UNIVERSITÄT
KOBLENZ · LANDAU
Fachbereich 4: Informatik

Google-Online-Kalender: Datenschutzproblematik und Lösung

Bachelorarbeit

zur Erlangung des Grades eines Bachelor of Science
im Studiengang Informatik

vorgelegt von

Toni Rossberg

Erstgutachter:	Prof. Dr. Rüdiger Grimm Institut für Wirtschafts- und Verwaltungsinformatik
Zweitgutachter:	Dipl.-Inform. Daniel Pähler Institut für Wirtschafts- und Verwaltungsinformatik

Koblenz, im April 2012

Erklärung

Ich versichere, dass ich die vorliegende Arbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe.

	Ja	Nein
Mit der Einstellung der Arbeit in die Bibliothek bin ich einverstanden.	☐	☐
Der Veröffentlichung dieser Arbeit im Internet stimme ich zu.	☐	☐

. . . . . .

(Ort, Datum) (Unterschrift)

Diese Arbeit setzt sich kritisch mit dem Google Kalender auseinander. Zu diesem Zweck werden die angebotenen Funktionen des Kernprodukts auf Aspekte des Datenschutzes untersucht. Es wird zum einen ermittelt, in welchem Umfang das Produkt die Privatsphäre der Nutzer verletzen kann, zum anderen werden die dadurch entstehenden Risiken aufgezeigt. Des Weiteren werden die Funktionen im Hinblick auf ihren Nutzen, sowohl für den Dienstanbieter Google, als auch für den Nutzer betrachtet. Eine eingehende Analyse zeigt die kritischen Stellen auf, an denen zwischen Datenschutz und Funktionalität entschieden werden muss. Die Lösungsmöglichkeiten, um die aufgezeigten Risiken mit Mechanismen der IT-Sicherheit zu minimieren, werden im Folgenden vorgestellt, diskutiert und in Bezug auf ihre Umsetzbarkeit untersucht. Die einzelnen Lösungsansätze werden daraufhin in einem Sicherheitskonzept zusammengefasst und weitere Anforderungen erläutert. Abschließend soll ein Addon für Firefox erstellt werden, welches das beschriebene Lösungskonzept umsetzt, um so die bestehenden Schwachstellen bestmöglich zu beheben. Letztlich wird der Funktionsumfang des Addons mit technischer Umsetzung im Einzelnen erläutert.

Schlüsselwörter - Google, Kalender, Firefox, Addon

This paper critically examines the Google Calendar. For this purpose, the offered functions of the core product are studied on privacy aspects. On one hand, it is identified, to which extent the product could infringe the users' privacy, on the other accuring risks are discussed. Furthermore, the functions in terms of their use for both, the service provider Google and for the user, are considered. A detailed analysis demonstrates the critical aspects, in which we have to decide between privacy and functionality. The identified solutions to minimize discussed risks of IT security mechanisms, are presented, discussed and analyzed in terms of their feasibility. Afterwards the individual solutions are summarized in a security concept and other requirements are explained. Finally, a Firefox-Addon which implements the described solution concept should be created, to resolve the existing weaknesses to the best of its ability. Ultimately, the functionality of the addon with technical implementation is illustrated in detail.

Keywords - Google, calendar, Firefox addon

Inhaltsverzeichnis

Abbildungsverzeichnis

Codeverzeichnis

Kapitel 1

Einleitung

Dieser Abschnitt liefert eine Einleitung in den thematischen Schwerpunkt der Arbeit. Im Teil der Motivation wird die Bedeutung vom Wissens über Nutzer für Konzerne, die im Internet agieren, dargelegt. Im einführenden Teil werden Veränderungen durch das Web 2.0 beschrieben und die Bedeutung von Spuren im Internet aufgezeigt. Eine Betrachtung der jüngsten Ereignisse bezüglich der überarbeiteten Datenschutzerklärung von Google Inc. verdeutlicht, welche Bemühungen im Bereich des Datenschutzes vom Unternehmen in Zukunft zu erwarten sind. Aus den gewonnen Erkenntnissen ergibt sich die Notwendigkeit dieser Arbeit.

1.1 Motivation

Der Ausdruck „Wissen ist Macht“ geht auf den englischen Philosophen Francis Bacon zurück. Der im Jahr 1597 entwickelte Grundgedanke wurde in Bacons 1620 erschienenen Hauptwerk *Novum Organum* weitergeführt. Bacon schreibt in Satz drei sinngemäß: „Wissen und Macht des Menschen fallen zusammen, weil Unkenntnis der Ursache die Wirkung verfehlen lässt“ [Bac20].

Demnach erkannte Bacon, dass das Wissen über die Dinge den Zusammenhang von Ursache und Wirkung offen legt. In der heutigen Zeit hat das Wissen über Zusammenhänge einen ökonomischen Wert. So schreibt Stefan Schultz über Facebook, das soziale Netzwerk, welches bekanntlicherweise viel über seine Nutzer weiß, dass Insider das Unternehmen mit 100 Milliarden Dollar bewerten. Weiterhin merkt er an: „Das soziale Netzwerk wäre damit schlagartig höher bewertet

als Deutsche Bank, Deutsche Post und Lufthansa zusammen“ [Sch11]. Da Facebook Inc. lediglich eine Dienstleistung anbietet, begründet sich dieser Wert neben dem minimalen Anteil für gebundenes Kapital in Form von Hardware vermutlich ausschließlich auf dem Wissen des Unternehmens über seine 845 Millionen aktiven[1] Nutzer [FP12]. Auch Google Inc. weiß viel über die Nutzer der vom Unternehmen angebotenen Dienste. In den Medien steht der US-Konzern insbesondere aufgrund des mangelndes Datenschutzes und der allgemeinen Sammelleidenschaft des Unternehmens häufig unter Kritik.

Im Gegensatz zu den Diensten von Facebook, in denen die Nutzer größtenteils bewusst Daten angeben und veröffentlichen, erhält Google Inc. durch Dienste wie *Google Analytics* die meisten Daten implizit. Der Nutzer gibt seine Daten demnach nicht bewusst explizit an, sondern wird unbewusst ausgespäht, wobei die Daten gespeichert und ausgewertet werden. Prof. Björn Bloching, Strategieberater bei Roland Berger sagte gegenüber der Tagesschau am 01.03.2012: „Sie wissen was uns interessiert, was wir kaufen, welche Werbung wir uns anschauen. Sie wissen über die Android Betriebssysteme auch, wie wir uns bewegen in der Welt - über die Smartphones. Sie wissen welche Videos wir mögen, welche Reiseziele uns interessieren. Alles das weiß Google und das werden sie kapitalisieren.“

Bedenklich ist dieses Wissen in den Händen eines ausländischen Unternehmens allemal, da hohe deutsche Standards aus dem Datenschutz nicht gelten. Besonders kritisch wird es dann, wenn nationale Gesetzgebungen den Dienstanbieter dazu zwingen Daten offen zu legen oder bewusst zu verfälschen. So zensierte Google Inc. bis ins erste Quartal 2010 auf Wunsch der chinesischen Regierung die Suchergebnisse von *google.cn*, sodass keine heiklen Inhalte beispielsweise zu den Themen Tibet oder Taiwan gefunden werden konnten [Age10]. Das letztlich ein solches Monopol wie Google Inc. die Wissensaufnahme der Nutzer und das daraus entstehende Weltbild formen oder das Kaufverhalten manipulieren kann, ist in hohem Maße kritisch.

In dieser Arbeit soll einer der Dienste der Google-Produktpalette mit geeigneten Maßnahmen gesichert werden, sodass möglichst wenige Informationen an den Dienstanbieter übertragen werden müssen. Dieser Beitrag zur Verminderung des Wissens eines Unternehmens über seine Nutzer soll somit den aufgezeigten Gefahren entgegenwirken.

[1] Nutzer, die sich binnen 30 Tage mindestens einmal einloggen

1.2 Einführung

In den letzten Jahren hat sich die Nutzung des Internets gravierend verändert. Durch Entwicklungen im Bereich des Web 2.0 war es möglich, den Nutzern nicht nur Informationen anzubieten, sondern diese aktiv an den Prozessen auf den unterschiedlichen Plattformen teilhaben zu lassen. Heute gehören Aktivitäten in sozialen Netzwerken, Blogs sowie Cloudcomputing-Diensten zum Alltag vieler Internetnutzer. Bei der Verwendung fallen dabei eine Vielzahl von Informationen an.

Internetnutzer hinterlassen überall ihre Spuren. Wird beispielsweise bei Amazon nach einem Artikel recherchiert, versucht das System aus den vorhandenen Informationen weitere Kaufempfehlungen zu generieren. Solche Recommender Systeme sind dabei umso effektiver, je mehr Daten über einen Nutzer vorliegen. Da verwundert es nicht, dass Dienste versuchen, möglichst viele personenbezogene Daten ihrer Nutzer zu erfassen. Mittels Bindung an ein Benutzerkonto, die Verwendung von Cookies oder den Einbau von Pixel-Tags können implizite Sitzungsinformationen zusätzlich mit einem Pseudonym oder sogar mit natürlichen Personen in Verbindung gebracht werden. Durch Technologien des Web 2.0 können Nutzer weiterhin diverse weitere Inhalte wie Bilder, Textnachrichten oder Interessengebiete explizit angeben, wodurch solche Nutzerprofile weiter verfeinert werden können. Diese weitreichenden explizit und implizit erhobenen Daten bilden bei vermehrter Nutzung eines Dienstes ein klares Bild über die Nutzer und somit je nach Dienst ihre Interessengebiete, Freunde oder beispielsweise beliebte Reiseziele.

Insbesondere im Bereich der Werbung hat solches Kundenwissen einen konkreten Wert. Es liegt daher die Vermutung nahe, dass auch eine der erfolgreichsten Firmen im Onlinegeschäft versucht, ihr Wissen über den Nutzer zu erhöhen. Dass Google Inc. Bemühungen in diesem Themenbereich anstellt, zeigen diverse Patente des Konzerns. Beispielhaft seien hier die Patente „determining advertising using user behavior information such as past navigation information“[2] oder „systems and methods for modifying search results based on the users history“[3] genannt.

Aber auch für den Kunden ergeben sich Vorteile durch die Preisgabe ihrer Daten. So können entsprechend bessere Suchergebnisse oder Werbung präsen-

[2]US-Patentnummer: 20060069616
[3]US-Patentnummer: 20060224587

tiert werden, die den Kunden auch interessieren. Es wird jedoch oft nicht berücksichtigt, ob ein Kunde eine solche Personalisierung eines Dienstes überhaupt wünscht. Da bei den unterschiedlichen Dienstanbietern dazu selten Informationen und meist nur versteckte Regulierungsmöglichkeiten zu finden sind, stellt sich die Frage, wem die Bildung von Nutzerprofilen mehr Vorteile bringt, dem Nutzer oder dem Anbieter.

Im Grunde handelt es sich um die Frage nach einem Identitätsmanagement, welches dem Nutzer gestattet, wie im Recht für informationelle Selbstbestimmung ausgeführt, selbst über die Preisgabe und Verwendung seiner Daten entscheiden zu können. Die Einwilligung zur Erhebung und Nutzung der entsprechenden Daten gibt der Nutzer meist schon bei der Bestätigung der Datenschutzerklärung des Dienstes. Dies bedeutet nicht, dass die Dienste zwingend sehr freizügig mit den Daten der Nutzer umgehen - viele Dienste wie Facebook oder Google+ geben dem Nutzer sehr feingranulare Möglichkeiten die Daten vor den Augen anderer zu schützen, jedoch wird an dieser Stelle von vielen Nutzern ignoriert oder nicht bemerkt, dass der Dienstanbieter selbst nicht reguliert werden kann. Es gibt Dienste, die personenbezogene Daten wie die Adresse des Nutzers zum Beispiel für die Lieferung von Produkten eindeutig benötigen. Müssen die unterschiedliche Dienstabieter aber tatsächlich wissen, welche weiteren Personen auf Urlaubsbildern zu sehen sind oder sollte diese Information nicht eigentlich nur mit Familienmitgliedern geteilt werden?

Diese Arbeit betrachtet genau die Daten, die vom Nutzer an das System übergeben werden, ohne dass das System diese Daten zur Erfüllung des (Haupt-) Dienstes überhaupt benötigt. Da diese Systeme, wie bereits im Vorfeld beschrieben, keine Regulierungsmöglichkeiten anbieten - der Systemdatenschutz[4] an dieser Stelle also versagt - gilt es Wege zu finden, diesen Datenschutz mithilfe von Maßnahmen des Selbstdatenschutzes[5] zu gewährleisten. In den folgenden Ausführungen steht der Kalender-Dienst von Google Inc. im Fokus. Der Dienst soll zunächst untersucht und der genaue Funktionsumfang bestimmt werden. Die

[4] „Systemimmanente technische und organisatorische Vorkehrungen, die für den Schutz des Rechts für informationelle Selbstbestimmung förderlich/rechtlich geboten sind“[Gri03]

[5] „Datenschutzmaßnahmen, für Nutzer einzeln oder in Gruppen, ohne dabei von Systemangeboten unterstützt zu werden“[Gri03]

dort explizit angegeben Datengruppen werden betrachtet und im Hinblick auf ihre Sensibilität klar erläutert. Eine eingehende Analyse soll danach aufzeigen, welche Daten schutzwürdig sind und wie ein entsprechender Schutz realisiert werden kann. Dazu sollen etablierte IT-Sicherheitsmaßnahmen herangezogen werden. Letztlich soll das Produkt mithilfe von Maßnahmen des Selbstdatenschutzes gesichert werden, sodass der Dienst ohne Bedenken im Hinblick auf die Preisgabe personenbezogener Daten genutzt werden kann.

1.3 Aktueller Bezug

Dieser kurze Exkurs soll verdeutlichen, welche aktuellen Tendenzen bei Google Inc. im Bereich des Datenschutzes festzustellen sind.

Seit dem 01.03.2012 gilt die überarbeitete Datenschutzerklärung von Google Inc. Die zuvor bestehenden circa 60 verschiedenen Datenschutzerklärungen der unterschiedlichen Google-Dienste wurden dabei vereinfacht und zusammengefasst. Lediglich die Dienste Chrome, Chrome OS, Wallet und Books haben auch weiterhin abweichende Erklärungen. Die zusammengefasste Datenschutzerklärung steht bereits seit Ihrer Bekanntgabe unter Kritik. Im Rahmen dieser Arbeit wurde die neue Datenschutzerklärung ebenfalls betrachtet [Goo12].

Einer der in den Medien genannten Kritikpunkte ist die nun nur noch einmalige Bestätigung durch den Nutzer. Es kann somit nicht mehr separat entschieden werden, welchem Dienst die unterschiedlichen Rechte eingeräumt werden und welchem Dienst diese Rechte untersagt werden. Bernd Behr, Redakteur von heise online schreibt dazu sinngemäß: „Die Möglichkeit, der Zusammenfassung der Daten zu widersprechen, sei von einem Weltunternehmen zu erwarten. Wahlfreiheit für Nutzer sehe anders aus, als nur zustimmen zu können oder eben andere Dienste zu verwenden.“ [Beh12]. Dies zwingt den Nutzer, bei der Verwendung eines Dienstes automatisch der gesamten Erklärung für alle betreffenden Dienste zuzustimmen.

In der Datenschutzerklärung fällt besonders die Wortwahl auf. Oft werden Phrasen wie *möglicherweise*, *gegebenenfalls* oder *unter Umständen* verwendet. Insbesondere bei Erläuterungen zu weitreichenden Eingriffen in die Privatsphäre kommen diese Ausdrücke häufig vor. Die Verbraucherzentrale Bundesverband (VZBV) hat den US-Konzern aufgrund dieser zu unbestimmten Formulierungen bereits Ende März 2012 abgemahnt. Die Datenschutzerklärung erfüllt nach

Meinung der Verbraucherschützer die Voraussetzungen für eine rechtskonforme Datenschutzerklärung nicht [Age12]. VZBV-Chef Gerd Billen sagte zudem: „Der Verbraucher weiß am Ende nicht, wozu genau er seine Zustimmung erteilt und wozu nicht."

Zudem schreibt Google Inc. in der Datenschutzerklärung: „Wir erfassen möglicherweise Informationen über die von Ihnen genutzten Dienste und die Art und Weise, wie Sie diese nutzen, beispielsweise wenn Sie eine Website besuchen, auf der unsere Werbedienste verwendet werden oder wenn Sie unsere Werbung und unsere Inhalte ansehen und damit interagieren.". Demnach werden Daten vom Dienstanbieter nicht nur bei der direkten Nutzung der Dienste erhoben, sondern auch wenn Seiten besucht werden, auf denen eine *Google+* Schaltfläche[6] oder *Google Analytics* eingebunden ist.

Weiterhin wird vermerkt: „Unsere Datenschutzerklärung gilt für alle Dienste, die von Google Inc. und den verbundenen Unternehmen angeboten werden, einschließlich Dienste, die auf anderen Webseiten angeboten werden (wie beispielsweise unsere Werbedienste)." Bundesverbraucherministerin Ilse Aigner kritisierte Google gegenüber der Deutschen Presse-Agentur scharf: „Mit der Zusammenlegung der Daten hat das Unternehmen eine Kehrtwende vollzogen und alle Bedenken europäischer und US-amerikanischer Datenschützer ignoriert". Mit einer Zustimmung der Nutzer kann das Unternehmen die Daten aller Dienste verbinden und Nutzerprofile erstellen, welche womöglich mehr Informationen enthalten, als den unterschiedlichen Geheimdiensten zur Verfügung stehen. Die Bestrebungen des Unternehmens, im Konflikt zwischen Wissen über den Nutzer und Einhaltung des Datenschutzes, haben daher eine im Bezug auf die personenbezogenen Daten der Nutzer negative Tendenz. Daher ist es umso wichtiger, dass den Nutzern Werkzeuge angeboten werden, mit deren Hilfe sie die Preisgabe ihrer Daten regulieren können.

[6] zur Interessenbekundung im gleichnamigen sozialen Netzwerk des Unternehmens, vergleichbar mit den Facebook *Gefällt mir* Schaltflächen

Kapitel 2

Google Kalender

In diesem Kapitel wird der Kalender-Dienst von Google Inc. vorgestellt und analysiert. Zunächst wird das Produkt, seine Geschichte sowie dessen Funktionsumfang beschrieben. Daraufhin wird strukturiert aufgezeigt, welche personenbezogenen Daten der Dienstanbieter vom Nutzer erlangt. Eine Analyse weiterführender Dienste macht deutlich, welche Abhängigkeiten einzelner angegebener Daten zu diesen Diensten bestehen. Weiterhin wird die Datenschutzrelevanz der einzelnen angegebenen Daten untersucht. Darauf aufbauend werden Datengruppen definiert und anhand von Beispielszenarien Datenschutzproblematiken aufgezeigt.

2.1 Produkt

In diesem Abschnitt wird der Google-Dienst genauer analysiert. Zunächst wird mithilfe einer Kurzbeschreibung die Geschichte und der Nutzen dieses Dienstes dargelegt. Die einzelnen Funktionen werden daraufhin im Detail erläutert und die Verwendungsmöglichkeiten dargestellt.

2.1.1 Kurzbeschreibung

Der *Google Kalender* ist ein online-basierter Dienst zur Verwaltung von Terminen. Vorgestellt wurde dieser erstmals am 13. April 2006 [ho06] und befand sich bis Juli 2009 im öffentlichen Beta-Test [Sch06, Her09].

Google bietet den Dienst sowohl für Unternehmen, als auch für Privatpersonen an. Dabei zahlen Unternehmen für das Paket *Google Apps for Business*, in dem neben dem *Google Kalender* eine Vielzahl weiterer Google-Dienste gebündelt sind, 40 Euro pro Nutzer und Jahr. Privatpersonen wird der Dienst kostenlos angeboten. Will ein Nutzer auf den Kalender zugreifen, meldet sich dieser bei Google an und erhält vollen Zugriff auf *Google Mail*, den *Google Kalender* und diverse andere Dienste wie *Google docs*.

Ein Nutzer kann den Kalender über einen beliebigen Browser aufrufen. Es handelt sich bei dem Google-Dienst um eine auf Ajax[1] aufbauende Webanwendung, die plattform- und browserunabhängig lauffähig ist. Die entsprechenden Systeme müssen lediglich das Zusammenspiel zwischen JavaScript, Dokument-Objekt-Modell (DOM) und XML unterstützen [ho06]. Zugriff erhält ein beim Dienst angemeldeter Nutzer durch Auswählen des Kalender-Reiters. Beim ersten Start müssen zudem einige Einstellungen zur Zeitzone und zur Sichtbarkeit des Kalenders getätigt werden.

2.1.2 Funktionen

Der *Google Kalender* bietet eine Vielzahl von Funktionen zur persönlichen Terminverwaltung, die im folgenden Abschnitt erläutert werden. Dabei wurden Anregungen und Beispiele aus [Min06] übernommen. Die Funktionen werden im Folgenden innerhalb der Rubriken Basis-Funktionen, Community-Funktionen und Zusatz-Funktionen betrachtet. Mit dem *Google Kalender* können neben der einfachen Kalenderfunktion auch komplexere Aufgaben wie die Verwaltung von Dienstplänen für eine überschaubare Anzahl von Mitarbeitern realisiert werden.

2.1.2.1 Basis-Funktionen

In diesem Abschnitt werden die üblichen Funktionen von Terminverwaltungsprogrammen beleuchtet. Dazu zählen die optische Aufbereitung des Terminkalenders, die Erstellung neuer Termine sowie die Wiederholbarkeit eines Termins.

Das Layout des *Google Kalenders* unterscheidet sich kaum von anderen Terminverwaltungsprogrammen. Der Nutzer erhält, wie in Abbildung 2.1 links erkennbar, eine klassische Monatsübersicht zur Navigation sowie eine detaillierte Ansicht für Termine im Hauptteil. Diese kann je nach Wunsch auf einen Tag, ei-

[1] Asynchronous JavaScript and XML - ein Konzept um asynchron Daten zwischen Browser und Server auszutauschen

ne Woche oder eine einstellbare Anzahl von Tagen eingestellt werden. Weiterhin wird der aktuelle Tag sowie die aktuelle Uhrzeit hervorgehoben. Zusätzlich ist auch eine *Terminübersicht* darstellbar, die in Listenform Termine des Kalenders darstellt. Eine weitere Ansicht stellt alle Tage eines Monats im quadratischen Raster dar. Der Kalender kann zudem nach diversen Informationen durchsucht werden, um einen Termin ausfindig zu machen.

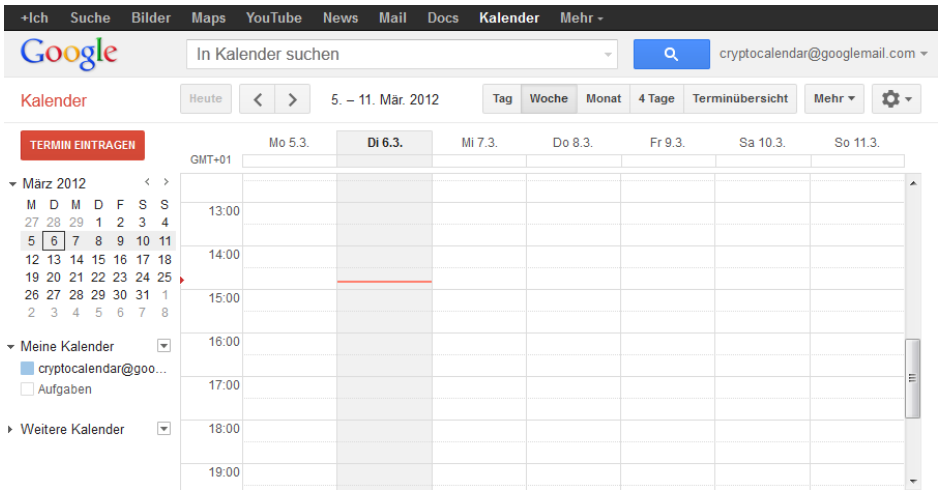

Abbildung 2.1: Layout des Google Kalenders

Neue Termine können über die Schaltfläche *Termin eintragen* oder über die dynamische Erstellung innerhalb der aktuellen Kalenderansicht im Hauptteil erzeugt werden. Dabei wird ein bestimmter Zeitpunkt ausgewählt und durch Ziehen der Maus bei gedrückter linker Taste ein Termin beliebiger Dauer erstellt. Ein Termin besteht im einfachsten Fall aus einem Titel, einem Startzeitpunkt und seiner Dauer. Die beiden Varianten werden in den Abbildung 2.2 dargestellt.

