Hochschule Luzern
Technik & Architektur

Informatikprojekt | TA.PAWI.FS2012

Aspects of Privacy-Preserving Toll Pricing

Projektplan

Horw, 8. Februar 2012

Projekt	Aspects of Privacy-Preserving Toll Pricing
Dokument	Projektplan
Schule	Hochschule Luzern, Technik & Architektur
Modul	TA.PAWI.FS2012
Projektteam	**Galliker Thomas** Studiengang Informatik (BB) Panorama 6123 Geiss Tel. +41 79 504 80 70 thomas.galliker@stud.hslu.ch **Moser Christoph** Studiengang Informatik (VZ) Zugerbergstrasse 41 6314 Unterägeri Tel. +41 79 785 19 07 christoph.moser@stud.hslu.ch
Dozent Experte	**Dr. Marc Pouly** **Dr. Josef F. Bürgler**
Letzte Änderung	8. Februar 2012, 13:44:00 Uhr

Änderungsprotokoll

Version	Datum	Autor	Beschreibung
0.1	03.01.2012	gat	Initialversion von Vorlage erstellt
0.2	04.01.2012	gat/moc	Meilenstein- und Rahmenplan erstellt
0.3	05.01.2012	moc	Risikomanagement angefügt
0.4	06.01.2012	gat/moc	Dokumentationsplan erstellt, diverse Ergänzungen
0.5	17.01.2012	gat	Risiken neu bewertet
0.6	30.01.2012	gat	Risiken neu bewertet, Aufwände erfasst
0.8	05.02.2012	moc	Meilensteinberichte ergänzt, IST-Aufwand übertragen
0.9	06.02.2012	gat	Restaufwände erfasst
1.0	07.02.2012	gat/moc	Persönliches Fazit

Inhalt

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

1.1 Ziel & Zweck dieses Dokuments

Dieser Projektplan ist das zentrale Dokument für das Projekt Management des PAWI Projektes „Aspects of Privacy-Preserving Toll Pricing“.

1.2 Projektübersicht

Das Projekt „Aspects of Privacy-Preserving Toll Pricing“ befasst sich mit der Entwicklung eines Prototyps für ein elektronisches Road Pricing Systems.

1.3 Begriffe & Abkürzungen

Abkürzung	Erklärung
CL-RSA	Signaturalgorithmus von Camenisch und Lysyanskaya basierend auf RSA
gat	Namenskürzel für Thomas Galliker
GPS	Global Positioning System
HSLU	Hochschule Luzern
JPA	Java Persistance API
moc	Namenskürzel für Christoph Moser
OBU	On-board Unit
PAWI	Modulbezeichnung für das Modul Informatikprojekt der HSLU T&A
RSA	Rivest, Shamir, Adelson Algorithmus; asymmetrische Verschlüsselung/Signatur
SQLite	Dateibasiertes, leichtgewichtiges Datenbanksystem
TSP	Toll Service Provider
XMPP	Extensible Messaging and Presence Protocol, ehem. „Jabber”, Kommunikationsprotokoll für Instant Messanging (Facebook Chat, Google Talk)

Tabelle 1: Abkürzungserklärungen

2 Projektorganisation

2.1 Projektmitglieder

Name / Adresse	Telefon	E-Mail
Galliker Thomas Studiengang Informatik (BB) Panorama 6123 Geiss	+41 79 504 80 70	thomas.galliker@stud.hslu.ch
Moser Christoph Studiengang Informatik (VZ) Zugerbergstrasse 41 6314 Unterägeri	+41 79 785 19 07	christoph.moser@stud.hslu.ch

