Bern University
of Applied Sciences

Bachelor's Thesis

Unlinkability of Verifiable Credentials in a practical approach: Project Management

Course of study	Bachelor of Science in Computer Science
Author	Joël Gabriel Robles Gasser
Advisor	Prof. Dr. Annett Laube, Prof. Dr. Reto Koenig
Expert	Dr. Andreas Spichiger

Version 1.0 of June 13, 2024

- Engineering and Computer Science
- Computer Science

Contents

1 Risks

In this chapter, we define risks that may happen in this thesis.

1.1 Project Risks

1.1.1 VC

- Risk: There is the possibility that the structure of VCs might break the unlinkability of BBS
- Solution: If that is the case, the structure of VCs needs to be reworked so there is no linkability
- Possibility: Low

1.1.2 OIDC4VP

- Risk: There is the possibility that the implementation of OIDC4VP leaks data
- Solution: If that is the case, the structure of the OIDC4VC protocol needs to be reworked so there are no more data leaks
- Possibility: Low

1.1.3 OIDC4VP

- Risk: There is the possibility that the implementation of OIDC4VP leaks data
- Solution: If that is the case, the structure of the OIDC4VC protocol needs to be reworked so there are no more data leaks
- Possibility: Low
- Risk: There is the possibility that the implementation of OIDC4VP breaks the unlinkability of BBS
- Solution: If that is the case, the structure of the OIDC4VP protocol needs to be reworked so there is no linkability
- Possibility: Medium

1.1.4 Pseudonyms

- Risk: There is the possibility that the implementation of pseudonyms breaks the unlinkability of BBS
- Solution: If that is the case, the structure of pseudonyms needs to be reworked, so there is no linkability
- Possibility: Low

1.1.5 Link Secrets

- Risk: There is the possibility that the implementation of Link Secrets breaks the unlinkability of BBS
- Solution: If that is the case, the implementation of the Link Secrets needs to be reworked, so there is no linkability
- Possibility: Medium
- Risk: There is the possibility that the implementation of Link Secrets allows the holder of multiple VCs to link them together on a different Secret
- Solution: If that is the case, the implementation of the Link Secrets needs to be reworked, so that this is no longer possible
- Possibility: Low

1.2 Environmental risks

1.2.1 Sickness

- Risk: There is a possibility that I might become sick
- Solution: If the sickness is less than 1 week, there is a buffer in the project plan at the end of the semester for that. If it's more than 1 week, there is a chance that the project would need to be moved to another semester
- Possibility: Medium

1.2.2 Hardware

- Risk: There is a possibility that the hardware used (laptop) may break due to unknown reasons
- Solution: The deliverables are backed up to GitHub and mirrored to the BFH-TI GitLab. There is also a backup on other hardware. There also backup hardware if the main hardware would break

- Possibility: Low
- Risk: There is the possibility that the backups are not accessible
- Solution: In that case, there is also a backup on different devices
- Possibility: Low

1.2.3 Project Plan/Ideas

- Risk: There is the possibility that the project plan is bad, so that the planned time frames are too short
- Solution: In that case, there is 1 week buffer at the end of the semester. If that is not enough time, then there needs to be an explanation in the documentation why that happened
- Possibility: Medium
- Risk: There is the possibility that the expert of the project may bring new ideas into the project
- Solution: If those ideas further the project goals, they may be added to the project plan. In that case the project plan needs to be reworked
- Possibility: Low

2 Meetings

In this semester I've attended many meetings with different parties: with my advisors, with the expert and with the BBS working group.

Meetings with advisors:
Nearly each week I met with my advisors. In those meetings, we discussed my new findings, about the sprint results or about the documentation. Those meetings helped me a lot to stay more or less within my sprint deadlines, and I learned a lot of things about researching and documenting.

