DeBug Mode. Hint: the option of anoymization is linked to the selection of the debug level. Level 1 and 2: name fields + date of birth are anonymized; -Level 3: all fields not anonymized.		Debug Mode is initially OFF. The anonymization-option is set.
			2	User scans a failing DCC-VAC.		A yellow screen with text "Limited Validity" is shown as well as the payload of the certificate.
			3	User enables debug mode for level 2 from the settings screen and selects the country that corresponds to the certificate's issuance country.		The debug mode switch is ON (toggle pulled to the right) and issuance country has been selected. Level 2 is selected.
			4	Then user scans the failing certificate a second time.		This time a detailed debug view of the failing certificate's data is shown for level 2. A "share button" is available.
			5	User shares the certificate data via the "Share button"		The certificate data is shared and all of the personal data are anonymized. The option of anoymization is linked to the selection of the debug level. Level 1 and 2: name fields + date of birth are anonymized; -Level 3: all fields not anonymized.
			6	Repeat the testcase with setting debug-level 1		The test shows the same test results as for debug-level 2.
TXR-3976		The anonymization of the personal data in the qr code should be selectable by the user of the app and must follow the rules of the DCC Anomaly Capture Process In this test case a user of the Verifer App must be able to select the configuration option for anonymization of the personal data in the DCC for the Emergency Mode (level 2) and all of the personal data of the DCC-REC shared after a failed verification are anonymized.		Step	Input/Data	Expected Results
			1	User opens the app and navigates to the settings screen. He/she selects the option for anonymization of personal data in DeBug Mode. Hint: the option of anoymization is linked to the selection of the debug level.		Debug Mode is initially OFF. The anonymization-option is set.

	TB_ENHANCE_VerifierApp_Anonymization_DCC_REC_for_DebugMode_Level_1&2			Level 1 and 2: name fields + date of birth are anonymized; -Level 3: all fields not anonymized.		
			2	User scans a failing DCC-REC.		A yellow screen with text "Limited Validity" is shown as well as the payload of the certificate.
			3	User enables debug mode for level 2 from the settings screen and selects the country that corresponds to the certificate's issuance country.		The debug mode switch is ON (toggle pulled to the right) and issuance country has been selected. Level 2 is selected.
			4	Then user scans the failing certificate a second time.		This time a detailed debug view of the failing certificate's data is shown for level 2. A "share button" is available.
			5	User shares the certificate data via the "Share button"		The certificate data is shared and all of the personal data are anonymized. Level 1 and 2: name fields + date of birth are anonymized; -Level 3: all fields not anonymized.
			6	Repeat the testcase with setting the debug-level 1.		The test shows the same test results as for debug-level 2.
TXR-3977	TB_ENHANCE_VerifierApp_Anonymization_DCC_REC_for_DebugMode_Level_3	The anonymization of the personal data in the qr code should be selectable by the user of the app and must follow the rules of the DCC Anomaly Capture Process In this test case a user of the Verifer App must be able to select the configuration option for anonymization of the personal data in the DCC for the Emergency Mode (level 3) and all of the personal data of the DCC-REC shared after a failed verification are anonymized.		Step	Input/Data	Expected Results
			1	User opens the app and navigates to the settings screen. He/she selects the option for anonymization of personal data in DeBug Mode.		Debug Mode is initially OFF. The anonymization-option is set.
			2	User scans a failing DCC-REC.		A yellow screen with text "Limited Validity" is shown as well as the payload of the certificate.
			3	User enables debug mode for level 3 from the settings screen and selects the country that corresponds to the certificate's issuance country.		The debug mode switch is ON (toggle pulled to the right) and issuance country has been selected. Level 3 is selected.
			4	Then user scans the failing certificate a second time.		This time a detailed debug view of the failing certificate's data is shown for level 3. A "share button" is available.
			5	User shares the certificate data via the "Share button"		The certificate data is shared and all of the personal data are anonymized.
TXR-3978		The anonymization of the personal data in the qr code should be selectable by the user of the app and must follow the rules of the DCC Anomaly Capture Process In this test case a user of the Verifer App must be able to select the configuration option for anonymization of the personal data in the DCC for the Emergency Mode (level 2) and all of the personal data of the DCC-TEST shared after a failed verification are anonymized.		Step	Input/Data	Expected Results
			1	User opens the app and navigates to the settings screen.		Debug Mode is initially OFF.

