Swiss Covid Certificate – Overview about findings and vulnerabilities

Aktuelle Meldungen - Notifications actuelles - Notifiche attuali - Current reports

14.02.2022 / 15:00

NB:
Aus Gründen der Transparenz und zur Information der Öffentlichkeit wurden die Ergebnisse aus dem öffentlichen Test und verschiedenen intern durchgeführten Tests in die Liste aufgenommen. Die Ergebnisse des Nationalen Testinstituts für Cybersicherheit (NTC) werden Gegenstand eines eigenen Berichts sein, der in Kürze veröffentlicht wird. Dieser wird weitere technische Details beinhalten.Kritische Schwachstellen, die zurzeit noch analysiert werden, werden zum jetzigen Zeitpunkt aus Sicherheitsgründen noch nicht veröffentlicht.

Dans un souci de transparence et d'information du public, les résultats du test public et de différents tests internes ont été inclus dans la liste. Les résultats rapportés par l'Institut national de test pour la cybersécurité (NTC) feront l'objet d'un rapport dédié qui sera publié prochainement. Des détails plus techniques seront donnés dans le rapport. Les lacunes critiques, qui sont toujours en cours d'analyse, ne sont pas publiées pour l'instant pour des raisons de sécurité.

Per questioni di trasparenza e di informazione al pubblico, nella lista sono stati inseriti i findings provenienti dal test pubblico e da differenti test interni. I findings segnalati dall'Istituto nazionale di test per la cibersicurezza (NTC) saranno oggetto di un rapporto dedicato che sarà pubblicato prossimamente. Nel rapporto verranno forniti maggiori dettagli tecnici. Lacune di sicurezza critiche, che si trovano ancora in fase di analisi, non sono per ora pubblicate per motivi di sicurezza.

For reasons of transparency and public information, findings from the public test and different internal tests have been included in the list. The findings reported by the National Test institute for Cyber Security (NTC) will be the subject of a dedicated report to be published soon. More technical details will be given in the report. Critical vulnerabilities, which are still being analysed, are not published for the time being for security reasons.

Number	Subject	Date received	Summary / Keyword	Description	Impact	Mitigation	Credits	Status	Remarks
1	Cert Error	31.5.2021		Cert Error for the website covidcertificate.admin.ch	Website certificate is not trusted by browser	Message to BK sent (31.05.2021)		fixed	
2	Signatur von beliebigen Eingaben	31.5.2021		https://github.com/admin-ch/CovidCertificate-Api-Gateway-Service/blob/develop/src/main/java/ch/admin/bag/covidcertificate/gateway/web/controller/utils/SignatureTestController.java#L41 Eine erreichbare Test-Funktionalität, welche beliebige Eingaben mit einem private key signiert und wieder zurücksendet. Eine solche Funktionalität ist grundsätzlich unsicher, beliebige Inhalte ohne zusätzliche Überprüfung zu signieren ist ein Problem, schliesslich sollte immer geprüft werden ob etwas signiert werden soll.	Mit hoher Warscheinlichkeit keine Auswirkung bezüglich technischer Security, da der hartkodierte Pfad des Private Keys im Release hoffentlich nicht besteht, der Code niemals die Produktion erreicht und ähnliche Vorbedingungen. Auswirkung grundsätzlich daher unklar da lediglich anhand von code review gefunden. Code stört jedoch bei Code review da es sich um ein klares kryptografisches Anti-Pattern handelt.	Grundsätzlich sollte eine solche Klasse nicht im *main* Ordner vorhanden sein oder überhaupt im produktiven Code, wenn dann höchstens im Test-Ordner, aber auch da lieber nicht.		wontfix	Not in PROD deployment.
3	Supply Chain attack	31.5.2021	Supply Chain attack possible due to untrusted third-party GitHub Actions usage	Multiple components make use of external untrusted third-party GitHub Actions such as these ones: - https://github.com/marvinpinto/action-automatic-releases - https://github.com/ncipollo/release-action	As per GitHub's Official Documentation (https://docs.github.com/en/actions/learn-github-actions/security-hardening-for-github-actions#using-third-party-actions): ```	You can help mitigate this risk by following these good practices (As per GitHub's Documentation): ### Pin actions to a full length commit SHA		fixed	