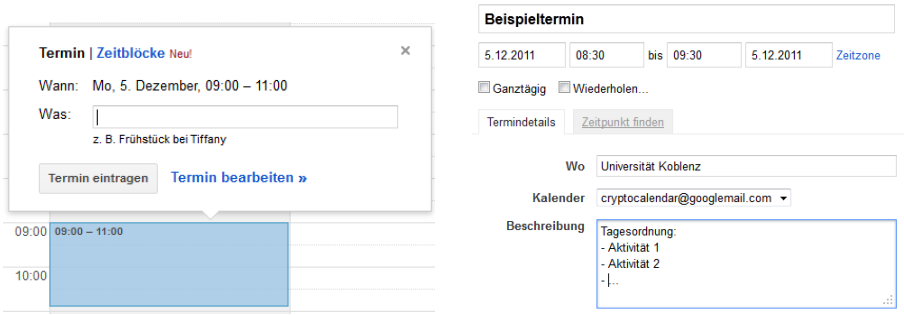

Abbildung 2.2: Dynamische und statische Terminerzeugung

Sollen zusätzlich Termineinzelheiten festgelegt werden, können im detaillierten Dialog eine Ortsangabe sowie eine weiterführende Beschreibung hinzugefügt werden. Termine können ganztägig stattfinden und sich wiederholen. Ist ein Termin als ganztägig eingetragen, so erscheint dieser direkt unter dem Datum innerhalb der jeweiligen Ansicht.

Abbildung 2.3: Termin-Wiederholung

Bei der Terminwiederholung kann, wie in Abbildung 2.3 zu sehen, eingestellt werden, in welchem Zyklus und an welchen Tagen sich der Termin wiederholen soll. Zudem ist optional ein Ende nach einer bestimmten Anzahl von Wiederholungen oder an einem bestimmten Datum definierbar. Eine nachträgliche Bearbeitung oder zeitliche Anpassung der Termine ist ebenfalls möglich.

2.1.2.2 Community-Funktionen

Terminkalender sind insbesondere für Personen wichtig, die beruflich oder privat mit vielen Menschen interagieren. Diese Personen müssen innerhalb ihrer Zeitplanung andere Personen berücksichtigen. Für einen zeitgemäßen Terminverwaltungsdienst ist es somit unabkömmlich, diese Interaktionen abzubilden und möglichst sinnvoll zu integrieren. Dieser Abschnitt stellt die Community-Funktionen des *Google-Kalenders* vor. Dazu zählen das Einladen von Gästen sowie deren Reaktionen, die Freigabe des Kalenders und die Möglichkeiten von Terminvorschlägen.

Zunächst wird die Funktionalität zum Einladen von Gästen betrachtet. Auf diese Weise wird ein Termin mit anderen geteilt. So kann beispielsweise ein Termin für einen gesellschaftlichen Anlass erzeugt werden, zu dem beliebig viele weitere Nutzer eingeladen werden. Dazu werden lediglich die Mail-Adressen aller Gäste benötigt. Bei Nutzern, die über eine Google Mail-Adresse verfügen und ebenfalls den Kalender eingerichtet haben, werden diese Termine direkt in den entsprechenden Kalender eingetragen. Sonstige Nutzer können mit einer Nach-

richt auf ihre Einladung aufmerksam gemacht werden. Der Dienst generiert daraufhin Mails, in denen die Empfänger eingeladen und über die Termineinzelheiten aufgeklärt werden.

Gäste, die über keinen Google-Kalender verfügen, werden im entsprechenden Dialog mit einem Stern markiert. Dies zeigt nebenstehende Abbildung 2.4. Weiterhin können Gäste bestimmte Berechtigungen erhalten. Ein Gast kann zusätzlich als optional markiert werden, wenn beispielsweise dargestellt werden soll, dass dieser dem Termin nicht zwingend beiwohnen muss, damit der Termin stattfindet. Unter allen Teilnehmern kann der Google-Dienst einen geeigneten Zeitpunkt finden. Dazu werden die Kalender der Gäste, die ebenfalls den *Google Kalender* nutzen, analysiert und Vorschläge generiert.

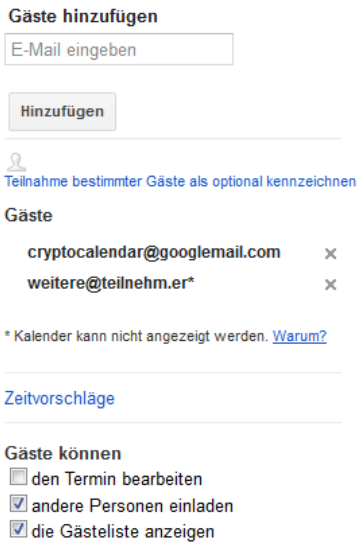

Abbildung 2.4: Einladen

In den Kalendern der Gäste können geteilte Termine abgelehnt, bestätigt oder als unentschlossen markiert werden. Zusätzlich können Kommentare verfasst werden, die Zusatzinformationen für den Initianten enthalten.

Wie in Abbildung 2.5 dargestellt, kann der Einladende die Entscheidungen und Kommentare innerhalb der Terminbearbeitung einsehen. Sowohl die Bestätigung als auch die Zusatzinformationen in Form von Kommentaren werden an dieser Stelle angezeigt. Weitere Gäste können nachträglich hinzugefügt oder entfernt werden. Zudem besteht die Möglichkeit, alle Gäste per Mail zu kontaktieren.

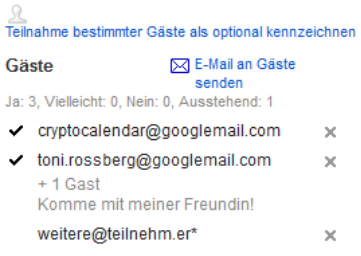

Abbildung 2.5: Übersicht

Eine weitere Funktion ist das Erstellen mehrerer Teilkalender. Somit ist beispielsweise die Trennung von beruflichen und privaten Terminen leicht umsetzbar. Optisch können die Teilkalender farblich angepasst werden. Zusätzlich können einzelne Teilkalender ausgeblendet werden, um die Übersichtlichkeit des gesamten Kalenders zu erhöhen.

Weiterhin ist die Sichtbarkeit eines Kalenders einstellbar. Der gesamte, aber auch jeder Teilkalender, kann demnach öffentlich verfügbar gemacht werden. Solche öffentlichen Kalender können von anderen Dienst-Nutzern abonniert werden und werden bei diesen als zusätzlicher Teilkalender angezeigt. Google bietet beispielsweise für diverse Sportarten einen öffentlichen Kalender an. Die Einstellung über die Sichtbarkeit kann ebenfalls für jeden Termin separat eingestellt werden.

Bei der Veröffentlichung eines Kalenders ist es allerdings nicht zwingend notwendig, alle Details zu einem Termin preis zu geben. Eine Person, die Ihren Kalender freigibt, kann entscheiden, ob lediglich offen gelegt werden soll, ob sie zu einem bestimmten Zeitpunkt verfügbar ist oder nicht. Bei einer Terminerstellung kann jeweils festgelegt werden, ob dieser Status auf *Beschäftigt* geändert werden soll. Diese Einstellungsmöglichkeiten werden im Dialog in Abbildung 2.6 dargestellt. Versuchen beispielsweise mehrere sehr beschäftigte Nutzer einen gemeinsamen Termin zu vereinbaren, kann Google die Informationen über die Verfügbarkeit der einzelnen Teilnehmer dazu nutzen, selbstständig einen geeigneten Zeitpunkt zu finden.

2.1.2.3 Zusatz-Funktionen

Der *Google Kalender* bietet zahlreiche Zusatzfunktionen an, die hier vorgestellt werden sollen. Dazu zählen die Erinnerungsfunktion, die Möglichkeit zur Synchronisierung mit anderen Produkten sowie der Export der Kalenderdaten oder die Kopplung mit weiteren Google-Diensten wie *Google maps*.

Eine weitere Funktionalität des *Google Kalenders* ist die Erinnerungsfunktion. Abbildung 2.6 zeigt, dass zu einem einstellbaren Zeitpunkt ein Popup erscheint und eine Mail verschickt werden soll. Konfiguriert der Dienst-Nutzer zusätzlich ein Mobiltelefon, benachrichtigt Google den Nutzer optional auch per SMS.

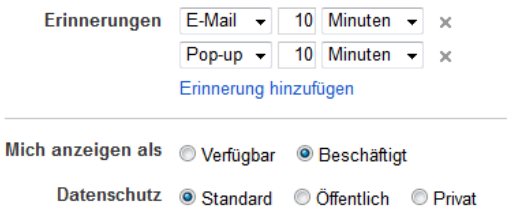

Abbildung 2.6: Detaileinstellungen

Da viele Nutzer bereits andere Terminverwaltungsprogramme wie *Microsoft Outlook* sowie mobile Lösungen auf den unterschiedlichen Smartphone-Plattformen nutzen, bietet Google zudem den Dienst *Google sync* an [Goo11b]. Dieser ermöglicht es, die Kalender der unterschiedlichen Plattformen mit dem *Google Kalender* zu synchronisieren. Dies erleichtert einerseits den zusätzlichen Einsatz des *Google Kalenders* auch bei Nutzung anderer Programme zur Terminverwaltung. Anderseits ermöglicht dies vor allem aber den bequemen Umstieg auf den Google-Dienst. Weiterhin kann sich der Dienst-Nutzer auch über RSS- oder iCal-Feeds über anstehende Termine informieren lassen. Soll der Kalender in eine Webseite oder einen Blog integriert werden, stellt Google den nötigen Code zur Verfügung. Ein Assistent kann zusätzlich dabei helfen das gewünschte Layout zu erzeugen. Ein Export der Kalenderdaten für andere Anwendungen ist in den Formaten iCal, XML und HTML möglich.

2.2 Analyse

In diesem Abschnitt wird analysiert, welche personenbezogenen Daten der Google-Dienst zurzeit speichert und welche weiteren Dienste Google mithilfe dieser Daten anbietet.

2.2.1 Personenbezogene Daten

Der Dienstanbieter Google stellt dem Nutzer mit dem *Google Kalender* ein von überall via Internet verfügbares und vergleichsweise mächtiges Tool zur Verfügung, welches im funktionalen Umfang anderen kostenlosen Diensten voraus ist. Verwendet ein Nutzer dieses Angebot, erhält der Dienstanbieter allerdings auch eine Vielzahl personenbezogener Daten, die bei offline verwendeten Produkten an niemanden weitergereicht würden. Die verschiedenen Datengruppen sollen im Folgenden zusammenfassend dargestellt werden.

Zunächst ist für die Nutzung des *Google Kalenders* ein Google-Account nötig, der bei der Erstellung einer Mail-Adresse bei Google automatisch erzeugt wird. Bei dieser Anmeldung fordert der Dienstanbieter, den **Namen und Vornamen** anzugeben. Ein großer Teil der Nutzer verwenden Pseudonyme, um ihre Identität zu verbergen. Somit werden bei der Anmeldung oftmals falsche Angaben getä-

tigt. Ein Schutz der Identität ist so allerdings kaum möglich, da der Dienstanbieter diese anderweitig herausfinden kann. Dies gelingt beispielsweise durch die Analyse des Mail-Verkehrs. Dies ist praktisch möglich, da jeder Nutzer durch Bestätigen der AGBs die maschinelle Analyse gestattet. So könnte sowohl aus der Anrede eingehender Mails, als auch der Schlussformel ausgehender Mails der tatsächliche Name des Nutzers ermittelt werden. Selbst wenn der Nutzer für den Mail-Verkehr eine andere Adresse verwendet, werden auch im Rahmen der Google-Kalender-Funktionen Mails generiert. Es kann somit davon ausgegangen werden, dass der Dienstanbieter über den korrekten, wenn auch nicht zwingend vollständigen Namen des Nutzers verfügt.

Bei Verwendung des Kalenders gibt der Nutzer zusätzlich weitaus persönlichere Daten preis. So wird durch einen Termin, der im ersten Ansatz nur den Nutzer selbst betrifft, eine bestimmte **Aktivität** preisgegeben, die zu einen bestimmten **Zeitpunkt**, an einen bestimmten **Ort** ausgeführt werden soll. Zusätzlich wird zu einem Termin eine bestimmte **Dauer** angegeben. Wird die Wiederholungsfunktion verwendet, erfährt der Dienstanbieter auch, **wie oft** eine bestimmte Tätigkeit ausgeführt wird. Werden zusätzlich Gäste zu einem Termin eingeladen, werden somit auch Daten über den **persönlichen Bekanntenkreis** preisgegeben. Des Weiteren erfährt der Google-Dienst den **Beschäftigungsgrad** eines Nutzers. Je intensiver der Anwender den Dienst nutzt, desto feingranularer können die genannten Datengruppen zu einem Persönlichkeitsprofil zusammengesetzt werden. Welche Gefahren dadurch entstehen und welche weiteren Informationen der Dienstanbieter aus diesen Daten schließen kann, wird in Kapitel 2.3 genauer analysiert.

2.2.2 Weiterführende Dienste

Durch die Datengruppen, welche im vorherigen Abschnitt aufgezeigt wurden, können dem Nutzer auch weitere Dienste angeboten werden. Diese beruhen auf den detaillierten Informationen eines Termins. Welche Daten welchen Dienst ermöglicht, wird im Folgenden aufgeschlüsselt.

Google bietet einen Zusatzdienst an, der auf verschiedene Datenfelder zugreift. Dabei handelt es sich um die **Such-Funktion** innerhalb des Kalenders. Ein weiterer Dienst, der ebenfalls alle Datenfelder heranzieht, ist der Google-Dienst zur **Synchronisierung**. Mithilfe des Zeitpunktes eines Termins bietet Google dem

Nutzer die Möglichkeit zur **Erinnerung** per Mail, Popup oder SMS. Weiterhin ermittelt Google mithilfe des Zeitpunktes auch, wie beschäftigt ein Dienst-Nutzer ist. Dies kann auf Wunsch veröffentlicht werden. So erfährt jeder anderer Nutzer, der ersteren als Gast einladen möchte, ob dieser bereits beschäftigt ist. Ein weiterer Zusatzdienst ist die **Anzeige der Ortes** mithilfe von *Google maps*. Dazu wird die Angabe aus dem Feld zur Ortsangabe ausgewertet. Klickt der Nutzer auf den Link *Karte* hinter der Ortsangabe eines Termins, so öffnet sich ein neues Browserfenster, in dem diese Angabe von *Google maps* ausgewertet wird. Je präziser die Ortsangabe selbst, desto sinnbringender ist dieser Dienst. Ein weiterer Dienst, den Google den Nutzern bereitstellt, ist das Verfassen einer **Nachricht an alle Teilnehmer** eines Termins.

2.3 Datenschutz

In diesem Abschnitt werden die unterschiedlichen personenbezogenen Daten untersucht, welche der Nutzer bei intensiver Verwendung des *Google Kalenders* bei der Terminverwaltung speichert. Die Angaben werden anhand ihrer Charakteristik gruppiert betrachtet. Diese Zusammenlegung mehrerer personenbezogener Daten wird im Folgenden als Datengruppe bezeichnet. Die Gruppierung ergibt sich dabei aus der Art der Verarbeitung der Daten im *Google Kalender*. Abhängig von den unterschiedlichen Verarbeitungsarten müssen verschiedene Techniken verwendet werden, um diese Daten zu schützen.

Die Angaben zu Titel, Beschreibung und Ort stellen lediglich Zeichenketten dar, die von Google zur Verarbeitung nicht benötigt werden. Diese werden in Datengruppe 1 betrachtet. Die Zeitspanne und das Datum, welche in Datengruppe 2 beleuchtet werden, verwendet der Dienst, um einen Termin innerhalb des Kalenders zum korrekten Zeitpunkt anzuzeigen. Die Angaben werden für jeden Termin separat gespeichert. In Datengruppe 3 wird die Wiederholung von Terminen betrachtet. Die dazu benötigten Angaben werden im *Google Kalender* innerhalb eines Termins hinterlegt und zur korrekten Anzeige aller Wiederholungen verwendet. Demnach werden diese Angaben als Metainformationen des Haupttermins gespeichert. In Datengruppe 4 werden die Informationen betrachtet, die zum Teilen von Terminen benötigt werden. Diese werden ebenfalls für jeden Termin gespeichert, lösen aber diverse Protokolle des Google-Dienstes aus, um mit anderen Dienst-Nutzern zu interagieren.

Im Folgenden werden die einzelnen Datengruppen genauer definiert und der jeweilige Nutzen, den Google aus diesen Daten ziehen kann, an Beispielen aufgezeigt. Welche Folgen die Preisgabe der einzelnen Datengruppe haben kann, wird innerhalb einer Datengruppe hervorgehoben und als Datenschutzproblematik bezeichnet.

2.3.1 Datengruppe 1: Was? / Wo?

Die erste Datengruppe ergibt sich aus dem Titel, der Beschreibung und der Ortsangabe eines Termins. Es kann daher die Problematik erfasst werden, dass der Google-Dienst in Erfahrung bringen kann, was ein Nutzer plant und an welchen Orten die jeweiligen Aktivitäten durchgeführt werden sollen.

Stehen einem einzelnen Unternehmen die Informationen über Aktivitäten mit dazugehörigen Ortsangaben zur Verfügung ist es möglich, ein individuelles Nutzerprofil zu erstellen. Es können beispielsweise Vorlieben, Hobbys oder Reiseziele ermittelt werden. So kann der Dienstanbieter Google das Stamm-Café, den Zahnarzt, den Arbeitsplatz, den Wohnort und weitere Lokalitäten identifizieren. Es wäre sogar möglich, anzugeben, ob der Google-Nutzer über ein Automobil verfügt oder wie intensiv öffentliche Verkehrsmittel genutzt werden. Dazu wird der Kalender analytisch untersucht und die einzelnen Termine mithilfe von Heuristiken analysiert. So sind beispielsweise häufig wiederkehrende, werktags stattfindende Termine solche Aktivitäten, die mit dem Beruf des Nutzers in Zusammenhang stehen.

Die Bandbreite der personalisierten Werbung kann mit diesen Informationen erweitert werden. Wenn Google den Werbeträgern anbieten kann, Reiseangebote lediglich an Nutzer zu verteilen, die sehr reiselustig sind oder aus beruflichen Gründen oft reisen, ist dies für die entsprechenden Anbieter sehr reizvoll.

2.3.2 Datengruppe 2: Wann? / Wie lang?

Diese Datengruppe ergibt sich aus den Angaben zum Zeitpunkt und der angegebenen Dauer des Termins. Die Gruppe befasst sich demnach mit der Problematik, dass dem Dienstanbieter offen liegt, wann ein Nutzer Termine wahrnehmen will und wie lang diese andauern.

Mithilfe dieser Zusatzinformationen kann ein Nutzerprofil weiter verfeinert werden. Anhand der Angaben zum Zeitpunkt und zur Dauer kann ermittelt wer-

den, wie lang der Arbeitstag eines Nutzers ist, ob dieser im Schichtdienst arbeitet, wann ein Urlaub geplant wird oder wann ein Nutzer zu Hause erreichbar ist.

Gekoppelt mit Auswertungen zu Ortsangaben ist es zudem möglich, ein Bewegungsprofil zu erstellen. Verwendet der Nutzer zudem die Erinnerungsfunktion kann weiterhin ermittelt werden, wie weit der Nutzer vom derzeitigen Standort zum Zielort des Termins entfernt ist. Umso intensiver der Kalender genutzt wird, desto genauer fallen die Positionsangaben aus. Der Dienstanbieter kann so Daten erheben, die angeben, wann sich welcher Nutzer wo und für welche Dauer aufhält.

2.3.3 Datengruppe 3: Wie oft?

Die dritte Datengruppe ergibt sich aus sich wiederholenden Terminen. Der Dienstanbieter verfügt mit diesen Angaben über Daten, die aussagen, wie oft und in welchen Abständen ein Nutzer eine bestimmte Aktivität ausführt. Auch wenn ein Termin im *Google-Kalender* nicht mittels der dafür vorgesehen Funktion, sondern manuell mit jeweils neuen Terminen wiederholt wird, können wiederkehrende Termine durch Analyse des Kalenders ermittelt werden.

Das Nutzerprofil wird entsprechend erweitert und eröffnet dem Unternehmen weitere Schlussfolgerungen. Es kann durch Analyse dieser Angaben beispielsweise ermittelt werden, ob der Nutzer in einem Verein tätig ist oder wann für das Kraftfahrzeug eine neue Hauptuntersuchung ansteht. Wird vom Dienst festgestellt, dass ein bestimmtes Freizeitangebot vom Nutzer im vergangenen Quartal unterdurchschnittlich oft wahrgenommen wurde, kann der Anbieter dieses Freizeitangebots von Google darauf aufmerksam gemacht werden. Mit geringem Aufwand kann dieser den Kunden durch Werbung oder Gutscheinaktionen leicht motivieren, das Angebot in Zukunft wieder öfter wahrzunehmen. Für werbende Unternehmen haben solche Informationen einen hohen ökonomischen Wert.

2.3.4 Datengruppe 4: Mit wem?

Datengruppe 4 entsteht durch die Angabe von Gästen innerhalb eines Termins. Der Dienstanbieter erhält somit Informationen über die sozialen Kontakte seiner Nutzer.

Bei lang andauernder Nutzung des Dienstes und Analyse des Nutzerverhaltens kann herausgefunden werden, in welchem Verhältnis die Nutzer zueinander stehen. So gehören Gäste von Wochenend-Terminen eher zum Freundeskreis, wohingegen Termine an bestimmten Feiertagen darauf schließen lassen, dass es sich bei den Gästen um Familienmitglieder handelt. All diese scheinbar unzusammenhängenden Teile geben ein hohes Maß an Privatsphäre preis. Im Gesamten erhält das analysierende Unternehmen ein Netz aus Beziehungen der Nutzer untereinander, kann wichtige Knotenpunkte ersehen und die Bedürfnisse und Vorlieben bestimmter Nutzergruppen bestimmen. Im Gegensatz zu Datengruppe 1 sind nun also auch Informationen betroffen, die es ermöglichen, einen kontextbasierten Zusammenhang zwischen Nutzern zu erstellen.

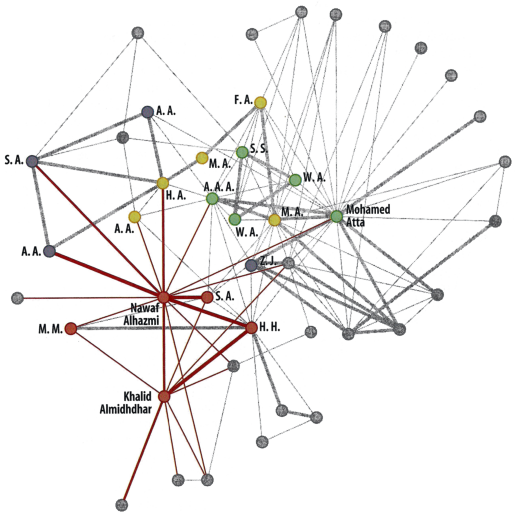

Abbildung 2.7: Soziale Netzwerkanalyse

Welchen Nutzen eine solche Netzwerkanalyse haben kann, wurde beispielsweise in der Terrorismusbekämpfung 2001 deutlich. So konnte Mohamed Atta von US-Geheimdiensten als eine Schlüsselfigur der Hamburger al-Quaida-Zelle identifiziert werden. Dabei wurden Verbindungsdaten von bekannten Terroristen untersucht, um die interne Gruppenstruktur aufzudecken. Abbildung 2.7 zeigt die grafische Aufbereitung einer solchen Analyse [Gie10].

Auch der Dienstanbieter Google kann solche Analysemethoden verwenden, um die Interessen und Vorlieben von Benutzern zu ermitteln. Einige Nutzer, die mit vielen weiteren in Verbindung stehen, werden bei solchen Analysen hervorgehoben und als Knoten bezeichnet. Diese bringen oft weitere Personen in das Netz und binden Nutzer an den Dienst, die sonst eventuell andere Produkte nutzen würden. Solang der Knoten im Netz aktiv bleibt, bleiben auch die Personen mit wenigen Verbindungen ins Netz als Kunden erhalten. Das gesamte Netz gewinnt dadurch an Stabilität. Werden die Bedürfnisse der Knoten erfüllt, kann die vorübergehende Stabilität des Netzes gesichert und weitere Nutzer durch andere Maßnahmen stärker an den Dienst gebunden werden.

Ordnet beispielsweise ein mit dem Google-Dienst zufriedener Abteilungsleiter die Nutzung des *Google Kalenders* an, so wird dieser eine bestimmten Personengruppe spürbar oft zu Terminen einladen. Einige dieser Personen sind neue *Google Kalender* Nutzer, die den Dienst nur aufgrund einer Anweisung verwenden. Die Aktivität der neuen Nutzer hängt zunächst nur vom Abteilungsleiter ab. Können die Bedürfnisse dieser Nutzer aber ermittelt werden, ist es möglich, diese auch über den beruflichen Zweck hinaus für den Dienst zu gewinnen. Eine Analyse wird weiterhin den Abteilungsleiter als Knoten identifizieren. Die Bedürfnisse des Knotens sind entsprechend von größerer Bedeutung. Insbesondere macht es eine Betrachtung des Nutzerverhaltens erst möglich, die zu Grunde liegende soziale Struktur der Nutzer allein aufgrund ihres Verhaltens zu bestimmen.

