Hogeschool van Amsterdam
Amsterdam University of Applied Sciences

Project From Moonshot to Mars

Plan of Approach

Remy Bien, Ruben Bras, Marvin Hiemstra,
Sebastiaan Groot, Wouter Miltenburg, Koen Veelenturf

22 February 2013, revised on 22 March 2013
Version 1.2

NIKHEF

Table of Contents

1. Introduction

As part of our minor Forensics Intelligence and Security our team will be working on Project Moonshot. Last year another team worked on the same project, and even though they came a long way, they did not finish the entire project. Their implementation worked up to a certain point but did not guarantee the privacy and security of the users' credentials. This year we will pick up on their work, and either improve upon, or rethink and rebuild their implementation to make sure user credentials are stored and handled securely.

The goal of this project is to secure the existing federated access to an SSH-shell using the user's existing credentials. This should be done without making the password or passwordhash known anywhere but the user's instance's RADIUS-server. This includes availability by sniffing.

The exact approach to reach our goal will be determined after adequate research and conversing with the client has been done.

2. Project Definition

2.1 Goal

The goal of this project is to secure the existing federated access to an SSH-shell using the user's existing credentials. This should be done without making the password or passwordhash known anywhere but the user's instance's RADIUS-server. This includes availability by sniffing.

During the development, the focus will be at following security principles and the creation of a standardised solution.

2.2 Approach and phases

The project is divided into three phases: initiation, building and delivery. See Appendix B and C for the planning and phases of the project.

2.3 Results

The following products together form the end result that will be delivered to NIKHEF:

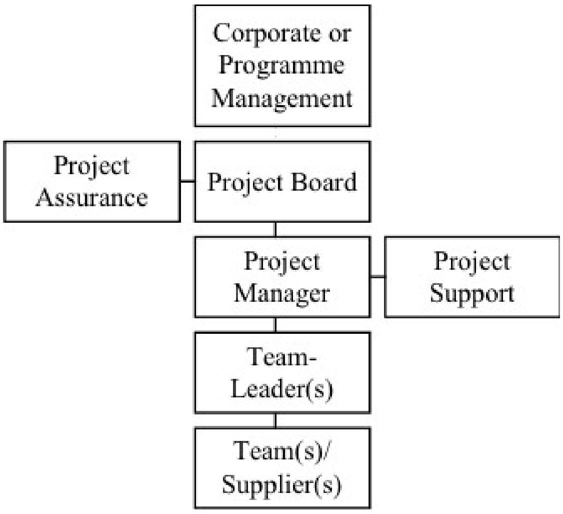
- Presentation GSSAPI, RADIUS & EAP-TTLS
- Plan of Approach
- Research report
  - Containing solutions for securely setting-up a security-context from an OpenSSH client to an OpenSSH server.
  - Containing solutions for securely transmitting the user credentials to a Radius server using an end-to-end connection.
- Moonshot OpenSSH
- Final Report
- Final Presentation

2.4 Project conditions and limitations

The scope of the project is the studying of existing literature and presenting the findings, the development of a solution that will enable the user to securely connect to an OpenSSH server using Radius. The priority of the project, taking the time restrictions into account, is the delivery of solutions that can be presented and used on an international level. This priority has precedence over the delivery of all the products named above.

3. Organisational structure

In the period of running the From Moonshot to Mars Project, there will be a temporary organisation:



Corporate or Programme Management	
Name	*Role/Responsibility*
Oscar Koeroo	Client
Mischa Salle	Client

The client of the From Moonshot to Mars Project is mister Oscar Koeroo. Mr Koeroo is client on behalf of NIKHEF (The Dutch Institute for Subatatomic Physics) in Amsterdam.

Project Assurance	
Name	*Role/Responsibility*
Sebastiaan Groot	Internal Team Coordinator
Koen Veelenturf	Internal Quality Assurance

During this project, the team will not get any Quality Assurance from ITopia, but will be responsible for their own Quality Assurance. The Project Assurance is responsible for monitoring the quality aspects of the project and the deliverables. The Project Assurance is independent from the Project Manager. The Project Assurance will keep the project in scope and makes sure that the goals will be achieved. The Project Assurance will report to the Project Manager.

Project Manager / Project Board	
Name	Role/Responsibility
Sebastiaan Groot	Team Coordinator a.k.a. Project Manager

The Project Manager is responsible for the daily activities of the Project Team. The Project Manager is allowed to make decisions within the boundaries of the Project Board. The main responsibility of the Project Manager is to ensure the deliverables will be delivered in time, within budget and according to the quality standards.

Project Team	
Name	*Role/Responsibility*
Remy Bien	
Ruben Bras	
Sebastiaan Groot	Team Coordinator
Marvin Hiemstra	
Wouter Miltenburg	
Koen Veelenturf	Internal Quality Assurance

The team is responsible for delivering the products according to specifications, described by the client and Project Manager. The team reports to the Team Coordinator; the Team Coordinator reports to the client and the (Hogeschool van Amsterdam) Project Board.