				The following workflows make use of these untrusted actions: - `admin-ch/CovidCertificate-Management-Service/.github/workflows/release.yml` - `admin-ch/CovidCertificate-Api-Gateway-Service/.github/workflows/release.yml` - `admin-ch/CovidCertificate-App-Config-Service/.github/workflows/tagged_release.yaml` - `admin-ch/CovidCertificate-Api-Gateway-Service/.github/workflows/maven.yml` - `admin-ch/CovidCode-Service/.github/workflows/maven.yml` - `admin-ch/CovidCertificate-Management-Service/.github/workflows/maven.yml` - `admin-ch/CovidCertificate-App-Config-Service/.github/workflows/maven.yml` The following link shows that `marvinpinto/action-automatic-releases` was executed while building the latest `master` release: https://github.com/admin-ch/CovidCertificate-Management-Service/runs/2708296617?check_suite_focus=true	The individual jobs in a workflow can interact with (and compromise) other jobs. ... This means that **a compromise of a single action within a workflow can be very significant**, as that compromised action would have access to all secrets configured on your repository, and may be able to use the `GITHUB_TOKEN` to write to the repository. ``` In a worst case scenario: both users `marvinpinto` and `ncipollo` could release malicious code that would fully compromise the integrity of `admin-ch`'s supply chain and (by extension) software builds. Recently such attacks were used against high-profile targets such as Codecov and Solarwinds. The following article provides an interesting insight on these ones: https://www.wolfe.id.au/2021/04/26/github-actions-supply-chain-attacks/	Pinning an action to a full length commit SHA is currently the only way to use an action as an immutable release. Pinning to a particular SHA helps mitigate the risk of a bad actor adding a backdoor to the action's repository, as they would need to generate a SHA-1 collision for a valid Git object payload. ### Audit the source code of the action Ensure that the action is handling the content of your repository and secrets as expected. For example, check that secrets are not sent to unintended hosts, or are not inadvertently logged. ### Pin actions to a tag only if you trust the creator Although pinning to a commit SHA is the most secure option, specifying a tag is more convenient and is widely used. If you'd like to specify a tag, then be sure that you trust the action's creators. The 'Verified creator' badge on GitHub Marketplace is a useful signal, as it indicates that the action was written by a team whose identity has been verified by GitHub. Note that there is risk to this approach even if you trust the author, because a tag can be moved or deleted if a bad actor gains access to the repository storing the action.			
4	Accessibility	01.06.2021	Anforderungen WCAG 2.1	Dies ist eine generelle Anforderung. Damit Menschen mit Behinderungen die App bedienen können, müssen die Anforderungen WCAG 2.1 der Konformitätsstufe AA erfüllt sein. Dies gilt auch für native Apps für Android und iOS. Die ist eine zwingende Vorgabe gemäss Behindertengleichstellungsgesetzt (BehiG). Weitere Informationen im eCH-Standard 0059. Es braucht hier detaillierte Accessibiltiy-Audits.	Falls die App nicht barrierefrei bedient werden kann, ist die besonders gefährdete Gruppe von Menschen mit Behinderungen ausgeschlossen. Die gesetzlichen Vorgaben sind nicht eingehalten. Gefahr der Ausgrenzung von Menschen mit Behinderungen und älteren Menschen und von Image- und Reputationsverlust.	Vollständige Accessibility Audits und kontinuierliche Verbesserung der Mängel.		Out of scope	
5	Webserver	02.06.2021		Your web server supports one or more ciphers that have a phase out status, because they are known to be fragile and are at risk of becoming insufficiently secure.	Technical details: Web server IP address Affected ciphers Status 162.23.147.222 AES256-GCM-SHA384 phase out ... AES128-GCM-SHA256 phase out ... AES128-SHA256 phase out ... AES256-SHA256 phase out For further Testexplanation please refere to https://www.internet.nl/site/www.covidcertificate.admin.ch/1249322/#	Die NCSC-NL taxiert in ihrem Tool www.internet.nl als gute Chiffrierroutinen: Good: ECDHE-ECDSA-AES256-GCM-SHA384 (TLS_AES_256_GCM_SHA384 in 1.3) [1.2] ECDHE-ECDSA-CHACHA20-POLY1305 (TLS_CHACHA20_POLY1305_SHA256 in 1.3) [1.2] ECDHE-ECDSA-AES128-GCM-SHA256 (TLS_AES_128_GCM_SHA256 in 1.3) [1.2]		ongoing	