	TB_ENHANCE_VerifierApp_Anonymization_DCC_TEST_for_DebugMode_Level_1&2			He/she selects the option for anonymization of personal data in DeBug Mode. Hint: The anonymization option is linked to the selection of the debug level.		The anonymization-option is set.
			2	User scans a failing DCC-TEST.		A yellow screen with text "Limited Validity" is shown as well as the payload of the certificate.
			3	User enables debug mode for level 2 from the settings screen and selects the country that corresponds to the certificate's issuance country.		The debug mode switch is ON (toggle pulled to the right) and issuance country has been selected. Level 2 is selected.
			4	Then user scans the failing certificate a second time.		This time a detailed debug view of the failing certificate's data is shown for level 2. A "share button" is available.
			5	User shares the certificate data via the "Share button"		The certificate data is shared and all of the personal data are anonymized. Level 1 and 2: name fields + date of birth are anonymized; -Level 3: all fields not anonymized.
			6	Repeat the testcase with setting debug-level 1.		The test shows the same test results as for debug-level 2.

Test specification E2E OAT Ticketing_Integration

TC-ID	Testcase	Description	Manual test steps			
TXR-3868	TB_ENHANCE_WalletApp_Booking_and_Ticketing_Integration_via_QR_Code_Scan_valid_vaccination	This test case checks the complete booking / check in process for the happy path scenario where the user can complete his booking / check in process and in the end receive his / her FFT e-ticket by providing a valid DCC of type VAC.		Step	Input/Data	Expected Results
			1	User visits website and starts booking or check-in process. User inputs: Personal data, flight departure/arrival time, country of arrival.		Service Provider presents QR Code with Validation Informations.Service Provider presents QR Code with Validation Informations.
			2	User scans QR code from the page with his wallet app.		"Choose certificate" will be shown. A list of certificates will be shown. The list is filterd, so only certificates for the person who is in booking qr-code saved, will be shown.
			3	User choose a valid vaccinaction certificate.		Confirmation is asked: Do you want to share the certificate with the validationservice?
			4	User selects "yes"		Trusted Validator Service confirms DCC validity to booking/check-in system. DCC is not stored Medical data is not stored Bookingsystem gets validationresult WalletApp gets the same validationresult
			5	User completes booking/check-in process.		User receives FFT e-ticket.
TXR-3872	TB_ENHANCE_WalletApp_Booking_and_Ticketing_Integration_via_DCC_Upload	To validate a DCC during an online booking or check-in process, the service provider must be connected to a trusted validation service. This validation service can receive and validate the DCC from the wallet app or the service frontend. The DCCs are encrypted by a public key of the validation service and only then transmitted during the process. After validation, the service provider's backend gets feedback about validation success or failure. The service provider can then decide whether the check process may continue or not.		Step	Input/Data	Expected Results
			1	User visits website and starts booking or check-in process. User inputs: Personal data, flight departure/arrival time, country of arrival.		Service Provider presents QR Code with Validation Informations.Service Provider presents QR Code with Validation Informations.
			2	User uploads DCC in a paper form directly.		Trusted Validator Service confirms DCC validity to booking/check-in system. No Data is stored.
			3	User completes booking/check-in process.		User receives FFT e-ticket.
TXR-4013		This test case checks the complete booking / check in process for the happy path scenario where the user can complete his booking / check in process and in the end receive his / her FFT e-ticket by providing a valid DCC of type REC.		Step	Input/Data	Expected Results
			1	User visits website and starts booking or check-in process. User inputs: Personal data, flight departure/arrival time, country of arrival.		Service Provider presents QR Code with Validation Informations.Service Provider presents QR Code with Validation Informations.
			2	User scans QR code from the page with his wallet app.		"Choose certificate" will be shown. A list of certificates will be shown. The list is filterd, so only certificates for the person who is in booking qr-code saved, will be shown.

