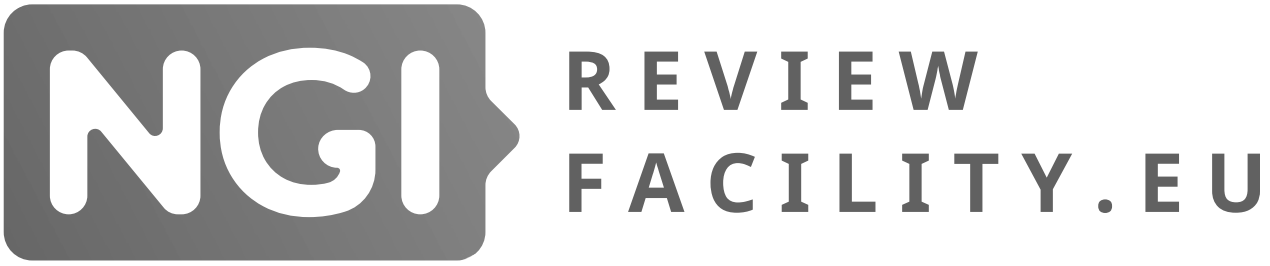

Name: NGI Emergency Tech Review Facility

Contract nr: LC-01499045

Date of signature: 30-04-2020

Name of the deliverable: Deliverable 3.9 –
In-depth assessment of the EU Digital COVID Certificates Gateway – part 1

Authors: Tim Hummel, Marcus Bointon (Radically Open Security)

Level of distribution: Confidential, only for members of the facility
(including the Commission Services)

Confidential: Yes

RADICALLY OPEN SECURITY

EU Digital COVID Certificates Gateway - Evaluation Report

European Commission -
Directorate General CONNECT

V 1.0
Amsterdam, March 1st, 2022
Confidential

Document Properties

Client	European Commission - Directorate General CONNECT
Title	EU Digital COVID Certificates Gateway - Evaluation Report
Targets	In the context of the newly added revocation feature: Source Code Audit of the Digital Covid Certificate (DCC) Gateway 1.3.4 Penetration test of the DCC Gateway as deployed in its acceptance (ACC) environment
Version	1.0
Pentesters	Tim Hummel, Robin Peraglie
Authors	Tim Hummel, Marcus Bointon
Reviewed by	Marcus Bointon
Approved by	Melanie Rieback

Version control

Version	Date	Author	Description
0.1	February 21st, 2022	Tim Hummel	Initial draft
0.2	February 24th, 2022	Tim Hummel	Additional findings
0.3	February 25th, 2022	Tim Hummel	Pre-review
0.4	February 28th, 2022	Marcus Bointon	Review
1.0	March 1st, 2022	Marcus Bointon	1.0

Contact

For more information about this document and its contents please contact Radically Open Security B.V.

Name	Melanie Rieback
Address	Science Park 608 1098 XH Amsterdam The Netherlands
Phone	+31 (0)20 2621 255
Email	info@radicallyopensecurity.com

Radically Open Security B.V. is registered at the trade register of the Dutch chamber of commerce under number 60628081.

Table of Contents

1 Executive Summary

1.1 Introduction

Between February 17, 2022 and February 25, 2022, Radically Open Security B.V. carried out a design evaluation, source code evaluation and penetration test for the European Commission - Directorate General CONNECT.

This report contains our analysis as well as detailed explanations of any findings discovered.

1.2 Scope of work

This is a retest of the gateway in the light of the recently added revocation feature. This evaluation focuses on the revocation feature, but also took another look at the other features. The gateway was previously evaluated by Radically Open Security B.V. [4].

The scope of the penetration test was:

- Penetration test of the DCC Gateway as deployed in its acceptance (ACC) environment from a grey-box perspective: Full access to the source code of the DCC gateway was given while specifics of the infrastructure and its configuration remained unknown.
- We evaluated the Source code and documentation of the European Federation Gateway Service retrieved from the public repository on github [1] up to and including release `1.3.4`.
- We evaluated the code parts referenced in the EU Digital COVID Certificate Lib [2] `1.1.11` .
- We used the EC eHealth and COVID-19 documentation [5] for reference where applicable.
- We did not examine any non-public developer repositories or take non-public documentation into account, with the sole exception of a draft design document for the "Backend to Backend revocation feature" [3].
- All other repository or documents are excluded from the scope.