					Es versteht sich von selbst, dass bei so heiklen Vorhaben (politisch, applikatorisch & infrastrukturtechnisch, reputaionstechnisch) keine löchrigen Chiffrierroutinen verwendet werden sollten.	ECDHE-RSA-AES256-GCM-SHA384 (TLS_AES_256_GCM_SHA384 in 1.3) [1.2] ECDHE-RSA-CHACHA20-POLY1305 (TLS_CHACHA20_POLY1305_SHA256 in 1.3) [1.2] ECDHE-RSA-AES128-GCM-SHA256 (TLS_AES_128_GCM_SHA256 in 1.3) [1.2]			
6	Hardcoded password	02.06.2021	Hardcoded Password	Hardcoded Password	the following code is vulnrable to Hardcoded password: https://github.com/admin-ch/CovidCertificate-Management-Service/blob/c1965356760315ce618b25c3db390d820bc503a2/src/main/java/ch/admin/bag/covidcertificate/CCManagementServiceApplication.java the password is "changeit" Hardcoded passwords may compromise system security in a way that cannot be easily remedied. It is never a good idea to hardcode a password. Not only does hardcoding a password allow all of the project's developers to view the password, it also makes fixing the problem extremely difficult. Once the code is in production, the password cannot be changed without patching the software. If the account protected by the password.	https://github.com/admin-ch/CovidCertificate-Management-Service/blob/c1965356760315ce618b25c3db390d820bc503a2/src/main/java/ch/admin/bag/covidcertificate/CCManagementServiceApplication.java	Asaf Feigenbaum	fixed	
7	Cypher Security	02.06.2021		WS supports weak ciphers	The acceptance environment supports weak ciphers, such as TLS_RSA_WITH_AES_128_CBC_SHA256 Since the prod env doesn't seem to be ready, I cannot confirm that this will be an issue there too. For more details see: https://www.ssllabs.com/ssltest/analyze.html?d=ws.covidcertificate-a.bag.admin.ch&hideResults=on		ozzi	ongoing	
8	Unbounded Query	02.06.2021		Unbounded Query when retrieving the revocation list	The implementation of findAllUvcis has an unbounded query. This is not an issue for 1000s of revocations, but considering that entire lots of certain vaccines could become known as ineffective, the number of revoked certificates may quickly increase by 10^5 certificates weekly. Devices calling this endpoint even in small numbers on a daily basis will potentially DoS the system, exceed any limits for		enzian	ongoing	

					response body sizes and provoke timeouts.
					
					@Repository
					public interface RevocationRepository extends JpaRepository<Revocation, UUID> {
					Revocation findByUvci(String uvci);
					
					@Query("SELECT r.uvci FROM Revocation r")
					List<String> findAllUvcis();
					}				

9	Use of signature is not thread-safe	02.06.2021		Use of signature is not thread-safe	It seems the use of Signature in the CryptoController is not thread-safe and parallel request could result in wrong signatures to be returned to the caller.
					
					The Signature is initialized as a Singleton bean in
					
					CovidCertificate-Signing-Service/src/main/java/ch/admin/bag/covidcertificate/signature/config/HsmConfig.java
					
					Line 63 in bb7af92
					Signature signingSignature(KeyStoreEntryReader keyStoreEntryReader) {
					
					So the signature is shared between all the requests and this could lead to wrong requests or a SignatureException when the update message has been reset by another call. Signature (JDK 11)
					
					CovidCertificate-Signing-Service/src/main/java/ch/admin/bag/covidcertificate/signature/web/controller/CryptoController.java
					
					Lines 23 to 24 in bb7af92
					this.signingSignature.update(message);
					return this.signingSignature.sign();
							Initdch	fixed	

10	Embedded credentials	03.06.2021	Embedded passwords for the PostgreSQL DB	Embedded passwords for the PostgreSQL DB created in docker	PostgreSQL in this specific docker configuration (version 13) also allows remote code execution of payloads	Perhaps it should be part of each docker image to generate some random passwords so that these are unique to each instance.	Pavel Jirout	Wont fix	Only used in local environment

				./CovidCertificate-Management-Service/docker/docker-compose.yml environment: - POSTGRES_USER=cc-management - POSTGRES_PASSWORD=secret - POSTGRES_DB=cc-management	Metasploit module used: (linux/postgres/postgres_payload) On some default Linux installations of PostgreSQL, the postgres service account may write to the /tmp directory, and may source UDF Shared Libraries from there as well, allowing execution of arbitrary code. This module compiles a Linux shared object file, uploads it to the target host via the UPDATE pg_largeobject method of binary injection, and creates a UDF (user defined function) from that shared object. Because the payload is run as the shared object's constructor, it does not need to conform to specific Postgres API versions. http://www.leidecker.info/pgshell/Having_Fun_With_PostgreSQL.txt https://nvd.nist.gov/vuln/detail/CVE-2007-3280 Currently this impacts the docker postgresql image ./CovidCertificate-Management-Service/docker/docker-compose.yml services: db-cc-management: image: postgres				
11	Embedded passwords	03.06.2021	CovidCertificate-Signing-Service has some embedded passwords	CovidCertificate-Signing-Service has some embedded passwords which should be handled differently There are a few entries of embedded credentials Searching for a simple "secret" string on the git cloned sources reveals user@CF31:~/WORK/SWISS-HACKATON-COVID/CovidCertificate-Signing-Service$ grep -R secret . ./src/test/resources/application-test.properties:server.ssl.key-store-password=secret	Secrets are shown		Pavel Jirout	ongoing	