Tabelle 2: Koordinaten der Projektmitglieder

2.2 Rollen & Zuständigkeiten

Rolle	Verant-wortung	Beschreibung / Aufgaben
Projektspezifisch		
Projektmanagement	moc	Ist für das Projekt verantwortlich - Organisiert und leitet die Sitzungen (intern + extern) - Verteilt Aufgaben an Teammitglieder - Hält den Projektplan aktuell (insb. Controlling Tabelle)
Programmierung	alle	- Ist verantwortlich für die Software-Entwicklung. (Siehe detaillierte Aufschlüsselung unten)
Testmanagement	moc	- Erstellt und ergänzt Testdokumente - Wertet die Tests aus - Ist für die Protokollierung der Testergebnisse zuständig
Architektur	gat	- Plant die Software-Architektur und erstellt das grobe Gerüst (Struktur & Files) in der Entwicklungsumgebung - hält den Lead bei der Programmierung (genauere Definition siehe unten)
Dokumentenverwaltung	gat	Erstellt Layout aller Dokumente, hält diese aktuell (z.T. durch Input der anderen Gruppenmitglieder) - verantwortlich für die Struktur - behält den Überblick über die Dokumente
Entwicklungsspezifisch		
OBU Applikation; Service related	gat	Kommunikation zwischen OBU und TSP, Implementation der kryptographischen Protokolle
OBU Applikation; GPS related	moc	GPS bezogene Aufgaben inkl. entsprechenden Tests
OBU Applikation; DB related	gat	OBU Datenbank bezogene Aufgaben
TSP Applikation; UI related	moc	User Interface der Toll Service Provider Applikation
TSP Applikation; Service related	moc	TSP Server Service
TSP Applikation; DB related	gat	TSP Datenbank bezogene Aufgaben

Tabelle 3: Rollen & Zuständigkeiten

3 Planung

3.1 Grobplanung

Projektstart	03.01.2012
Projektabschluss	08.02.2012
Projektphasen	2

3.2 Meilensteine

Woche	Inhalt	Meilenstein
1	• Projekt Kick-off • Erstellung Projektmanagementplan • Identifizierung und Bewertung von Risiken • Rahmenplan mit Meilensteinen erstellen • Recherchen über Toll Pricing Bestrebungen in der Schweiz • Recherchen über Kryptosysteme, Lösungsansätze	M1 06.01.2012
2	• Beschreibung der wichtigsten Geschäftsprozesse (Use Cases, Test Cases) • Erster Entwurf einer Systemspezifikation mit Systemübersicht • Definition der Arbeitspakete • Detaillierte Aufgabenteilung • Aufwandschätzung • Entwicklungs- und Testumgebung einrichten • Kurzvortrag über die Recherchen der kryptographischen Protokolle	M2 12.01.2012
3	• Softwarearchitektur definieren und dokumentieren • Datenmodell modellieren, Schnittstellen definieren • Testplan mit Testphilosophie und wesentlichen Testaspekten • Erster Prototyp (vertikal) sowie passende Test Cases erstellen	M3 24.01.2012
4	• System Tests durchführen und protokollieren • Proof of Concept: Vertikale Prototypen lauffähig	M4 01.02.2012
5	• Abgabe der Dokumentation und des Source Codes	M5 08.02.2012
6	• Präsentation der Projektarbeit	M6 15.02.2012

Tabelle 4: Detaillierte Aufschlüsselung der Meilensteine

3.3 Rahmenplan

	Phase 1									Phase 2																			
Kalenderwoche	**KW1**				**KW2**					**KW3**					**KW4**					**KW5**					**KW6**					**KW7**		
	Di	**Mi**	**Do**	**Fr**	**Mo**	**Di**	**Mi**	**Do**	**Fr**	**Mo**	**Di**	**Mi**	**Do**	**Fr**	**Mo**	**Di**	**Mi**	**Do**	**Fr**	**Mo**	**Di**	**Mi**	**Do**	**Fr**	**Mo**	**Di**	**Mi**	**Do**	**Fr**	**Mo**	**Di**	**Mi**
Projekt Kick-Off																															
Erstellung PMP																															
Risikoanalyse																															
Recherchen Road Pricing Schweiz																															
Recherchen Kryptosysteme																															
Meilenstein 1				♦																											
Entwicklungsumgebung einrichten																															
Geschäftsprozesse definieren																															
Systemspezifikation																															
Arbeitspakete erstellen																															
Aufwandschätzung																															
Kurzvortrag vorbereiten																															
Meilenstein 2								♦																							
SW-Architektur																															
ER-Modellierung																															
Testplan definieren, Protokolle vorb.																															
Prototyp: OBU																															
Prototyp: TSPMS																															
Meilenstein 3																♦															
Integrations- und Systemtests																															
Meilenstein 4																					♦										
Projektdokumentation abschliessen																															
Meilenstein 5																											♦				
Präsentationsvorbereitung																															
Präsentation																															♦