In angrenzenden Themengebieten wie sozialen Plattformen oder Online-Rollenspielen ist die Analyse und Befriedigung der Bedürfnisse dieser Knoten bereits weit fortgeschritten. Das Potential der kontextbasierten Daten stellt somit erwiesenermaßen eine treibende Kraft dar[2].

2.4 Abschluss

Die sich ergebenden Datengruppen zeigen unterschiedliche Ansätze für die Bildung von Nutzerprofilen auf. Das Google daran interessiert ist, zeigt die neue Datenschutzerklärung, in der der Nutzer zustimmt, dass die Daten aller Dienste zusammengeführt werden dürfen. Ein weiteres Beispiel für Bemühungen zur Bildung von Profilen zeigt die vom Unternehmen angebotene Zusatzfunktion Webprotokoll [Goo11c], welche eingeloggten Nutzern angeboten wird, um Suchanfragen zu optimieren und dem Nutzer bereits gefundene, hilfreiche Seiten zu präsentieren. Selbst wenn die Analyse der einzelnen Datengruppen wenig risikoreich erscheint, so ist zu bedenken, dass die Informationen im Kontext betrachtet ein feingranulares Nutzerprofil darstellen. Je intensiver ein Nutzer demnach die Vielzahl von Google-Diensten verwendet, desto klarer wird dessen digital vorliegendes Profil. Dieses gibt dann darüber Aufschluss, wer eine Person ist, wie das soziale Umfeld aufgebaut ist, wie diese sich in der Welt bewegt, wie die Zeit für Karriere und Familienleben verteilt wird oder welchen Hobbys die Person nachgeht. Da diese Informationen insbesondere für personalisierte Werbung sehr aufschlussreich sind kann nicht davon ausgegangen werden, dass der Dienstanbieter einen solchen nutzerbezogenen Kontext zurzeit nicht schon realisieren kann oder bereits realisiert hat.

[2] siehe dazu [Gie10]

Kapitel 3

Datenschutzkonzept

Dieses Kapitel greift die unter Abschnitt 2.3 beschriebenen Datengruppen auf und beschreibt die Lösungsansätze sowie die entsprechenden Maßnahmen, um die Preisgabe dieser personenbezogenen Daten zu minimieren. Die Kernproblematik jeder Datengruppe wurde bereits im genannten Abschnitt erläutert und somit aufgezeigt, dass jedwede Information Schlüsse auf das individuelle Verhalten eines Nutzers zulässt. Es gilt daher, dem Google-Dienst diese Information möglichst vorzuenthalten.

Um zu unterscheiden, welche Daten tatsächlich zu einem Termin gehören und welche Daten verändert im *Google Kalender* gespeichert werden, um die Datengruppen zu schützen, werden die Angaben im Folgenden mit *tatsächlich* oder *verändert gespeichert* gekennzeichnet. Ist ein Datum verändert gespeichert, handelt es sich um die manipulierte Angabe der tatsächlichen Daten. Veränderte Daten sind demnach Kryptogramme der tatsächlichen Daten. Für einige Zwecke werden zufällige Werte im Google System hinterlegt. Diese werden entsprechend als *randomisiert* gekennzeichnet.

3.1 Datengruppe 1

Datengruppe 1 befasst sich mit der Problemstellung, dass der Google-Dienst Information darüber erhält, was ein Nutzer plant und wo dies stattfinden soll. Dieser Abschnitt stellt einen Lösungsansatz für diese Datenschutzproblematik vor. Für das beschriebene Vorgehen wird anschließend die zu verwendende Sicherheitstechnik beschrieben.

3.1.1 Lösungsansatz

Um den Inhalt eines Termins vor dem Dienstanbieter zu verbergen, soll dieser verschlüsselt werden. Damit wird die Vertraulichkeit des Inhalts sichergestellt. Der Nutzer ist allerdings aufgrund der Kenntnis der Schlüssel auch weiterhin in der Lage den Inhalt aufzudecken. Titel, Terminbeschreibung und die zugehörigen Ortsangabe sollen verschlüsselt werden. Diese Verschlüsselung soll durch die Anwendung eines kryptografischen Verfahrens und entsprechender Verwaltung der Schlüssel in einem Modul realisiert werden. Auf diese Weise werden auf den Servern des Dienstanbieters lediglich Kryptogramme hinterlegt, die nur mit erheblichem Aufwand vom Dienst analysiert werden können. Somit werden die tatsächlichen Angaben zu Titel, Ort und Beschreibung dadurch geschützt, dass diese nach einer Verschlüsselung verändert im *Google Kalender* gespeichert werden.

3.1.2 Sicherheitstechnik

Die Art der Verschlüsselung spielt im Rahmen dieser Arbeit eine untergeordnete Rolle. Die einzelnen Chiffriermethoden werden daher nicht eingehend beleuchtet oder diskutiert. Jeder Termin wird mit einem eigenen Termin-Schlüssel verschlüsselt. Dies verhindert, dass der Dienst bei eingehender Analyse eines Termins und Berechnung dessen Schlüssels in der Lage ist, weitere Inhalte zu dekodieren.

Das Softwareprodukt verwendet AES als symmetrisches Verschlüsselungsverfahren. Nach derzeitigem Wissenstand können AES-verschlüsselte Kryptogramme nicht in vertretbarer Zeit ohne Wissen des symmetrischen Schlüssels dekodiert werden. Die im Softwareprodukt verwendete Schlüssellänge beträgt 256bit. Letztlich ist der Algorithmus selbst aufgrund der modularen Struktur des Softwareprodukts aber ohne Aufwand austauschbar.

3.2 Datengruppe 2

Datengruppe 2 befasst sich mit der Problemstellung, dass der Google-Dienst Information darüber erhält, wann ein Nutzer einen Termin wahrnehmen will. Zudem könnte der Dienstanbieter die Informationen über die Dauer eines Termins nutzen. Dieser Abschnitt stellt einen Lösungsansatz für diese Datenschutzproble-

matik vor. Für das beschriebene Vorgehen wird anschließend die Sicherheitstechnik beschrieben.

3.2.1 Lösungsansatz

Um den Zeitpunkt sowie die Dauer eines Termins zu verbergen, müssen diese Angaben verändert im *Google Kalender* gespeichert werden. Da das zu entwickelnde Softwareprodukt die korrekten Zeitangaben letztlich rekonstruieren können muss, werden die tatsächlichen Zeitangaben unverändert, innerhalb der Terminbeschreibung als Metadaten gespeichert und dem Google-Dienst stattdessen randomisierte Werte übermittelt. Ein Termin wird somit an einem beliebigen Datum zu einer zufälligen Zeit mit einer ebenfalls zufälligen Dauer gespeichert. Dazu soll ein Termin in einer nicht statischen Weise verschoben und zeitlich angepasst werden. Die dazu verwendete Methode zur Bestimmung der neuen Angaben soll dem Zufall unterliegen, sodass eine Wiederherstellung der tatsächlichen Zeitpunkte und Zeitspannen für den Dienst nicht, beziehungsweise nur sehr schwer möglich ist. Um bestimmte Rückschlüsse zu verhindern muss die Verschiebung der Termine in einem weiten Streubereich vollzogen werden. Werden Termine also nicht nur innerhalb einer Woche, sondern innerhalb mehrerer Monate verschoben, verhindert dies beispielsweise die Erkennung von Urlaubswochen.

3.2.2 Sicherheitstechnik

Um eine Verschiebung der Termine zu ermöglichen muss der Termin an einem anderen Tag, zu einem anderen Zeitpunkt und mit veränderter Dauer gespeichert werden. Dies soll durch das Softwareprodukt organisiert werden, sodass der Nutzer wie gewohnt die korrekten Daten eingeben kann. Die tatsächlichen Daten werden ausgelesen und kryptografisch gesichert innerhalb der Terminbeschreibung als Metadaten gespeichert. An den Google-Dienst werden lediglich randomisiert erzeugte Angaben zu Datum, Zeitpunkt und Dauer übermittelt. Dies verbirgt zudem den Beschäftigungsgrad eines Nutzers. Die Metainformationen müssen automatisiert gefunden, ausgelesen und verarbeitet werden, um dem Benutzer letztlich den Kalender wie gewohnt präsentieren zu können. Die unterschiedlichen manipulierten Termine müssen erkannt und mithilfe ihrer tat-

sächlichen Daten korrekt angezeigt werden. Die Software liest dazu die Daten des *Google Kalenders* aus und manipuliert die Anzeige der Zeitpunkte sowie die Dauer der Termine, sodass die vom Nutzer einst eingestellten Daten für den angezeigten Kalender ausschlaggebend sind.

3.3 Datengruppe 3

Datengruppe 3 befasst sich mit der Problemstellung, dass der Google-Dienst Informationen darüber erhält, wie oft ein Nutzer einen Termin wahrnehmen will. Im *Google Kalender* wird diese Angabe durch sich wiederholende Termine realisiert. Dieser Abschnitt stellt einen Lösungsansatz für dieses Problemfeld vor. Für das beschriebene Vorgehen wird anschließend die Sicherheitstechnik beschrieben.

3.3.1 Lösungsansatz

Um die Wiederholung eines Termins zu verschleiern, darf diese Information nicht mit dem Mechanismus des Google-Dienstes hinterlegt werden. Die Funktion zur Wiederholung von Terminen muss auf das Softwareprodukt ausgelagert werden. Wird ein sich wiederholender Termin erstellt, so sind die zusätzlichen Informationen zur Wiederholung nur innerhalb der kryptografisch gesicherten Metainformationen hinterlegt. Dem Google-Dienst wird lediglich ein einmal eintreffendes Ereignis übermittelt. Erkennt das zu entwickelnde Softwareprodukt einen solchen Termin, soll die korrekte Umwandlung als sich wiederholenden Termin im Kalender erfolgen, sodass die Darstellung für den Nutzer unverändert bleibt.

3.3.2 Sicherheitstechnik

Diese Manipulation wird ebenfalls mithilfe von Metainformationen realisiert. Diese müssen automatisiert gefunden, ausgelesen und verarbeitet werden, um dem Benutzer letztlich einen Kalender ohne Manipulationen anzuzeigen. Dazu liest die Software die Daten des *Google Kalenders* aus, interpretiert die Metainformationen und manipuliert die Anzeige des Kalenders in der Form, dass ein Termin, der im *Google Kalender* nur zu einem Zeitpunkt an einem bestimmten Tag stattfindet, nun an allen betroffenen Tagen angezeigt wird.

3.4 Datengruppe 4

Datengruppe 4 befasst sich mit der Problemstellung, dass der Google-Dienst Information darüber erhält, mit wem ein Nutzer interagiert. Darunter ist die Funktion zum Teilen von Terminen zu verstehen, auf welche in Abschnitt 2.1.2.2 detailliert eingegangen wurde. Dieser Abschnitt stellt einen Lösungsansatz für dieses Problemfeld vor. Für das beschriebene Vorgehen wird anschließend die Sicherheitstechnik dargestellt.

3.4.1 Lösungsansatz

Da die Interaktion mit anderen Dienstnutzern eine Kernfunktionalität des Dienstes darstellt, kann diese nicht gänzlich ohne erheblichen Mehraufwand unterbunden werden. Es ist zu untersuchen, welche Manipulationen bei gleichbleibender Nutzerfreundlichkeit einen möglichst hohen Grad an Verschleierung bieten.

Um andere Nutzer zu Terminen einzuladen, müssen diese als Gäste zu einem Termin hinzugefügt werden. Daraufhin erfolgt die Erstellung des Termins. Bis zu diesem Punkt sind keine Manipulationen möglich, da ein anderer Dienstnutzer darüber in Kenntnis gesetzt werden muss, dass er zu einem Termin eingeladen werden soll.

Soll selbst diese Funktionalität nicht genutzt werden, so wäre es alternativ möglich, die Funktion komplett auszulagern und händisch alle Teilnehmer durch Mails oder Anrufe über einen Termin zu informieren. Auf diese Weise würden auch Reaktionen und Änderungen des Termins publiziert. Da dies zu hohen Einbußen im Bereich der Nutzerfreundlichkeit führt, soll die initiale Einladung durch den Mechanismus des *Google Kalenders* nicht unterbunden werden.

Erst die Reaktion auf den Termin in Form von Bestätigung oder Ablehnung der Einladung sorgt abschließend dafür, dass die beiden Nutzer wirklich in Beziehung zu einander stehen. Der Mechanismus der validen Reaktionen muss also auf anderem Weg realisiert werden. Ein versehentlich eingeladener Teilnehmer wird den Termin höchstwahrscheinlich löschen. Diese Reaktion lässt am wenigsten Rückschlüsse auf die letztlich bestehende Verbindung zwischen zwei Teilnehmern schließen.

Allein das Löschen der Termine zu denen ein Nutzer eingeladen wird, reicht nicht aus, um eine Analyse des Nutzerverhaltens zu erschweren. Zwar scheinen

die Gäste eines Termins durch die Löschung wie versehentlich eingeladenen Nutzer, jedoch kann das System diese trotzdem als tatsächliche Gäste verstehen. Es sind also weiterhin Rückschlüsse auf die Gäste möglich.

Zur Vermeidung der Erkennung der tatsächlichen Gäste sollen neben diesen zusätzliche Gäste hinzugefügt werden. Zu einem Termin soll somit eine um einen bestimmten Faktor oder einen bestimmten Summanden erhöhte Anzahl an Personen eingeladen werden. Dies ermöglicht eine Verschleierung der tatsächlichen Gäste.

Rückschlüsse lassen sich bei diesem Vorgehen erst ziehen, wenn bestimmte Gruppen immer wieder in unvorhersehbaren Abständen eingeladen werden. Analysiert der Dienstanbieter die unterschiedlichen Mengen der eingeladenen Gäste, so werden bestimmte Gäste in allen diesen Mengen auftauchen. Diese Schnittmenge enthält demnach alle tatsächlichen Gäste. Die anderen Gäste sind in dieser Schnittmenge nicht mehr enthalten. Der Dienstanbieter kann die tatsächlichen Gäste in einem solchen Fall wieder systematisch, wenn auch mit erhöhtem Aufwand, erkennen.

3.4.2 Sicherheitstechnik

Zwei Methoden sind zu betrachten. Zum einen sollen mehr Gäste als nötig zu einem Termin eingeladen werden, zum anderen sollen diese nicht mit dem bisherigen Mechanismus zum Bestätigen oder Ablehnen der Einladung reagieren.

Zur Realisierung der ersten Methode sollen aus einem Pool ausgewählter Nutzer weitere Gäste zu einem Termin hinzugefügt werden. Dieser Pool besteht ausschließlich aus Nutzern des zu entwickelnden Softwareprodukts. Die unterschiedlichen Nutzer sollen sich durch ein entsprechendes Protokoll untereinander bekannt machen können. Letztlich soll jeder Nutzer ein Netzwerk bekannter Nutzer aufbauen können, die das Softwareprodukt ebenfalls verwenden. Der Aufbau dieses Netzwerks soll zudem vom Softwareprodukt unterstützt werden, sodass die manuelle Bekanntmachung mithilfe des genannten Protokolls nur selten nötig ist.

Erhält ein Nutzer einen Termin, zu dem dieser nur als zusätzlicher, nicht aber als tatsächlicher Gast eingetragen ist, soll der zusätzliche Termin nicht im Kalender erscheinen, sondern ausgeblendet und automatisch gelöscht werden. Den tatsächlichen Gästen wird der neue Termin angezeigt. Diese können nun auf die Termineinladung reagieren.

Um den anderen Nutzern die eigene Reaktion mitzuteilen, sollen die Mechanismen des Google-Dienstes aus genannten Gründen nicht verwendet werden. Die zweite Methode soll so realisiert werden, dass ein Gast die Einladung ignoriert und einen neuen Termin erzeugt, zu dem er wiederum den Einladenden und gegebenenfalls alle potentiellen weiteren Teilnehmer einlädt sowie erneut zusätzliche Gäste. Dieser Termin enthält Angaben zur eindeutigen Identifikation der ursprünglichen Einladung, sodass dieser der Reaktion zugeordnet werden kann. Der Reaktions-Termin wird von den anderen Teilnehmern ausgewertet, gelöscht und der Ursprungstermin entsprechend aktualisiert.

3.4.3 Alternative Sicherheitstechnik

Ein generell alternativer Ansatz ist die Verwendung von zusätzlichen Google-Accounts. Diese werden mit eigenem Konto erstellt und zusätzlich zu Terminen eingeladen. Dies verschleiert die Teilnehmer, da dem Google-Dienst nicht genau bekannt ist, wer tatsächlich am Termin teilnehmen soll und wer nicht. Da die zusätzlichen Accounts selbst aber nie aktiv werden, indem sie den Kalender selbst nutzen, würde ein solches Benutzerkonto leicht als Attrappe erkennbar sein. Weiter ist fraglich ob die Einrichtung solcher Accounts gegen die allgemeinen Geschätzsbedingungen des Google-Dienstes verstößt.

3.5 Kumuliertes Datenschutzkonzept

Da die Sicherheitstechniken für die unterschiedlichen Datengruppen (Kapitel 3.1-3.4) konzeptionell vorgestellt wurden, wird im folgenden Abschnitt das kumulierte Datenschutzkonzept beschrieben, welches die unterschiedlichen Maßnahmen bestmöglich vereint. Diese Kopplung bringt mehrere kritische Aspekte zum Vorschein, die ebenfalls diskutiert werden. Für die Betrachtung wird zunächst davon ausgegangen, dass jeder Dienst-Nutzer und jeder weitere involvierte Nutzer über das Softwareprodukt verfügt.

3.5.1 Einbindung zu Datengruppe 1

Datengruppe 1 (Kapitel 3.1) befasst sich mit der Verbergung von Inhalt und Ort eines Termins. Dies erfordert eine Verschlüsselung von Titel, Ortsangabe und

Beschreibung. Zu diesem Zweck wird für jeden Termin ein zufälliger Termin-Schlüssel erzeugt. Um einen Termin-Schlüssel einem Termin zuzuordnen wird zusätzlich ein einzigartiger Bezeichner (uID) generiert. Der Termin-Schlüssel und die uID werden zusammen im Dateisystem hinterlegt. Die uID wird zudem im ursprünglichen Titel-Feld des Termins gespeichert, um dem Termin später den korrekten Termin-Schlüssel zuordnen zu können. Jeder Termin wird demnach mit einem eindeutig identifizierbaren Schlüssel symmetrisch verschlüsselt.

Das Softwareprodukt muss folglich über eine Verwaltung für die uIDs und die zugehörigen Schlüssel verfügen. Fortlaufend wird diese als Schlüssel-Management bezeichnet. Bei initialem Aufruf des Kalenders werden die Termine dann sequenziell analysiert. Mithilfe der uIDs wird der zu benutzende Schlüssel nachgeschlagen und die weiteren Informationen entschlüsselt.

3.5.2 Einbindung zu Datengruppe 2 & 3

Datengruppe 2 (Kapitel 3.2) und Datengruppe 3 (Kapitel 3.3) behandeln die Geheimhaltung der Angaben zum Zeitpunkt, der Dauer sowie der Wiederholung und sollen konzeptionell durch Metainformationen gelöst werden. Die Informationen über die Dauer, den Zeitpunkt und die Wiederholung eines Termins werden so nicht mehr durch die ursprünglichen Mechanismen des Google-Dienstes, sondern verändert oder randomisiert gespeichert. Somit sind die Daten für eine mögliche Analyse durch den Dienstanbieter nicht in den eigentlich dafür vorgesehenen Feldern zu finden. Durch zusätzliche Verschlüsselung des Titels, der Beschreibung und der Ortsangabe des Termins sind diese auch an anderer Stelle nicht in Klartext hinterlegt.

Um einen Termin automatisiert verarbeiten und alle Metainformationen effizient auslesen zu können, sollen alle Angaben eines Termins durch eine XML-Struktur repräsentiert werden. Innerhalb dieser Struktur werden alle nötigen Daten gelagert, die das Softwareprodukt verarbeiten muss, um alle Informationen zu einem Termin korrekt anzuzeigen. Die einzelnen Elemente dieser Struktur spiegeln alle benötigten Daten wider, die verändert oder randomisiert gespeichert werden. Die XML-Struktur wird innerhalb des Beschreibungs-Feldes des *Google-Kalenders* gespeichert, da dies mit 2 hoch 13 Zeichen den meisten Speicherplatz bietet. Eine Terminbeschreibung in XML folgt demnach nachfolgenden Schema:

```
<Termin>                                                                    1
   <Titel> Beispieltitel </Titel>                                           2
   <Ort> Beispielort </Ort>                                                 3
   <Zeitpunkt manipuliert={true,false}>                                     4
      <Datum> Beispieldatum </Datum>                                        5
      <Uhrzeit> Beispieluhrzeit </Uhrzeit>                                  6
   </Zeitpunkt>                                                             7
   <Wiederholung aktiv={true,false}>                                        8
      <Zeitraum>                                                            9
         <Beginn> Beispielanfang </Beginn>                                  10
         <Ende> Beispielende </Ende>                                        11
         <Ausnahmen> Ausnahme1, Ausnahme2 </Ausnahmen>                      12
      </Zeitraum>                                                           13
   </Wiederholung>                                                          14
</Termin>                                                                   15
```

Codeauszug 3.1: Ansatz zur XML-Struktur eines Termins

3.5.3 Infrastrukturelle Veränderungen

Datengruppe 4 (Abschnitt 3.4) befasst sich mit Veränderung der tatsächlichen Informationen zu den eingeladenen Gästen eines Termins. Die Methoden diese Datengruppe zu schützen, sind zum einen die Einladung von mehr Gästen, als tatsächlich teilnehmen sollen, zum anderen die Entkopplung der Reaktion von den ursprünglich dafür vorgesehen Mechanismen des Google-Dienstes. Der hier neu auftauchende, bisher nicht berücksichtigte Aspekt ist, dass nun mehrere Nutzer einen Termin verwalten sollen. Bevor auf die Umsetzung dieser Methoden eingegangen werden kann, müssen die zuvor erläuterten Strategien hinsichtlich dieser neuen Anforderung angepasst werden.

Die Methodik zur Verschlüsselung, um Datengruppe 1 zu schützen impliziert, dass einem Nutzer der Termin-Schlüssel bekannt ist. Erstellt ein Nutzer einen Termin, wird der Termin-Schlüssel erzeugt und im Dateisystem hinterlegt. In diesem Fall kann die Entschlüsselung problemlos erfolgen. Soll ein Gast zu einem Termin eingeladen werden, so ist dieser nicht im Besitz des Termin-Schlüssels. Dieser muss demnach ebenfalls übermittelt werden. Zur Übertragung der Schlüssel zu anderen Nutzern soll das Eingabefeld zur Ortsangabe des Google-Dienstes verwendet werden. Dies erleichtert ebenfalls den Zugriff auf diese Informationen, da das Feld für andere Zwecke, wie das Speichern des tatsächlichen Ortes, nicht mehr benötigt wird. Da das Feld eine Zeichenkette bis 2 hoch 10 Zeichen erlaubt ist es für die Angabe der Schlüsselinformationen ebenfalls gut geeignet.

Der Schlüssel kann nicht im Klartext übertragen werden, da der eigentlich geheime Schlüssel veröffentlicht werden würde und eine konzeptionelle Schwachstelle entstünde. Um den Termin-Schlüssel zu sichern, muss dieser ebenfalls verschlüsselt werden. Ein globaler Schlüssel, den alle Nutzer des Softwareprodukts besitzen, ist ebenfalls nicht ausreichend. Auch ein Algorithmus, der diesen Schlüssel anhand von etwaigen im Code verankerten Merkmalen bei allen Nutzern gleich berechnet, stellt eine konzeptionelle Schwachstelle dar. Da der Code des Softwareprodukts offen ist, könnte der Dienstanbieter sowohl einen globalen Schlüssel, als auch den Algorithmus zur Berechnung eines global gleichen Schlüssels ermitteln. Alternativ könnte die Berechnung der Schlüssel durch die Verwendung eines allen Nutzern bekannten, geheimen Merkmals durchgeführt werden. Die Verteilung dieses Merkmals stellt allerdings die selben Anforderungen wie die Verteilung des Termin-Schlüssels selbst.

Das Problem zur Verteilung der Termin-Schlüssel wird durch den zusätzlichen Einsatz eines asymmetrischen Verfahrens zur Verschlüsselung gelöst. Das so entstehende hybride Verschlüsselungssystem erlaubt die sichere Übertragung eines Termin-Schlüssels. Für jeden Nutzer wird ein asymmetrisches Schlüsselpaar erzeugt. Der öffentliche Teil des Schlüssels wird, wie im nächsten Absatz näher beschrieben, publiziert. Ein Termin-Schlüssel kann folglich mit dem öffentlichen Schlüssel eines Gastes verschlüsselt und somit sicher zum Gast übertragen werden. Im Folgenden wird der mit dem öffentlichen Schlüssel eines Gastes gesicherte Termin-Schlüssel als Übertragungs-Schlüssel bezeichnet. Da jeder Gast einen eigenen Übertragungs-Schlüssel erhält, muss der individuelle Gast diesen finden können. Dazu wird die Mail-Adresse des Nutzers als eindeutiges Nutzer-gebundenes Merkmal verwendet. Zudem wird der öffentliche Schlüssel zur Verbesserten Verbreitung übertragen. Diese Angaben werden ebenfalls im Feld der Ortsangabe des *Google Kalenders* gespeichert. Innerhalb der Ortsangabe wird demnach eine Liste hinterlegt, die die jeweilige Mail-Adresse eines Gastes gefolgt von dessen öffentlichen Schlüssel und den verschlüsselten Termin-Schlüssel - den Übertragungs-Schlüssel - enthält. Im Fall mehrerer Gäste werden alle Tupel kommasepariert übertragen.