4. Product Dependencies

To give a good overview of the product dependancies, this chapter will describe the relationship between the individual products, which products run parallel and in which order the products are developed. See appendix C for a diagram depicting this information.

The project begins with the Plan of Approach, in order to properly define the scope, planning and project definition. Once this document is complete, research will start in the fields of Kerberos, RADIUS, GSSAPI and EAP-TTLS. These research results will be compiled into a presentation. After this product is finished, implementation of the test environment will begin, as well as a research in the possibilities of the previously researched subjects, this research will be described in a research report proposing solutions for setting up a secure connection for authenticating an OpenSSH client to an OpenSSH server. When the research report has been finished a proof of concept will be developed to support the claims made in the research report. In this phase OpenSSH client and server are made secure for authentication against Radius. This results in two parallel development processes, one concentrating in securely authenticating using an end-to-end connection from client through OpenSSH server to Radius and one securely transmitting all data through the network. The documentation of the products combined with the earlier made network documents will then result in the final report.

5. Planning

5.1 Project planning

For a detailed, graphical planning, see appendix B.

Project part	Start	Deadline
Project from Moonshot to Mars	**Mon 4-2-13**	**Fri 21-6-13**
Plan of Approach	**Mo 4-2-13**	**Fri 22-2-13**
GSSAPI Research	**Mon 4-2-13**	**Fri 22-2-13**
Presentation GSSAPI	**Thu 28-2-13**	**Thu 28-2-13**
Research of possibility's	**Mon 25-2-13**	**Fri 15-3-13**
Network Documents	**Fri 15-3-13**	**Fri 29-3-13**
Test environment	**Fri 15-3-13**	**Fri 29-3-13**
Connection client to SSHD	**Fri 29-3-13**	**Fri 12-4-13**
Connection server with PAM/GSS	**Fri 12-4-13**	**Fri 26-4-13**
Send information through SSHD	**Fri 26-4-13**	**Mon 13-5-13**
Security with Certificates	**Fri 26-4-13**	**Mon 13-5-13**
Testing & Debugging	**Fri 17-5-13**	**Mon 24-5-13**
Final document	**Fri 31-5-13**	**Mon 10-6-13**

For the description of the products, see appendix A.

6. Control mechanisms

This chapter describes which mechanisms will be applied to ensure that the project remains manageable and that the quality will be guaranteed.

6.1 Tolerances

The project team monitors and follows the project according to the planning described in the previous chapters. It is always possible, for all kind of reasons, that the team deviates from the plan. If this is the case the following rules will be retained:

- It is the intention that the projects will be finished according to the agreed end date. If this fails, a new target will be defined with the client.
- If the scope of the project need to be changed, requested by the team or client, it is possible to do so. This request has to be communicated in a timely manner and needs to be approved by the client and in cooperation with the project-team. If the request is approved, the planning will be changed according to the approved request.
- If one of the sub-projects cannot be finished in the agreed deadline, the team will describe the proposed solutions in the final report of the overall project.

6.2 Progress reports

There will be weekly meetings between the client and the team. These meetings will take place on Mondays or Fridays. During this meetings the progress will be reported with the client and when needed new targets will be defined. During the holidays or when a meeting is cancelled, the client will be reported via mail by the team leader of this project. When a deliverable is finished the client will be notified about this achievement and when a target is not achieved, or cannot be achieved on the agreed deadline, the client will also be notified about this event. When it is the case that a deliverable cannot be finished on the agreed deadline, new targets will be defined with the client.

Furthermore, meetings will be held inside the project team to assure that everyone is aware what the other members are doing. During this meeting the project status will be checked and team leader will check if everyone is on schedule. Consequently doing this will result in less complications during the project and it also ensures that everyone is aware of each other. These meetings will also take place once in a week.

6.3 Exception procedure

The exception procedure occurs when the project can no longer succeed in the expected tolerance limits, regarding time and money. The exception procedure defines that in the first part a so called "reporting phase" will start. In this phase, an investigation will start into what could be the cause of this fault. All possible solutions and changes in order to succeed the project in the expected tolerance limits. In the second phase there will be made an appointment with the client. During this meeting the report that describes the reasons and causes of the fault will be presented to the client, the possible corresponding solutions will also be presented to the client. When the solutions are discussed, the next stage starts where the client, in cooperation with the team, have to choose between one of the following situations:

- The project board will take measures to prevent/eliminate the cause
- The project board decides to not take action, because it thinks that the exceeding of tolerance will not take place
- There are concession to be made in respect of time, money quality or the projects that have to be delivered (the range of the project)

The first two situations will be reported during the meeting with the client (progress reports). The last situation will take place on the request of the project board and results in the creation of an exception plan with alternatives for dealing with the continuation of the project and for changing the planning.

7. Project risks

The following tables depict an overview of the as of now acknowledged threats to the project, including proposed countermeasures, the chance of occurrence and the rate of negative impact on the project (depicted on a scale of 1 to 5). The last column depicts the risk, which is chance*impact. In this way we can determine what threats need the most attention and/or resources.

During the project this list will be continually updated to account for new possible threats. If such an update occurs, it will be explicitly mentioned during the next meeting with the client.

