Technische Universität Ilmenau
Fakultät für Informatik und Automatisierung
Institut für Praktische Informatik
Fachgebiet Telematik
Prof. Dr.-Ing. habil. Dietrich Reschke

Projektarbeit
im SS 2002

„Analyse und Erfahrung mit Groove“

Betreuer: Dipl.-Inf. Thorsten Strufe

vorgelegt von:
Eric Niedling
Bachstelzenweg 8
99094 Erfurt
eric.niedling@wi.stud.tu-ilmenau.de
Matr.Nr.: 27553

Inhaltsverzeichnis

Abbildungsverzeichnis

Abkürzungen

ADO..... Abstract Data Objects
AES..... Advanced Encryption Standard
CA..... Certification Authority
DPP..... Device Presence Protocol
ERP..... Enterprise Ressource Planning
HTTP..... Hypertext Transmission Protocol
LDAP..... Lightweigth Directory Access Protocol
ODBC..... Open Database Connectivity
P2P..... Peer-to-Peer
PKI..... Public Key Infrastructure
RSA..... Rivest, Shamir and Adleman
SOAP..... Simple Object Access Protocol
SSTP..... Simple Symmetric Transmission Protocol
TCP/IP..... Transmission Control Protocol
UDP..... User Datagramm Packet
URL..... Uniform Ressource Locator
XML..... eXtensible Markup Language
XML-RPC..... eXtensible Markup Language – Remote Procedure Call

1 Einleitung

Filesharing-Anwendungen wie Gnutella und Naptser wurden in den letzten Jahren in zunehmendem Maße von Privatanwendern genutzt, um Dateien über das Internet auszutauschen.[1]
Dies erzeugte viel Aufregung in Bezug auf die Sicherheit von „Intellectual Capital". Besonders IT Manager sahen in der dezentralen Datenhaltung eine drohende Gefahr für Unternehmensnetzwerke. Zum einen muss aber zwischen privatem Musik-Austausch in großem Stile und unternehmensbezogener dezentraler Projektarbeit unterschieden werden. Zum anderen wurden Kommunikationsarchitekturen und Übertragungsmechanismen weiterentwickelt. Die Klasse der Peer-to-Peer-Anwendung (P2P) ist ebenso zu einem Forschungsgegenstand geworden. Dabei werden neben der Topologie der Netze Kriterien wie Ausfallsicherheit, Datenkonsistenz, Erweiterbarkeit, Sicherheit untersucht und bewertet.[2]
Statische Inhalte wie Analysen, Berichte und Dokumentationen werden nach ihrer Fertigstellung zum einen nicht mehr geändert, und zum anderen meist einer größeren Personenmenge zugänglich gemacht, als von der sie verfasst wurden. Außerdem werden sie im ganzen übertragen. Unter dynamischen Inhalten hingegen sind beispielsweise Dokumente während ihrer Entstehung zu verstehen. Sie werden von einer zumeist klar definierten Personenmenge erstellt und auszutauschende Änderungen erfolgen inkrementell, also in kleinen Schritten.
Gegenstand dieser Arbeit ist die Software Groove Workspace v2.0. In wie fern Groove diese Charakteristik berücksichtigt, um eine Groupware-Lösung bereitzustellen, soll im Rahmen dieser Arbeit ermittelt werden. Ob Groove in die Klasse der P2P-Anwendungen einzuordnen ist, soll durch eine Analyse der Architektur ermittelt werden und anschließend die Aspekte der Sicherheit, Datenkonsistenz und Erweiterbarkeit behandelt werden.
Ebenso soll der praktische Funktionsumfang der Software beleuchtet werden, um die Anwendungsmöglichkeiten abschätzen zu können.