Um ein solches Vorgehen zu ermöglichen, müssen dem Softwareprodukt des Einladenden alle öffentlichen Schlüssel der Gäste bekannt sein. Zum einen wird folglich ein Mechanismus benötigt, der den initialen Austausch der öffentlichen Schlüssel ermöglicht. Zum anderen ist erneut eine Verwaltungsstruktur notwen-

dig, die Nutzer und deren öffentliche Schlüssel erfasst. Fortlaufend wird diese Verwaltung als Partner-Management bezeichnet.

Um einen Schlüsselaustausch zu initiieren erstellt Benutzer A einen Termin, zu dem er Benutzer B einlädt. Das Softwareprodukt von Benutzer B erkennt die Anfrage anhand des eindeutigen Titels *PublicKeyRequest*. Weiterhin enthält dieser Termin innerhalb der Beschreibung die eindeutige Mail-Adresse von Benutzer A sowie dessen öffentlichen Schlüssel. Nutzt Benutzer B bereits das Softwareprodukt, so erkennt dieses die Konfigurationsmitteilung und hinterlegt die Mail-Adresse als eindeutiges Identifizierungsmerkmal von Benutzer A samt dessen öffentlichen Schlüssel in seinem Partner-Management. Auf diese Weise werden zwei Nutzer miteinander bekannt gemacht. Jedwede Kommunikation ist bis zu diesem Zeitpunkt unverschlüsselt. Weiterhin wird im Beschreibungstext nach der kurzen XML-Struktur, die die Mail-Adresse und den öffentlichen Schlüssel des Nutzers enthält, dem Dienst-Nutzer, der das Softwareprodukt noch nicht verwendet, erläutert, dass es sich um einen Konfigurationsmechanismus eines Softwareproduktes zum Selbstdatenschutz handelt. Zusätzlich wird ein Link angegeben, der genauere Informationen enthält. Auf diese Weise wird ermöglicht, dass ein Nutzer des Google-Dienstes seine Bekannten darauf aufmerksam machen kann, dass eine kostenlose Software verfügbar ist, die hilft, die eigenen personenbezogenen Daten zu schützen. Abbildung 3.1 veranschaulicht diesen Ablauf.

Die von Datengruppe 1 geforderte Verschlüsselung kann mithilfe der Erweiterung zu einem hybriden Verfahren beibehalten werden. Zu diesem Zweck wurde verdeutlicht, wie der symmetrische Termin-Schlüssel geschützt und den Gästen zugänglich gemacht wird. Ebenfalls wurden die notwendigen Verwaltungsstrukturen eingeführt, um dies zu bewerkstelligen. Im Folgenden können die Techniken aus Datengruppe 4 genauer betrachtet werden.

3.5.4 Einbindung zu Datengruppe 4

Zunächst wird die Methodik betrachtet, mit deren Hilfe mehr Gäste eingeladen werden, als tatsächlich teilnehmen sollen. Die Gästeliste wird somit verändert gespeichert. Die zweite zu betrachtende Schutzmaßnahme ist die alternative Methode zur Reaktion auf einen Termin.

Um Termine vom Kalender eines Nutzers an den Kalender eines anderen Nutzers zu übertragen, muss dies entweder mit der vom Google-Dienst angebotenen Funktionalität zum Teilen von Terminen oder händisch organisiert werden.

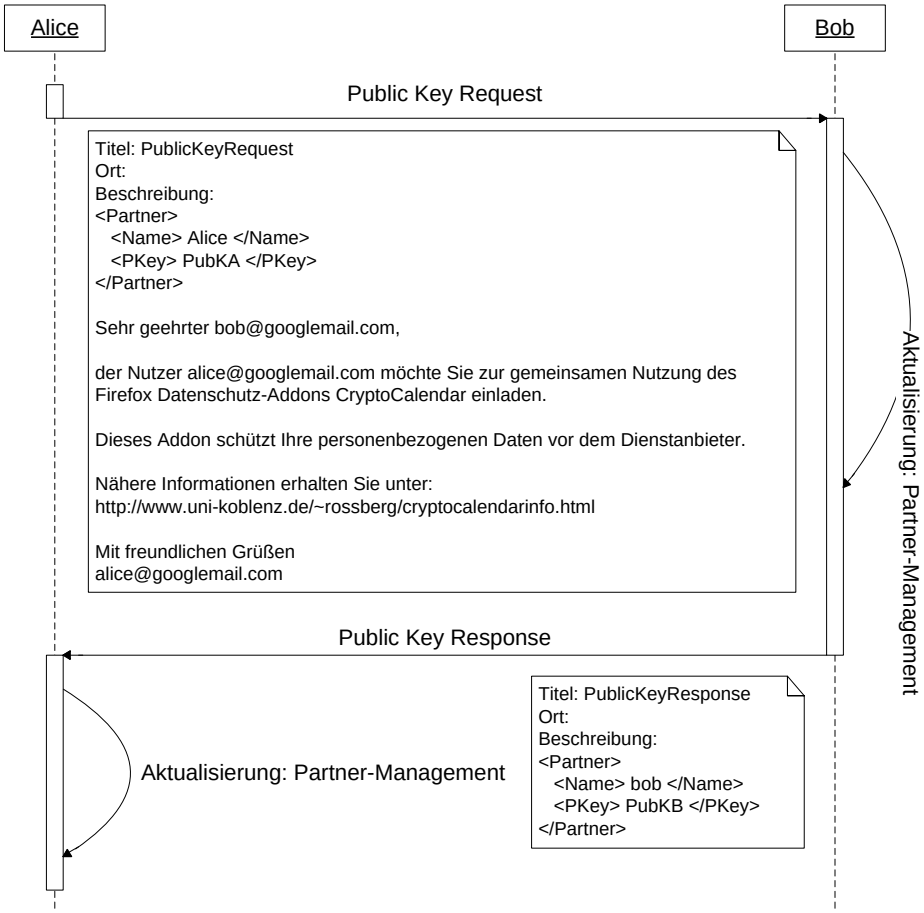

Abbildung 3.1: Schlüsselaustausch

Aufgrund der dazu beschriebenen Einbußen im Bereich der Nutzerfreundlichkeit kann an dieser Stelle nicht auf die vom Google-Dienst angebotene Funktion verzichtet werden. Der Einladevorgang, der ausgelöst wird, wenn ein Nutzer einen Gast zu einem Termin einlädt, bleibt daher bestehen. Zunächst muss die XML-Struktur eines Termins für die Verwaltung von Gästen um folgende Elemente erweitert werden:

```
<Termin>                                          1
   <Gäste aktiv={true,false}>                     2
      <Gast>                                      3
         <Name> ID_Gast </Name>                   4
      </Gast>                                     5
   </Gäste>                                       6
</Termin>                                         7
```

Codeauszug 3.2: 1. Erweiterung der XML-Struktur eines Termins

Sind keine Gäste für den Termin vorgesehen, so wird die Eigenschaft *aktiv* des Elements *Gäste* entsprechend auf *false* gesetzt. Für die Identifizierung eines bestimmten Nutzers wird ein eindeutiges Identifizierungsmerkmal benötigt. An dieser Stelle wird erneut die Nutzer-eindeutige Mail-Adresse verwendet. Innerhalb der XML-Struktur eines Termins werden nur die tatsächlichen Gäste vermerkt.

Um die tatsächlichen Teilnehmer mittels zusätzlicher Gäste, die scheinbar auch an einem Termin teilnehmen sollen, zu verschleiern, wird die Gästeliste verändert gespeichert. Die tatsächliche Gästeliste kann der XML-Struktur des Termins entnommen werden, da nur diese Gäste entsprechend vermerkt sind. Sei n also die Anzahl der tatsächlichen Gäste, so wird eine Anzahl von Nutzern eingeladen, die größer als n ist. Um keine unbeteiligten Dienst-Nutzer mit scheinbar sinnlosen Termineinladungen zu belästigen, müssen die zusätzlichen Gäste aus einer Menge von Nutzern ausgewählt werden, die ebenfalls über das hier entwickelte Softwareprodukt verfügen. Aus diesem Grund werden die zusätzlichen Gäste mithilfe des Partner-Managements hinzugefügt, da in diesem Verzeichnis alle Nutzer enthalten sind, mit denen das Softwareprodukt gemeinsam genutzt werden kann.

Dieses Verzeichnis ist initial nicht gefüllt. Durch Verwendung des Protokolls zum Schlüsselaustausch, welches in Abschnitt 3.5.3 beschrieben wurde, können neue Partner hinzugefügt werden. Wird ein Nutzer zu einem Termin eingeladen, an dem noch weitere ihm unbekannte Gäste teilnehmen sollen, so werden die öffentlichen Schlüssel dieser Gäste ebenfalls dem Partner-Management hinzugefügt. Sobald dieses Verzeichnis ausreichend gefüllt ist, können zusätzliche Gäste zu Terminen eingeladen werden. Bei der Terminerstellung wird dies entsprechend geprüft. Die Einladungen, die an Nutzer gesendet werden, welche lediglich den Zusatz darstellen, werden fortan als Dummys bezeichnet.

Bekommt der Nutzer eine Termineinladung, ist zunächst nicht feststellbar, ob es sich um einen Dummy oder eine tatsächliche Termineinladung handelt. Das Softwareprodukt erkennt dies nach der Dekodierung des Übertragungs-Schlüssels. Die Filterung erfolgt über die Analyse des Orts-Feldes, in dem die Übertragungs-Schlüssel aller Gäste hinterlegt sind. Nutzer, die lediglich einen Dummy erhalten haben, erhalten statt dem verschlüsselten Termin-Schlüssel eine verschlüsselte Indikator-Zeichenkette. Nach der Entschlüsselung des individuellen Kryptogramms erkennt das Softwareprodukt die Einladung als Dummy. Um zu

verhindern, dass dieser Mechanismus aufgrund stetig wiederkehrender Kryptogramme vom Dienstanbieter erkannt wird, fließt zusätzlich eine zufällige Zeichenkette mit ein. Das Softwareprodukt ist somit in der Lage einen Dummy zu erkennen und entfernt diesen nach einer zufälligen Zeitspanne aus dem Kalender. Diese Zeitspanne imitiert eine individuelle Entscheidung des Nutzers und verschleiert somit die automatisierte Verarbeitung der Einladung. Ist der Nutzer ein tatsächlicher Gast des Termins, erhält dieser nach Dekodierung des Übertragungs-Schlüssels den zum Termin gehörigen Termin-Schlüssel.

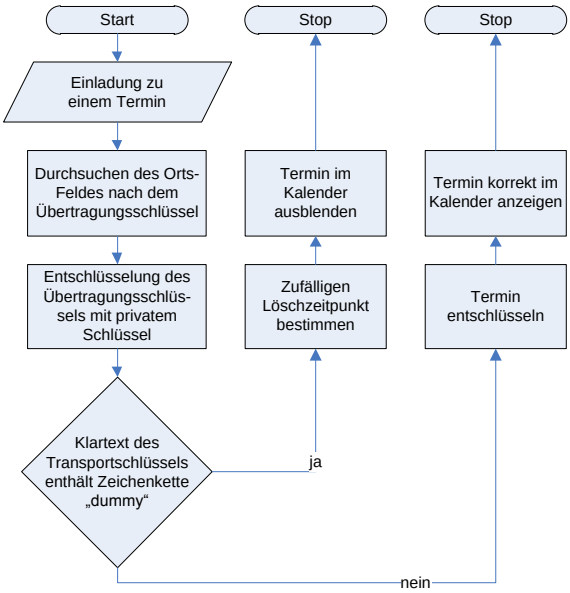

Abbildung 3.2: Filterung von Dummys

Ein tatsächlicher Empfänger einer Termineinladung analysiert bei Empfang ebenfalls das Orts-Feld, in dem alle Übertragungs-Schlüssel hinterlegt sind. Dieses enthält jedoch keine Indikator-Zeichenkette, sondern den verschlüsselten Termin-Schlüssel. Auf diesen wendet er seinen privaten Schlüssel des asymmetrischen Verschlüsselungsverfahrens an, um den unverschlüsselten Termin-Schlüssel zu erhalten. So gelangt jeder tatsächlich eingeladene Gast auch an den benötigten Termin-Schlüssel, um weitere Informationen des Termins zu erhalten und diesen korrekt darzustellen. Ein entschlüsselter Transportschlüssel enthält demnach entweder den Termin-Schlüssel oder die Indikator-Zeichenkette „dummy“ mit zusätzlichen zufälligen Zeichen. Beide Klartexte haben eine identische Länge. Entsprechend haben Termin-Schlüssel die Form „PiADpX5P6v5IyBte“ und verlängerte Indikatorzeichenketten die Form „dummyrYkjvDxuBiY“. Zur Veranschaulichung stellt Abbildung 3.2 dieses Vorgehen grafisch dar.

Anzumerken ist, dass bei steigender Nutzerzahl die Anzahl an Dummys, die ein Nutzer in einem gewissen Zeitraum erhält, verschwindend gering ist. Je mehr Anwender das Softwareprodukt verwenden, desto mehr Nutzer enthält das

Partner-Management eines einzelnen Nutzers. Da aus diesem Pool die Empfänger von Dummys ermittelt werden, ist die Wahrscheinlichkeit, dass ein bestimmter Nutzer eine solche Einladung erhält umso geringer, je größer der Pool ist.

Aus dieser Methodik ergibt sich ein Nachteil. Wie in Kapitel 2.1.2 beschrieben, ist es dem einladenden Nutzer überlassen, ob die Gäste untereinander bekannt gemacht werden oder nicht. Werden alle Gäste in der Ortsangabe hinterlegt, so ist das Verbergen der Gästeliste nicht zwingend gewährleistet. Zwar können diese Details innerhalb der sichtbaren Oberfläche des Kalenders ausgeblendet werden, übertragen werden diese Informationen dennoch und können somit auch sichtbar gemacht werden. Um dies zu umgehen, gilt es zu unterscheiden, ob die Gästeliste sichtbar gemacht werden soll oder nicht. Im erstgenannten Fall wird obiges Verhalten beibehalten. Soll die Gästeliste jedoch verborgen werden, muss für jeden Gast ein eigener Termin erzeugt werden. Das Softwareprodukt muss dann dafür sorgen, dass die Reaktionen der einzelnen Gäste in einem Haupttermin zusammengetragen werden. Damit diese beiden Aspekte erkannt und berücksichtigt werden können, muss anhand eines Indikators entschieden werden, ob die Gästeliste sichtbar sein soll oder nicht. Die Entscheidung obliegt dem Nutzer bei der Auswahl des entsprechenden Feldes während der Erstellung des Termins im *Google Kalender*. Die XML-Struktur wird weiter verfeinert:

```
<Termin>                                                          1
   <Gäste aktiv={true,false} sichtbar={true,false}>               2
      <Gast>                                                      3
         <Name> ID_Gast </Name>                                   4
      </Gast>                                                     5
   </Gäste>                                                       6
</Termin>                                                         7
```

Codeauszug 3.3: 2. Erweiterung der XML-Struktur eines Termins

Das zusätzliche Attribut *sichtbar* stellt den benötigten Indikator dar. Abhängig von der Belegung erstellt das Softwareprodukt einen gesammelten oder jeweils einzelne Termine mit einem Haupttermin, in dem die Informationen zusammenfließen.

Im letzten Schritt sollen alternative Reaktionsmechanismen für eine Einladung in die Lösung eingebettet werden. Wird der *Google Kalender* ohne zusätzliche Software verwendet, werden die Entscheidungen der Gäste an den Dienstanbieter übertragen, welcher diese global für den Termin festhält und an die unterschiedlichen Teilnehmer weitergibt. Um dem Dienstanbieter diese Angaben

ebenfalls vorzuenthalten, muss der Mechanismus zur Reaktion auf eine Termineinladung ersetzt werden. Da die Reaktion für jeden Gast individuell gespeichert werden muss, wird die XML-Struktur um das neue Element *Entscheidung* erweitert:

```
<Termin>                                                                    1
   <Gäste aktiv={true,false} sichtbar={true,false}>                         2
      <Gast>                                                                3
         <Name> ID_Gast </Name>                                             4
         <Entscheidung> {true,false,unknown} </Entscheidung>                5
      </Gast>                                                               6
   </Gäste>                                                                 7
</Termin>                                                                   8
```

Codeauszug 3.4: 3. Erweiterung der XML-Struktur eines Termins

Anhand der Sichtbarkeit der Gästeliste müssen nun die entsprechenden Lösungen diskutiert werden. Ist die Gästeliste nicht sichtbar, so erhält jeder tatsächliche eingeladene Gast eine Einladung zu einem separaten Termin. Weiterhin werden beispielsweise fünf Dummys verschickt, die vom Softwareprodukt des jeweiligen Nutzers wie beschrieben, nach einer zufälligen Zeitspanne gelöscht werden. Diese Zeitspanne imitiert die Entscheidungsfindung eines tatsächlichen Gastes und verhindert, dass Dummys aufgrund ihrer sofortigen Löschung erkannt werden können. Ein tatsächlich eingeladener Gast erhält Einblick in den Termin und entscheidet, ob er den Termin bestätigt, ablehnt oder ob er offen bleibt. Hat sich der Nutzer entschieden, wird ein neuer Termin erzeugt. Dieser trägt eine neue uID im Titel-Feld, enthält aber selbige XML-Struktur im Beschreibungsfeld. Innerhalb der XML-Struktur ist nur ein Gast-Element vorhanden, da andere Gäste nicht sichtbar sein sollen. Daher besteht keine Manipulationsgefahr für den Status anderer Gäste. Die Zuordnung zwischen Termin und Einladung erfolgt über ein zusätzliches Feld innerhalb der XML-Struktur, das den Ursprungstermin durch dessen uID kennzeichnet.

Der Einladende erhält den Reaktions-Termin mit entsprechendem verschlüsselten Termin-Schlüssel. Fünf weitere Nutzer erhalten einen Dummy, sodass der Reaktions-Termin nicht als solcher identifiziert werden kann, da er mehrere Empfänger hat. Der Einladende kann nun mithilfe des Eintrags der uID des Ursprungstermins die Reaktion seiner ursprünglichen Einladung zuordnen und vermerkt die Entscheidung seines Gastes innerhalb des Haupttermins. Nach der Reaktion eines Gastes kann der Reaktions-Termin von diesem Gast gelöscht werden. Abbildung 3.3 stellt diese Vorgehensweise vereinfacht dar.

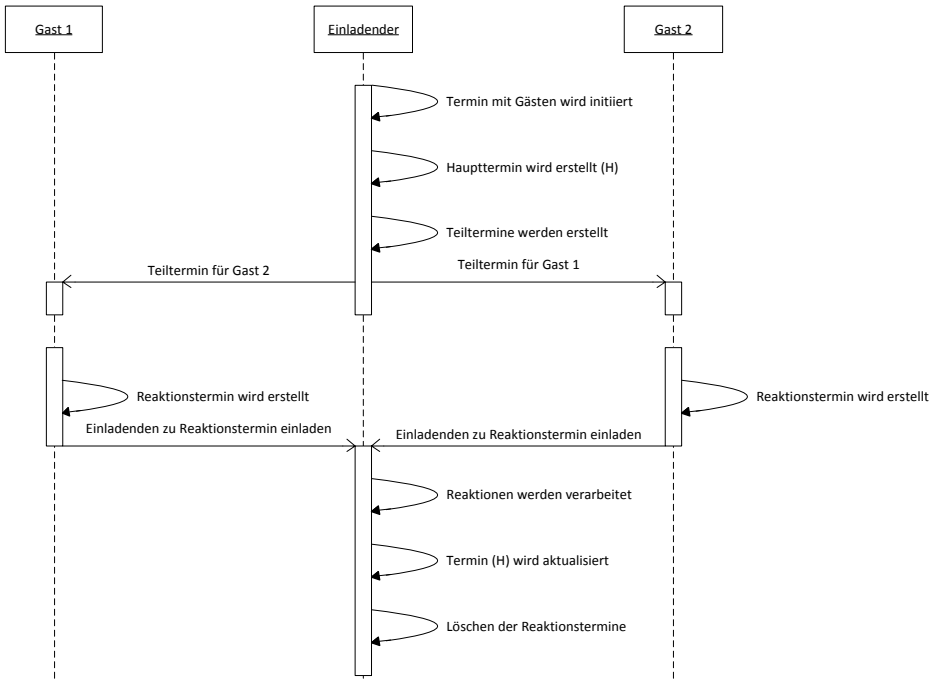

Abbildung 3.3: Terminreaktion bei versteckter Gästeliste

Ist die Gästeliste sichtbar, so muss dafür gesorgt werden, dass jeder tatsächliche Teilnehmer alle anderen über seine Entscheidung informieren kann. Dies setzt voraus, dass jedem Teilnehmer die öffentlichen Schlüssel aller anderen Teilnehmer bekannt sein müssen. Um dies zu gewährleisten, muss der Einladende zu der uID eines weiteren Nutzers ebenfalls dessen öffentliche Schlüssel übertragen. Das Partner-Management der anderen Nutzer greift diese Informationen ebenfalls ab. Der Pool anderer Nutzer, die das Softwareprodukt ebenfalls verwenden, kann so automatisiert erweitert werden. So können mit der Zeit zum einen deutlich breiter gestreute Dummys verschickt werden, zum anderen wird ein initialer Schlüsselaustausch zwischen zwei Nutzern in einer Großzahl der Fälle überflüssig.

Wie bei dem Vorgehen bei nicht sichtbarer Gästeliste, verschickt ein Gast seine Entscheidung innerhalb eines neuen Termins mit neuer uID aber selbiger Beschreibung. Er manipuliert lediglich den Eintrag seines Gast-Elements zur eigenen Entscheidung innerhalb der XML-Struktur. Dazu lädt er alle tatsächlichen Gäste sowie eine bestimmte Menge an Nutzern ein, die jeweils nur Dummys erhalten. Die Liste der tatsächlichen Gäste entnimmt das Softwareprodukt eines

Gastes der XML-Struktur innerhalb der Terminbeschreibung der Einladung. Der ursprüngliche Termin vom Einladenden wird beibehalten, um eine nachträgliche Änderung am Termin sowie das Eintragen nachfolgender Gäste durch den Einladenden zu ermöglichen. Alle Gäste erhalten allerdings stets den aktuellen Status eines anderen Gastes. Wird der Reaktions-Termin beim Einladenden verarbeitet, aktualisiert dieser den Ursprungstermin, indem er dessen XML-Struktur anpasst. Daraufhin löscht dieser den Reaktions-Termin. Nun können alle anderen Gäste diesen ebenfalls löschen, da der Ursprungstermin nun den aktuellen Status des Gastes enthält. Zusätzlich muss sichergestellt werden, dass ein Gast nur seinen eigenen Status, nicht aber den Status eines anderen Gastes manipulieren kann. Um dies zu erreichen sind Änderungen eines bestimmten Gast-Elements nur möglich, wenn dieser als Absender des Reaktions-Termins vermerkt ist.

3.5.5 Abschluss

Abschließend wird veranschaulicht, wie eine Termineinladung an zwei tatsächliche Nutzer sowie ein Dummy an einen weiteren Nutzer bei sichtbarer Gästeliste verschickt wird und welche Informationen jeweils übermittelt werden.

Die am Ende dieses Abschnitts dargestellte XML-Struktur *m* wird mit dem symmetrischen Schlüssel *x* gesichert. Der Termin wird daraufhin an den Kalender übertragen. Das Kryptogramm *x(m)* wird dabei in der Beschreibung des Termins hinterlegt. Die uID des Termins wird als Titel übertragen. Innerhalb des Orts-Feldes werden die öffentlichen Schlüssel *PubK* des Einladenden *A*, sowie der beiden Gäste *B* und *C* mit entsprechenden Übertragungs-Schlüsseln *PubK(x)* übertragen. Das Orts-Feld enthält somit *A, PubK_A, PubK_A(x); B, PubK_B, PubK_B(x); C, PubK_C, PubK_C(x); D, PubK_D, PubK_D(Dummi-Indikator,Zufallszahl)*.