Abbildung 1: Gantt-Diagramm des Rahmenplans

4 Arbeitspakete und Aufwandschätzung

Die nachfolgenden Schätzungen beziehen sich auf den Gesamtaufwand, welcher das Team zu leisten hat. Die einzelnen Stundenangaben sind als Mannstunden zu verstehen. Um einen guten IST-SOLL Vergleich zu erlangen, wird in regelmässigen Zeitabschnitten der ungefähre IST Aufwand erfasst.

	SOLL Aufwand	**IST Aufwand**							**Auswertung**
	in [h]	KW1 in [h]	KW2 in [h]	KW3 in [h]	KW4 in [h]	KW5 in [h]	KW6 in [h]	KW7 in [h]	in [h]
Projektmanagement									
Projekt Kick-Off	**3.0**	3							**3**
Erstellen des Projektmanagementplan	**10.0**	4			4				**8**
Risikomanagement: Identifizierung und Bewertung von Risiken; laufende Beobachtung der Risiken	**2.0**	2							**2**
Rahmenplan mit Meilensteinen und grobe Aufwandschätzung erstellen	**2.0**		2						**2**
Erstellen des Geschäftsprozesse (Use Cases)	**20.0**		2		2				**4**
Erstellen des Testplans (Test Cases), Definition der Testfälle	**20.0**					3			**3**
Systemspezifikation erstellen und nachführen	**11.0**	4	4						**8**
Zwischenbesprechungen	**12.0**	2		6		3			**11**
Recherchen									
Strassenfinanzierung Schweiz	**10.0**	4							**4**
Kryptographische Primitive	**50.0**	16	18						**34**
Privacy-Preserving Applications	**20.0**	17	11	2	1				**31**
Entwicklungsaufwand									
Software-Architektur erstellen	**10.0**			3					**3**
Datenmodellierung	**3.0**		2	3					**5**

Definieren der Schnittstellen	**3.0**			2					**2**
Programmierung									
- *Implementation Security Library*	***50.0***		*12*	*26*	*15*	*7*			**60**
- *Implementation OBU Android App*	***30.0***	*6*		*40*	*22*	*20*	*12*		**100**
- *Implementation TSP*	***30.0***			*4*	*30*	*8*	*2*		**44**
- *Implementation Kommunikationsschicht*	***10.0***	*5*		*4*	*23*	*4*			**36**
Testing									
Testdaten generieren: Preis- und Lokationsinformationen	**10.0**				4				**4**
Unit-Tests	**20.0**					8			**8**
Integrations-/Systemtests	**20.0**					15	10		**25**
Projektabschluss									
Projekt Report schreiben	**20.0**	4	5		13	54	36		**112**
Vorbereitung und Durchführung der Präsentation	**6.0**								**0**
Reserve	**16.0**								**0**
	388.0h								**509.0h**

Tabelle 5: Aufwandschätzung und Controlling

5 Meilensteinberichte

5.1 Meilenstein 1

Die Gruppe ist organisiert, die Rollen sind verteilt. Die Initialrisiken des Projekts wurden identifiziert und gewichtet. Während den ersten Tagen wurde der Meilenstein- sowie der Rahmenplan erstellt und laufend ergänzt. Danach folgten die Recherchen über die Strassenfinanzierung, wie sie heute in der Schweiz angewendet wird. Die technischen Recherchen über die kryptographischen Primitive wurden lanciert. Eine Projektübersicht mit verschiedenen Lösungsansätzen und den damit verbundenen Problemen wurde im Projektteam diskutiert.

5.2 Meilenstein 2

Eine Systemübersicht wurde erstellt. Erste Teile des Gesamtsystems wurden spezifiziert, sodass Arbeitspakete geschnürrt und Aufwände (soweit möglich) geschätzt werden konnten. Die Entwicklungs- und Testumgebung mit Netbeans und Subversion war ebenfalls per Meilenstein 2 lauffähig. Zahlreiche Recherchen zu den in diesem Projekt benötigten Krypto-Algorithmen wurden durchgeführt. Meilenstein 2 wurde mit der Kurzpräsentation über die kryptographischen Primitive abgeschlossen.