[1] Ganzer Abschnitt Vgl. Groove /Bandwidth/ 1
[2] Vgl. Minar /Topologies/ 5

2 Grundlagen

2.1 Groove Architektur

2.1.1 Groove System Architektur

Groove ist eine Groupware-Lösung oder im Selbstverständnis von Groove eine „decentralised collaboration platform“[3]. Die Software soll folglich die lose Zusammenarbeit von räumlich und zeitlich verteilt bzw. versetzt arbeitenden Anwendern als ein flexibel erweiterbares System unterstützten. Entgegen dem zentralen webbasierendem Ansatz, welcher vor allem bei der (anonymen) Informationsverteilung offensichtlich erfolgreich ist, ermöglicht der dezentrale Ansatz einen hohen Grad an persönlicher Interaktion, vergleichbar mit dem Telefonsystem. Abbildung 2-1 zeigt ein konventionelles Peer Modell, bei dem alle Daten auf den Clients liegen[4]. Das heißt für die Groove Clients, dass die Arbeitsgruppendatenbestände identisch sind oder noch synchronisiert werden müssen.

Abbildung 2-1: Groove System - Peers

Da Groove als Groupware-Anwendung aber häufig in Verbindung mit bereits bestehenden Systemen verwendet wird, muss Groove entsprechende Integrationsmöglichkeiten bereithalten, um einen Informationsaustausch zu gewährleisten.[5]
Bei dem „Multi Point Integration“-Ansatz kann jedes Arbeitsgruppenmitglied Daten zwischen dem Groove System und externen Systemen austauschen.[6] Jeder Client besitzt entsprechende Konnektoren um mit dem externen System (z.B. Webserver) zu kommunizieren. Wird beispielsweise im Browser eine URL angegeben, so wird den anderen Groove-Clients nur diese URL übermittelt. Den Zugriff auf den Webserver, siehe Abbildung 2-2, unternimmt die Clientsoftware selbständig. Dadurch wird die innerhalb der Arbeitsgruppe zu übertragende Datenmenge minimiert.

[3] Vgl. Groove /Product Backgrounder/ 1
[4] Ozzie /GrooveSystemsIntegration/ 13
[5] Vgl. Groove /Enterprise Integration/ 1
[6] Vgl. Suthar, Ozzie /GrooveSharedSpaceArchitecture/ 15

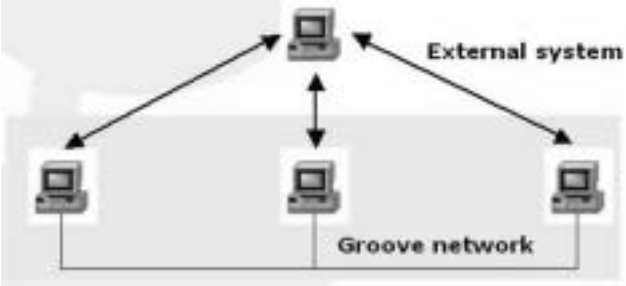

Abbildung 2-2: Groove System - Multi Point Integration

Der „Single Point Integration“-Ansatz stellt ein Infrastrukturkonzept zur Integration externer Systeme und Ressourcen (Enterprise Application Integration) dar.[7] Unter externen Systemen können unternehmensinterne oder unternehmensexterne Systeme verstanden werden. Abbildung 2-3 stellt dies schematisch dar. Es wird davon ausgegangen, dass aus Gründen der Performanz und der Datenintegrität ein Zugriff aller Clients wenig vorteilhaft ist. Dies gilt sowohl für Lese- als auch für Schreiboperationen. Der Zugriff auf externe Systeme ist außerdem eine sehr spezifische Aufgabe und häufig mit Schutzmechanismen (Nutzerkonten) versehen. Groove realisiert die „Single Point Integration“ mit Hilfe von Bots. Bots sind Software-Agenten, die bestimmte Aufgaben erledigen, wie beispielsweise in Datenbanken recherchieren, Diskussionen verfolgen oder Sicherheitskopien nach abgeschlossenem Review-Prozess anlegen. Der Software-Agent wird mit dem Groove Enterprise Integration Server verwaltet und kommuniziert mit den Backend-Systemen über Programmierschnittstellen oder die Protokolle SOAP, ADO und ODBC.
Wesentlicher Vorteil dieser Architektur ist die zentrale Verwaltung der Dienste und Zugriffsrechte. Dienste werden zentral auf dem Server verwaltet, gruppiert, gewartet(update) und gelöscht.[8] Von entsprechend berechtigten Nutzern können sie als Identität in eine Arbeitsgruppe eingeladen werden. Ebenso können Bots bei der Informationsverteilung zwischen Arbeitsgruppenmitgliedern unterscheiden, also beispielsweise nach Unternehmenszugehörigkeit.