Chance	Assigned number
Very small chance	1
Small chance	2
Intermediate chance	3
Reasonable chance	4
Big chance	5

Tabel 7.1: Explanation of the rate of occurrence

Impact	Assigned number
Very small impact	1
Small impact	2
Intermediate impact	3
Big impact	4
Great impact	5

Tabel 7.2: Explanation of the impact

Threat	Countermeasures	Chance	Impact	Risk
The project gets canceled.	Communicate with the client as to the reason of the cancellation. Try to get the project back on it's feet again. If this proves impossible, try close the project to the satisfaction of both parties.	1	5	5
Work is done outside of the scope of the project.	Assign a team member to guard the scope and ensure all work done is absolutely necessary. Update planning to account for lost time.	2	4	8

Threat	Countermeasures	Chance	Impact	Risk
Product does not meet the client's expectations.	Inform client of the state of the products during the meetings to keep to set the correct expectations and if needed update the scope of the project. Ask the client if an updated product should be made, or an alternate solution should be found.	2	4	8
Longterm absence of one or more team members.	Update the planning and scope of the project, depending on the duration of the absence. Re-assign roles in the team if necessary.	2	3	6
Employees struggle to understand the hard/software used in the project.	Take extra time to familiarize at least one person on the team with the hard/software, who can then relay this information to others. Consult with the client and other sources for help if needed.	3	4	12
Test environment is delayed by unforeseen circumstances.	The time which is lost will be used to do extra research. When the test environment is delayed by more than two weeks, the project team will start building a test environment on their local machines.	4	4	16

Appendix A: Product description

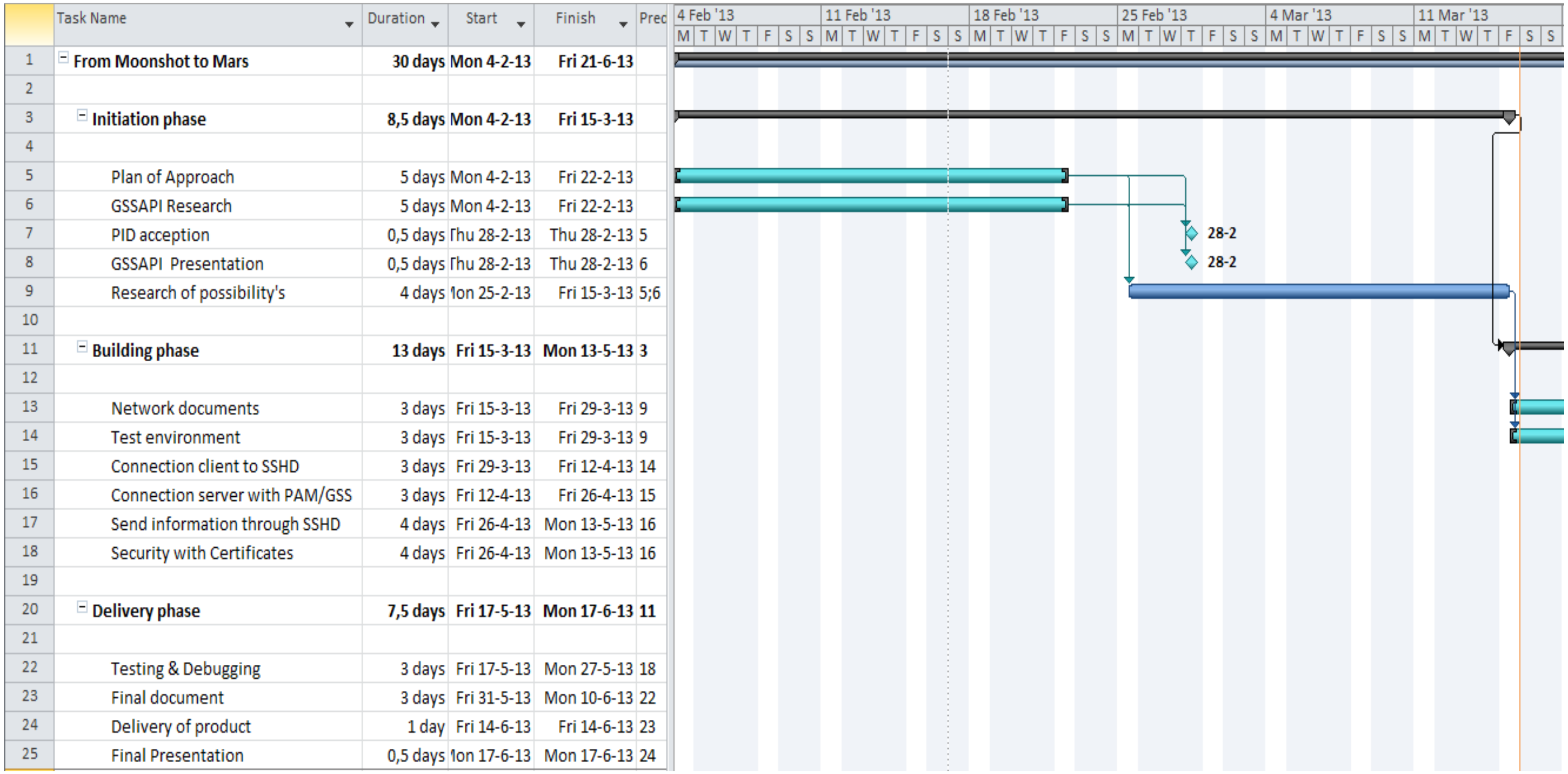
Productname / -number	01	Presentation GSSAPI, RADIUS & EAP-TTLS
Description	Presentation on the inner workings and applications of the GSSAPI, RADIUS protocol and EAP-TTLS protocol.	
Duration (days)	18	
Deadline	28-02-2013	