				./src/test/resources/application-test.properties:server.ssl.key-password=secret ./src/test/resources/application-test.properties:server.ssl.trust-store-password=secret ./src/test/resources/application-test.properties:app.signing-service.monitor.prometheus.password={noop}secret ./src/test/java/ch/admin/bag/covidcertificate/signature/web/controller/CryptoControllerIntegrationLocalTest.java: .keyStore(getFile(keystore), "secret") ./src/test/java/ch/admin/bag/covidcertificate/signature/web/controller/CryptoControllerIntegrationLocalTest.java: .trustStore(getFile(keystore), "secret"); ./src/test/java/ch/admin/bag/covidcertificate/signature/web/controller/CryptoControllerIntegrationTest.java: "app.signing-service.monitor.prometheus.password={noop}secret"}) ./src/main/resources/application-local.properties:server.ssl.key-store-password=secret ./src/main/resources/application-local.properties:server.ssl.key-password=secret ./src/main/resources/application-local.properties:server.ssl.trust-store-password=secret ./src/main/resources/application-local.properties:app.signing-service.monitor.prometheus.password={noop}secret ./src/main/java/ch/admin/bag/covidcertificate/signature/service/KeyStoreEntryReader.java: private static final String MOCK_AND_TEST_PASS = "secret"; ./src/main/java/ch/admin/bag/covidcertificate/signature/config/HsmMockConfig.java: private static final String KEY_STORE_PASSWORD = "secret"; Interesting files containing plaintext creds are ./src/main/resources/application-local.properties ./src/test/resources/application-test.properties ./src/main/resources/application-local.properties					
12	Embedded passwords	03.06.2021	CovidCertificate-Management-Service has some embedded plaintext passwords	CovidCertificate-Management-Service has some embedded plaintext passwords namely the "secret" string when recursively searched through the git sources Affected files ./CovidCertificate-Management-Service/src/main/resources/application.yml ./CovidCertificate-Management-Service/src/main/resources/application-local.yml ./CovidCertificate-Management-Service/target/classes/application.yml	plaintext secrets readable		Pavel Jirout	ongoing	

				./CovidCertificate-Management-Service/target/classes/application-local.yml					
13	Mobile Apps: WebView JavaScript enabled	04.06.2021	Bei beiden mobile Apps Covid Check und Covid Cert wird im File ch/admin/bag/covidcertificate/common/html/HtmlFragment.java JavaScript für WebView aktiviert mittels: settings.setJavaScriptEnabled(true)	Standardmässig ist JavaScript in WebView deaktiviert, falls nicht explizit benötigt sollte dies deaktiviert werden. OWASP beschreibt die Auswirkung einer Aktivierung wie folgt: "JavaScript can be injected into web applications via reflected, stored, or DOM-based Cross-Site Scripting (XSS). Mobile apps are executed in a sandboxed environment and don't have this vulnerability when implemented natively. Nevertheless, WebViews may be part of a native app to allow web page viewing. Every app has its own WebView cache, which isn't shared with the native Browser or other apps. On Android, WebViews use the WebKit rendering engine to display web pages, but the pages are stripped down to minimal functions, for example, pages don't have address bars. If the WebView implementation is too lax and allows usage of JavaScript, JavaScript can be used to attack the app and gain access to its data." - https://github.com/OWASP/owasp-mstg/blob/1.1.3/Document/0x05h-Testing-Platform-Interaction.md#testing-javascript-execution-in-webviews-mstg-platform-5		Falls möglich, JavaScript im WebView nicht aktivieren und die entsprechende Zeile löschen oder auf false setzen. Weitere Infos unter: https://github.com/OWASP/owasp-mstg/blob/1.1.3/Document/0x05h-Testing-Platform-Interaction.md#testing-javascript-execution-in-webviews-mstg-platform-5	0x142	wontfix	Webview hat feste Contents. Injections sind nicht möglich. JavaScript wurde deaktiviert.
14	http api au lieu de https	07.06.2021	Le code github propose un site pour les api en http au lieu de https.	https://github.com/admin-ch/CovidCertificate-Apidoc/blob/main/api-doc.json	Cela pourrais poser un problème, car les informations envoyées passent en clair, et une option pour recouvrer un certificat, existe dans le code.	passer en https évitera l'interception des données		fixed	
15	Timestamp issue	11.6.2021	Certificate issue timestamp not adapted to daylight saving time	Im Zertifikat steht "Zertifikat erstellt am 08.06.2021 um 21:08", SMS von vacme.ch kam um 21:23 (local time, also UTC+2h), ich holte es um 21:26. Das PDF hat intern einen Timestamp 20:08:06. Vermutlich läuft die Plattform mit einem festen UTC-Offset, d.h. hat noch Winterzeit.		Korrekter Timestamp oder korrekte Systemzeit	Andrea Schlapbach	wontfix	Not reproducible
16	Generation API accepts nonvisible characters	12.6.2021	Generation API accepts nonvisible characters (unbreakable spaces, newlines , etc.) which relocate or hide information in the pdf.	The Generation and Revocation API for system integrators (integration with one-time-passwords) allows the usage of nonvisible characters for the following data fields: • familyName • givenName The API generates valid CovidCert-PDF-Documents, that have shifted names or no person identifying information at all. See some JSON input examples in the attachment. Chinese Characters and Emojis show a similar behaviour. They are not visible in the PDF, but displayed in the Verifier-App.	Such documents could invite people to fill in their names and the document could be accepted when the verifier only checks the paper version (and does not use the Verifier-App to check the information in the QR-Code). The existence of such CovidCert-PDF-Documents could reduce the trust in the CovidCerts and disrupt verification processes.	Define a list of permitted character and character chains (at least 2 visible characters should be mandatory) and filter the input accordingly.	Annett Laube	fixed	
17	App non disponible si pays du profil utilisateur Google Play n'est pas en Suisse	17.6.2021	App non disponible si pays du profil utilisateur Google Play n'est pas en Suisse	Bonjour, Il s'agit ici d'un bug, plutôt qu'une faille de sécurité. Mon profil Google Play est paramétré sur "France" (profil de paiement).	Application non disponible au téléchargement pour des profils utilisateurs Google Play défini en dehors de la Suisse (ou du moins si paramétré comme étant en France).	Rendre le téléchargement sur Google Play indépendant de la localisation géographique, que ce soit par l'adresse IP ou le paramétrage du profil GG Play.		wontfix	