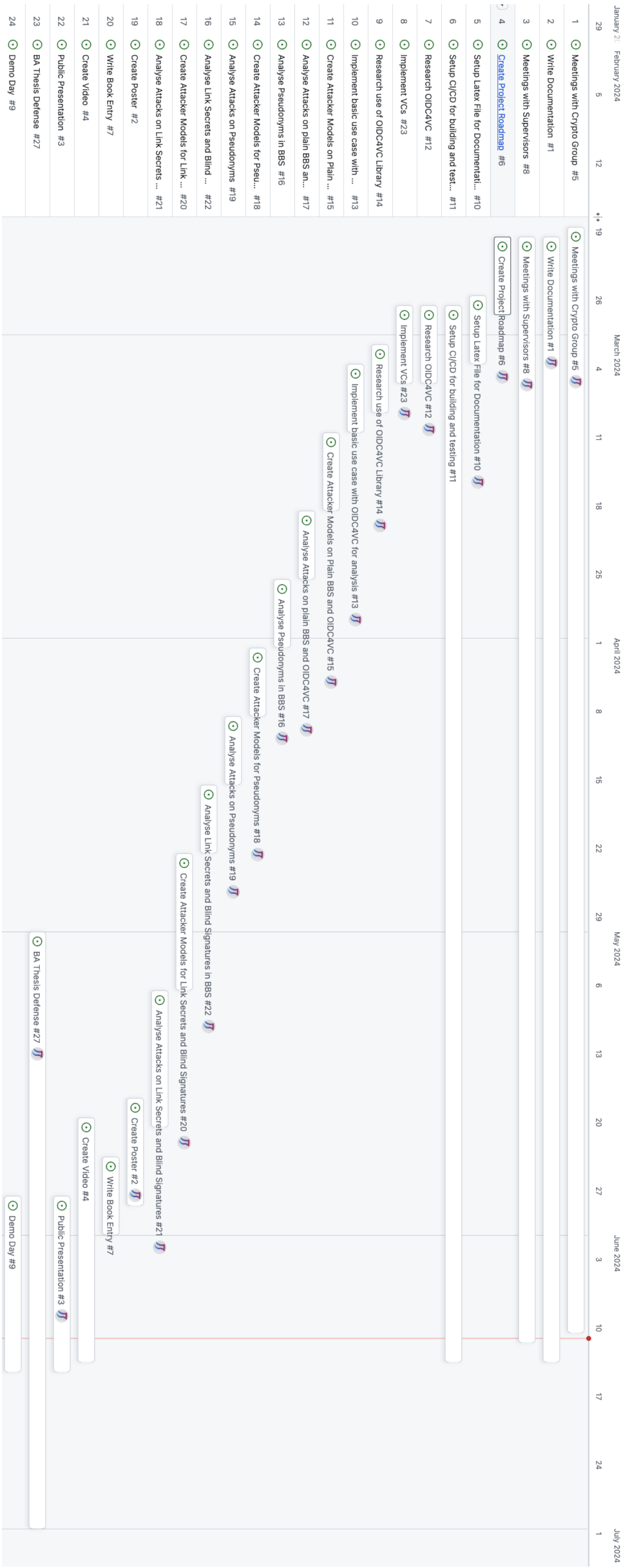
Meetings with expert:
This semesters, I had three meetings with the expert. The first meeting was all about the project management, the goal and the first results. The second meeting was around the half way mark of the semester, where I presented a first version of the my defense, with results up to that point. I got some feedback, which I used to improve the defense. Then there was a third meeting one week before the due date, where I presented the full defense as a test run. On that date there were also three other listeners that were interested in the technologies. After the presentation, I got feedback from all of them, which I can use to again improve the defense.

Meetings with the BBS working group:
Nearly each monday evening, the BBS working group meets online to talk about new issues, new ideas or updates to the BBS specifications. I participated in many of those meetings and asked questions based on my current findings, to better understand the whole picture.

3 Project Management

In this chapter the project management which was done in this semester is thematized. In figure 3 one can see the roadmap created for this thesis. This roadmap contains all the planned sprints for the whole project.

I've used Scrum for the project management. All the tasks (besides the documenting and meetings) were split up into one- or two-week sprints. At the end of each sprint, I looked back on what was done within that timeframe and used the new knowledge for the sprint. Using Scrum as my project management framework helped me to change directions when something unexpected happened, and thus assisted me in staying organized.



1 Meetings with Crypto Group #5
2 Write Documentation #1
3 Meetings with Supervisors #8
4 Create Project Roadmap #6
5 Setup Latex File for Documentati... #10
6 Setup CI/CD for building and test... #11
7 Research OIDC4VC #12
8 Implement VCs #23
9 Research use of OIDC4VC Library #14
10 Implement basic use case with ... #13
11 Create Attacker Models on Plain ... #15
12 Analyse Attacks on plain BBS an... #17
13 Analyse Pseudonyms in BBS #16
14 Create Attacker Models for Pseu... #18
15 Analyse Attacks on Pseudonyms #19
16 Analyse Link Secrets and Blind ... #22
17 Create Attacker Models for Link ... #20
18 Analyse Attacks on Link Secrets ... #21
19 Create Poster #2
20 Write Book Entry #7
21 Create Video #4
22 Public Presentation #3
23 BA Thesis Defense #27
24 Demo Day #9