Productname / -number	02	Plan of Approach
Description	A document covering the subjects of project definition, global planning, project scope, risk analysis and other information related to the project.	
Duration (days)	12	
Deadline	22-02-2013	

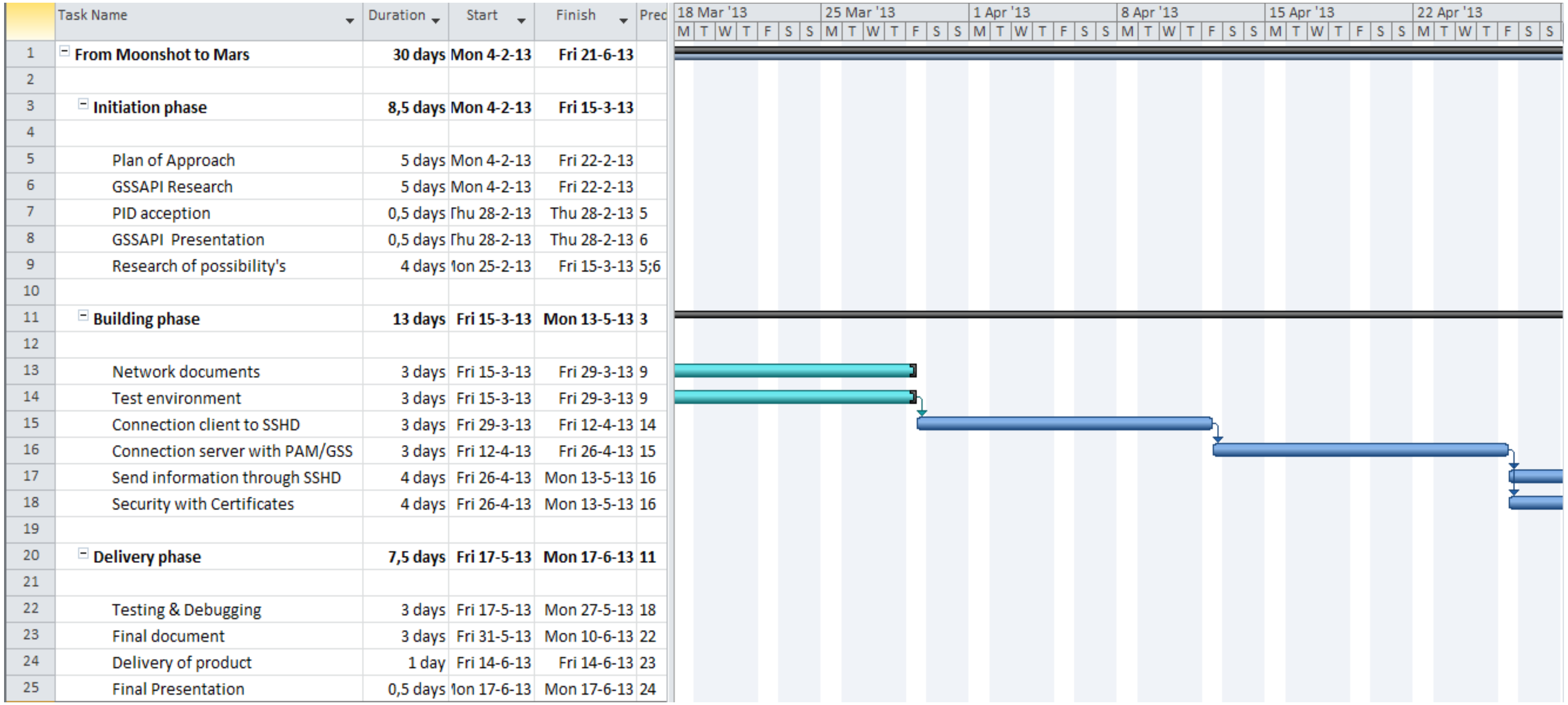
Productname / -number	03	Research report
Description	A research report that describes possible solutions for securely authenticating an client to an OpenSSH server. Passwords (clear-text or hash) should not be seen by other Radius servers when connecting from another realm then your user-realm.	
Duration (days)		
Deadline		

Productname / -number	04	Moonshot OpenSSH
Description	An implementation method of OpenSSH using the implementation principles of Project Moonshot to allow federative authentication and eventually authorization.	
Duration (days)		
Deadline		