				La recherche de l'app Covid Certificate dans Google Play à partir de mon smartphone fait apparaitre que l'application n'est pas disponible dans ma région (alors que je suis connecté en WIFI sur une ligne fixe à Yverdon-les-Bains). La recherche sur Google Play depuis mon PC connecté à la même adresse IP, mais sans être loggé, fait bien apparaitre l'application à télécharger. Dès que je me log sur mon PC avec mon profil Google, l'application disparait de la liste et n'est plus disponible au téléchargement. Conclusion: la disponibilité de l'application dépend du sign in, et donc de la localisation paramétrée dans l'application Google Play, et non pas de l'adresse IP					
18	Access Token Logging in Production	17.6.2021	Im Management-Service wird das Loglevel für "ch.admin.bag.*" global auf DEBUG gesetzt	Im Management-Service wird das Loglevel für "ch.admin.bag.*" global auf DEBUG gesetzt. https://github.com/admin-ch/CovidCertificate-Management-Service/blob/6d7bbd85ab75b1ea603e2112c02758ce1769a260/src/main/resources/application.yml#L13 Das Loglevel wird nicht spezifisch pro Umgebung überschrieben und führt dadurch dazu, dass sensitive Daten (Access Tokens) auf die Console geloggt werden. https://github.com/admin-ch/CovidCertificate-Management-Service/blob/47cfe9bdf9b9eee9f14639bd703b4c2eaad8d1c7/src/main/java/ch/admin/bag/covidcertificate/web/controller/SecurityHelper.java#L22 https://cheatsheetseries.owasp.org/cheatsheets/Logging_Cheat_Sheet.html#data-to-exclude	Access Tokens können aus den Logs kopiert und verwendet werden, um sich als jemand anderes auszugeben.	Access Tokens sollten nur ohne Signatur geloggt werden oder das Loglevel entsprechend angepasst werden. Achtung beim Umstellen, die Nachvollziehbarkeit wer wann welches Zertifikat ausgestellt hat geht ohne Anpassung verloren. https://github.com/admin-ch/CovidCertificate-Management-Service/blob/6d7bbd85ab75b1ea603e2112c02758ce1769a260/src/main/java/ch/admin/bag/covidcertificate/web/controller/CovidCertificateGenerationController.java#L48	Jw Martin	fixed	
19	iText Version Legacy	18.6.2021	EOL Software für PDF Generierung	Backend-seitig wird offenbar eine Version von iText zur PDF-Kreierung verwendet, welche Stand heute bereits End-of-Life ist. Die Informationen dazu sind in den Metadaten der erstellten PDF sichtbar.	EoL Software wird nicht mehr unterhalten und erhält Üblicherweise auch keine Patches mehr für Sicherheits-Lücken. Entsprechend entsteht das Risiko, dass in der PDF-Generierung nicht behobene Vulnerabilities bestehen. Da sämtlicher Input für die PDF-Genererierung durch die Applikation selbst erzeugt wird, ist das entstehende Risiko klein. Es wärde lediglich dann zu einem Problem werden, wenn nicht validierter Benutzer-Input in das PDF Übernommen wird.	Auch wenn kein nicht validierter Input in das PDF Übernommen wird, empfiehlt es sich eine aktuelle Version von iText zu verwenden. Dies einerseits weil die Verwendung von EoL Software bei Go-Live immer vermieden werden sollte, andererseits auch um allfällig künftigen funktionalen Erweiterungen (welche eben diese Vulnerability triggern könnten) vorzubeugen.		wontfix	Version 5 is the latest open source version. Security releases still happen for iText5.
20	DGC – Date of birth validation	19.6.2021	The Management-Service verifies that the date of birth is in this	The Digital Green Certificate specification states that the date of birth shall be in range 1900-2099 (https://ec.europa.eu/health/sites/default/files/ehealth/docs/digital-green-certificates_dt-specifications_en.pdf)	The Management-Service accepts to generate and sign a certificate for a person which is not yet born (date of birth in the future).	Add an additional check in the Management-Service to enforce that the date of birth is not in the future	Christian Conus	Fixed	

			range but it doesn't check that the date is not in the future.	The Management-Service verifies that the date of birth is in this range but it doesn't check that the date is not in the future.
				