1.3 Project objectives

The objective of this evaluation was to check the design, source code, and deployment to see if there are any concerns from a security perspective following the rollout of the recently added revocation feature.

1.4 Timeline

The Security Audit took place between February 17, 2022 and February 25, 2022.

1.5 Results In A Nutshell

During this penetration test we found 3 Moderate and 3 Low-severity issues.

We found only issues that can be exploited by on-boarded users (member states) or that increase the likelihood of human error e.g. during deployment and management.

We found no issues that could allow compromise of the gateway by a 3rd party.

1.6 Summary of Findings

ID	Type	Description	Threat level
F-004	Design issue	There are only limited checks on the revocation data, some by design, some due to missing implementation. Some limitations are documented and some are not.	Moderate
F-006	Missing implementation	There is no role assignment interface implemented.	Moderate
F-007	Secure coding	The JSON parser ignores the schema, allows duplicate keys, and leaves wrong and unverified data in place.	Moderate
F-001	Information disclosure	Configuration files in the repository contain passwords.	Low
F-002	Secure coding	CertificateAuthenticationFilter defaults to not filtering in error cases.	Low
F-003	Open issues	Some issues from the previous report were not addressed.	Low

1.7 Summary of Recommendations

ID	Type	Recommendation
F-004	Design issue	• Describe these limitations clearly in the documentation. • Explicitly mention that these limitations also apply to the KID. • Recommend verification options implementable by the member states.
F-006	Missing implementation	• Implement a role management interface. • Implement a database management system or methods that prevent human error for all admin tasks.
F-007	Secure coding	• Verify the JSON schema of revocation batches and do not allow duplicate or unintended JSON keys. • Perform validation and write documentation similar to that provided for the validation-rules endpoint.
F-001	Information disclosure	• Do not store (test) credentials in a public repository. • Provide deployment guidelines indicating that these credentials should not be used in an actual deployment.
F-002	Secure coding	• Require authentication by default, even in error cases.

F-003	Open issues	• Consider addressing the remaining issues from the previous report.

2 Risk Classification

Throughout the report, vulnerabilities or risks are labeled and categorized according to the Penetration Testing Execution Standard (PTES). For more information, see: http://www.pentest-standard.org/index.php/Reporting

These categories are:

- **Extreme**
  Extreme risk of security controls being compromised with the possibility of catastrophic financial/reputational losses occurring as a result.
- **High**
  High risk of security controls being compromised with the potential for significant financial/reputational losses occurring as a result.
- **Elevated**
  Elevated risk of security controls being compromised with the potential for material financial/reputational losses occurring as a result.
- **Moderate**
  Moderate risk of security controls being compromised with the potential for limited financial/reputational losses occurring as a result.
- **Low**
  Low risk of security controls being compromised with measurable negative impacts as a result.

3 Pentest Technical Summary

3.1 Findings

We have identified the following issues:

3.1.1 F-004 — Limited checks on revocation data

Vulnerability ID: F-004

Vulnerability type: Design issue

Threat level: Moderate

Description:

There are only limited checks on the revocation data, some by design, some due to missing implementation. Some limitations are documented and some are not.

Technical description:

There are some limitations on the validity of the revocation data the gateway makes available. Member states or other consumers of this data should be aware of that, but it ultimately causes no issues as long as the data is checked properly on the consumer side.

The primary guarantee is only that revocation data was indeed uploaded by an on-boarded country, and that the country mentioned in the revocation data download is verified as the one that uploaded it. There is very limited checking on the data itself.

Member states should never revoke others DCCs. This is forbidden in the design document. The back-end does not, and in the current design cannot, check if the uploaded DCC revocation hashes were issued by the same member state which is trying to revoke them. With the limited information available to the gateway this is not possible. This should be no surprise to developers who have read the B2B documentation. This however can lead to member states accidentally or deliberately revoking DCCs issued by other member states.