Durch das beschriebene Vorgehen können alle Forderungen des Datenschutzes umgesetzt werden. Das Softwareprodukt ist demnach in der Lage, Termine verschlüsselt im *Google Kalender* zu hinterlegen, die Dauer und die Wiederholung eines Termins zu verbergen und die Informationen zu den Gästen zu verschleiern. Es wird ebenfalls dafür gesorgt, dass diese Informationen rekonstruiert und dem Nutzer wie gewohnt angezeigt werden können. Dazu muss lediglich die Terminbeschreibung, welche die XML-Struktur enthält, entschlüsselt und die enthaltenen Informationen ausgewertet werden. Mithilfe dieser Informationen wird die Ansicht des *Google Kalenders* insofern verändert, dass der Nutzer den Ein-

druck erhält, es hätte sich nichts verändert. Um dies zu erreichen wird mittels JavaScript die DOM-Struktur des Kalenders im Browser manipuliert. Die Termine werden zeitlich neu gesetzt, die Inhalte entschlüsselt und gegebenenfalls eingeladene Gäste dargestellt sowie Wiederholungen erzeugt. Abschließend wird nun die gesamte XML-Struktur eines Termins, welche innerhalb des Beschreibungs-Feldes vorrätig gehalten wird, dargestellt.

```
<Termin>                                                                    1
   <Titel> Beispieltitel </Titel>                                           2
   <Ort> Beispielort </Ort>                                                 3
   <Zeitpunkt manipuliert=true>                                             4
      <Datum> Beispieldatum </Datum>                                        5
      <Uhrzeit> Beispieluhrzeit </Uhrzeit>                                  6
   </Zeitpunkt>                                                             7
   <Wiederholung aktiv=false>                                               8
      <Zeitraum>                                                            9
         <Beginn> </Beginn>                                                 10
         <Ende> </Ende>                                                     11
         <Ausnahmen> </Ausnahmen>                                           12
      </Zeitraum>                                                           13
   </Wiederholung>                                                          14
   <Gäste aktiv=true sichtbar=true}>                                        15
      <Ursprungstermin> ID_Ursprungstermin </Ursprungstermin>               16
      <Gast>                                                                17
         <Name> B </Name>                                                   18
         <Entscheidung> ausstehend </Entscheidung>                          19
      </Gast>                                                               20
      <Gast>                                                                21
         <Name> C </Name>                                                   22
         <Entscheidung> ausstehend </Entscheidung>                          23
      </Gast>                                                               24
   </Gäste>                                                                 25
</Termin>                                                                   26
```

Codeauszug 3.5: Endgültige XML-Struktur eines Termins

3.5.6 Anmerkungen

Bisher wurde nicht betrachtet, dass auch mit Google-Dienst Nutzern interagiert werden könnte, die das Softwareprodukt nicht nutzen. Sollen Gäste eingeladen werden, deren Software nicht in der Lage ist die Manipulationen aufzuheben, so würden diese nur kryptische Termine erhalten, bei denen weder der Inhalt noch der Zeitpunkt erkennbar ist. Um dennoch Nutzer einzuladen, die nicht über das Softwareprodukt verfügen, muss dieses bei der Erstellung von Einladungen er-

mitteln, ob alle Empfänger dieses nutzen. Wer definitiv von dem Softwareprodukt Gebrauch macht, kann über das Partner-Management erfragt werden. Teilnehmer, die das Softwareprodukt zwar nutzen, dem Einladenden aber noch nicht bekannt sind, können zuvor mit der entsprechenden Routine hinzugefügt werden.

Da das Softwareprodukt nun zwischen den Nutzergruppen unterscheiden kann, wird bei der Terminerstellung zunächst geprüft, ob alle gewählten Empfänger laut Partner-Management über das Softwareprodukt verwenden. Ist dies nicht der Fall, wird neben dem verschleierten Termin ein Termin in vollem Klartext und mit korrekten Zeit und Ortsangaben erstellt.

Dieses Vorgehen legt wiederum personenbezogene Daten frei, die ursprünglich geschützt werden sollten. Der einzige Vorteil des Softwareproduktes besteht nun nur noch darin, die Menge der Teilnehmer zu verkleinern. Für alle Empfänger, die über das Softwareprodukt verfügen, wird demnach ein geschützter Termin erstellt, die restlichen Teilnehmer erhalten einen ungeschützten Termin, der nun alle Angaben in Klartext beinhaltet und lediglich weniger Gäste enthält.

Kapitel 4

Entwicklungsvorhaben

Das Entwicklungsvorhaben wird nach den Ansätzen der Grundlagen der Softwaretechnik beschrieben. Zunächst wird das Produkt und dessen Nutzen vorgestellt und die spezifischen Anforderungen formuliert. Aus den Anforderungen gehen im Anschluss die Voraussetzungen für die Infrastruktur des Produkt hervor. Diese werden aufgegriffen und die Umsetzung beschrieben.

4.1 Allgemeine Beschreibung

Das zu entwickelnde Softwareprodukt soll es dem Nutzer ermöglichen, den *Google Kalender* zu nutzen, ohne dem Dienstanbieter die unterschiedlichen personenbezogenen Daten zur Verfügung stellen zu müssen. Die Verwendung des Google-Dienstes soll dabei über die Webseite erfolgen. Der Anwender greift demnach weiterhin mit seinem Browser auf den Dienst zu. Die zusätzlichen Nutzerinteraktionen, die durch das Softwareprodukt zum Schutz der Daten entstehen, sollen dabei möglichst gering gehalten werden. Ein Nutzer muss sich lediglich gegenüber dem Softwareprodukt authentisieren. Abgesehen von dieser Nutzerauthentisierung soll die Bedienbarkeit möglichst identisch mit dem Google-Dienst ohne Schutz personenbezogener Daten gewährleistet werden.

4.1.1 Produkteinbettung

Innerhalb der bestehenden Systemumgebung wird das Softwareprodukt als Erweiterung in einem Browser integriert. Im Rahmen dieser Arbeit wurde der Web-

browser *Firefox* der Mozilla Foundation verwendet. Aufgrund der Trennung von Sicht und Modell, ist eine Einbettung in eine andere Umgebung wie dem Internet Explorer oder speziellen Anwendungen im Bereich der mobilen Endgeräte ebenfalls möglich. Das Firefox-Addon ist nach der Installation in der Oberfläche des Browsers integriert und arbeitet im Hintergrund. Sobald der *Google Kalender* aufgerufen wird, wird die Erweiterung aktiv und passt nach einer Nutzerauthentifizierung die Ansicht des Kalenders an. Im Hintergrund ablaufende Prozesse und Steuerkommandos werden dabei verborgen, sodass der Nutzer den Dienst weiterhin wie gewohnt verwenden kann.

Das Firefox-Addon verwendet die Webschnittstelle des Google-Dienstes. Nach der Nutzerauthentifizierung wird der Anwender explizit um Erlaubnis zur Nutzung dieser Schnittstelle gebeten. Nach erfolgreicher Bestätigung erfolgt eine automatische Authentifizierung des Softwareproduktes mit der Google-Schnittstelle. Diese ermöglicht es, Termine des Kalenders zu erzeugen, zu ändern oder zu löschen. Diese Nutzerinteraktionen werden daraufhin innerhalb der Oberfläche des Kalenders vom Firefox-Addon registriert und in entsprechende Anfragen an die Google-Schnittstelle umgewandelt. Die Elemente der Benutzeroberfläche und damit die Schnittstellen zum Nutzer werden durch ein Menü in der Addon-Leiste von *Mozilla Firefox* sowie durch ein Fenster für Optionen und Einstellungen realisiert. Auf diese Weise kann der Nutzer das Verhalten des Firefox-Addons beeinflussen und beispielsweise Aktualisierungen der Ansicht manuell erzwingen oder neue Partner einladen. Eine weitere Schnittstelle zum verwendeten Betriebssystem ermöglicht es, mithilfe von Funktionalitäten des Browsers benötigte Daten auf der Festplatte abzulegen. Weiterhin werden die Einstellungen des Firefox-Addons als Variablen des Browsers gespeichert. Diese enthalten die Umgebungsparameter und Einstellungen des Browsers und ermöglichen es zudem, globale Variablen eines Firefox-Addons zu sichern[1].

Die Hard- und Softwareanforderungen des Softwareprodukts dieser Arbeit sind abhängig von den Anforderungen des Mozilla Browsers. Systeme, die den Browser unterstützen, ermöglichen demnach ebenfalls die Nutzung des Firefox-Addons. Da dieses über die Funktionen des Browsers auf das Dateisystem zugreift, kann es zu weiteren Einschränkungen kommen. Die Kombinationen von Betriebssystem und Browserversion wurden im Rahmen der Entwicklung nicht

[1]Der Variablenspeicher ist über die Eingabe des Kommandos *about:config* in der Adresszeile des Browsers zu erreichen.

erschöpfend getestet. Da das Firefox-Addon kryptographische Verfahren einsetzt, sollte die verwendete Hardware den daraus resultierenden Anforderungen genügen. Zu den verwendeten Verfahren zählen SHA1, RSA und AES. Da es sich bei dem Kalender-Dienst von Google Inc. um einen Online-Dienst handelt, muss zusätzlich eine Internetverbindung bestehen.

4.1.2 Benutzeranforderungen

Unter optimalen Umständen werden geringe Anforderungen an den Anwender gestellt. Die Ausbildung und technisches Hintergrundwissen sind kaum von Bedeutung. Die grundsätzliche Funktionsweise wird mittels einer Hilfe-Funktion erläutert. Hat der Nutzer die grundlegenden Prinzipien verstanden, ist die Verwendung ohne Probleme möglich. Alle zusätzlichen Dialoge oder Optionen sind zudem ausführlich erklärt. Interessiert sich der Anwender für den genauen Programmablauf und die Sicherheitsmaßnahmen, sind weitreichende Kenntnisse im Bereich des IT-Risk-Managements und insbesondere der Funktionsweise der verwendeten kryptographischen Protokolle erforderlich.

4.2 Anforderungen an das Softwareprodukt

In diesem Abschnitt werden die unterschiedlichen Anforderungen, die an das Softwareprodukt gestellt werden, untersucht. Nach der Betrachtung der funktionalen Anforderungen folgt die Beschreibung der nicht-funktionalen Anforderungen, welche in Benutzerschnittstellen-, Qualitäts- und technische Anforderungen unterteilt sind.

4.2.1 Funktionale Anforderungen

Das Firefox-Addon soll mehrere Nutzer unterstützen. Bei Betreten der Webseite des *Google Kalenders* soll das Softwareprodukt den Nutzer authentifizieren. Um die Fehleranfälligkeit zu verringern, soll dabei nur der beim Google-Dienst angemeldete Nutzer akzeptiert werden. Die Identifizierung soll über ein vom Nutzer gewähltes Passwort erfolgen. Dieses soll beim Betreten der Webseite des Google-Dienstes mithilfe eines Dialogs abgefragt werden. Ist der aktive, also bei Google angemeldete Nutzer dem Softwareprodukt nicht bekannt, so erscheint ein Dialog

zur Erstellung eines Passworts. Die für einen bestimmten Nutzer auf dem Datenträger abgelegten Daten sollen dabei von anderen Anwendern weder lesbar noch manipulierbar sein. Das Datenschutzkonzept aus Abschnitt 3.5 soll möglichst erschöpfend integriert werden. Dabei soll der Funktionsumfang des ursprünglichen Kalender-Dienstes möglichst beibehalten werden. Funktionalitäten, welche durch Anwendung von Mechanismen zum Datenschutz generell nicht funktionieren können, werden im Abschnitt 4.4 erläutert. Das Firefox-Addon soll weiterhin die Nutzung der „normalen“ Kalender-Funktion unterstützen, sodass der Nutzer den Google-Dienst verwenden kann, ohne dass das Softwareprodukt tätig wird. Sollte ein Termin mit einem Nutzer geteilt werden, der das Firefox-Addon nicht nutzt, so wären die im Termin enthaltenen Informationen für den Teilnehmer nicht interpretierbar. Daher muss beim Erstellen eines geteilten Termins beziehungsweise beim Teilen eines bestehenden Termins vom Softwareprodukt geprüft werden, ob eine Sicherung der Privatsphäre für den entsprechenden Termin möglich ist. Zusätzlich ist der Nutzer darüber aufzuklären, dass auch die Partner über das Firefox-Addon verfügen müssen, um den Termin korrekt darzustellen. Die Ein- und Ausgabe soll sich im Wesentlichen nach der bestehenden Oberfläche des Google-Dienstes richten. Durch zusätzliche Schaltflächen soll der Anwender zwischen sicherem und unsicherem Speichern eines Termins unterscheiden können.

4.2.2 Benutzerschnittstellenanforderungen

Solange der Google-Dienst im Browser nicht aufgerufen wird, soll das Firefox-Addon lediglich im Hintergrund arbeiten und die Adresse der aktiven Webseite betrachten, bis es die Adresse des *Google-Kalenders* identifiziert. Da der Nutzer den Dienst angewählt hat, wird die Benutzerauthentisierung initiiert. Dabei gilt es zu unterscheiden, ob der Nutzer dem Softwareprodukt bereits bekannt ist oder nicht. Bei der Verwendung des *Google Kalenders*, soll das Firefox-Addon ebenfalls lediglich im Hintergrund arbeiten, sodass der Nutzer durch die unterschiedlichen Manipulationen nicht irritiert wird. Letztlich soll der Nutzer den Eindruck erhalten, der Kalender habe sich nicht verändert. Lediglich die im Kalender gespeicherten Daten sind so angepasst, dass der Datenschutz weitestgehend gewährleistet wird. Um dem Nutzer die Unterscheidung zwischen gesicherten und ungesicherten Terminen zu vereinfachen, soll die Farbe der sicheren Termine durch eine Option frei wählbar sein.

4.2.3 Qualitätsanforderungen

Das Softwareprodukt sollte nach bestehenden Standards zur Sicherung der Qualität entwickelt werden. Insbesondere soll ein modularer Aufbau dafür sorgen, dass nur eine geringe Anpassung notwendig ist, um beispielsweise die Verschlüsselungsalgorithmen zu ersetzen. Durch Verwendung des Model-View-Controller-Musters[2] soll zusätzlich eine hohe Portabilität gesichert werden. Durch Austauschen der Sicht-Ebene ist so die Verwendung auf einer anderen Plattform denkbar. Weiterhin ist auf die Benutzerfreundlichkeit zu achten. So ist die Oberfläche des Google-Dienstes möglichst beizubehalten. Wenig transparente Vorgänge sollen durch entsprechende Meldungen oder Hinweise an den Nutzer herangetragen werden. Zusätzlich soll bei der Entwicklung des Softwareprodukts auf Effizienz und Wartbarkeit geachtet werden. Dies soll zum einen durch die angewendeten Muster zur Softwareentwicklung erfüllt werden, zum anderen mithilfe durchdachter Funktionalitäten sowie aussagekräftige Kommentierung im Code erreicht werden. Mögliches Fehlverhalten von Nutzer, Software oder Umgebung soll entsprechend behandelt werden. Der Nutzer ist dabei jeweils über die Missstände aufzuklären.

4.2.4 Technische Anforderungen

Wie in Abschnitt 4.2.3 beschrieben, soll das Muster Model-View-Controller und ein modularer Aufbau bei der Entwicklung verwendet werden. Da es sich bei dem Anwendungsgebiet um einen im Internet verfügbaren Dienst handelt, wird eine Internetverbindung vorausgesetzt. Die Implementierung erfolgt in Form eines Firefox-Addons. Dies setzt den Einsatz des Browsers *Mozilla Firefox* voraus. Das zugrunde liegende Betriebssystem soll für das Softwareprodukt möglichst unerheblich sein. Plattform-spezifische Anpassungen, wie beispielsweise das Speichern von Daten auf dem Datenträger wird vom Browser gesteuert. Zur korrekten Funktion muss zusätzlich JavaScript im Browser aktiviert sein. Sowohl das zu entwickelnde Softwareprodukt als auch der Google-Dienst nutzen diese Technologie, um den Inhalt der Webseite dynamisch anzupassen.

[2] Model-View-Controller ist ein Entwurfsmuster, das in der Entwicklung objektorientierter Software verwendet wird und die klare Trennung von Modell, Sicht und Steuerungseinheit vorsieht. Siehe dazu [GHJV10]

4.3 Benötigte Infrastruktur

Dieser Abschnitt beschreibt die benötigte Infrastruktur des Firefox-Addons. Aus den funktionalen Anforderungen im Abschnitt 4.2.1 geht hervor, dass das Firefox-Addon für mehrere Nutzer ausgelegt sein soll. Die dafür benötigte Komponente wird fortan als Nutzer-Management bezeichnet. In Abschnitt 3.5 wurden zudem die Begriffe Schlüssel-Management und Partner-Management eingeführt. Diese drei Komponenten werden im Folgenden näher beschrieben. Dabei wird sowohl auf die Funktionsweise als auch auf den Aufbau eingegangen.

4.3.1 Nutzer-Management

Da auf einem Computer mehrere Nutzer unterschiedliche *Google Kalender* nutzen können ist es notwendig, den Nutzer bei Aufruf des Dienstes durch ein entsprechendes Kennwort zu identifizieren. Der aktive Nutzer wird durch Auslesen eines Feldes der Webseite ermittelt. Auf diese Weise erkennt das Firefox-Addon, welcher Nutzer zum Zeitpunkt des Aufrufs beim Google-Dienst angemeldet ist. So wird vermieden, dass versehentlich falsche Daten geladen werden und folglich fehlerhaftes Verhalten der Software hervorgerufen wird. Nachdem sich ein Nutzer beim Firefox-Addon mithilfe seines Passworts eingeloggt hat, muss dieser den Zugang zu allen benötigten Partnern und Schlüsseln erhalten. Die dem Nutzer zugehörigen individuellen Dateien werden in einem Unterordner des Addon-Verzeichnisses des Browsers hinterlegt und entsprechend dem Nutzer benannt. Bei erstmaliger Anmeldung beim Firefox-Addon werden die Grundgerüste für Partner- und Schlüsselmanagement erzeugt und nach dem Muster *Mail-Adresse_pm.txt* beziehungsweise *Mail-Adresse_km.txt* abgespeichert. Diese Dateien, welche später Partner und Schlüssel enthalten, sind mit dem Nutzerpasswort verschlüsselt und können so von Anderen weder eingesehen noch sinnvoll manipuliert werden. Zur Validierung des Nutzerpasswortes wird bei der Nutzererstellung der Hash des Passworts verwendet. Dieser Hash ist zusammen mit dem Nutzernamen in der Datei des Nutzer-Managements hinterlegt. Beim Login wird der Hash des eingegebenen Passwortes mit dem hinterlegten Hash verglichen. Die Nutzung der Hashfunktion vermeidet, dass ein anderer Nutzer das Passwort aus den auf dem Datenträger hinterlegten Informationen ermitteln kann. Das Nutzer-Management verwaltet die Einträge in einer XML-Datei. Beispielhaft ist der Aufbau wie folgt darzustellen:

```
<Users>                                                                    1
        <User>                                                             2
                <Mail>cryptocalendar@googlemail.com</Mail>                 3
                <Key>8ce87b8ec346ff4c80635f667d1592ae</Key>                4
        </User>                                                            5
</Users>                                                                   6
```

Codeauszug 4.1: XML-Struktur des Nutzermanagements

4.3.2 Partner-Management

Die Notwendigkeit des Partner-Managements wurde bereits in Abschnitt 3.5.3 erläutert. Demnach wird ein asymmetrisches Verschlüsselungsverfahren benötigt, um einen Termin-Schlüssel für einen bestimmten Termin sicher zu einem Gast übertragen zu können. Im Partner-Management werden die bekannten Partner mit dem jeweiligen öffentlichen Schlüssel hinterlegt. Für eine Verbesserung der Effizienz wird der aktive Nutzer mit zugehörigem öffentlichen Schlüssel ebenfalls dort abgelegt.

Das Partner-Management wird mit einem symmetrischen Verfahren geschützt auf dem Datenträger gespeichert. Nach erfolgreicher Nutzerauthentifizierung wird das Nutzerpasswort zur Entschlüsselung verwendet und die Daten temporär in Klartext im Speicher verwaltet. Sollen Gäste zu einem Termin eingeladen werden, so werden beim Partner-Management die öffentlichen Schlüssel der jeweiligen Gäste nachgeschlagen. Die Übertragungs-Schlüssel werden mithilfe der jeweiligen öffentlichen Schlüssel über den Termin-Schlüssel berechnet. Die Übertragungs-Schlüssel werden daraufhin im Orts-Feld eines Termins hinterlegt. Zusätzlich wird zur Erkennung des zum Empfänger passenden Übertragungs-Schlüssels die jeweilig zugehörige Mail-Adresse des Empfängers übertragen. Weiterhin wird der öffentliche Schlüssel selbst übermittelt. Dies fördert zum einen den Austausch der öffentlichen Schlüssel, zum anderen werden diese aus funktionalen Gründen bei der Reaktion auf Einladungen benötigt. Das Orts-Feld enthält demnach Tupel der folgenden Form: „Mail-Adresse des Gastes, öffentlicher Schlüssel des Gastes, Übertragungs-Schlüssel für den Termin; ...“ (siehe dazu auch Abschnitt 3.5.5). Das Partner-Management verwaltet die Einträge in einer verschlüsselten Datei, die entschlüsselt eine XML-Struktur aufweist. Beispielhaft ist der Aufbau wie folgt darzustellen:

```
<PartnerManagement>
        <User>
                <Mail>cryptocalendar@googlemail.com</Mail>
                <Key>Af9XfBa8DH8oFwXMPb2iUophDIY2pJDufiNnwejmLoBCP325mh ... </Key>
        </User>
        <User>
        <Mail>toni.rossberg@googlemail.com</Mail>
                <Key>AQCB70DrvYGW1SVSPjkx7P5xKrXM+yQMDrWou9vPi92qKwAFEQ ... </Key>
    </User>
</PartnerManagement>
```

Codeauszug 4.2: XML-Struktur des entschlüsselten Partnermanagements

4.3.3 Schlüssel-Management

Im Rahmen dieser Arbeit spielt das Schlüssel-Management eine essenzielle Rolle. Alle Termine, die mithilfe des Firefox-Addons erstellt werden, werden mit einem symmetrischen Schlüssel geschützt. Jeder symmetrische Schlüssel wird daraufhin im Dateisystem hinterlegt. Zudem wird für jeden Termin ein eindeutiger Bezeichner erzeugt, die uID, mit deren Hilfe ein bestimmter Termin eindeutig identifizierbar ist. Um den zu einem Termin passenden Termin-Schlüssel im Schlüssel-Management zu finden, wird jeweils nach der entsprechenden uID gesucht. Im Schlüssel-Management wird zusätzlich das RSA-Schlüsselpaar verwaltet. Wird der Nutzer zu einem Termin eingeladen, so benötigt dieser den privaten Schlüssel dieses Schlüsselpaares, um den Termin-Schlüssel des geteilten Termins zu ermitteln.

Um das Arbeiten mit mehreren Systemen zu ermöglichen besteht die Möglichkeit, das Schlüssel-Management zu exportieren. Dabei wird lediglich die XML-Rahmenstruktur inklusive des RSA-Schlüsselpaares in einer Datei gespeichert. Die Termine, welche mithilfe des Firefox-Addon erstellt werden sind so konzipiert, dass der symmetrische Schlüssel mittels des RSA-Schlüsselpaares stets wiederhergestellt werden kann. Dies ermöglicht es zudem, das Schlüssel-Management manuell von überflüssigen Einträgen zu bereinigen.

Das Schlüssel-Management wird ebenfalls mit einem symmetrischen Verfahren geschützt auf dem Datenträger hinterlegt. Nach erfolgreicher Nutzerauthentifizierung wird das Nutzerpasswort zur Entschlüsselung verwendet und die Da-

ten temporär in Klartext im Speicher verwaltet. Das Schlüssel-Management verwaltet die Einträge in einer verschlüsselten Datei, die entschlüsselt eine XML-Struktur aufweist. Beispielhaft ist der Aufbau wie folgt darzustellen:

```
<KeyManagement>                                                          1
    <RsaKeyPair>                                                         2
        <PublicKey>Af9XfBa8DH8oFwXMPb2iUophDIY2pJDufiNnw ... </PublicKey>  3
        <PrivateKey>                                                     4
            <d>0b3e2bc8f18d4b0b74e7a01d10ad11a8a21fbfb697b ... </d>      5
            <p>3582188895631aa42c44175c841da7110b43db9e76c ... </p>      6
            <q>0d821f4a62b522ae32fcd0ddef80c54312b97bcf656 ... </q>      7
            <u>39ce39de10953ef7c0203d4aeb1849e7c934f3d4e2b ... </u>      8
        </PrivateKey>                                                    9
    </RsaKeyPair>                                                        10
    <Event>                                                              11
        <ID>kPgFFtptuTM6dVUy</ID>                                        12
        <Key>SE8QXRjepWGWnw6N</Key>                                      13
    </Event>                                                             14
    <Event>                                                              15
        <ID>zpdPOZT2aYzPwwiY</ID>                                        16
        <Key>OWsju8poEtvvLVcL</Key>                                      17
    </Event>                                                             18
</KeyManagement>                                                         19
```

Codeauszug 4.3: XML-Struktur des entschlüsselten Schlüsselmanagements

Bei der Zeichenfolge „kPgFFtptuTM6dVUy“ handelt es sich um die uID eines Termins. Diese wurde bei der Terminerstellung zufällig erzeugt und im Titel-Feld des Termins gespeichert. Der zugehörige Schlüssel wird als Wert des Tags „Key“ abgespeichert. Im Beispiel lautet dieser „SE8QXRjepWGWnw6N“.