				https://github.com/admin-ch/CovidCertificate-Management-Service/blob/develop/src/main/java/ch/admin/bag/covidcertificate/api/request/CovidCertificatePersonDto.java
				
				if (dateOfBirth == null || dateOfBirth.isBefore(MIN_DATE_OF_BIRTH) || dateOfBirth.isAfter(MAX_DATE_OF_BIRTH)) {
				throw new CreateCertificateException(INVALID_DATE_OF_BIRTH);
				}					

21	100 Versuche bzw. mind. 3 Minuten halten des Smartphones bis QR-Code gescannt wird	19.6.2021	100 Versuche bzw. mind. 3 Minuten halten des Smartphones bis QR-Code gescannt wird	100 Versuche bzw. mind. 3 Minuten halten des Smartphones bis QR-Code gescannt wird ohne dass Anzeige für Bearbeitung oder Fehler angezeigt wird – dachte scho. App oder Phone/Kamera funktioniert nicht	QR-Cose wird nicht gescannt bzw. Vorgang wird wom User abgebrochen	Beschleunigung scanner oder Anzeige über Vortschritt der Aufnahme bzw. Fehmermeldung		wontfix	Not reproducible
22	Potentielles operatives Kompatibilitätsproblem mit den EU Staaten	20.6.2021	Potentielles operatives Kompatibilitätsproblem mit den EU Staaten durch Verwendung von RSASSA-PSS stat ECDSA	Die Schweiz verwendet als einziger Teilnehmer den secondary Algorithm RSAPSS-SSA währender die restlichen EU Staaten ausschliesslich den recommended primary Algorithm ECDSA verwenden. Die released Spezifikation 1.0.5 https://github.com/ehn-dcc-development/hcert-spec/blob/1.0.5/hcert_spec.md Sektion 3.3.2 beschreibt die akzeptierten Algorithmen, beide RSAPSS-SSA und ECDSA sind explizit vorgesehen. Jedoch sollte der secondary Algorithm nur dann eingesetz 9arden, wenn Zitat "the primary algorithm is not acceptable within the rules and regulations imposed on the implementor". Das ist in der Schweiz jedoch kein Problem. Auch wenn die Spezifikation ebenfalls fordert, dass sämtliche Implementationen mit beiden Algorithmen auskommen müssen, so besteht ein Risiko, dass diese nicht überall implementiert sind. Denn zum Einen umfasst die Quality Assurance nur die QR Codes, nicht aber die Verifikationsimplementationen, zum anderen wird unter Zeitdruck unter Umständen nicht überall beides implementiert (Erfahrung aus dem SW Development). Auch die Roadmap im oft referenzierten Dokument https://ec.europa.eu/health/sites/default/files/ehealth/docs/digital-green-certificates_v3_en.pdf enthält für Version 1 nur ECDSA. Die publizierten Testdaten https://github.com/eu-digital-green-certificates/dgc-testdata zeigen, dass die Schweiz der einzige Teilnehmer ist, der ausschliesslich RSAPSS-SSA einsetzt.	Es besteht ein potentielles operatives Risiko, dass Schweizer Covid Zertifikate nicht in allen Teilnehmerstaaten verifiziert werden können.	Auf den recommended primary Algorithm (ECDSA) wechseln.		Closed N/A	
23	Tracker	7.7.2021	Https://certivac.ch arbeitet mit dem Tracker	Https://certivac.ch arbeitet mit dem Tracker cdnjs.cloudflare.com		Ein digitales Covid-Zertifikat wird unbegründet verweigert. Ich betrachte dieses Vorgehen nicht als rechtskonform.		wontfix	out of scope, Nicht in Verbindung mit dem COVID-Zertifikat