[7] Vgl. Groove /Enterprise Integration/ 3
[8] Vgl. Groove /Enterprise Integration Server/ 1

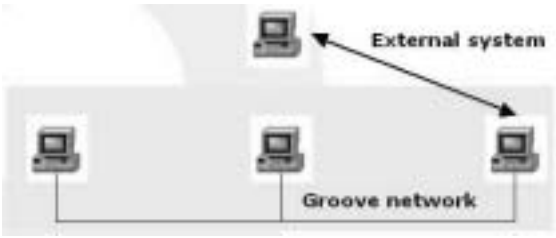

Abbildung 2-3: Groove System - Single Point Integration

2.1.2 Groove Client Architektur

Zentrale Komponenten der Client Software sind der Transceiver und die Arbeitsgruppen(Shared Spaces). Wie der nachfolgenden Abbildung[9] zu entnehmen ist, gehören zu einem Nutzerkonto(Account) mehrere Identitäten, mit denen über den Transceiver an Arbeitsgruppen teilgenommen wird. Zu einer Arbeitsgruppe gehören Werkzeuge (Tools), welche wiederum aus Elementen zur Ansicht (ActiveX- Komponenten), zur Verarbeitung (Engine) und/oder zur Erweiterung der Funktionalität (Code Components) bestehen. Die zu einer Arbeitsgruppe gehörenden Daten werden in der Metasprache XML beschrieben und auf dem lokalen Datenträger verschlüsselt abgelegt.