Erhält der Nutzer einen geteilten Termin, so wird zunächst das Orts-Feld analysiert, in dem der Übertragungs-Schlüssel hinterlegt ist. Dieser wird mithilfe des privaten Schlüssels des RSA-Schlüsselpaares ermittelt und ebenfalls im Schlüssel-Management hinterlegt. Dieses Vorgehen erhöht die Effizienz, da so hauptsächlich das symmetrische Verschlüsselungsverfahren angewandt werden muss.

4.4 Einschränkungen des Funktionsumfangs

In diesem und dem vergangenen Kapitel wurde das Datenschutzkonzept sowie das Entwicklungsvorhaben ausgeführt. Dabei wurde ein Vorhaben dargelegt, welches die unterschiedlichen personenbezogenen Daten schützen soll. Die ein-

zelnen Angaben wurden in Abschnitt 2.2.1 aufgezeigt und die an diese Angaben gekoppelten Dienste in Abschnitt 2.2.2 vorgestellt.

Einige Zusatzdienste können bei einem hohen Maß an Datenschutz von Google nicht weiter zur Verfügung gestellt werden. Einige Dienste können allerdings imitiert oder ersetzt werden. Im Folgenden werden die Zusatzdienste auf ihre Funktionstüchtigkeit bei Anwendung des kumulierten Datenschutzkonzeptes geprüft und etwaige Alternativen beschrieben.

Google bietet zwei Zusatzdienste an, die von jeglicher Manipulation beeinflusst werden. Diese Zusatzdienste sind die **Such-Funktion** innerhalb des Kalenders und der Google-Dienst zur **Synchronisierung** beispielsweise zu anderen Terminverwaltungsprogrammen oder zu mobilen Endgeräten mit dem Android Betriebssystem. Sobald eine bestimmte Datengruppe geschützt wird, wird die Funktionalität dieser Dienste eingeschränkt. Werden alle Datengruppen geschützt, so sind diese Dienste gänzlich nicht nutzbar. Durch zusätzlichen Programmieraufwand lässt sich zumindest die Suchfunktion alternativ realisieren.

Da der Datenschutz mithilfe eines Firefox-Addons erreicht werden soll, existiert für die unterschiedlichen Plattformen der Smartphones oder andere Kalendersoftware derzeit keine Möglichkeit, die manipulierten Daten korrekt darzustellen. Für die unterschiedlichen Zielsysteme müssen entsprechend kompatible Softwareprodukte erstellt werden, um die Synchronisierung nutzen zu können.

Die Möglichkeit zur **Erinnerung** per Mail, Popup oder SMS wird durch manipulierte Angaben fehlerhaft oder entfällt. Unter der Annahme, dass sowohl Titel und Ortsangabe, als auch der Beschreibungstext manipuliert werden, kann der Nutzer aus den veränderten Daten keine Informationen über den tatsächlichen Termin erhalten. Er wird somit lediglich daran erinnert, dass er in Kürze irgendeinen Termin wahrnehmen wollte. Wird zusätzlich Datum und Uhrzeit manipuliert, ist die Erinnerungsfunktion komplett unbrauchbar. Die Erinnerung mithilfe einer Mail oder eines Popups kann durch ein zusätzliches Modul innerhalb der Lösung realisiert werden. Der Erinnerungsmechanismus mithilfe von Kurznachrichten benötigt eine entsprechende Infrastruktur und ist daher nicht portierbar.

Durch Manipulation von Datum und Dauer eines Termins wird zusätzlich der Beschäftigungsgrad beeinflusst. Der Zusatzdienst zur **automatischen Terminfindung** zwischen mehreren Teilnehmern ist dann ebenfalls nicht mehr nutzbar. Durch ein entsprechendes Modul kann diese Funktion theoretisch zwar ebenfalls realisiert werden, da diese jedoch auf der Freigabe von Kalenderinformationen

beruht, müsste das Softwareprodukt um einen aufwendigen Mechanismus zur Organisation von Freigaben erweitert werden.

Die **Anzeige der Ortes** mithilfe von *Google maps* ist aufgrund der Manipulation des Ortes nicht möglich. Die Funktion kann durch eine gezielte nicht manipulierte Anfrage an den Kartendienst trotz Verbergen des Ortes weiterhin verwendet werden.

Um eine **Nachricht an alle Teilnehmer** zu versenden, soll der Dienst Nachrichten nur an tatsächliche Empfänger versenden. Die Empfänger von Dummys sollen keine Nachricht erhalten. Um dies umzusetzen kann ein zusätzliches Mail-Modul, welches auch für die Erinnerung verwendet werden würde, genutzt werden.

Abschließend ist festzuhalten, dass bei einer Verbesserung des Datenschutzes auf eine Vielzahl von Funktionen verzichtet werden muss. Einige dieser Funktionen, wie die Anzeige des Ortes, können ersetzt oder vom Nutzer mit geringen Mehraufwand weiterhin verwendet werden. Andere, wie die Erinnerung per SMS oder der Dienst *Google sync*, sind nicht weiter nutzbar.

Kapitel 5

CryptoCalendar

In diesem Kapitel wird das Firefox-Addon *CryptoCalendar* vorgestellt. Zunächst werden Funktionen beschrieben und das Verhalten anhand von Beispielen verdeutlicht. Anschließend wird ein Verständnis über die einzelnen Komponenten und deren Zusammenspiel im Gesamtsystem vermittelt. Im Weiteren wird die Benutzeroberfläche vorgestellt und der Umgang mit dem Firefox-Addon veranschaulicht.

5.1 Verhalten und Funktionen

Dieser Abschnitt vermittelt ein grobes Verständnis über das Verhalten des Firefox-Addons aus Sicht des Anwenders und ermöglicht einen Überblick über den Funktionsumfang des Softwareprodukts. Für diesen Zweck werden einige einfache Szenarien beschrieben, die diese Vorgehensweisen verdeutlichen sollen. Dabei werden bestimmte Teilaufgaben beginnend mit dem initialen Verhalten des Firefox-Addons mithilfe von Sequenzdiagrammen beschrieben und analysiert. Dieses erste Szenario wird in Abbildung 5.1 dargestellt.

Sobald der Browser startet, ist das Firefox-Addon aktiv, befindet sich aber in einem wartenden Modus. Im Allgemeinen arbeitet das Softwareprodukt größtenteils im Hintergrund, sodass dem Nutzer die gewohnte Komfortabilität des Google-Dienstes zur Verfügung gestellt werden kann. Die Termine, welche vom Firefox-Addon geschützt wurden, werden farblich hervorgehoben, sodass der Nutzer leicht zwischen geschützten und ungeschützten Terminen unterscheiden kann.

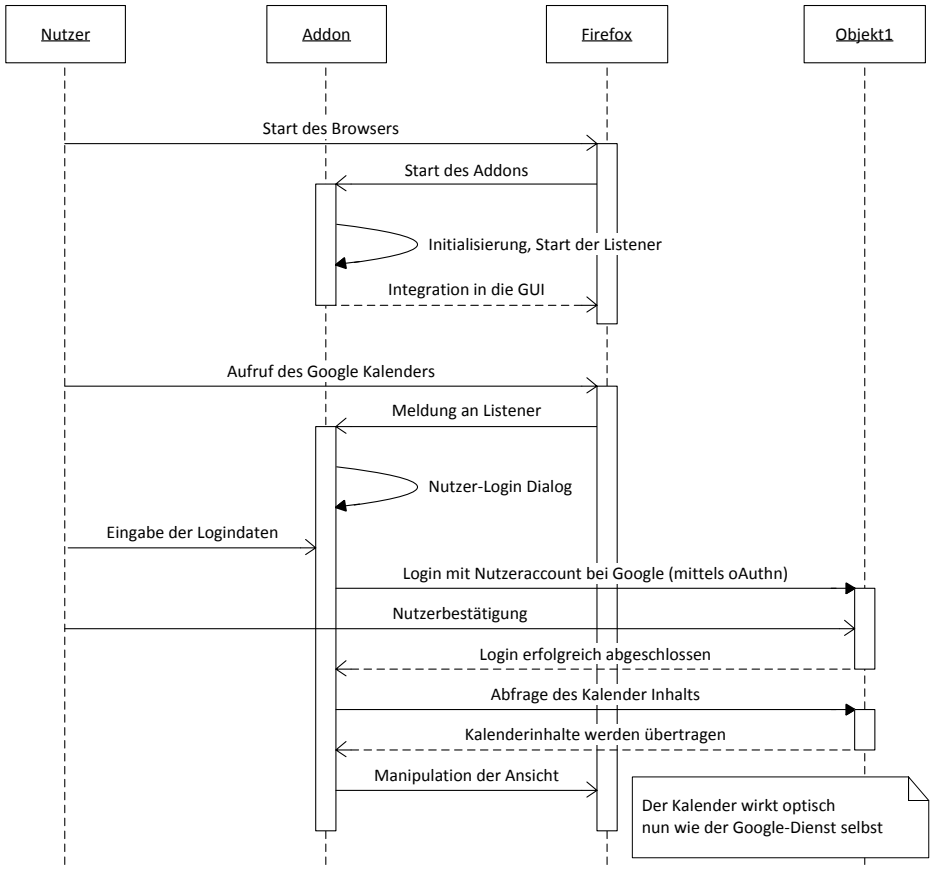

Abbildung 5.1: Initiales Verhalten des Firefox-Addons

Während der Nutzer mit dem Browser arbeitet, wird stetig überprüft, ob es sich bei der momentan angewählten URL um die Adresse des *Google Kalenders* handelt. Insbesondere muss der Nutzer beim Dienstanbieter Google eingeloggt sein. Sind beide Bedingungen erfüllt startet das Firefox-Addon den Login-Dialog. Der Nutzer kann sich nun einloggen. Wird das Firefox-Addon zum ersten mal mit dem Google-Account aufgerufen, erscheint ein Dialog zur Nutzererstellung. Ist der Login abgeschlossen, wird der Kalenderinhalt abgerufen und die Termine im internen Speicher verwaltet. Kalendereinträge werden, wie im kumulierten Datenschutzkonzept in Abschnitt 3.5 beschrieben, geschützt. Termine werden demnach mit einem hybriden System verschlüsselt und mit veränderten Angaben bezüglich Datum und Dauer abgelegt. Ebenfalls werden mögliche Gäste verschleiert. Der genaue Funktionsumfang wird in diesem Abschnitt Schritt für Schritt anhand der entsprechenden Komponenten dargelegt.

Das nun folgende Szenario beschreibt die Erstellung eines Termins, zu dem ein Gast eingeladen wird. Der Nutzer ruft die Terminerstellung wie gewohnt über die Schaltfläche *Termin eintragen* auf und gelangt somit in die Detail-Ansicht eines neuen Termins, in der er die einzelnen Daten eingeben kann. Neben dem vom Google bereitgestellten *Speichern*-Button, erzeugt das Firefox-Addon einen weiteren Button, der mit *Sicher Speichern* betitelt ist. Der Nutzer kann auf diese Weise selbst entscheiden, ob das Firefox-Addon zum Speichern verwendet werden soll oder nicht. Klickt der Nutzer nach Eingabe der Daten auf *Sicher Speichern*, so beginnt das Softwareprodukt mit dem Auslesen der eingebenen Angaben zum Termin.

Das Auslesen wurde mithilfe von xPath realisiert. xPath ermöglicht es, Elemente einer Webseite möglichst genau abzufragen. Dazu wird das Dokument Object Model der Webseite analysiert. Mithilfe von xPath muss daher nicht nach Tag-IDs oder Tag-Namen gesucht und durch die Struktur der Seite navigiert werden, da weitaus detailliertere Anfragen möglich sind. xPath stellt beispielsweise Funktionen zur Verfügung, die Knoten mit einem bestimmten Attribut ermitteln.

Wurden alle Daten aus der Ansicht ausgelesen, werden diese in die unter Abschnitt 3.5.5 beschriebene XML-Struktur eingepflegt. Zu dem Termin wird ein symmetrischer Schlüssel erzeugt, mit welchem die XML-Struktur gesichert wird. Weiterhin wird eine uID erzeugt und diese mit dem Schlüssel im Schlüssel-Management gespeichert. Mithilfe der Informationen über die eingeladenen Gäste werden die öffentlichen Schlüssel der Partner im Partner-Management nachgeschlagen. Mit dessen Hilfe werden die Übertragungs-Schlüssel berechnet. Die gesamten Daten werden in einem Termin-Objekt gespeichert. Im nächsten Schritt wird der Google-Schnittstelle mitgeteilt, dass ein neuer Termin erstellt werden soll. Dabei werden die uID als Titel des Termins, die Liste der Übertragungs-Schlüssel zusammen mit Angaben zu den Mail-Adressen und den öffentlichen Schlüsseln der Partner als Ortsangabe und die gesamten verschlüsselten Termin-Daten (inklusive eigentlichem Ort und Titel) an die Schnittstelle übergeben. Dabei wird das Datum sowie die Dauer des Termins durch zufällige Werte ersetzt. Außerdem werden neben den Einladungen an die tatsächlichen Gäste auch Dummys an zusätzliche Gäste verschickt. Auf diese Weise lässt ein Termin weder Rückschlüsse auf Inhalt oder Datum noch auf die eindeutig involvierten Personen zu.

Nachdem der Termin an Google übergeben wurde, fragt das Firefox-Addon diesen Termin im nächsten Schritt von der Schnittstelle ab. Dies ist nötig, da der

Google-Dienst dem Termin weitere Attribute zuordnet, die nicht im Voraus berechnet werden können. Dazu zählt beispielsweise die Google-ID des Termins, welche bei einer nachträglichen Bearbeitung angegeben werden muss. Nachdem die Antwort des Google-Dienstes ausgewertet wurde, wird das Termin-Objekt um die entsprechenden Daten erweitert und die Ansicht im Browser aktualisiert. Der Nutzer gelangt darauf zur Übersicht der laufenden Woche. Der gesamte Ablauf wird in Abbildung 5.2 detailliert dargestellt.

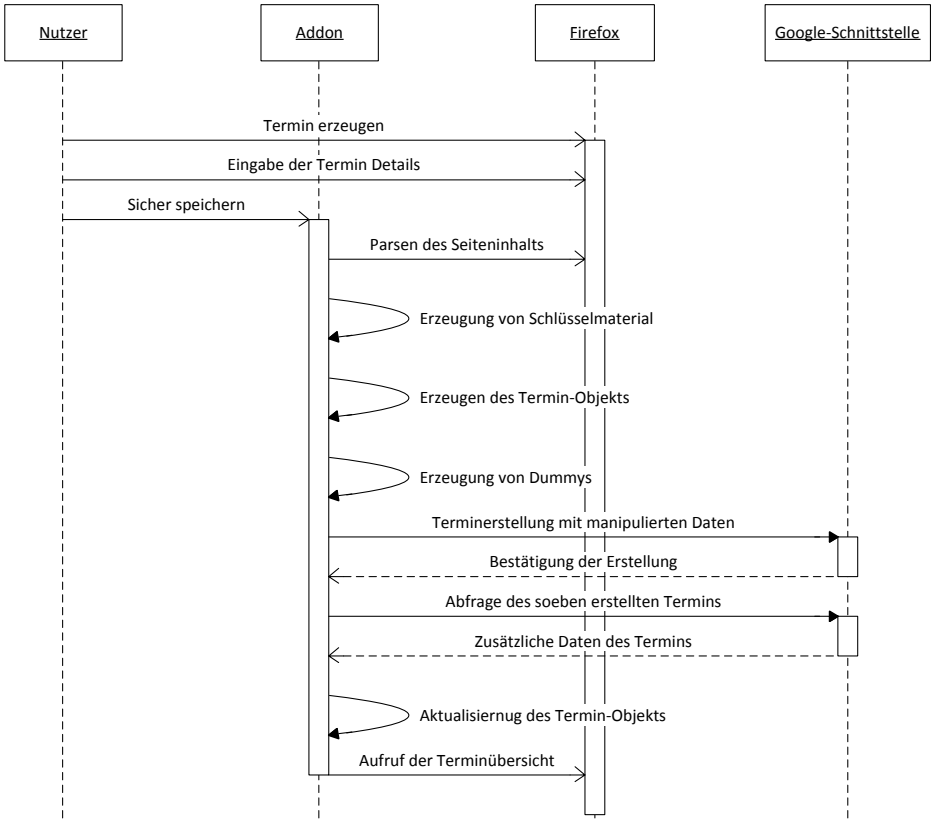

Abbildung 5.2: Erzeugen eines Termins

Soll ein Termin geändert werden, wird der Google-Schnittstelle die Aktualisierung des Termins mitgeteilt. Dabei wird die interne XML-Struktur des Termins an die geänderten tatsächlichen Daten angepasst, mit dem Termin-Schlüssel verschlüsselt und der Schnittstelle mit veränderten Angaben zu Dauer und Zeitpunkt übermittelt.

Eine wesentliche Funktion des Google-Dienstes ist das Einladen von Gästen zu Terminen. Dazu sind bestimmte Anpassungen der Infrastruktur nötig, welche

in Abschnitt 3.5.3 bereits erläutert wurden. Insbesondere das Hinzufügen von Partnern mit dem im genannten Abschnitt dargestellten Schlüssel-Austausch-Protokoll ist essenzieller Bestandteil des Funktionsumfangs des Firefox-Addons. In Abschnitt 3.5.4 wurde zudem die alternative Reaktionsmethode bei Terminen mit Gästen eingehend beleuchtet. Abweichend von dieser Beschreibung wurde im Firefox-Addon auf die Möglichkeit verzichtet, die Gästeliste eines Termins auszublenden. Nach eingehender Analyse zeigte sich, dass der geringe Mehrwert den zusätzlich hohen Implementierungsaufwand nicht rechtfertigt. Als Beispiel sei hier die aufwändige Synchronisierung der einzelnen Teiltermine genannt, welche im Rahmen des kumulierten Datenschutzkonzeptes in Abschnitt 3.5.4 beschrieben wurde.

Das zuvor beschriebene Szenario hat die Erzeugung eines Termins aus Sicht des Einladenden ausführlich beschrieben. Beim Empfänger wird der Termin nun registriert und der Termin-Schlüssel mithilfe des Übertragungs-Schlüssels ermittelt, sodass der Termin in Klartext in korrekter Form angezeigt werden kann. Die Symbolik von Einladungen des Google-Dienstes wurde dabei übernommen. Entsprechend wird ein Symbol mehrerer Köpfe angezeigt. Öffnet der Nutzer den Termin, so kann er sich wie gewohnt entscheiden, ob der Termin bestätigt, abgelehnt oder als offen gekennzeichnet werden soll. Hat der eingeladene Nutzer eine Reaktion festgelegt und *Sicher Speichern* gewählt, wird ein neuer Termin - der Reaktionstermin - erzeugt. Dieser Termin hat eine eigene uID, besitzt aber die selbe interne XML-Struktur, wie die Einladung. Diese Struktur ist dahingehend manipuliert, dass der Eingeladene seine Entscheidung hinterlegt hat. Zu diesem Termin werden der Gastgeber und alle weiteren Gäste eingeladen.

Der Gastgeber erhält nun einen neuen Termin, der lediglich zur Publikation der Reaktion des Gastes erstellt wurde. Erkennt das Softwareprodukt einen solchen Reaktions-Termin, wird die Reaktion des Gastes und somit des Urhebers des zweiten Termins extrahiert und in die XML-Struktur des ersten Termins eingepflegt. Dabei wird nur der Teil der XML-Struktur überprüft, der dem Urheber des Reaktions-Termins zuzuordnen ist. Somit wird sichergestellt, dass kein Gast die Reaktion eines anderen Gastes manipulieren kann. Nach der Verarbeitung des Reaktions-Termins wird dieser beim Gastgeber gelöscht. Da der Reaktions-Termin die uID der ursprünglichen Einladung enthält, kann der Reaktions-Termin eindeutig einer Einladung zugeordnet werden.

Der Gast erkennt die korrekte Verarbeitung nun daran, dass der Gastgeber den Reaktions-Termin aus seinem Kalender entfernt hat. Dies wir dadurch deutlich, dass der Google-Dienst die Reaktion des Gastgebers im Reaktions-Termin als abgelehnt markiert. Den Status des Gastgebers entnimmt der Gast dabei den von Google übermittelten Status-Daten der Gäste des Reaktions-Termin. Sobald dieser Fall eintritt, kann der Gast den Reaktions-Termin löschen. Damit ist die Übermittlung der Entscheidung abgeschlossen. Diese Methodik führt dazu, dass der Gastgeber erst aktiv werden muss, bevor die Reaktion eines Gastes in den eigentlichen Termin - die Einladung - eingeht. Daher werden neben Dummys auch alle anderen Gäste zu einem Reaktions-Termin eingeladen, sodass dieser temporär dazu verwendet werden kann, den aktuellen Status eines Gastes anzuzeigen. Der Gastgeber muss den ursprünglichen Termin demnach nicht erst anpassen, damit anderen Gästen die Entscheidung publiziert wird. Ebenfalls kann es passieren, dass ein Gast seine Entscheidung mehrmals ändert, ohne dass der Gastgeber eine Reaktion analysiert und verarbeitet hat. Um Fehler zu vermeiden wird lediglich der letzte Reaktions-Termin gehalten. Erneuert ein Gast seine Entscheidung, so löscht dieser alte und noch nicht registrierte Entscheidungen, sodass nur die letzte Reaktion verteilt wird.

Zur Veranschaulichung wird in Abbildung 5.3 ein Szenario visualisiert in dem der Gastgeber einen Gast zu einem Termin einlädt und dieser seine Entscheidung einmal erneuert, ohne dass der Gastgeber die Reaktion vorher verarbeitet hat.

Das Firefox-Addon unterscheidet bei der Aktualisierung der Ansicht zwischen dem Aktualisieren des Kalenderinhalts und dem Aktualisieren der derzeitigen Ansicht im Browser. Ersteres wird im Weiteren als Scannen des Kalenders bezeichnet. Bei der Aktualisierung der Ansicht wird der intern verwaltete Datensatz der geschützten Termine verwendet, um die aktuelle Ansicht im Browser anzupassen. Das Scannen des Kalenders ist nötig, da bestimmte Situationen vom Softwareprodukt nicht erkannt werden können, ohne die gesamten Kalenderinhalte erneut von der Google-Schnittstelle abzufragen. Dazu zählen das Eintreffen einer Reaktion auf eine Termineinladung oder eine Partneranfrage. Da bei der Abfrage des gesamten Kalenders vergleichsweise große Datenmengen mit dem Server ausgetauscht und eine Vielzahl interner Operationen durchgeführt werden, wird der Scan des Kalenders nur periodisch und nicht bei jeder Nutzerinteraktion mit dem Google Dienst durchgeführt. Die Zeit zwischen den Scans kann in den Optionen des Firefox-Addons angepasst werden.