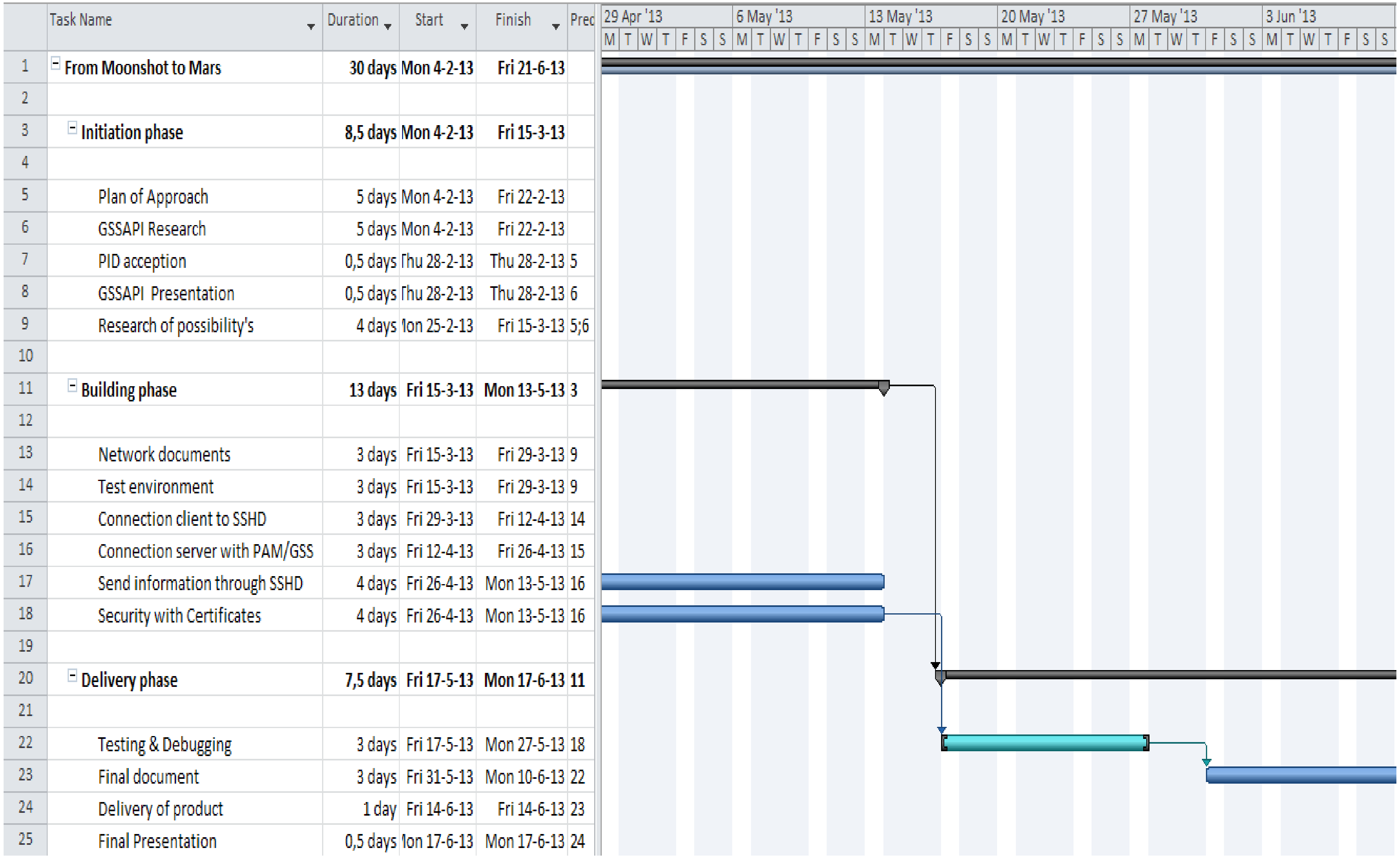
Appendix B: Project planning



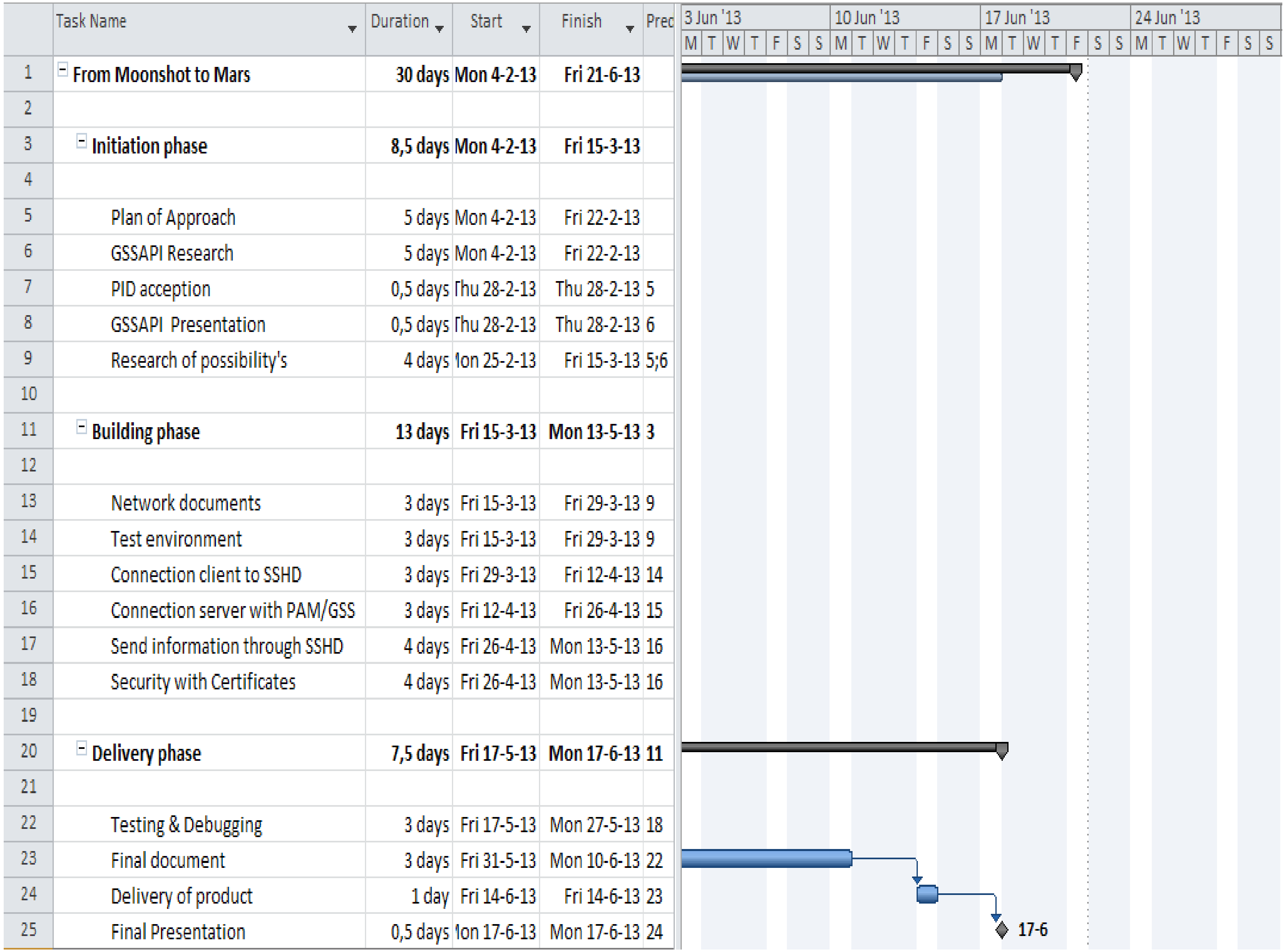
	Task Name	Duration	Start	Finish	Prec
1	**From Moonshot to Mars**	**30 days**	**Mon 4-2-13**	**Fri 21-6-13**	
2					
3	**Initiation phase**	**8,5 days**	**Mon 4-2-13**	**Fri 15-3-13**	
4					
5	Plan of Approach	5 days	Mon 4-2-13	Fri 22-2-13	
6	GSSAPI Research	5 days	Mon 4-2-13	Fri 22-2-13	
7	PID acception	0,5 days	Thu 28-2-13	Thu 28-2-13	5
8	GSSAPI Presentation	0,5 days	Thu 28-2-13	Thu 28-2-13	6
9	Research of possibility's	4 days	Mon 25-2-13	Fri 15-3-13	5;6
10					
11	**Building phase**	**13 days**	**Fri 15-3-13**	**Mon 13-5-13**	**3**
12					
13	Network documents	3 days	Fri 15-3-13	Fri 29-3-13	9
14	Test environment	3 days	Fri 15-3-13	Fri 29-3-13	9
15	Connection client to SSHD	3 days	Fri 29-3-13	Fri 12-4-13	14
16	Connection server with PAM/GSS	3 days	Fri 12-4-13	Fri 26-4-13	15
17	Send information through SSHD	4 days	Fri 26-4-13	Mon 13-5-13	16
18	Security with Certificates	4 days	Fri 26-4-13	Mon 13-5-13	16
19					
20	**Delivery phase**	**7,5 days**	**Fri 17-5-13**	**Mon 17-6-13**	**11**
21					
22	Testing & Debugging	3 days	Fri 17-5-13	Mon 27-5-13	18
23	Final document	3 days	Fri 31-5-13	Mon 10-6-13	22
24	Delivery of product	1 day	Fri 14-6-13	Fri 14-6-13	23
25	Final Presentation	0,5 days	Mon 17-6-13	Mon 17-6-13	24