			cdnjs.cloudflare.com	(Cloudflare, Inc., San Francisco / USA; https://www.cloudflare.com). Falls man den Tracker nicht akzeptiert (aktiviert) bliebt einem das digitale Covid-Zertifikat verwehrt.		Der Tracker eines US-amerikanischen Anbieters (cdnjs.cloudflare.com) darf einem Kunden in der CH das Covid-Zertifikat infolge beschriebener Tatsache nicht verwehren. Seitens des BAG gilt das hiesige DSG.			
24	Datenkompromittierung durch unvollständige Implementierung	8.7.2021	Datenkompromittierung durch unvollständige Implementierung	Grundsätzlich ist für die Speicherung der Daten die App “Covid Certificate” https://play.google.com/store/apps/details?id=ch.admin.bag.covidcertificate.wallet vorgesehen. Für die Prüfung des Zertifikats ist die App “Covid Certificate Check” https://play.google.com/store/apps/details?id=ch.admin.bag.covidcertificate.verifier vorgesehen. Für die Person, die sich einer Prüfung unterzieht, ist nicht nachvollziehbar, welche App zur Prüfung des Zertifikats verwendet wird. Dadurch ist es auf einfachste Weise möglich, direkt die kompletten Gesundheitsdaten durch die App “Covid Certificate” auszulesen und zu speichern. Alternativ kann auf einfache und unauffällige Weise ein Screenshot angefertigt werden, der später mit selbiger App ausgelesen wird. (Unter Android schneller Doppelklick auf den Powerbutton und zum fotografieren den Lautstärkeknopf.) Es ist kommuniziert, dass ein datensparsamer QR-Code aufgelegt werden soll, der dieses Problem beseitigt. Nach meinem Kenntnisstand gibt es dafür kein kommuniziertes Datum. Grundsätzlich mutet es durchaus seltsam an, dass mit der App “Covid Certificate” das Werkzeug zur Datenschutzverletzung und -speicherung auch noch offiziell vom BAG angeboten wird. Gleichzeitig wird in der Beschreibung der App in Fettschrift mit “Data protection is a top priority” geworben.	Kompromittierung aller im Zertifikat enthaltenen Daten (darunter Gesundheitsdaten). Für alle Zertifikatsinhaber, die sich einer Prüfung durch staatliche oder private Stellen unterziehen wollen.	Datensparsamen QR-Code implementieren.		fixed	
25	Single key for all QR Code signing						NTC	wontfix	
26	Centralized blacklist service not compliant with EU recommendation						NTC	wontfix	
27	Centralize blacklist service stores PII						NTC	false positive	
28	Data shared with US-based company						NTC	wontfix	
29	UVCI generation is not optimal						NTC	wontfix	
30	PII is sent to backend for signing						NTC	wontfix	
31	Insecure onboarding process of DGC issuers						NTC	fixed	
32	In-app download based on Direct Certificate						NTC	false positive	

	Delivery Codes is insecure								
33	Every user can revoke any DGC						NTC	wontfix	
34	Bypass of the 2-factor authentication of the M2M interface						NTC	ongoing	
35	Missing audit table						NTC	wontfix	
36	Verbose information in Swiss QR codes						NTC	wontfix	
37	Data shared with Google						NTC	wontfix	
38	iOS verifier and wallet apps use hardcoded keys for DGC validation						NTC	wontfix	
39	Immunity request match list						NTC	wontfix	
40	The match lists of the immunity request application pose a unnecessary risk						NTC	wontfix	
41	Offline COVID certificate verification restricted						NTC	fixed	
42	Swiss digital COVID certificate impersonation and theft possible						NTC	wontfix	
43	The immunity request form can be used as privacy leaking information oracle						NTC	wontfix	
44	Swiss COVID light certificate accessible to app users only						NTC	wontfix	
45	Holder PII is logged						NTC	fixed	
46	OTP validity time deviates from documentation						NTC	wontfix	
47	Private key is used to verify JWT signature						NTC	fixed	
48	OTP can be use multiple times						NTC	wontfix	
49	OTP signature algorithm not specified						NTC	fixed	
50	Vulnerable third-party dependencies						NTC	fixed	
51	Insufficient role based access control						NTC	wontfix	

52	JWT audience validation deviates from RFC7519						NTC	fixed	
53	Credential logged						NTC	fixed	
54	OTP JWT signature not enforced						NTC	false positive	
55	OTP JWT validation doesn't check IDP sources						NTC	Fixed	
56	M2M additional signature header validation incomplete						NTC	can't be fixed	
57	OTP token not used in backend API						NTC	fixed	
58	API gateway uses service account						NTC	wontfix	
59	Hardcoded credentials in source code						NTC	fixed	
60	Weak credential in source code						NTC	fixed	
61	OTP JWT validation does not check issuer claim						NTC	wontfix	
62	Unrestricted Spring Actuator Configuration						NTC	fixed	
63	OTP JWT are not issued with explicit typing						NTC	fixed	
64	The issued OpenID Connect tokens are not revoked on logout						NTC	wontfix	
65	Refresh token issued but never used						NTC	wontfix	Refresh token is needed
66	Simultaneous session logons are allowed in the issuer web application						NTC	wontifx	
67	Wrong algorithm used for DGC document signing						NTC	fixed	
68	Missing connection between JWT requester and mTLS client certificate						NTC	ongoing	
69	Keycloak configuration violates best practices						NTC	fixed	
70	Some characters do not appear in the PDF						NTC	fixed	
71	M2M test TLS certificate valid for production						NTC	false positive	
72	M2M WAF policy less restrictive than web						NTC	wontfix	