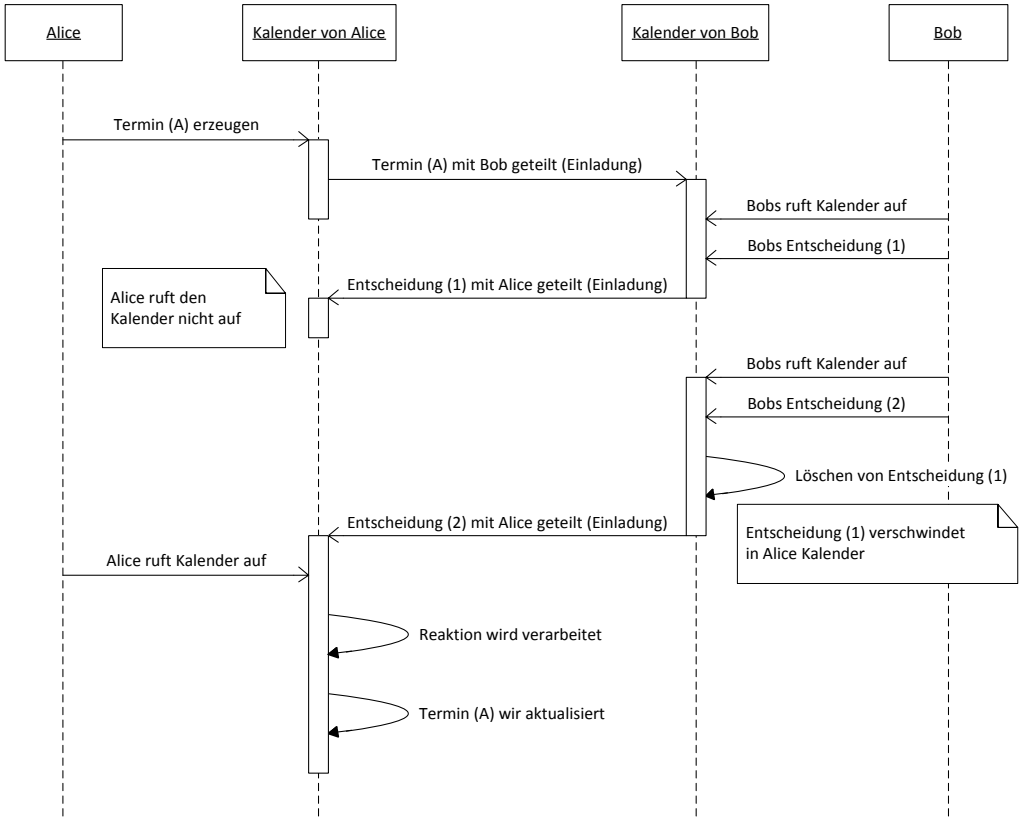

Abbildung 5.3: Reagieren auf einen Termin

Nun soll die Manipulation der Ansicht des Kalenders im Browser erläutert werden. Um dies zu bewerkstelligen wird zunächst die Perspektive innerhalb des aktuellen Browserfensters ermittelt. Dazu zählen beispielsweise die Wochenübersicht, die Tagesübersicht oder die detaillierte Ansicht eines Termins. Entsprechend dieser Zuordnung wird die Ansicht im Browser auf unterschiedliche Weise angepasst. Bei einer Übersicht blendet das Softwareprodukt alle Termine aus, die es als geschützt identifizieren konnte. So wird vermieden, dass aufgrund der Verschiebung von Terminen fälschlicherweise solche Termine angezeigt werden, die eigentlich zu einem völlig anderen Zeitpunkt stattfinden. Weiter wird geprüft, welche Tage angezeigt werden. Daraufhin sucht das Firefox-Addon nach allen Terminen, die an den gefundenen Tagen anzuzeigen sind und fügt diese in die Ansicht ein. Die Parameter über die Start- und Endzeitpunkte bestimmen dabei die Position sowie die Höhe des darzustellenden Termins. Wird eine Detailan-

sicht eines geschützten Termins angezeigt, so entfernt das Firefox-Addon den Inhalt der Felder für Titel, Ort und Beschreibung und ersetzt den Inhalt durch die entsprechenden Werte des Termins, welche aus der entschlüsselten XML-Struktur extrahiert wurden. Bei geteilten Terminen werden diese Felder von Google im Normafall erst in Textfelder umgewandelt, wenn der Nutzer diese anklickt. Daher werden die bei Einladungen angezeigten Felder zunächst angepasst und somit in Textfelder umgewandelt. Weiterhin wird der eigene Status sowie der Status der eingeladenen Gäste angepasst.

Aufgrund des hohen Implementierungsaufwandes werden nicht alle Ansichten des Kalenders unterstützt. So werden die Inhalte der *Kalenderübersicht*, in der eine geringe Anzahl von Terminen in einer Listenansicht angeordnet werden sowie die *Monatsansicht*, die an einen klassischen Kalender erinnert und jeden Tag des Monats durch ein Quadrat repräsentiert, vom Firefox-Addon nicht manipuliert. Beide Ansichten enthalten eine Vielzahl von Spezialfällen oder sehr dynamische Inhalte, sodass der zusätzliche Vorteil den Aufwand der Integration dieser beiden Ansichten nicht rechtfertigt.

Abschließend soll beschrieben werden, wie das Firefox-Addon erkennt, wann es aktiv werden muss. Dazu werden unterschiedliche Listener verwendet. Diese warten auf Ereignisse, beispielsweise zuvor festgelegte Aktionen der Nutzer, die bei der Nutzung des Dienstes auftreten können und lösen daraufhin Aktivitäten der Software aus.

Bei der Initialisierung werden jeweils ein Eventlistener und ein Progresslistener registriert, welche zum einen den Tabwechsel innerhalb des Browsers überwachen und zum anderen benachrichtigt werden, wenn eine Webseite im aktuellen Tab des Browsers komplett geladen wurde. Auf diese Weise kann das Firefox-Addon feststellen, wann der Nutzer in einen Tab wechselt, in dem der Kalender bereits geladen ist oder einen neuen Aufruf des *Google Kalenders* im aktuellen Browsertab durchführt. Nicht jeder Seitenwechsel bewirkt allerdings ein erneutes Laden des Seiteninhalts. Verwendet der Nutzer beispielsweise den *Zurück*-Button des Browsers oder des *Google Kalenders*, um zur vorherigen Seite zu gelangen, wird ein Teil der Seite aus dem Cache des Browsers abgerufen und nur die aktualisierten Inhalte nachgeladen. Um diese Vorgänge zu erkennen wird der Progresslistener erweitert, um auf jede Änderung der URL zu reagieren. Innerhalb der Tagesübersicht oder Wochenübersicht können dynamisch

Termine erzeugt oder verändert werden. Dabei wird weder die Adresszeile geändert, noch komplette Seiteninhalte neu geladen. Es werden jedoch Daten mit dem Server ausgetauscht und die Elemente im Browserfenster aktualisiert. Die vom Firefox-Addon durchgeführten Anpassungen der Ansicht gehen dadurch verloren. Dieser mit dem Server durchgeführte Datenaustausch wird durch einen Observer überwacht, welcher bei diesen Ansichten hinzugeschaltet wird. Ein Observer überwacht eine festgelegte Komponente, wie beispielsweise Antworten eines Servers und kann ähnlich einem Listener bestimmte Aktivitäten der Software auslösen. Der Observer wird über jeden Verkehr auf dem http-Kanal informiert und registriert somit jede Anfrage an den Server. Sobald eine Antwort eintrifft, werden die entsprechenden Routinen gestartet, um die Ansicht innerhalb des Browsers anzupassen. Da dieser Listener innerhalb der anderen Ansichten nicht benötigt wird, wird er entfernt, sobald eine neue Ansicht vom Firefox-Addon festgestellt wird.

5.2 Aufbau

Das Softwareprodukt CryptoCalendar wird als Addon in den Mozilla Browser Firefox eingebunden. Durch den modularen Aufbau des Browsers können mittels Overlays Inhalte von Drittanbietern in das normale Layout des Browsers nachgeladen werden. Auf diese Weise werden zusätzliche Menüs, Buttons oder Statusmeldungen im Browser integriert. Das implementierte Firefox-Addon wird beim Starten des Browsers ebenfalls geladen und aktiviert seine Funktionen. Im Folgenden wird nun der interne Aufbau des Softwareprodukts beschrieben.

Das Firefox-Addon besteht aus mehreren Komponenten, die sich im Wesentlichen in die Kategorien Datenhaltung, Sicht und Logik unterteilen lassen. Die Komponente *CalendarEvent* stellt den Container für einen Termin dar. Die Komponente *CalendarInteractor* steuert die Interaktion mit der sichtbaren Oberfläche innerhalb des Google-Dienstes. Die Komponenten *CalendarCommunicator*, *Controller* sowie die Komponenten für *Key-, Partner- und Nutzermanagement* halten die Programmlogik. Letztere werden im Abschnitt 4.3 genauer erläutert. Weitere Module kapseln den Zugriff auf den Datenträger, die Verschlüsselungsalgorithmen und die Authentifizierung beim Google-Dienst. Die folgende Abbildung 5.4 visualisiert die Komponenten und deren Zusammenspiel. Dabei stellen die Pfeile den Zugriff einer Komponente auf eine andere dar.

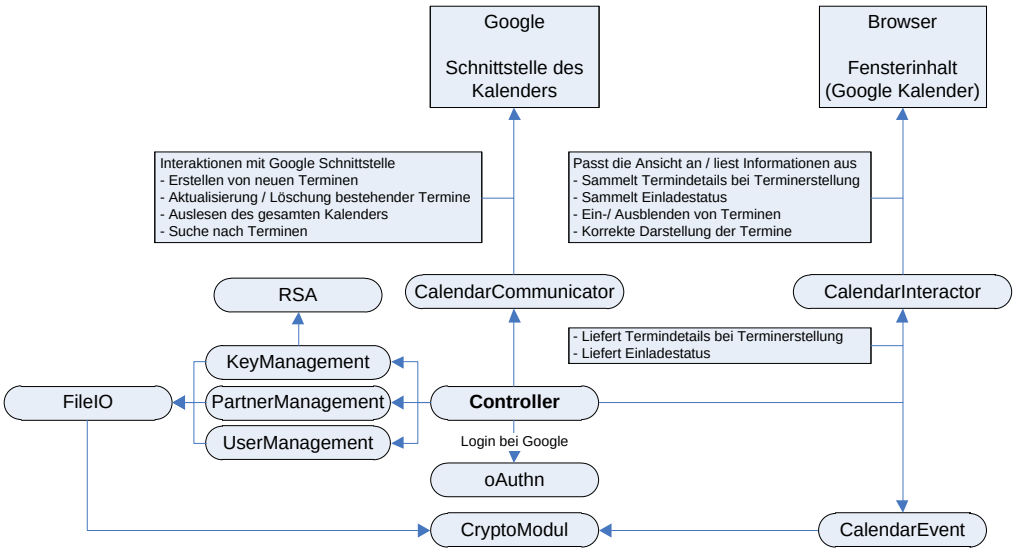

Abbildung 5.4: Klassenstruktur des Firefox-Addons

Die Kernkomponente *Controller* steuert das Firefox-Addon, indem es die unterschiedlichen Funktionalitäten der anderen Komponenten gezielt und zweckgebunden aufruft. Das Verhalten des *Controllers* wird dabei in erster Linie durch den Benutzer gesteuert. Beim Start des Firefox-Addons ruft der *Controller* die Management-Komponenten auf, welche per Dateizugriff die verschlüsselten Inhalte vom Datenträger laden und diese mithilfe der Logindaten des Nutzers und durch Verwendung des *CryptoModuls* entschlüsseln. Daraufhin baut das Firefox-Addon mit der Komponente *CalendarCommunicator* eine Verbindung zur Schnittstelle des *Google Kalenders* auf. Dabei wird die Authentifizierungsmethode *oAuthn* verwendet, welche in der gleichnamigen Komponente implementiert ist. Nach der erfolgreichen Authentifizierung werden die Termine des Kalenders über diese Schnittstelle abgefragt und die Ansicht im Browser durch Funktionen des *CalendarInteractors* manipuliert. Der *Controller* übernimmt dabei die Verwaltung der Termine mithilfe eines Arrays vom Datentyp *CalendarEvent*.

5.3 Komponenten

Im Abschnitt 5.2 wurden die einzelnen Komponenten und deren Zusammenspiel vorgestellt. Im Folgenden werden diese im Detail betrachtet sowie die Funktionen und die Arbeitsweise individuell beleuchtet.

Die Komponente *FileIO* steuert den Zugriff auf das vorherrschende Dateisystem. Es befähigt den Browser Dateien vom Datenträger zu lesen und auf diesen zu schreiben. Die Rechte des Firefox-Addons sind dabei abhängig von den Rechten des Browsers. Die Daten des CryptoCalendars werden innerhalb der Verzeichnisstruktur der Anwendungsdaten von Firefox abgelegt. Der Browser verfügt im Normalfall über ausreichende Rechte für dieses Verzeichnis. Die Komponente *FileIO* verfügt über Methoden zum Initialisieren, Laden, Speichern und Überprüfen der Dateien. Loggt sich ein Nutzer beim Firefox-Addon ein, so wird zunächst überprüft, ob die entsprechenden Daten auf dem Datenträger zu finden sind. Es wird zwischen drei Dateitypen unterschieden. Die Datei „users.xml“ beinhaltet alle bekannten Nutzer sowie die Hashwerte des jeweiligen Nutzerpassworts zur Validierung beim Login. Für jeden Nutzer werden zudem zwei Nutzer-spezifische Dateien angelegt. Diese folgen nachstehendem Bezeichnungsmuster: „Mail-Adresse des Nutzers“ gefolgt vom Postfix „_km“ beziehungsweise „_pm“. Bei diesen Dateien handelt es sich um verschlüsselte XML-Dokumente, die jeweils die Daten des Partner-Managements und des Schlüssel-Managements enthalten. Bei der Initialisierung wird jeweils zwischen Nutzer-, Partner und Schlüsselmanagement unterschieden sowie die Existenz der entsprechenden Dateien überprüft und falls nötig die initiale Struktur erzeugt und gespeichert. Die Methoden zum Laden und Speichern bedienen sich jeweils den Funktionalitäten des *CryptoModuls*, welches die Algorithmen für Ver- und Entschlüsselung beinhaltet. Zusätzlich besteht die Möglichkeit mittels einer weiteren Methode Zeichenketten in einer Datei zu sichern. Diese Funktion wurde zu Debug-Zwecken verwendet.

Im Folgenden werden die Management-Komponenten, welche im Abschnitt 4.3 als infrastrukturelle Anforderungen bereits beschriebenen wurden, betrachtet. Das Nutzermanagement wurde in der Komponente *UserManagement* realisiert. Dieses startet die Dialoge für den Login sowie für die Nutzererstellung über entsprechende Methoden. Das *KeyManagement* enthält die folgenden Funktionen: Erstellung des RSA-Schlüsselpaares mithilfe der Komponente *RSA*, die Erstellung und Sicherung für den symmetrischen Schlüssel eines Termin, Erstellung des Übertragungs-Schlüssels eines Termins, Finden eines symmetrischen Schlüssels zu einer bestehenden uID, Entfernen eines symmetrischen Schlüssels beim Löschen eines Termins sowie einer Methode zur Berechnung des symmetrischen Termin-Schlüssels aus den Übertragungs-Schlüsseln bei geteilten Terminen. Da

das *PartnerManagement* zur Organisation der Partner eines Nutzers verwendet wird, sind in dieser Komponente Funktionen zum Speichern, Finden oder Löschen eines Partners vorhanden. Zusätzlich übernimmt diese Komponente die Generierung einer Empfängerliste, in der auch Dummys enthalten sind, um die unter Abschnitt 3.4 beschriebene Problematik zu lösen, die dazu führt, dass die Gäste eines geteilten Termins verschleiert werden.

Die Komponente *oAuthn* dient der Authentifizierung des Firefox-Addons mit der Google-Schnittstelle. Mithilfe dieses Mechanismus kann es Drittanbietern durch die Einwilligung des Google-Nutzers gestattet werden, auf Nutzer-generierte Daten zuzugreifen und diese zu verändern. Das Firefox-Addon beansprucht lediglich den Zugriff auf den *Google Kalender*. Mit einem entsprechenden Dialog nach der Nutzerauthentifizierung des Firefox-Addons wird dieser von Google mithilfe eines Dialogs transparent um diese Einwilligung gebeten. Zudem ist diesem Dialog eine Meldung des Softwareproduktes vorgeschaltet, die den Nutzer über die Notwendigkeit der Zustimmung aufklärt. Mithilfe dieser Schnittstelle ist es dem Firefox-Addon möglich, Inhalte des Kalenders abzufragen, zu ändern oder neue Inhalte hinzuzufügen.

Diese Aufgaben erfüllt die Komponente *CalendarCommunicator*. Diese kommuniziert direkt mit der Schnittstelle und reagiert auf deren Antworten. Die Komponente verfügt über zwei Methoden, um Kalendereinträge hinzuzufügen. Dabei handelt es sich zum einen um die Quickadd-Funktion des Kalenders, zum anderen ist eine stark Parameter-gebundene Methode implementiert. Erstere wird separat von Google angeboten und soll den Nutzern das Hinzufügen von Einträgen erleichtern. Dabei sollen allgemeine Kurzbeschreibungen in natürlicher Sprache genug Informationen bereitstellen, um diese maschinell verarbeiten zu können. Bisher ist diese Funktion nur in englischer Sprache verfügbar und erlaubt Phrasen wie: „Language Class every Wednesday 7-8pm for 5 months in Atlanta“ [Goo11a]. Sobald die deutsche Unterstützung verfügbar ist, kann diese Methode dem Funktionsumfang hinzugefügt werden. Die Parameter-gebundene Variante erfordert die Eingabe aller für einen Termin erforderlichen Felder und wird vom Firefox-Addon bei der Erstellung neuer Termine und bei Änderungen von Terminen verwendet. Weiterhin sind Methoden zur Abfrage des Kalenders implementiert, welche auf einer Zeitspanne oder einer zu suchenden Zeichenkette basieren. Diese werden hauptsächlich für die initiale und regelmäßige Abfrage

des Kalenders in einem festgelegten Zeitintervall benötigt. Mithilfe dieser Komponente ist es ebenfalls möglich, bestehende Termine zu löschen oder zu verändern.

Die Komponente *CalenderInteractor* steuert die Interaktion mit der Kalenderansicht im Browser und ist somit der dynamische Teil der Sicht-Ebene. Wird der Kalender im Browserfenster angezeigt, so ermittelt diese Komponente zunächst die angezeigten Tage. Die Ansicht wird analysiert und Einträge, welche vom Firefox-Addon erzeugt wurden, anhand ihrer 16-stelligen uID erkannt. Diese Termine, die möglicherweise von den eigentlichen Zeitangaben innerhalb des Termins abweichen, werden von jeweils einer Methode dieser Komponente markiert und im nächsten Schritt ausgeblendet. Mithilfe des Wissens über die in der aktuellen Ansicht angezeigten Tage ermittelt das Firefox-Addon, welche der Termine des Kalenders angezeigt werden müssen. Diese werden in der Ansicht dynamisch erstellt und dem Nutzer im gewohnten Layout präsentiert. Zu diesem Zeitpunkt wurde der korrekte Titel, das Datum sowie die Zeitangaben und Dauer des Termins bereits aufgelöst, sodass dem Nutzer der geschützte Termin auf die bekannte Weise angezeigt wird. In den Optionen des Firefox-Addons ist eine Anpassung der Farbe der geschützten Termine möglich, wodurch diese gesondert hervorgehoben werden können. Sollte ein geteilter Termin angezeigt werden, so sorgt diese Komponente ebenfalls für die korrekte Anzeige des eigenen Status. Des Weiteren ist diese Komponente auch beim Einlesen neuer Termine aktiv. Wird die Seite zur Erstellung oder Bearbeitung eines Termins aufgerufen, so werden die Buttons zum Speichern und Löschen angepasst. Der Button *Sicher speichern* wird bei der Neuerstellung eines Termins neben dem ursprünglichen Button angezeigt, um den Nutzer die klassischen Funktionen des Google-Dienstes auch weiterhin bereitzustellen. Bei der Bearbeitung eines vom Firefox-Addon erzeugten Termins wird dieser Button ausgeblendet. Will der Nutzer einen neuen Termin oder eine Änderung eines bestehenden Termins mithilfe des Firefox-Addons speichern, so analysiert die Komponente *CalenderInteractor* die Eingabefelder sowie die Liste der Gäste und übergibt diese an die Steuerkomponente.

Die Komponente *Controller* stellt diese Steuereinheit dar. Sie bildet den Kern des Firefox-Addons und organisiert die Ausführung der anderen Komponenten. Entgegen dem Model-View-Controller-Entwicklungsmuster befindet sich al-

lerdings ebenfalls ein Großteil der Logik in dieser Komponente. Beim Start des Browsers wird eine initiale Methode aufgerufen, die entsprechende Listener erzeugt, um sowohl die aktuelle URL, als auch einen Tabwechsel zu erkennen. Bei diversen Nutzerinteraktionen wird auf diese Weise eine Routine zum aktualisieren der Ansicht gestartet. Wird die URL des Google-Kalenders erstmalig angewählt, so startet diese Komponente den Dialog zur Nutzerauthentifizierung. Die Komponente verwaltet nach erfolgreichem Login die Schlüssel- und Partnermanagement-Daten im temporären Speicher. Sobald der Nutzer innerhalb des Kalenders aktiv ist, werden stetig neue Daten vom Google-Server übertragen und die Ansicht des Kalenders aktualisiert. Diese Aktualisierungen erkennt das Firefox-Addon und führt die nötigen Schritte aus, um dem Nutzer die geschützten Inhalte korrekt anzuzeigen. Der *Controller* initiiert ebenfalls die Anmeldung an der Google-Schnittstelle. Wird diese Anmeldung vom Nutzer abgebrochen oder das Loginfenster beim Aufruf des Kalenders geschlossen, so sorgt diese Komponente für die Deaktivierung des vollen Funktionsumfangs, sodass der Nutzer nicht durch stetig aufkommende Fenster gestört wird. Beim Schließen des Browsers wird zudem die Verbindung zur Google-Schnittstelle beendet und die Listener entfernt.

Nach Aktivierung der Google-Schnittstelle baut der *Controller* eine interne Verwaltung aller geschützten Termine auf. Dies vermindert die Anfragen an die Google-Schnittstelle, erleichtert den Zugriff auf diese Daten und erhöht die Effizienz des Softwareprodukts. Der *Google Kalender* wird in einem eingestellten Zeitintervall erneut von der Schnittstelle abgerufen und nach 16-stelligen Terminen durchsucht, zu denen ein Schlüssel in der Schlüssel-Verwaltung zu finden ist. Sollte ein solcher nicht gefunden werden, so wird in der Ortszeile des Termins, in der die Übertragungs-Schlüssels hinterlegt sind, nach dem geeigneten Schlüssel gesucht. Wird dieser ebenfalls nicht gefunden, wertet die Komponente den 16-stelligen Termin als einen nicht dem Firefox-Addon zugehörigen Termin. Alle gefundenen Termine werden intern in einem Array verwaltet. Jeder Termin wird dabei als eigenständiges Objekt hinterlegt. Der Objekttyp lautet *CalendarEvent*. Jedes dieser Objekte enthält einige essenzielle Elemente wie Autor oder den direkten Link sowie die XML-Struktur, welche im Abschnitt 3.5.5 spezifiziert ist. Die beim Google-Dienst abgerufenen Daten werden vom *Controller* den Objekten durch Parsen hinzugefügt. Bei der Abfrage des Kalenders werden zudem Reaktionen auf Termineinladungen und Anfragen zum öffentlichen Schlüssel des

RSA-Schlüsselpaares erkannt. Bei Letzterem wird der öffentliche Schlüssel des anfragenden Partners automatisch im Partner-Management des Nutzers gespeichert und die entsprechende Antwort an den Anfragenden gesendet. Der Austausch der öffentlichen Schlüssel verwendet dabei das unter 3.5.3 beschriebene Protokoll. Bei den Reaktionen auf Termineinladungen unterscheidet der *Controller* zwischen Terminen, die der Nutzer selbst erzeugt hat und zu denen Reaktionen erwartet werden sowie eigenen Reaktionen, bei denen darauf gewartet wird, dass der Einladende entsprechend auf die Reaktion des Nutzers reagiert hat. Im erstgenannten Fall wird die Reaktion der Eingeladenen verarbeitet und der Reaktions-Termin beim Nutzer gelöscht. Der Eingeladene Nutzer erkennt dieses Verhalten und kann so auf die Verarbeitung seiner Reaktion schließen. Diese Analyse erfolgt anschließend ebenfalls beim Nutzer. Wenn der Einladende eines Termins auf den Reaktions-Termin des Nutzers durch Löschen reagiert hat, kann dieser Termin beim Nutzer ebenfalls gelöscht werden. Abbildung 5.3 veranschaulicht diese Vorgehensweise.

Eine weiter Aufgabe des *Controllers* ist die Reaktion auf das Bestätigen des *Sicher Speichern*- und *Löschen*-Buttons. Entgegen der Google-Funktionalität muss beim Löschen ebenfalls das Schlüsselmanagement und das interne Array über das Entfernen eines Termins informiert werden. Die Komponente verarbeitet diese Interaktion und stößt die Funktionalitäten der anderen Komponenten an. Beim Speichern entscheidet der *Controller*, welche Umstände beim entsprechenden Vorgang zugegen waren. Gemäß den Informationen über einen bestehenden oder neuen Termin, über Gäste sowie über die eigene Rolle als Gast eines Termins entscheidet diese Komponente, welche Funktionalitäten anderer Komponenten aufgerufen werden müssen. Ist die Verschiebung der zu schützenden Termine aktiviert, erzeugt eine Methode einen zufälligen Zeitstempel für Beginn und Ende des Termins. Auf diese Weise wird sowohl der Zeitpunkt als auch die Dauer verschleiert. Für Termine mit Gästen berechnet eine weitere Methode die Übertragungs-Schlüssel, mithilfe derer die Gäste des Termins den Termin-Schlüssel berechnen können.

Eine weitere Funktion dieser Komponente ist das Analysieren der derzeitigen Ansicht im Browser. Dazu zählen die Tages-, Wochen- und Monatsansicht sowie die Detail-Ansicht, in der neue Termine erstellt oder bestehende Termine bearbeitet werden. Zudem verwaltet diese Komponente das Hinzufügen eines neues Partners. Über einen Dialog wird die Adresse des Partners abgefragt und ein ent-

sprechender Termin, welche die Anfrage enthält, erzeugt. Zusätzlich organisiert diese Komponente das Aktualisieren der Einstellungen.