	Task Name	Duration	Start	Finish	Prec
1	**From Moonshot to Mars**	**30 days**	**Mon 4-2-13**	**Fri 21-6-13**	
2					
3	**Initiation phase**	**8,5 days**	**Mon 4-2-13**	**Fri 15-3-13**	
4					
5	Plan of Approach	5 days	Mon 4-2-13	Fri 22-2-13	
6	GSSAPI Research	5 days	Mon 4-2-13	Fri 22-2-13	
7	PID acception	0,5 days	Thu 28-2-13	Thu 28-2-13	5
8	GSSAPI Presentation	0,5 days	Thu 28-2-13	Thu 28-2-13	6
9	Research of possibility's	4 days	1on 25-2-13	Fri 15-3-13	5;6
10					
11	**Building phase**	**13 days**	**Fri 15-3-13**	**Mon 13-5-13**	**3**
12					
13	Network documents	3 days	Fri 15-3-13	Fri 29-3-13	9
14	Test environment	3 days	Fri 15-3-13	Fri 29-3-13	9
15	Connection client to SSHD	3 days	Fri 29-3-13	Fri 12-4-13	14
16	Connection server with PAM/GSS	3 days	Fri 12-4-13	Fri 26-4-13	15
17	Send information through SSHD	4 days	Fri 26-4-13	Mon 13-5-13	16
18	Security with Certificates	4 days	Fri 26-4-13	Mon 13-5-13	16
19					
20	**Delivery phase**	**7,5 days**	**Fri 17-5-13**	**Mon 17-6-13**	**11**
21					
22	Testing & Debugging	3 days	Fri 17-5-13	Mon 27-5-13	18
23	Final document	3 days	Fri 31-5-13	Mon 10-6-13	22
24	Delivery of product	1 day	Fri 14-6-13	Fri 14-6-13	23
25	Final Presentation	0,5 days	1on 17-6-13	Mon 17-6-13	24