January 2
February 2024
29
5
12
19
26
March 2024
4
11
18
25
April 2024
1
8
15
22
29
May 2024
6
13
20
27
June 2024
3
10
17
24
July 2024
1
Meetings with Crypto Group #5
Write Documentation #1
Meetings with Supervisors #8
Create Project Roadmap #6
Setup Latex File for Documentation #10
Setup CI/CD for building and testing #11
Research OIDC4VC #12
Implement VCs #23
Research use of OIDC4VC Library #14
Implement basic use case with OIDC4VC for analysis #13
Create Attacker Models on Plain BBS and OIDC4VC #15
Analyse Attacks on plain BBS and OIDC4VC #17
Analyse Pseudonyms in BBS #16
Create Attacker Models for Pseudonyms #18
Analyse Attacks on Pseudonyms #19
Analyse Link Secrets and Blind Signatures in BBS #22
Create Attacker Models for Link Secrets and Blind Signatures #20
Analyse Attacks on Link Secrets and Blind Signatures #21
Create Poster #2
Write Book Entry #7
Create Video #4
Public Presentation #3
BA Thesis Defense #27
Demo Day #9

Figure 3.1: Roadmap

4 Found Issues

While researching for this thesis, many issues were found. This chapter summarizes all the raised issues/written mails.

4.1 Github Issues

These are the issues that were reported in the *Data Integrity BBS Cryptosuites v1.0*[1] GitHub Repository.

Typo & missing check
see: `https://github.com/w3c/vc-di-bbs/issues/154`
In this issue I mentioned a typo. I also mentioned that there is a missing check for a value in an object, as if that value is empty it could raise an error. The typo was fixed, but the check was not added.

Missing attributes
see: `https://github.com/w3c/vc-di-bbs/issues/155`
In this issue I mentioned that some attributes used in the algorithm were not passed as parameters. At the same time the authors were changing where all the parameters come from, as the part of the addition of optional features. Error was fixed with the optional features update.

Missing reference
see: `https://github.com/w3c/vc-di-bbs/issues/157`
In this issue I noted that there was a missing reference to a used algorithm. After searching for a bit, I found that algorithm defined in an other specification. The error was fixed a standalone pull request.

Missing reference: The second
see: `https://github.com/w3c/vc-di-bbs/issues/163`
Same as in the above mentioned issue, there was a missing reference. At the same time, the wrong algorithm was called. The called algorithm has been corrected and the reference was added, but the pull request was not approved yet.

Unused variables
see: `https://github.com/w3c/vc-di-bbs/issues/164`
In an algorithm, a variable was defined, but never used. The error was corrected, but the pull request was not accepted yet.

Typo & missing information
see: `https://github.com/w3c/vc-di-bbs/issues/166`
There was another small typo, which was changed with the next pull request. There was also the problem of how to retrieve the public key, as it is used as an input to an algorithm. This information was also added in the same pull request but was not accepted and merged yet.

Add SHA-3
see: `https://github.com/w3c/vc-di-bbs/issues/162`
In the Data Integrity BBS Cryptosuites[1] specification, SHA-256 is used for all hashing operations. I suggested adding the information that SHA-3 would also be a possibility, as the BBS specification also allows hashing with a kmac. This suggestion was rejected, the reason being that a big part of the internet is using SHA-256 and thus the implementation using SHA-256 instead of SHA-3 would be easier.

4.2 Written Mails

While researching OIDC4VP, in the chapters 11.5 and 6 of OpenID for Verifiable Presentations [3] it wasn't stated in where the nonce value and the client_id values should be included. After contacting the authors of the specification, Olivier Terbu responded with the instruction where to add these values in the VP.

5 Problems

In this chapter the problems that came up while researching and writing this thesis are mentioned.

Sickness
During the project, I was sick twice. Both times for around a week. Although there was a buffer for being sick for one week, the second time shortened my timeframe in which I could work on the thesis.

Extensive Specification
Verifiable Credentials Data Model v2.0[2] is a very extensive specification. There are many optional features that are not really needed for this thesis. So it took some time to determine which features should be used.

Unclear Specification
The *Data Integrity BBS Cryptosuites v1.0*[1] specification was very unclear. I did not really understand what the different algorithms did, or what the required inputs where. I used Greg Bernsteins, one of the authors, implementation to understand each step in the algorithms. I needed to write up the specification in a way that was more or less understandable. This used a lot of time and was not planned, thus leaving less time for other parts of the thesis.

Documentation
For me, the documentation was the biggest problem of the whole thesis. It is very hard for me to write up something that reads more or less ok. Therefore, many revisions were needed, which used up way more time than expected. So at the end I needed more than double the time than I planned for the documentation alone.

Bibliography

[1] Greg Bernstein and Manu Sporny. Data integrity bbs cryptosuites v1.0. `https://www.w3.org/TR/vc-di-bbs/`, 2024. Accessed on April 1, 2024.

[2] Manu Sporny, Dave Longley, David Chadwick, and Orie Steel. Verifiable credentials data model v2.0. `https://www.w3.org/TR/vc-data-model-2.0`, 2023. Accessed on March 19, 2024.

[3] O. Terbu, T. Lodderstedt, K. Yasuda, and T.Looker. Openid for verifiable presentations - draft 20. `https://openid.net/specs/openid-4-verifiable-presentations-1_0.html`, 2023. Accessed on March 24, 2024.