5.3 Meilenstein 3

Viele kritische Funktionen wurden bereits in Form von vertikalen Prototypen implementiert und auf einen möglichen Einsatz in unserem Projektsystem vorbereitet. Es sind dies im Wesentlichen: GPS Tracking auf Android Plattform, Datenbankanbindung mit JPA bzw. SQLite, kryptographische Commitments erstellen und verifizieren inkl. Homomorphie-Test.

Die Implementation der Kryptolibrary stellte sich einmal mehr als grosse Hürde heraus. Die Formeln zur Erreichung der gewünschten Ziele sind jeweils gegeben, doch bereiteten uns Berechnungen von grossen Exponenten einige Schwierigkeiten. Einige Pow-Aufrufe wurden danach durch ModPow, einer Modular-Exponentialfunktion, ersetzt. Diese Funktion teilt grosse Exponenten in kleinere und wendet die Modulo Operation auf diese kleineren Exponenten an. So konnte beim Berechnen von grossen Exponenten viel CPU-Zeit eingespart werden.

5.4 Meilenstein 4

Das Ziel bei Meilenstein 4 einem lauffähigen Prototyp vorzuweisen, wurde nur teilweise erreicht. Auf dem TSP Service ist zwar die komplette Funktionalität, bis auf die Prüfung des t_z-Wertes im Proof, implementiert und mit Hilfe von JUnit Tests getestet worden. In der Android Applikation hingegen gibt es noch einiges zu tun. Die System Tests haben gezeigt, dass die Android Applikation Daten an den TSP sendet. Allerdings stimmen diese Daten nicht mit den erwarteten Payment Records überein. Zudem muss auf der Android Applikation noch die Funktionalität für das Beantworten einer Challenge-Anfrage implementiert werden.

5.5 Meilenstein 5

In den Tagen zwischen Meilenstein 4 und Meilenstein 5 wurden die Arbeitsstunden mehrheitlich in die Dokumentation investiert. Während dem Projekt wurden zwar laufend Probleme und Erkenntnisse als Notiz festgehalten, trotzdem benötigte es einige Stunden diese Notizen für den Abschlussbericht aufzubereiten. Durch das Fokussieren auf die Dokumentation konnte diese Termingerecht fertiggestellt werden.
Auch die Entwicklung des Prototyps wurde vorangetrieben. So sind die Funktionalitäten für das Optimistic Payment auf beiden Seiten (TSP und OBU) implementiert. Bis zur Demonstration des Prototyps muss neben dem durchführen der Systemtests, noch das Beantworten einer Challenge auf der OBU implementiert werden. Die vorangehend genannten Schritte sind nötig, damit am 13. Februar ein stabiler Prototyp präsentiert werden kann.

6 Risikomanagement

Das nachfolgende Risikomanagement beschäftigt sich mit der Identifikation von möglichen Risiken welche im Verlauf des Projekts eintreten können sowie die entsprechenden Gegenmassnahmen.

Beschreibung	**Initialrisiko** [1]	**Vermeidungs-aufwand** [2]	**Gewichtung** [3]	**Massnahmen**	**Risiko** [1] in M2	**Risiko** [1] in M3	**Risiko** [1] in M4
Abweichungen im Zeitplan	3	1	3	Erst durch eine Analyse die Arbeitspakete festlegen, danach durch Synthese einen realistischen Rahmenplan erstellen. Controlling sauber nachführen.	3	3	2
Missverständnisse im Projektauftrag	1	1	1	Projektauftrag sauber lesen und alle Unklarheiten beseitigen.	1	1	1
Kommunikation zwischen Schichten	3	1	3	Frühzeitig Prototyp erstellen und falls nötig alternative Technologie suchen	1	3	2
Kryptographische Protokolle zu komplex	3	2	1.5	Rechtzeitig Hilfe anfordern bei Unklarheiten	3	2	2
Fehlendes Android Vorwissen	2	2	1	Komplexität der Android Applikation gering halten.	1	1	1
Definierte Aspekte des Systemtests sind nicht durchführbar	1	1	1	Vorausschauende Definition der Testaspekte und Durchführung anhand eines Prototyps.	1	1	1