In the current design the responsibility for only uploading revocation for owned certificates rests with the member states. Additional checks in a member state's verifier app/service can eliminate or reduce the risk that a revocation could be issued by the wrong member state, for example by checking the country of revocation against the issuer of a revocation list. Additionally, member states that do not trust another member state can choose to not use their uploads, as uploads are marked with the uploading country.

Additional limitations:

- The gateway does not guarantee that the KID has anything to do with the country which uploaded a revocation batch or is related to the DCC hashes it contains. It also fails to check whether the KID was ever valid and trusted by the system. Similar to the DCC hashes, a KID could be from an unrelated country that holds no trust. This is not immediately obvious from the documentation; One could imagine an alternative design in which the gateway requests proof of ownership of a key for a KID before allowing that value to be used by a country.
- The gateway does not guarantee that the DCC hashes or KID uploaded to or downloaded from the gateway are valid base64; they can be arbitrary strings.
- The gateway does not guarantee that the expiry time is reasonable.
- The gateway does not check for duplicate submissions.

Impact:

Not being aware of the revocation data limitations could lead to parsing errors or an inappropriate level of trust in provided revocation hashes and KIDs. The impact is limited because only on-boarded member states could create faulty/ malicious data.

Recommendation:

- Describe these limitations clearly in the documentation.
- Explicitly mention that these limitations also apply to the KID.
- Recommend verification options implementable by the member states.

3.1.2 F-006 — No reliable method for role assignment

Vulnerability ID: F-006

Vulnerability type: Missing implementation

Threat level: Moderate

Description:

There is no role assignment interface implemented.

Technical description:

The B2B documentation says:

> "The Gateway must also provide a reliable method whereby the administrators can manage the Roles that are linked to the Users in such a way as to reduce the chance of human errors whilst also not burdening the functional administrators."

This is not implemented in the code. We assume this is currently done via raw database access.

This is not only a reasonable measure for the role assignment but for all administration tasks, especially since (according to the source code) the whole on-boarding process is built using raw databases queries.

Impact:

Human error could lead to entities being assigned certificates or roles they shouldn't have in the system, that shouldn't be there at all, or via other faults in the database. The impact is hard to assess completely, but all roles are likely assigned to everyone anyway. There are checks to ensure that added certificates are signed by the trust anchor anyway. It also depends on how this is all performed by administrators, who might have developed a reasonable method.

Recommendation:

- Implement a role management interface.
- Implement a database management system or methods that prevent human error for all admin tasks.

3.1.3 F-007 — JSON parsing problems

Vulnerability ID: F-007

Vulnerability type: Secure coding

Threat level: Moderate

Description:

The JSON parser ignores the schema, allows duplicate keys, and leaves wrong and unverified data in place.

Technical description:

The following JSON is a revocation batch that was successfully uploaded to the gateway using the YA country certificates:

```
{
    "country": "NL",
    "country": "CZ",
    "expires": "2003-11-01T00:00:00Z",
    "expires": "2022-11-01T00:00:00Z",
    "kid":"hui",
    "kid":"abcdabcdabcd",
    "note":"Hacking is cool!",
    "hashType":"COUNTRYCODEUCI",
    "hashType":"SIGNATURE",
    "country": "YA",
    "entries":[
        {
        "kekse":"haha",
        "hash":"e2e2e2e2e2e2e2e2e2e2e2e2"
        }
    ]
}
```

We used the following commands for the upload:

```
CERTPATH="./Pentest_YA"
CREDENTIALS="--cert $CERTPATH/cert_auth.pem --key $CERTPATH/key_auth.pem"
curl -vvv --request POST -H "Accept: */*" -H "Content-Type: application/cms" $CREDENTIALS 'https://
url-removed/revocation-list' --data-binary "@cms.b64"
```

The batch appears in the batch list as:

```
{
    "batchId": "uuid-removed",
    "country": "YA",
    "date": "2022-02-24T13:24:28+01:00",
    "deleted": false
}
```

The malicious data was ignored by the gateway, but it is stored for, relayed to, and parsed by the other national back-ends. This could become a problem when the gateway's parser and national back-ends parse the same (invalid) JSON in different ways.