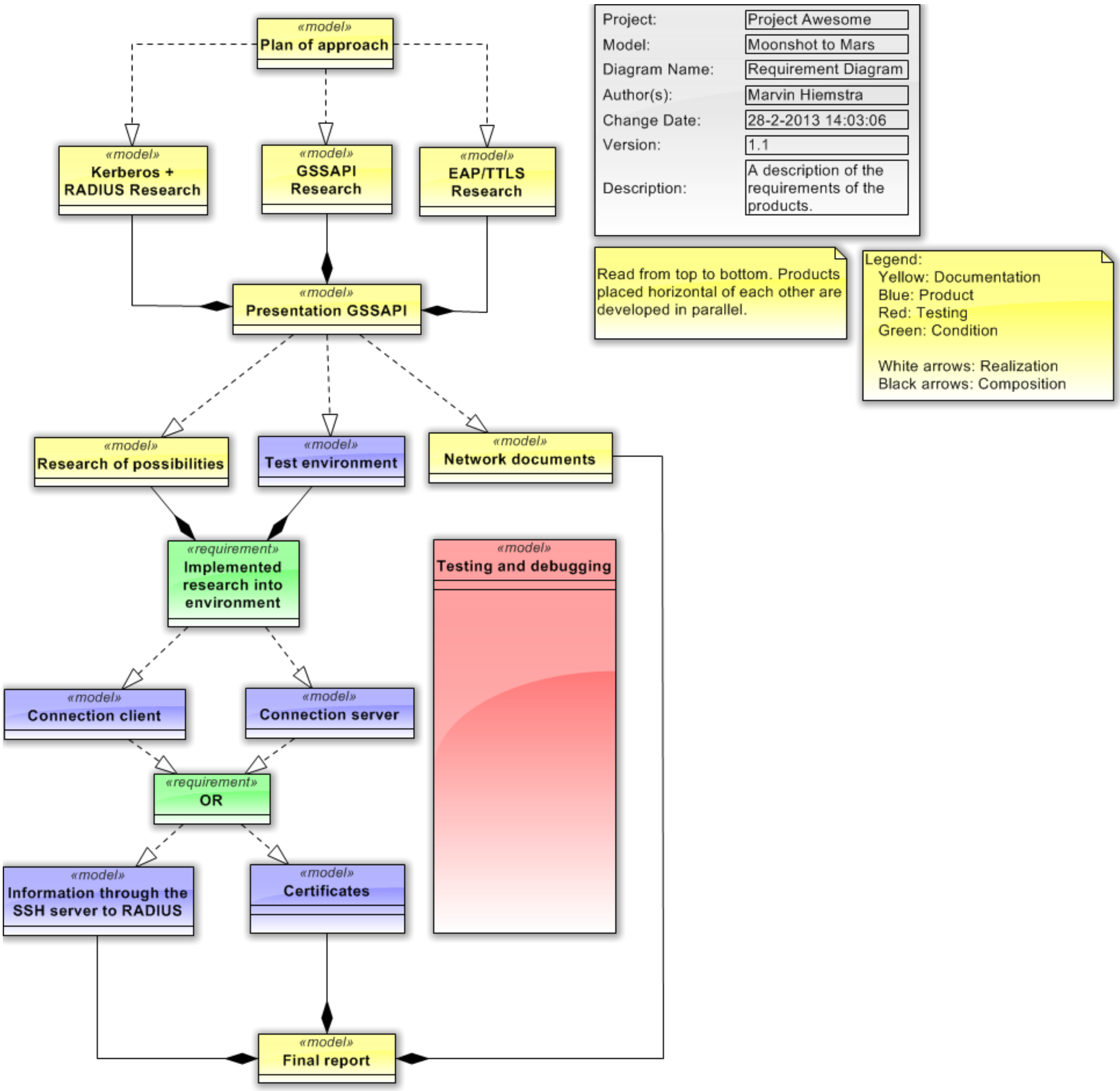


	Task Name	Duration	Start	Finish	Prec
1	**From Moonshot to Mars**	**30 days**	**Mon 4-2-13**	**Fri 21-6-13**	
2					
3	**Initiation phase**	**8,5 days**	**Mon 4-2-13**	**Fri 15-3-13**	
4					
5	Plan of Approach	5 days	Mon 4-2-13	Fri 22-2-13	
6	GSSAPI Research	5 days	Mon 4-2-13	Fri 22-2-13	
7	PID acception	0,5 days	Thu 28-2-13	Thu 28-2-13	5
8	GSSAPI Presentation	0,5 days	Thu 28-2-13	Thu 28-2-13	6
9	Research of possibility's	4 days	Mon 25-2-13	Fri 15-3-13	5;6
10					
11	**Building phase**	**13 days**	**Fri 15-3-13**	**Mon 13-5-13**	**3**
12					
13	Network documents	3 days	Fri 15-3-13	Fri 29-3-13	9
14	Test environment	3 days	Fri 15-3-13	Fri 29-3-13	9
15	Connection client to SSHD	3 days	Fri 29-3-13	Fri 12-4-13	14
16	Connection server with PAM/GSS	3 days	Fri 12-4-13	Fri 26-4-13	15
17	Send information through SSHD	4 days	Fri 26-4-13	Mon 13-5-13	16
18	Security with Certificates	4 days	Fri 26-4-13	Mon 13-5-13	16
19					
20	**Delivery phase**	**7,5 days**	**Fri 17-5-13**	**Mon 17-6-13**	**11**
21					
22	Testing & Debugging	3 days	Fri 17-5-13	Mon 27-5-13	18
23	Final document	3 days	Fri 31-5-13	Mon 10-6-13	22
24	Delivery of product	1 day	Fri 14-6-13	Fri 14-6-13	23
25	Final Presentation	0,5 days	Mon 17-6-13	Mon 17-6-13	24



	Task Name	Duration	Start	Finish	Prec
1	**From Moonshot to Mars**	**30 days**	**Mon 4-2-13**	**Fri 21-6-13**	
2					
3	**Initiation phase**	**8,5 days**	**Mon 4-2-13**	**Fri 15-3-13**	
4					
5	Plan of Approach	5 days	Mon 4-2-13	Fri 22-2-13	
6	GSSAPI Research	5 days	Mon 4-2-13	Fri 22-2-13	
7	PID acception	0,5 days	Thu 28-2-13	Thu 28-2-13	5
8	GSSAPI Presentation	0,5 days	Thu 28-2-13	Thu 28-2-13	6
9	Research of possibility's	4 days	Mon 25-2-13	Fri 15-3-13	5;6
10					
11	**Building phase**	**13 days**	**Fri 15-3-13**	**Mon 13-5-13**	**3**
12					
13	Network documents	3 days	Fri 15-3-13	Fri 29-3-13	9
14	Test environment	3 days	Fri 15-3-13	Fri 29-3-13	9
15	Connection client to SSHD	3 days	Fri 29-3-13	Fri 12-4-13	14
16	Connection server with PAM/GSS	3 days	Fri 12-4-13	Fri 26-4-13	15
17	Send information through SSHD	4 days	Fri 26-4-13	Mon 13-5-13	16
18	Security with Certificates	4 days	Fri 26-4-13	Mon 13-5-13	16
19					
20	**Delivery phase**	**7,5 days**	**Fri 17-5-13**	**Mon 17-6-13**	**11**
21					
22	Testing & Debugging	3 days	Fri 17-5-13	Mon 27-5-13	18
23	Final document	3 days	Fri 31-5-13	Mon 10-6-13	22
24	Delivery of product	1 day	Fri 14-6-13	Fri 14-6-13	23
25	Final Presentation	0,5 days	Mon 17-6-13	Mon 17-6-13	24

Appendix C: Product Dependencies



Project:	Project Awesome
Model:	Moonshot to Mars
Diagram Name:	Requirement Diagram
Author(s):	Marvin Hiemstra
Change Date:	28-2-2013 14:03:06
Version:	1.1
Description:	A description of the requirements of the products.

Read from top to bottom. Products placed horizontal of each other are developed in parallel.

Legend:
Yellow: Documentation
Blue: Product
Red: Testing
Green: Condition

White arrows: Realization
Black arrows: Composition

«model» Plan of approach
«model» Kerberos + RADIUS Research
«model» GSSAPI Research
«model» EAP/TTLS Research
«model» Presentation GSSAPI
«model» Research of possibilities
«model» Test environment
«model» Network documents
«requirement» Implemented research into environment
«model» Testing and debugging
«model» Connection client
«model» Connection server
«requirement» OR
«model» Information through the SSH server to RADIUS
«model» Certificates
«model» Final report