Tabelle 6: Risikoanalyse: Risiken und geplante Gegenmassnahmen

[1] Risiko (R): 1= Geringes Risiko, 2=Mittleres Risiko, 3= Hohes Risiko
[2] Vermeidungsaufwand (V): 1=Geringer Aufwand, 2=Mittlerer Aufwand, 3=Hoher Aufwand
[3] Diejenige Massnahme, welche das grösste Gewicht erreicht, wird in erster Priorität umgesetzt.
D.h. das Gewicht stellt eine Sortierreihenfolge zur Festlegung der Umsetzungspriorität dar. Berechnung: (G) = (R) / (V)

7 Projektunterstützung

7.1 Konfigurationsmanagement

7.1.1 Versionisierung

Der gesamte Java Programmcode wird in NetBeans 7.0.1 erstellt und mit Hilfe eines Subversion Plug-Ins versionisiert. Somit können Änderungen am Code vollständig nachvollzogen und im Fehlerfall auch rückgängig gemacht werden. Der Subversion Server wird von der HSLU bereitgestellt:
`https://dev.enterpriselab.ch/education/pawi.h11.tagallik.tbmoser`

7.1.2 Configuration Items

- Applikation des OBU Clients: ch.hslu.pawi.obuclient
- Datenbank des OBU Clients: obudb
- User Interface des Toll Service Providers: ch.hslu.pawi.tspclient
- Application Service des Toll Service Providers: ch.hslu.pawi.tspservice
- Datenbank des Toll Service Providers: tspdb
- Gemeinsam genutzte Bibliothek: ch.hslu.pawi.common
- Dokumentation: (siehe Dokumentationsplan)
- Betriebssystem mit Java resp. Android Runtime Environment

7.2 Dokumentationsplan

Das Projektmanagement und die damit verbundene Dokumentationsarbeit wird mit Hilfe des Prozessmodells HTAgil abgewickelt. Alle im Rahmen des Projekts erarbeiteten Dokumente werden von den Autoren manuell versionisiert. Dafür wurde eine Versionisierungstabelle am Anfang jedes Dokuments eingefügt.

Dokument	Kommentar zur Abgabe	Verant-wortung	Autor
PAWI_Projektplan.doc	Gedruckt und als PDF	moc	Alle
PAWI_Report.doc	Gedruckt und als PDF	gat	Alle
PAWI_Testplan.doc	Gedruckt und als PDF	gat	Alle
PAWI_Präsentation.ppt	Präsentieren und als PDF abgeben	moc	Alle

Tabelle 7: Liste der Dokumente, welche im Rahmen des Projekts entstanden sind

8 Arbeitsjournal

Datum	Aktivitäten	Bemerkungen	Aufwand (h)	
			gat	moc
03.01.2012	Initialisierung des Projekts	Projektübersicht erlangen Dokumente vorbereiten, Meilensteinplanung erstellen,	3	3
	Recherche/Studium von sicheren, elektronischen Abrechnungssystemen	Artikel „PrETP: Privacy-Preserving Electronic Toll Pricing" u.a.	4	4
04.01.2012	Bericht Strassenverkehrsabgaben Schweiz			4
	Recherche Cryphtographic Commitments, Zero-Knowledge Proof		2	3
	Konzepte für Informationsaustausch zwischen TPS-OBU	Android Remoting resp. Remote Invocation	5	
	Entwurf der Systemübersicht		2	
05.01.2012	Risikoanalyse erstellt		1	1
	Systemübersicht			1
	Status-Meeting		1	1
	Recherchen über Commitment schemes, Signature schemes, Zero Knowledge Proof		3	3
06.01.2012	Recherche über sichere, elektronische Abrechnungssystemen	Artikel „PrETP: Privacy-Preserving Electronic Toll Pricing" u.a.	5	5
	Challenge und Payment Abläufe visualisieren		2	2
	Diverse Prototypen adoptiert/entwickelt für Android Plattform	GPS Logger und Datenbank Prototyp, Tests mit Android Privacy Guard (Implementation von PGP), TCP Socket Test App	4	2
09.01.2012	Ablauf „Proof Challenge" visualisiert	proof_challenge.vsd		2
	Kurzvortrag „Asymmetrische Kryptographien" erstellt		1	4
	Recherchen über Non-interaktive Zero-Knowledge Proof und Commitment Schemes		2	3
	Crypto Libraries „Qilin" (Harvard) und „Idmix" (IBM) studiert und Funktionsumfang geprüft.		6	
10.01.2012	Kurzvortrag Kryptographie erstellt und präsentiert		5	5
	Aufwandschätzung erstellt		1	1
11.01.2012	Crypto Library „Idmix" (IBM) analysiert			5