Notably, these problems do not exist in the validation-rule upload endpoint. The validation-rule endpoint is documented in the repository, and describes which checks are performed. We recommend a similar level of care for the revocation endpoint.

Impact:

On-boarded member states can upload revocation batches that contain faulty/malicious values. Member states' implementations that handle this data could misinterpret it, for example to misidentify a batch as originating from the wrong member state.

Recommendation:

- Verify the JSON schema of revocation batches and do not allow duplicate or unintended JSON keys.
- Perform validation and write documentation similar to that provided for the validation-rules endpoint.

3.1.4 F-001 — Repository Contains Passwords

Vulnerability ID: F-001

Vulnerability type: Information disclosure

Threat level: Low

Description:

Configuration files in the repository contain passwords.

Technical description:

Various files in the `dgc-gateway` and the `dgc-lib` repositories contain passwords e.g.

- `docker-compose.yml`
- `application.yml`
- `application-mysql.yml`

These credentials are handy for testing and are probably only examples that are not used during deployment, but we cannot verify that. Their existence and the absence of any clear deployment guidelines relating to them carries the risk that these values might be used by anyone using this code.

Impact:

Adding "example" credentials to a repository caries the risk of people deploying them to use them. However, even if these credentials are publicly known it carries little risk as they are not for components that are publicly accessible.

Recommendation:

- Do not store (test) credentials in a public repository.
- Provide deployment guidelines indicating that these credentials should not be used in an actual deployment.

3.1.5 F-002 — CertificateAuthenticationFilter shouldNotFilter

Vulnerability ID: F-002

Vulnerability type: Secure coding

Threat level: Low

Description:

`CertificateAuthenticationFilter` defaults to not filtering in error cases.

Technical description:

The function `shouldNotFilter` in class `CertificateAuthenticationFilter` decides whether it should not apply authentication on a client request to the gateway:

```
protected boolean shouldNotFilter(HttpServletRequest request) {
        try {
            HandlerExecutionChain handlerExecutionChain = requestMap.getHandler(request);

            if (handlerExecutionChain == null) {
                return true;
            } else {
                return !((HandlerMethod) handlerExecutionChain.getHandler()).getMethod()
                    .isAnnotationPresent(CertificateAuthenticationRequired.class);
            }
        } catch (Exception e) {
            handlerExceptionResolver.resolveException(request, null, null, e);
            return true;
        }
    }
```

The spring documentation for `shouldNotFilter` states "Can be overridden in subclasses for custom filtering control, returning true to avoid filtering of the given request." https://docs.spring.io/spring-framework/docs/1.2.x/javadoc-api/org/springframework/web/filter/OncePerRequestFilter.html

The above code thus defaults in error cases to not filter a presented request.

Impact:

In error cases client requests are passed through without authentication. However, we don't see a scenario in which such an error could occur.

Recommendation:

- Require authentication by default, even in error cases.

3.1.6 F-003 — Unfixed issues from previous report

Vulnerability ID: F-003

Vulnerability type: Open issues

Threat level: Low

Description:

Some issues from the previous report were not addressed.

Technical description:

The following issues from the previous evaluation were not addressed:

- Reflected Cross-Site Scripting Vulnerability on CIRCABC (Proof of concept code still produces an XSS).
- Race Condition allows to upload two certificates with the same Thumbprint or KID (no code change observed).

Impact:

The remaining issues have a low impact rating.

Recommendation:

- Consider addressing the remaining issues from the previous report.

3.2 Non-Findings

In this section we list some of the things that were tried but turned out to be dead ends.

3.2.1 NF-005 — /revocation-list/delete endpoint misses OpenApi authorization fields

In contrast to all other endpoints of the gateway the endpoint `/revocation-list/delete` is missing the `SecurityRequirement` annotation that is present for the other endpoints:

```
@Operation(
    security = {
        @SecurityRequirement(name = OpenApiConfig.SECURITY_SCHEMA_HASH),
        @SecurityRequirement(name = OpenApiConfig.SECURITY_SCHEMA_DISTINGUISH_NAME)
    },
```

It was confirmed that this does not have any influence on the security by verifying that the endpoint still enforces authentication on contact.