73	M2M certificate common name check disabled						NTC	fixed	
74	Routes for verifier access via CDN do not restrict paths						NTC	fixed	
75	iOS verifier and wallet apps expose sensitive data on iOS task switcher						NTC	fixed	
76	iOS wallet app has insufficient iOS Keychain item access control attribute						NTC	wontfix	
77	iOS wallet app lacks application layer encryption of DGCs						NTC	wontfix	
78	Android wallet app lacks option for strong authentication						NTC	wontfix	
79	iOS wallet app lacks option for application passphrase or biometric authentication						NTC	wontfix	
80	iOS/Android wallet app does not validate if device passcode is set						NTC	wontfix	
81	Insufficient certificate pinning						NTC	fixed	
82	Android apps use hardcoded keys for COVID certificate validation						NTC	fixed	
83	iOS apps use hardcoded keys for COVID certificate validation						NTC	fixed	
84	Downloaded revocation list cannot be verified						NTC	fixed	
85	Revocation list endpoint available without role check						NTC	fixed	
86	SQL injection in immunity request backend						NTC	wontfix	
87	Internal Atlantica cloud hostname exposed in partially public GitHub repositories						NTC	fixed	
88	Overview of overall code quality						NTC	fixed	
89	CSV injection in immunity request form						NTC	fixed	

90	Insufficient Security Headers						NTC	fixed	
91	CSV import without proper input validation						NTC	fixed	
92	Minimum login level issue						NTC	fixed	
93	The function HasRoleWithType defaults to true):						NTC	fixed	
94	Patient plausibility check returns wrong error message						NTC	fixed	
95	Missing link of canton user and UVCI						NTC	fixed	
96	Deviation in default retention period						NTC	fixed	
97	Hardcoded values in Config file						NTC	wontfix	
98	OTP validation bypass						NTC	fixed	
99	Phone lockout not working as intended						NTC	wontfix	
100	Function named TODO						NTC	fixed	
101	CSRF on CSV import						NTC	fixed	
102	CSV inport can lead to CSRF Attack						NTC	N/A	false positive
103	Potentially insecure TLS setting						NTC	fixed	
104	Configuration download as user LevelS3						NTC	fixed	
105	SQL parameterization missing						NTC	fixed	
106	Unnecessary obfuscation						NTC	fixed	
107	Public key can be re-used						NTC	fixed	
108	Read can return zero bytes						NTC	fixed	
109	SFTP does not verify hostkey						NTC	fixed	
120	SFTP username/password based authentication						NTC	ongoing	
110	JWT audience validation deviates from RFC7519						NTC	fixed	

111	HTTP client has wiretap functionality enabled						NTC	fixed	
112	In-app delivery COVID certificate deletion						NTC	fixed	
113	In-app delivery RSA key size validation						NTC	fixed	
114	EU backend is a blind signing oracle						NTC	wontfix	
115	Irrevocable COVID certificates						NTC	wontfix	
116	Cookies werden unverschlüsselt übermittelt						NTC	wontfix	
117	Error Handling gibt Java Stacktrace raus						NTC	fixed	
118	Härtung der Content Policy						NTC	fixed	
119	Möglicher DoS auf E-Mail Gateway						NTC	fixed	
120	Information Disclosure beim Passwort Reset						NTC	fixed	
121	Fehlende Validierung von Eingabedaten (HTML Eingabe Möglich)						NTC	ongoing	
122	UVCI könnte mehrfach generiert werden						NTC	fixed	
123	Kein UVCI-Filter für Revocation-Liste						NTC	wontfix	
124	Schwache 2FA Reset-Implementation						NTC	can't be fixed	
125	Authentication Bypas						NTC	fixed	
126	Apache Range Header DoS (CVE-2011-3192)						NTC	ongoing	
127	CSP: Wildcard Directive						NTC	can't be fixed	
128	Proxy Disclosure						NTC	fixed	
129	Trace.axd Information Leak						NTC	Wontfix	N/A
130	Keycloak Session Fixation						NTC	fixed	
131	Cookie Without SameSite Attribute						NTC	fixed	
132	Cross-Domain Script Inclusion (XSSI)						NTC	ongoing	

133	Insufficient Anti-Automation						NTC	fixed	
134	Revocation-API nicht vor massenhaften Anfragen geschützt						NTC	ongoing	
135	Insufficient Entropy						NTC	fixed	
136	Sensitive Information in Github Repositories						NTC	fixed	
137	Covid Check QRcode Crash App (dos)	04.08.2021	Covid Check QRcode Crash App (dos)				Noah Chiovetta	fixed	
139	ID Cards are not checked	25.08.2021						Out of scope	Not a software bug
140	gespeicherte Zertifikate	09.09.2021						Out of scope	Not a software bug
141	Selbstverifikation Refresh Button	18.09.2021						fixed	
143	Timemachine	21.10.2021		By modifying the date and time of the smartphone hosting the COVID Certificate Check app, an attacker is able to make the verification of an expired certificate successful.				wontfix	Der Aufwand, das Problem auszunutzen, ist sehr hoch. Eine Ausnutzung ist unwahrscheinlich
144	Claims of private key leak	27.10.2021						fixed	Private key leaked in a different country have been revoked
145	QR Decoding issue	04.11.2021						fixed	QR code revoked