	Kundenanforderung erstellt			2
	Artikel über „Integer Commitment Scheme“ und „Signature Scheme“ studiert	Artikel: • „A Statistically-Hiding Integer Commitment Scheme Based on Groups with Hidden Order“ • „A Signature Scheme with Efficient Protocols“		3
12.01.2012	API für eigene Crypto Library entworfen	Klassen und Methoden definiert		3
	Crypto Library „Idmix“ (IBM) analysiert und versucht in der Entworfenen API zu verwenden.			5
13.01.2012	Kryptographie Primitiven dokumentiert			3
	Commitment Library implementiert anhand von „Qilin“ (Harvard)	Problem: Homomorphie funktioniert nicht.		4
15.01.2012	Modellierung der Datenbanken angefangen		2	
16.01.2012	Komponentenübersicht, Risiko neu bewerten		2	
	Datenbank-Modellierung		3	
	GPS Datenlogger Prototyp fertig		2	
	RPC-XMPP Prototyp fertig		2	
	Recherche zu Point-In-Location Problem		2	
	Key Generation von Idmx adaptiert			3
	Commitment Scheme implementiert	Homomorphie funktioniert.		4
	Übersicht über Crypto Library erstellt			1
17.01.2012	Besprechung Kryptographie	Probleme mit hohen Exp. besprochen (modPow als Lösung).	2	2
	Übersicht über Crypto Library überarbeitet			1
	ZeroKnowledgeProof implementiert	Bereits bei der Erstellung der Signatur gab es Problem, da die Methode „pow“ anstelle von „modPow“ verwendet wurde		3
	TSP Service entwickeln	Rudimentäres Gerüst der TSP Applikation	4	
	OBU Applikation entwickeln	Persistenz Framework für Android bereitet grosse Probleme	6	
18.01.2012	Besprechung Kryptographie	Problem mit zu hohen Werten bei Division. Anstelle der Division kann eine Multiplikation mit dem Inversen vorgenommen werden.	1	1

	Key Generation überarbeitet	Bei der Key Generation vom idmix werden diverse Parameter verwendet, welche für unser Projekt nicht verwendet werden.		3
	Signature vom ZeroKnowledgeProof überarbeitet			4
19.01.2012.	OBU Client (Android Applikation) weiterentwickelt		12	
19.01.2012.	SQLite Datenbank Entwicklung auf Android		12	
20.01.2012	Provider Klassen auf Android entwickelt und getestet		10	
	Android: Kommunikation zwischen Activity und Service realisiert		2	
20.01.2012	Fehlersuche im Signaturverfahren	Signatur und Verifikation stimmen nicht überein.	3	
21.01.2012	Fehler im Signaturverfahren bereinigt	Berechnung von d aus e*d mod phi war nicht korrekt. Zudem wurde für e immer der Wert 3 gefunden.	5	
23.01.2012	Projektplanung	Planen der nächsten Schritte	1	1
	Outline für Projekt-Bericht überarbeitet		2	2
	ZeroKnowledgeProof implementiert	Das Signieren funktioniert nun, somit kann die Methode „computeProof“ und „verifyProof“ implementiert werden.		5
	Android Applikation für OBU Client entwickeln		8	
	Dokumentieren PAWI Bericht			3
24.01.2012	UnitTests für SecurityLibrary erstellt			2
	ZeroKnowledgeProof implementiert	Das Verifizieren des Commitments (t_prime_Z) der Signature funktioniert nicht. Die Werte von t_z und t_prime_Z sind jeweils unterschiedlich		6
	Android Applikation für OBU Client entwickeln	Diverse Probleme mit SQLite Datenbank	8	
	XMPP Connector Klasse als Singleton	Refactoring, Code Bereinigung	1	
25.01.2012	TSPClient erstellt			4
	OptimisticPayment Model erstellt für Zugriff auf DB			4
	Zentrale Testumgebung auf EnterpriseLab eingerichtet	MySQL und Openfire Server migriert	2	
	Recherche und Testcode zu Android Preferences und „Properties“ Files		3	
	ArrayListFactory und Serializer für XMPP-RPC		3	