	TB_ENHANCE_WalletApp_Booking_and_Ticketing_Integration_via_QR_Code_Scan_valid_Recovery		3	User choose a valid recovery certificate.		Confirmation is asked: Do you want to share the certifictae with the validationservice?
			4	User selects "yes"		Trusted Validator Service confirms DCC validity to booking/check-in system. DCC is not stored Medical data is not stored Bookingsystem gets validationresult WalletApp gets the same validationresult
			5	User complete booking/check-in process.		User receives FFT e-ticket.
TXR-4014	TB_ENHANCE_WalletApp_Booking_and_Ticketing_Integration_via_QR_Code_Scan_valid_Test	This test case checks the complete booking / check in process for the happy path scenario where the user can complete his booking / check in process and in the end receive his / her FFT e-ticket by providing a valid DCC of type TEST.		Step	Input/Data	Expected Results
			1	User visits website and starts booking or check-in process. User inputs: Personal data, flight departure/arrival time, country of arrival.		Service Provider presents QR Code with Validation Informations.Service Provider presents QR Code with Validation Informations.
			2	User scans QR code from the page with his wallet app.		"Choose certificate" will be shown. A list of certificates will be shown. The list is filterd, so only certificates for the person who is in booking qr-code saved, will be shown.
			3	User choose a valid test certificate.	A testcertificate expires after short time. Does ist make sense?	Confirmation is asked: Do you want to share the certifictae with the validationservice?
			4	User selects "yes"		Trusted Validator Service confirms DCC validity to booking/check-in system. DCC is not stored Medical data is not stored Bookingsystem gets validationresult WalletApp gets the same validationresult
			5	User completes booking/check-in process.		User receives FFT e-ticket.
TXR-4015		This test case checks the complete booking / check in process for the "unhappy" path scenario where the user cannot complete his booking / check in process and in the end does not receive his / her FFT e-ticket due to providing an invalid DCC of type VAC.		Step	Input/Data	Expected Results
			1	User visits website and starts booking or check-in process. User inputs: Personal data, flight departure/arrival time, country of arrival.		Service Provider presents QR Code with Validation Informations.Service Provider presents QR Code with Validation Informations.
			2	User scans QR code from the page with his wallet app.		"Choose certificate" will be shown. A list of certificates will be shown. The list is filterd, so only certificates for the person who is in booking qr-code saved, will be shown.

	TB_ENHANCE_WalletApp_Booking_and_Ticketing_Integration_via_QR_Code_Scan_invalid_vaccination		3	User choose a invalid vaccinaction certificate.	Variante 1: vaccination has expired Variante 2: vaccination is not completed yet Variante 3: vaccination is completed after 3 days	Confirmation is asked: Do you want to share the certifictae with the validationservice?
			4	User selects "yes"		Trusted Validator Service confirms DCC validity to booking/check-in system. DCC is not stored Medical data is not stored Bookingsystem gets validationresult WalletApp gets the same validationresult
TXR-4016	TB_ENHANCE_WalletApp_Booking_and_Ticketing_Integration_via_QR_Code_Scan_invalid_Recovery	This test case checks the complete booking / check in process for the "unhappy" path scenario where the user cannot complete his booking / check in process and in the end does not receive his / her FFT e-ticket due to providing an invalid DCC of type REC.		Step	Input/Data	Expected Results
			1	User visits website and starts booking or check-in process. User inputs: Personal data, flight departure/arrival time, country of arrival.		Service Provider presents QR Code with Validation Informations.Service Provider presents QR Code with Validation Informations.
			2	User scans QR code from the page with his wallet app.		"Choose certificate" will be shown. A list of certificates will be shown. The list is filterd, so only certificates for the person who is in booking qr-code saved, will be shown.
			3	User choose a valid recovery certificate.	Variante 1: recovery certificate has expired Variante 2: Acceptance rule violation	Confirmation is asked: Do you want to share the certifictae with the validationservice?
			4	User selects "yes"		Trusted Validator Service confirms DCC validity to booking/check-in system. DCC is not stored Medical data is not stored Bookingsystem gets validationresult WalletApp gets the same validationresult
			5	User can not complete booking/check-in process.		User does not receive FFT e-ticket.
TXR-4017		This test case checks the complete booking / check in process for		Step	Input/Data	Expected Results