We assume the absence of the annotation will result in the generated OpenApi specification not documenting or describing that authentication is required for this endpoint. While this is not a security risk itself, we advise fixing it for documentation and testing purposes.

3.2.2 NF-008 — Port scan

We performed a port/vulnerability scan on the acceptance environment IP addresses. This did not reveal any additional entry points.

3.2.3 NF-009 — External attackers

The gateway has a relatively small attack surface because its service is only available to TLS-authenticated on-boarded users (member states). Completely external attackers will have to, for example, successfully attack the reverse-proxy servers which are responsible for TLS authentication before relaying an HTTP request to the gateway application. For

this reason, we experimented with sending malformed and malicious requests to the acceptance environment, but we did not manage to bypass authentication without a valid certificate.

4 Future Work

- **Reverse Proxy configuration review**
  The reverse-proxy(s) are responsible for user authentication of the gateway. Our grey-box bypass attempts were fruitless, but a white-box configuration review could provide additional insights.
- **Retest of findings**
  When mitigations for the vulnerabilities described in this report have been deployed, a repeat test could be performed to ensure that they are effective and have not introduced other security problems.

5 Conclusion

We discovered 3 Moderate and 3 Low-severity issues during this penetration test.

Except for the minor issues identified during the security audit, the general design and source code make a solid impression. The absence of any serious vulnerabilities in this evaluation is a good indication that system security is generally good.

The gateway presents a very limited attack surface while being only accessible for on-boarded users (member states). We did not find any issues that might allow bypassing authentication and thus compromise the gateway from a third party perspective.

We found only issues that can either only be exploited by authenticated users, or that increase the likelihood of human error during administration.

A successful exploitation of the identified issues related to data processing requires either a malicious on-boarded member state or compromised authentication. Even in the event of a key compromise the findings are only relevant for the national back-ends if they do not sanitize the data coming from the gateway properly, or assume the wrong level of checks from the gateway.

The absence of a management interface for the admins e.g for on-boarding and role management, could lead to some limited opportunity for human error. Therefore, we suggest that the admins use a suitable process to minimize error.

We recommend fixing all of the issues found, and then performing a retest in order to ensure that mitigations are effective and that no new vulnerabilities have been introduced.

Finally, we want to emphasize that security is a process – this penetration test is just a one-time snapshot. Security posture must be continuously evaluated and improved.

Please don't hesitate to let us know if you have any further questions, or need further clarification on anything in this report.

6 Bibliography

[1] EU Federation Gateway Service Github repository. https://github.com/eu-digital-green-certificates/dgc-gateway.

[2] EU Digital COVID Certificate Lib Github repository. https://github.com/eu-digital-green-certificates/dgc-lib.

[3] Revocation B2B Centralized Version 0.7 2021-12-08.

[4] Radically Open Security B.V.: Penetration Test of the Digital Covid Certificate Gateway v1.0 2021-06-04.

[5] EC eHealth and COVID-19 documentation. https://ec.europa.eu/health/ehealth-digital-health-and-care/ehealth-and-covid-19_en.

Appendix 1 Testing team

Tim Hummel	Tim Hummel is a senior IT-security analyst, consultant, developer and trainer. His specialty is hardware, crypto, and related software security. In his work he tests everything from apps, car components, payment solutions, white-box crypto, pay TV, mobile devices, IoT, TPMs, TEEs, bootloaders, entertainment systems to transport cards. He recently tested various Corona related apps and services for the EU and the Netherlands.
Robin Peraglie	Robin is a passionate bug hunter and security researcher. Since he was young he experimented with web security, cryptography and lockpicking. He received a M.Sc. degree in IT Security at the Ruhr-University Bochum, and has since gained industrial experience across many penetration tests and professional code audits.
Melanie Rieback	Melanie Rieback is a former Asst. Prof. of Computer Science from the VU, who is also the co-founder/CEO of Radically Open Security.

Front page image by Slava (https://secure.flickr.com/photos/slava/496607907/), "Mango HaX0ring",
Image styling by Patricia Piolon, https://creativecommons.org/licenses/by-sa/2.0/legalcode.