	JUnit Tests für Android implementiert	Netbeans ist offenbar nicht geeignet für Android JUnit Tests	2	
	Dokumentation	OBU Lifecycle als Visio erstellt	1	
26.01.2012	“Autostart on Boot” auf OBU Client implementiert.		1	
	Problemsuche auf Android Applikation	Kommunikationsprobleme sowie NullPointerExceptions bereinigt	5	
	Continous Integration Server aufgesetzt und Projekte eingebunden	Als CI Server wurde TeamCity verwendet	1	
	MultiUserChat und Room Concept implementiert		9	
	TSPClient and TSPService angebunden			4
	Datentransfer Objekte für den Datenaustausch „OptimisticPayment“ erstellt			2
	Security Library in TSPService integriert			4
27.01.2012	Security Library in TSPService integriert			8
	Security Library um HashScheme erweitert	Damit eine Hash eines beliebigen Objektes generiert werden kann.		2
	OBU Parameter (TSP Public Key, Group Parameters) Persistent speichern			4
28.01.2012	Testplan erstellt		1	
	Probleme mit XMPP ChatRoom behoben		3	
	Dokumentation Design-Entscheide	Lokalisierungsfunktionen, Preisberechnung, Map-Segmentierung	5	
	UseCase „Beweis prüfen“ auf TSP implementiert			4
29.01.2012	Projektdokumente überarbeitet		2	2
30.01.2012	Weiterentwicklung OBU Datenbank, Tabellen paymentrecord<->gpspoint		6	
	Probleme mit SQLite Primary Keys		3	
	UseCase “Beweis prüfen” auf TSP implementiert			8
31.01.2012	Kommunikationsprobleme zwischen TSP Service und TSP Client	Als Folge der Problemlösung wurde ein XMPP-RPC Diagramm erstellt, welches die Aufrufe visualisiert.	4	
	Android GUI (auf OBU Client) für Status Informationen erstellt		4	
	Testfälle für OptimisticPayment und VerifyChallenges implementiert			8

	Dokumentieren PAWI Bericht: Einleitung überarbeitet			3
	HashScheme angepasst	Im HashScheme wurde die Methode „serialize“ verwendet, dies hatte zur Folge, dass für gleiche Objekte unterschiedliche Output-Werte erhalten wurden. Deshalb muss im neuen HashScheme ein String vom Objekt übergeben werden.		3
01.02.2012	Systemtests Optimistic Payment		8	10
	Dokumentieren PAWI Bericht		2	
02.02.2012	Dokumentieren PAWI Bericht	Kryptographische Grundlagen, Abläufe & Prozesse, Klassendiagramme	9	9
	Problemlösung CL-RSA Signaturverfahren	Werte für t_z konnten nicht verifiziert werden	1	2
03.02.2012	Dokumentieren PAWI Bericht	u.a. Diskussion, Design-Entscheide	8	7
	Problemlösung CL-RSA Signaturverfahren	Wert für t_z kann nun korrekt verifiziert werden. Das Erstellen der Signatur musste angepasst werden.		2
	Weiterentwicklung OBU Client	Challenge-Response Verfahren	2	
04.02.2012	Dokumentieren PAWI Bericht	u.a. Design-Entscheide, Abstract	5	8
05.02.2012	Dokumentieren PAWI Bericht		0	8
06.02.2012	Dokumentieren PAWI Bericht	u.a. Diskussion, Testplan ergänzen	8	8
	Weiterentwicklung + Systemtests		2	
07.02.2012	Dokumentieren PAWI Bericht		8	8
	Weiterentwicklung + Systemtests	Demonstration vorbereiten	2	2
08.02.2012	Dokumentieren PAWI Bericht	Querlesen, Rechtschreibprüfung, logische Abläufe prüfen	2	2
	Projektpräsentation vorbereiten		3	3
	Abgabe vorbereiten	Druck + CD	3	3
			255.0h	**242.0h**