	TB_ENHANCE_WalletApp_Booking_and_Ticketing_Integration_via_QR_Code_Scan_invalid_test	the "unhappy" path scenario where the user cannot complete his booking / check in process and in the end does not receive his / her FFT e-ticket due to providing an invalid DCC of type TEST.	1	User visits website and starts booking or check-in process. User inputs: Personal data, flight departure/arrival time, country of arrival.		Service Provider presents QR Code with Validation Informations.Service Provider presents QR Code with Validation Informations.
			2	User scans QR code from the page with his wallet app.		"Choose certificate" will be shown. A list of certificates will be shown. The list is filterd, so only certificates for the person who is in booking qr-code saved, will be shown.
			3	User choose an invalid test certificate.	Variante 1: a positive test Variante 2: Expired test Variante 3: Acceptance rule violation	Confirmation is asked: Do you want to share the certifictae with the validationservice?
			4	User selects "yes"		Trusted Validator Service confirms DCC validity to booking/check-in system. DCC is not stored Medical data is not stored Bookingsystem gets validationresult WalletApp gets the same validationresult
			5	User can not complete booking/check-in process.		User does not receive FFT e-ticket.
TXR-4027	TB_ENHANCE_WalletApp_Booking_and_Ticketing_Integration_via_QR_Code_Scan_valid_vaccination_family	This testcase is to check whether a second booking can be made within the same workflow as in the case of a family booking scenario.		Step	Input/Data	Expected Results
			1	User visits website and starts booking or check-in process. User inputs: Personal data for 2 or more persons, flight departure/arrival time, country of arrival.		Service Provider presents a QR Code with Validation Informations for each persn. Service Provider presents QR Code with Validation Informations.
			2	User scans one QR code from the page with his wallet app.		"Choose certificate" will be shown. A list of certificates will be shown. The list is filterd, so only certificates for the person who is in booking qr-code saved, will be shown.
			3	User choose a valid vaccinaction certificate.		Confirmation is asked: Do you want to share the certifictae with the validationservice?
			4	User selects "yes"		Trusted Validator Service confirms DCC validity to booking/check-in system. DCC is not stored Medical data is not stored Bookingsystem gets validationresult

						WalletApp gets the same validationresult
			5	user switchs to booking system and scans second QR code from the page with his wallet app.		"Choose certificate" will be shown. A list of certificates will be shown. The list is filterd, so only certificates for the person who is in booking qr-code saved, will be shown.
			6	User choose a valid vaccinaction certificate.		Confirmation is asked: Do you want to share the certifictae with the validationservice?
			7	User selects "yes"		Trusted Validator Service confirms DCC validity to booking/check-in system. DCC is not stored Medical data is not stored Bookingsystem gets validationresult WalletApp gets the same validationresult
			8	User completes booking/check-in process.		User receives FFT e-ticket.
TXR-4028	TB_ENHANCE_WalletApp_Booking_and_Ticketing_Integration_via_corrupt_QR_Code_Scan	This test case checks the complete booking / check in process for the "unhappy" path scenario where the user cannot complete his booking / check in process and in the end does not receive his / her FFT e-ticket due to providing a corrupt QR Code. Furthermore, it checks that he wallet app can withstand such a scenario without crashing.		Step	Input/Data	Expected Results
			1	User visits website and starts booking or check-in process. User inputs: Personal data, flight departure/arrival time, country of arrival.	Variante 1: The Data are not completed. Variante 2: the qr code is empty Variante 3: the qr-code is not from booking system	Service Provider presents QR Code with Validation Informations.Service Provider presents a corrupt QR Code.
			2	User scans QR code from the page with his wallet app.		The wallet app reconize that the QR-code is corrupt