Sowohl die Einstellungen, als auch weitere Dialoge und Menüelemente stellen den statischen Teil der Sicht-Ebene dar. Über Menüelemente kann die Verbindung zur Google-Schnittstelle manuell getrennt, der Kalender neu gescannt, die aktuelle Ansicht aktualisiert oder ein neuer Partner hinzugefügt werden. Weitere Funktionen, wie die Anzeige der intern verwalteten Termine sowie eine detaillierte Ansicht der mit einem Termin verbundenen Daten, wurden zu Debugzwecken implementiert, werden allerdings nach Beenden der Testphase nicht mehr angezeigt. Bei Bedarf können diese Funktionalitäten wieder hinzugeschaltet werden, indem der Code geringfügig angepasst wird.

Im Optionsmenü des Firefox-Addons können diverse Parameter eingestellt werden. So ist die Verschiebung der Termine aufgrund der in Abschnitt 2.2.2 gezeigten eingeschränkten Funktionalität des Google-Dienstes optional. Ebenfalls kann das Sicherheitsniveau dahingehend angepasst werden, dass zu einem geteilten Termin ebenfalls Dummys verschickt werden. Weiterhin sind allgemeine Einstellungen möglich. So ist das Zeitintervall, in dem der Schutz genutzt werden soll sowie die Zeit zwischen durchzuführenden Kalenderscans, einstellbar. Diese Scans sind notwendig, um neue Reaktionen auf geteilte Termine oder Anfragen beziehungsweise Antworten des Austauschprotokolls der öffentlichen Schlüssel zu registrieren. Wenn der Parameter des Kalenderscans auf „0“ gesetzt wird, führt das Firefox-Addon keinen erneuten Scan des Kalenders durch. Ein Scan im 15 Minuten-Intervall ist grundsätzlich aber sinnvoll. Weiterhin kann das asymmetrische Schlüsselpaar ex- und importiert werden, um das Softwareprodukt auf mehreren Systemen betreiben zu können. Da das Schlüssel-Management mithilfe dieses Schlüsselpaares komplett neu aufgebaut werden kann, ist der Export des gesamten Schlüsselmaterials nicht notwendig. Das Partner-Management kann ebenfalls ex- und importiert werden. Zwar kann auch das Partner-Management aus den im Kalender befindlichen Terminen neu aufgebaut werden, jedoch besteht die Möglichkeit, dass nicht alle Partner in einem Termin auftauchen und so deren öffentliche Schlüssel nicht ermittelt werden können.

Zudem existieren einige Einstellungen für optische Aspekte. So kann die Farbe für einen geschützten Termin sowie die Schriftfarbe eingestellt werden. Da der Google-Dienst die Möglichkeit bietet vergangene Termine auszugrauen, besteht ebenfalls die Möglichkeit, für vergangene Termine eine abweichende Farbwahl zu treffen. Im Optionsmenü befindet sich ebenfalls die Möglichkeit, zusätzliche

Informationen zum Firefox-Addon aufzurufen. Darin wird auch auf eine Internetseite mit Zusatzinformationen verwiesen.

5.4 Benutzeroberfläche

Die Benutzeroberfläche des Firefox-Addons richtet sich im Wesentlichen nach dem ursprünglichen Layout des *Google Kalenders*. Die direkte Interaktion mit dem Firefox-Addon erfolgt vorrangig bei der Nutzerauthentisierung. Erkennt das Softwareprodukt einen neuen Google-Account, so wird ein Dialog zur Nutzererstellung angezeigt. Sollte diese bereits durchgeführt worden sein, erfolgt die Abfrage des Passworts. Die beiden Dialoge werden in den Abbildungen 5.5 dargestellt. Bei der Nutzererstellung überprüft das Softwareprodukt zudem die Länge sowie die Übereinstimmung der beiden eingegebenen Passwörter.

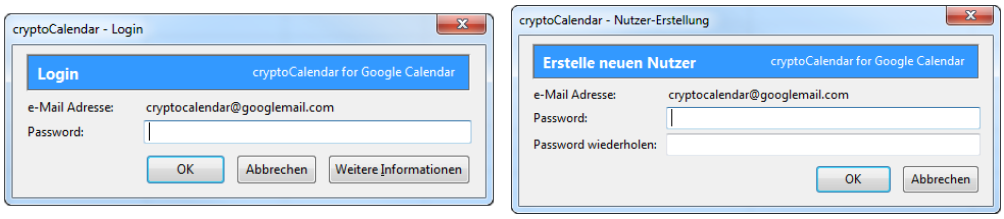

Abbildung 5.5: Dialoge für Login und Nutzererstellung

Nach erfolgreicher Nutzerauthentifizierung erhält der Nutzer einen Hinweis über die Verbindung zur Google-Schnittstelle. Dieser klärt den Nutzer über die Notwendigkeit dieser Verbindung auf. Die Meldung ist in Abbildung 5.6 dargestellt. Bestätigt der Nutzer diesen Dialog, wird er zu einer Seite des Dienstanbieters umgeleitet, welche die Nutzungserlaubnis für die Google-Schnittstelle einholt.

Ab diesem Zeitpunkt ist das Firefox-Addon über die Addon-Leiste des Browsers am unteren Rand des Browserfensters abrufbar. Diese Statusleiste ist in den Einstellungen zur Ansicht aller-

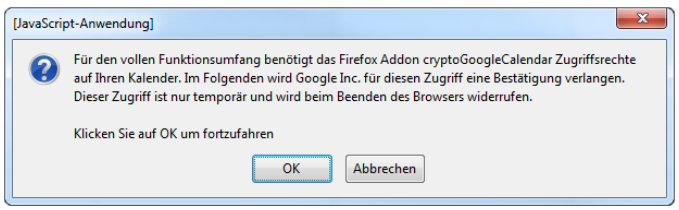

Abbildung 5.6: Meldung

dings in den neuen Versionen des Browsers nicht zwingend standardmäßig aktiviert. Das Menü des Eintrags innerhalb der Addon-Leiste erlaubt es dem Nutzer, einen manuellen Scan des Kalenders zu veranlassen, die aktuelle Ansicht im Browserfenster zu erneuern, den Ex- oder Import der Nutzerdaten zu veranlassen oder einen Partner hinzuzufügen. Ebenfalls kann ein Logout bezüglich der Schnittstelle zu Google initiiert werden, sollte ein Nutzer diese während der aktuellen Sitzung schließen wollen. Über die Einstellungen zu Addons im *Mozilla Firefox* gelangt der Nutzer in den Optionsdialog des Softwareprodukts. Dieser wird in Abbildung 5.7 dargestellt.

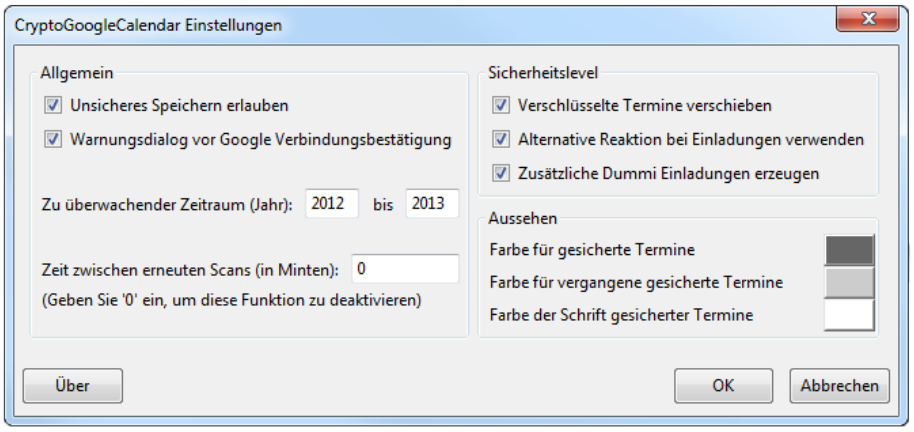

Abbildung 5.7: Options-Dialog

Für die generelle Verwendung des Firefox-Addons ist keine spezielle Nutzerinteraktion nötig, da sich das Addon in den *Google Kalender* integriert. Bei der Nutzung des Google-Dienstes ist lediglich darauf zu achten, dass nicht alle Funktionen des Kalenders vom Firefox-Addon berücksichtigt werden. Diese Differenzen werden im folgenden Abschnitt beleuchtet.

5.5 Fehlende Funktionen

Der Funktionsumfang des *Google Kalenders* wurde in Kapitel 2 ausführlich dargelegt. In Kapitel 4 wurde die Funktionalität des Firefox-Addons beschrieben. Dieser Abschnitt soll nun die Defizite aufzeigen, welche zwischen gesicherter und ungesicherter Kalendernutzung festzustellen sind. Dazu sollen die fehlenden Funktionalitäten aufgezeigt und kurz beschrieben werden. Falls möglich wer-

den Umsetzungsstrategien erklärt. Es sei anzumerken, dass eine Vielzahl der fehlenden Funktionen prinzipiell realisierbar sind, dies jedoch im Rahmen dieser Arbeit nicht erschöpfend möglich war.

Im Abschnitt 5.1 wurde bereits erläutert, dass nicht alle Ansichten des Kalenders bei der Manipulation der Ansicht berücksichtigt werden. Dazu zählen die Monatsansicht und die Terminübersicht. Beide Ansichten könnten in die Manipulation einfließen, jedoch werden ein Großteil der Inhalte sehr dynamisch erzeugt. Als Beispiel sei der Sachverhalt zu nennen, dass sich innerhalb der Monatsansicht die Größe der Quadrate zu jedem Tag, abhängig von der Anzahl der Termine verändert. Teils werden dabei nicht alle Termine eines Tages angezeigt, diese können der Ansicht aber durch eine weitere Schaltfläche nachträglich hinzugefügt werden. Ebenfalls wurde bereits erläutert, dass das Verstecken der Gästeliste bei Verwendung des Firefox-Addons nicht realisiert wurde, was durch den geringen Nutzen dieser Möglichkeit zu begründen ist. Eine ausführliche Lösungsmöglichkeit wird in Abschnitt 3.5 dargelegt. Des Weiteren ist es nicht möglich, den Gästen eines Termins zu gestatten, diesen zu bearbeiten. Diese Funktionalität ist zwar implementiert, wird aber von der Google-Schnittstelle derzeit nicht unterstützt.

Eine weitere sehr aufwändig zu integrierende Funktion ist die Möglichkeit Termine zu wiederholen. Hierfür verwendet Google selbst den iCal-Standard, welcher unter [DS11] spezifiziert ist. Innerhalb der internen Terminverwaltung von Google werden 21 XML-Elemente verwendet, um eine Wiederholung von Terminen zu realisieren. Um diese Funktion zu adaptieren, muss eine ähnlich mächtige Umsetzung im Firefox-Addon erfolgen.

Zudem ermöglicht es der Google-Dienst den Nutzern mehrere Teil-Kalender zu erstellen. Das Firefox-Addon verwendet ausschließlich den Standard-Kalender eines Nutzers[1].

Weitere Funktionen, die bei der sicheren Speicherung von Terminen nicht berücksichtigt werden, sind Farbe, Erinnerungen, Verfügbarkeitstatus und die Google-internen Einstellungen zum Datenschutz. Abbildung 2.2 in Abschnitt 2.1 zeigt diese Einstellungsmöglichkeiten.

Ebenfalls müssen alle bei einem geteilten Termin eingetragenen Gäste über das Firefox-Addon verfügen. Die Integration der Möglichkeit, einen geteilten Termin sowohl in geschützter als auch ungeschützter Form gleichzeitig zu organisie-

[1]Dieser ist bei einem angemeldeten Nutzern unter der URL https://www.google.com/calendar/feeds/default/private/full zu erreichen

ren wurde nicht durchgeführt. Insbesondere die Synchronisation bei Änderungen des Termins hätten eine zu hohen Implementierungsaufwand dargestellt.

Weiterhin ist es nicht möglich, die dynamische Terminerstellung zu sichern. Bei dieser Variante zieht der Nutzer den Termin an die gewünschte Position im Kalender und trägt lediglich einen Titel ein. Um diese Möglichkeit ebenfalls zu schützen, muss entweder die Position des Termins innerhalb der Ansicht ermittelt werden oder der Nutzer kann mithilfe einer Weiterleitung auf den detaillierten Dialog zur Terminerstellung umgeleitet werden. In beiden Fällen ist ein Listener nötig, welcher beim Auftauchen des Erstellungs-Popups den Button erfasst, löscht und durch eine Umleitung oder Routine zum sicheren Speichern ersetzt.

Das Firefox-Addons lässt sich zudem um eine Vielzahl weiterer Funktionen zur leichteren Verwendung erweitern. Beispielsweise kann der gesamte Kalender analysiert und systematisch durch geschützte Termine ersetzt werden. Eine reverse Methode ist ebenfalls denkbar, um so den Umstieg auf einen gesicherten oder ungesicherten Kalender zu erleichtern. Weiterhin kann die Implementierung eines Mail-Moduls die Erinnerungsfunktion des Google-Dienstes ersetzen.

Kapitel 6

Fazit

Diese Arbeit konnte erfolgreich demonstrieren, dass der Datenschutz bei im Internet verfügbaren Diensten durch Maßnahmen des Selbstdatenschutzes gesteigert werden kann. Dazu wurde der *Google Kalender* als Beispiel für einen solchen Dienst im Detail betrachtet. Eine eingehende Analyse des Funktionsumfangs konnte aufzeigen, welche personenbezogenen Daten der Dienst zur Ausführung diverser Dienstleistungen benötigt. Dazu wurden sowohl die Kernfunktionalitäten als auch Zusatzdienste betrachtet. Bei der Analyse konnte zudem verdeutlicht werden, dass Maßnahmen des Selbstdatenschutzes den Funktionsumfang des Google-Dienstes einschränken.

Ferner wurde dargelegt, welche personenbezogenen Daten vom Nutzer an den Dienstanbieter übermittelt werden und welche Problematik sich aus Sicht des Datenschutzes ergibt. Für die unterschiedlichen Datengruppen wurden entsprechende Schutzmaßnahmen vorgestellt, die in einem Datenschutzkonzept kumuliert wurden. Mithilfe dieses Konzeptes kann der *Google Kalender* genutzt werden, ohne dass dem Dienstanbieter Daten übermittelt werden, die dieser zur Ausführung der Dienstleistung nicht zwingend benötigt.

Die feingranulare Beschreibung des Datenschutzkonzeptes ermöglicht es zudem, die Schutzmechanismen nachvollziehbar darzustellen und die für diese Arbeit erstellte Implementierung entsprechend zu validieren. Das beschriebene Entwicklungsvorhaben zeigt die spezifischen Anforderungen an die Implementierung auf. Die abschließende detaillierte Vorstellung des entwickelten Firefox-Addons dient dazu, das Verhalten des Firefox-Addons sowie dessen Funktionsumfang zu erfassen. Eine nähere Betrachtung der Implementierung verdeutlicht

den internen Aufbau und beschreibt die Komponenten des Softwareprodukts im Detail. Nach einer Vorstellung der Benutzeroberfläche werden letztlich fehlende Funktionen bzw. Teile des Datenschutzkonzeptes aufgeführt, die im Rahmen dieser Arbeit nicht behandelt werden konnten.

Die Aufmerksamkeit der Nutzer im Hinblick auf den Schutz der eigenen Privatsphäre ist aus Sicht des Autors derzeit nicht ausreichend. Da Unternehmen aus der Naivität der Nutzer deutliche Profite erwirtschaften, sind Fortschritte im Systemdatenschutz nicht zu erwarten. Mittel zum Selbstdatenschutz sind daher zwingend notwendig, um die Privatsphäre ausreichend zu schützen. Diese Arbeit macht zum einen auf bestehende Risiken aufmerksam und bietet zum anderen eine praktikable Möglichkeit, diesen in einer bestimmten Anwendung entgegen zu wirken.

Es konnte gezeigt werden, dass aktuelle im Internet angebotene Dienste durch Eigeninitiative von Seiten der Nutzer, ohne die übermäßige Preisgabe von personenbezogenen Daten verwendet werden können. Die Angebote werden dabei auch weiterhin als Plattform genutzt, diese erhalten jedoch keine Daten, die für die Erstellung von Nutzerprofilen oder für Netzwerkanalysen genutzt werden können. Werden Bestrebungen im Bereich des Selbstdatenschutzes auch für weitere im Internet verfügbare Dienste angestrebt, könnten Nutzer in Zukunft wieder mehr kontrollieren, welche Daten sie preisgeben möchten. Diese Arbeit demonstriert prototypisch die Umsetzung einer Sofware-gesteuerten, veränderten Nutzbarkeit des *Google Kalenders*. Ein solcher Ansatz könnte in Zukunft auch für weitere Plattformen umgesetzt werden. In sozialen Netzwerken könnte so sichergestellt werden, dass Information ausschließlich mit Freunden und nicht mit dem Dienstanbieter geteilt werden, wenn dies nicht erwünscht ist.

Die Erfahrungen und Ergebnisse dieser Arbeit tragen somit dazu bei, einen Fortschritt im Bereich des Datenschutzes durch Maßnahmen des Selbstdatenschutzes bei im Internet verfügbaren Diensten voranzutreiben. Entsprechende Bestrebungen könnten einen Trend auslösen und den Verfechtern des Datenschutzes ein durchaus praktikables Werkzeug zur Verfügung stellen, mithilfe dessen Dienste aktiv verbessert werden können, ohne auf ein Entgegenkommen der entsprechenden Anbieter angewiesen zu sein. Im Idealfall würden die Anbieter diese sich ändernden Ansprüche der Nutzer zum Anlass nehmen, ihre Dienste bezüglich des Datenschutzes konformer zu gestalten.

Glossar

Dummy Ein Dummy ist eine Einladung, die Nutzer erreicht, die lediglich zusätzlich zu einem Termin eingeladen werden, um eine Streuung der Gäste zu gewährleisten.. 32–37, 50, 53, 56, 62, 66

Firefox-Addon Ein Firefox-Addon ist eine Erweiterung der Firefox-Funktionalitäten. Diese können zudem das Erscheinungsbild der Benutzeroberfläche oder Seiteninhalte manipulieren. Beispiele: Werbeblocker, FTP-GUIs, Wetteranzeige in der Statusbar o.ä. 2, 3, 41–45, 47, 49, 51–53, 55–64, 66–71, 73, 74

Nutzer-Management Das Nutzer-Management dient dazu, die Nutzerdaten des Firefox-Addons der verschiedenen Google-Accounts zu verwalten, da jedem dieser Accounts ein eigener Kalender zuzuordnen ist. Die Funktionsweise wird in Kapitel 4.3.1 genauer spezifiziert. 45

Partner-Management Das Partner-Management dient dazu, alle Nutzer zu verwalten, die bekanntermaßen ebenfalls das Firefox-Addon verwenden. Es wird benötigt, um festzustellen, welche Nutzer des Google-Dienstes verschleierte Termine empfangen können. Die Funktionsweise wird in Kapitel 4.3.2 genauer spezifiziert. 30, 32, 34, 36, 39, 45, 46, 53, 61, 65, 66

Reaktions-Termin Ein Reaktionstermin ist einspezieller Termin, der die Entscheidung zu einer Termineinladung enthält und an den Einladenden sowie weitere Gäste des Termins verschickt wird. Der Reaktions-Termin ermöglicht somit einen Mechanismus zur Publikation einer Entscheidung, ohne die von Google angebotenen Mechanismen zu verwenden.. 26, 35, 37, 55, 56, 65

Schlüssel-Management Das Schlüssel-Management dient dazu pro Account eines Nutzers alle Termin-Schlüssel zu verwalten. Die Funktionsweise wird in Kapitel 4.3.3 genauer spezifiziert. 27, 45, 47, 48, 53, 61, 66

Termin-Schlüssel Bei einem Event-Schlüssel, handelt es sich um einen kryptographischen Schlüssel, welcher vom Firefox-Addon für die Entschlüsselung eines bestimmten Termins verwendet werden muss. 21, 27–30, 32, 33, 35, 46, 47, 54, 55, 61, 65, 74

uID Der Unique-Identifier (uID) dient dazu, bestimmte Informationen einem Termin diesem eindeutig zuordnen zu können. Da jeder Termin über einen eigenen Termin-Schlüssel verfügt, muss eine Zuordnung zwischen Termin und Schlüssel erfolgen. Der Unique-Identifier identifiziert einen Termin eindeutig und besteht aus einer 16-stelligen zufälligen Zeichenfolge.. 27, 35–37, 47, 48, 53, 55, 61, 63

Übertragungs-Schlüssel Bei einem Übertragungsschlüssel handelt es sich um einen Nutzer-spezifischen gesicherten Termin-Schlüssel eines bestimmten Termins. Der Termin-Schlüssel wird mithilfe des öffentlichen Schlüssels des Nutzers gesichert. Da es sich um ein asymmetrisches Verschlüsselungsverfahren handelt, ist nur der Nutzer selbst in der Lage, einen so verschlüsselten Termin-Schlüssel entschlüsseln zu können. 29, 32, 33, 37, 46, 48, 53, 55, 61, 64, 65

Literaturverzeichnis

[Age10] Deutsche Presse Agentur. *Zensurstreit mit China - Google wagt die Kraftprobe*. focus.de, März 2010. http://www.focus.de/digital/internet/zensurstreit-mit-china-google-wagt-die-kraftprobe_aid_492133.html.

[Age12] Deutsche Presse Agentur. *Verbraucherschützer mahnen Google ab*. spiegel.de, März 2012. http://www.spiegel.de/spiegel/vorab/0,1518,819069,00.html Zugriff: 26.04.2012.

[Bac20] Francis Bacon. *Novum Organum*. 1620.

[Beh12] Bernd Behr. *Aigner kritisiert neue Datenschutzregeln bei Google*. heise online News, März 2012. http://www.heise.de/newsticker/meldung/Aigner-kritisiert-neue-Datenschutzregeln-bei-Google-1447412.html Zugriff: 26.04.2012.

[DS11] F. Dawson and D. Stenerson. *Internet Calendaring and Scheduling Core Object Specification (iCalendar)*. Network Working Group, 2011. http://tools.ietf.org/html/rfc2445 Zugriff: 26.04.2012.

[FP12] Agence France-Presse. *HINTERGRUND: Facebook in Zahlen*. stern.de, Januar 2012. http://www.stern.de/news2/aktuell/facebook-in-zahlen-1781443.html Zugriff: 26.04.2012.

[GHJV10] Erich Gamma, Richard Helm, Ralph Johnson, and John Vlissides. *Entwurfsmuster: Elemente wiederverwendbarer objektorientierter Software*. Programmer's Choice. Addison Wesley Verlag, 2010. http://books.google.de/books?id=tmNNfSkfTlcC Zugriff: 26.04.2012.

[Gie10] Hartmut Gieselmann. *Der vermessene Spieler*. c't Magazin für Computertechnik, Juli 2010. http://www.heise.de/ct/artikel/Der-vermessene-Spieler-1042962.html Zugriff: 26.04.2012.

[Goo11a] Google. *About the 'Quick Add' feature*. Google, 2011. http://www.google.com/support/calendar/bin/answer.py?answer=36604 Zugriff: 26.04.2012.

[Goo11b] Google. *Google Sync services*. Google, 2011. http://www.google.com/sync/index.html Zugriff: 26.04.2012.

[Goo11c] Google. *Grundlagen: Webprotokoll*. Google, 2011. http://www.google.com/support/accounts/bin/answer.py?answer=54068&hl=de Zugriff: 26.04.2012.

[Goo12] Google. *Datenschutzerklärung*. Google, 2012. http://www.google.com/intl/de/policies/privacy/ Zugriff: 26.04.2012.

[Gri03] Rüdiger Grimm. *Datenschutz im Electronic Commerce: Technik–Recht–Praxis*. Schriftenreihe Kommunikation & Recht. Verlag Recht und Wirtschaft, 2003. http://books.google.de/books?id=9p-sAQAACAAJ Zugriff: 26.04.2012.

[Her09] Pascal Herbert. *Google nimmt Gmail aus der Beta - Docs, Calendar und Talk ebenfalls*. GoogleWatchBlog, Juli 2009. http://www.googlewatchblog.de/2009/07/google-nimmt-gmail-aus-der-beta-docs-calendar-und-talk-ebenfalls/ Zugriff: 26.04.2012.

[ho06] heise online. *Google startet Web-Kalender*. heise online, 2006. http://www.heise.de/newsticker/meldung/Google-startet-Web-Kalender-117277.html Zugriff: 26.04.2012.

[Min06] Jens Minor. *Einführung in den Google Calendar*. GoogleWatchBlog, Juli 2006. http://www.googlewatchblog.de/2006/07/einfuhrung-in-den-google-calendar/ Zugriff: 26.04.2012.

[Sch06] Peter Schüler. *Google Apps ohne Beta*. heise online, 2006. http://www.heise.de/newsticker/meldung/Google-Apps-ohne-Beta-6219.html.

[Sch11] Stefan Schultz. *Insider bewerten Facebook mit 100 Milliarden Dollar*. stern.de, Juni 2011. http://www.spiegel.de/wirtschaft/unternehmen/0,1518,768233,00.html Zugriff: 26.04.2012.