9 Projektabschluss

9.1 Persönliches Fazit von Christoph Moser

Zu Beginn des Projektes dachte ich, dass wir für das Umsetzen des Prototyps, sowie das Erstellen der Dokumentation genügend Zeit eingeplant hatten. Wie üblich traten auch bei diesem Projekt in der Realisierung unvorhergesehene Schwierigkeiten auf. Dies war sicherlich der Hauptgrund weshalb nicht alle Funktionalitäten implementiert werden konnten, welche wir ursprünglich für den Prototyp geplant hatten.

Eine Herausforderung welche wir meistern mussten, war die Kommunikation zwischen dem Android Mobile Phone und dem TSP (Server). Für die Kommunikation haben wir uns für den Einsatz des XMPP Protokolls entschieden. Da XMPP die Anforderung für unser System am besten erfüllt hat und wir innerhalb von kurzer Zeit bereits erste Daten über XMPP übertragen konnten. Allerdings hat sich dieser Entscheid während der Testphase als Nachteil herausgestellt, da wir oft Problem mit der Übertragung hatten und so viel Zeit in die Anpassung der Kommunikation investieren mussten. Diese Zeit fehlte uns am Ende bei der Implementation des Optimistic Payments.

Die Implementation der kryptographischen Primitiven war eine weitere Herausforderung. Wir kannten zwar zu Beginn einige Grundlagen der Security, wie beispielsweise RSA Verschlüsselung. Aber Homomorphe Commitments, sowie das Zero-Knowledge Proof Verfahren waren Neuland. Es war interessant zu sehen, für was diese Protokolle verwendet werden können und wie die Implementation aufgebaut ist.

Obwohl ich erwartet am Ende des Projekts einen Prototyp mit mehr Funktionalität zu haben, ziehe ich ein positives Fazit. Es war ein sehr lehrreiches und interessantes Projekt und ich konnte vor allem durch den Einsatz von Kryptographischen Primitiven viel neues Lernen.

9.2 Persönliches Fazit von Thomas Galliker

Das Projekt hat bereits auf der Ausschreibung einen interessanten Eindruck gemacht. Dass ich derart gefordert werden würde, hätte ich zu diesem Zeitpunkt allerdings nicht gedacht. Es gab vor allem zwei Punkte, die einem das Leben erschwerten: Einerseits waren die eingesetzten kryptographischen Primitiven zu Beginn nur vom Schulbuchlesen (z.B. RSA, Verschlüsselung, Signaturen, Message Digest, Challenge-Response) oder gar nicht bekannt (z.B. Commitments, Zero-Knowledge Proofs). Hinzu kam die knappe Zeit, welche es auf einen riesen Haufen Arbeit aufzuteilen galt.

Ich denke, wir haben in der zur Verfügung stehenden Zeit das bestmögliche herausgeholt. Die Teamarbeit klappte hervorragend. So teilten wir uns die Aufgaben ideal auf, sodass wir uns während der Entwicklungsphase nur für Diskussionen um gemeinsam genutzte Datentypen und Schnittstellen unterbrechen mussten. Der Erfolg dieser Zusammenarbeit zeigte sich kurz vor Meilenstein 4, als wir die Crypto Library erfolgreich in TSP Service und OBU Client integrieren konnten.

Als persönliche Top-Leistung würde ich die Integration von XMPP zwischen Android und einer Java Service Applikation sowie die erfolgreiche Problemsuche beim CL-RSA Signaturverfahren bezeichnen. Ohne Unterstützung unseres Experten, Dr. M. Pouly, wären wir aber ganz bestimmt nicht ans Ziel gekommen.