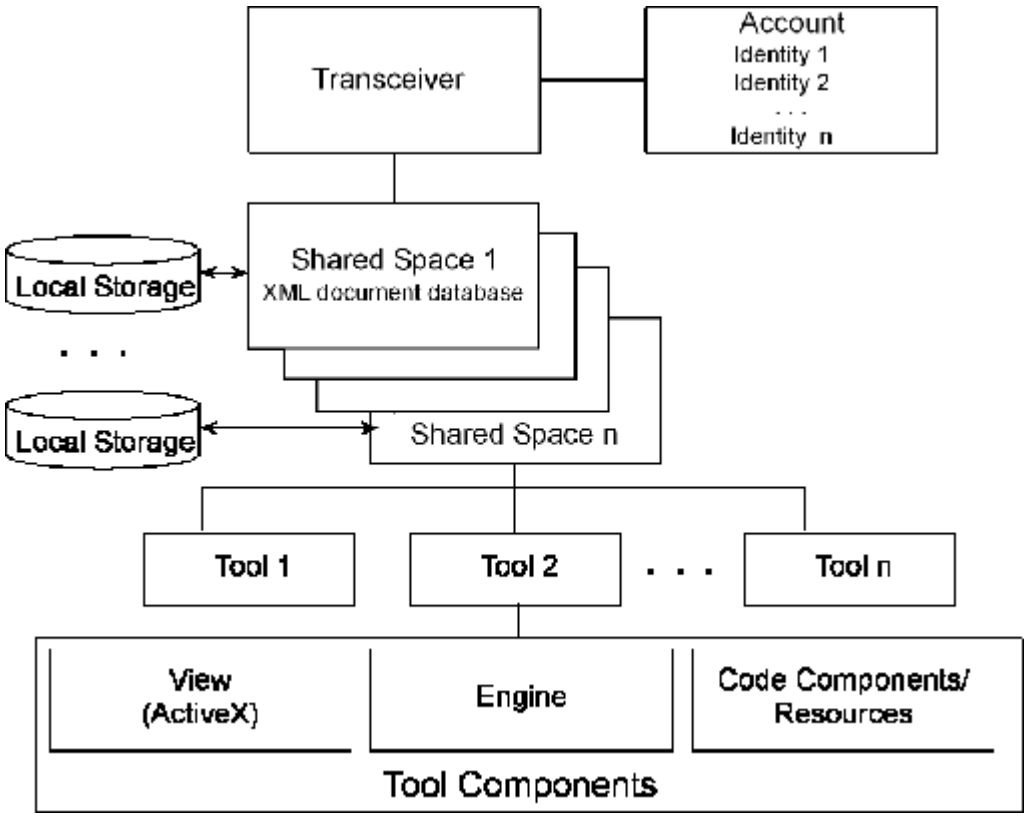

Abbildung 2-4: Groove Client Architektur

[9] Suthar, Ozzie /GrooveSharedSpaceArchitecture/ 4

Da Groove, wie bereits oben ausgeführt, eine dezentrale Groupware-Anwendung ist, werden alle Daten auf den entsprechenden Endgeräten abgelegt. Folglich ist eine Arbeitsgruppe in Groove die Menge von Kopien eines XML-Objekte-Speichers, der sämtliche Informationen über Teilnehmer, Arbeitsgruppenwerkzeuge und generierte Daten enthält. Auf einige Teile der Architektur wird im Rahmen der Arbeit ausführlicher eingegangen.

2.2 Groove-Verwendung: Nutzerkonten und Identitäten

Die Grundidee von Groove ist, die dynamische Verbindung von Personen zu stärken, die eng zusammenarbeiten.[10] Eine Person ist häufig in verschiedenen Gruppen aktiv. So ist ein wissenschaftlicher Mitarbeiter an einer Universität zum einen in der Arbeitsgruppe seines Fachgebietes aktiv, zum anderen wirkt er in einem oder mehreren Gremien innerhalb bzw. außerhalb der Universität mit. Sein Arbeitsgerät ist dabei nicht nur der PC an der Uni, sondern häufig auch ein zweiter PC an einer anderen Institution oder der PC zu Hause. Fallbeispiele dieser Art werden von Groove unterstützt, indem zwischen Nutzerkonto(Account), Endgerät(Device) und Identität(Identity) unterschieden wird.[11] Jede natürliche Person kann sich somit von verschiedenen Endgeräten aus unter Vorgabe der gewünschten Identität in einer entsprechenden Arbeitsgruppe aufhalten. Zu einem Nutzerkonto gehört mindestens eine Identität. Eine Groove-Identität kann außer einem frei wählbaren Namen zusätzliche Informationen(E-Mail, Anschrift, Telefon) enthalten, die sich wiederum nach persönlichen und geschäftlichen Informationen unterscheiden lassen (My Contacts). Um eine Arbeitsgruppe zu gründen oder eingeladen zu werden, benötigt man eine Groove-Identität.

Technisch gesehen, besteht eine Identität aus zwei Schlüsselpaaren (private und öffentliche Schlüssel). Diese werden benötigt, um die Kommunikation mit anderen Groove-Identitäten zu sichern. Detaillierte Informationen finden sich in Kapitel 4. Einfacher gesagt, werden Groove-Identitäten durch Namen repräsentiert, mit denen man in einer Arbeitsgruppe teilnehmen kann. Namen können Personen aber nicht immer eindeutig identifizieren, deswegen enthält jede Identität auch einen digitalen Fingerabdruck. Um Namenskonflikte aufzulösen, kann jedes Arbeitsgruppenmitglied ein Alias für einen Kontakt vergeben.

[10] Vgl. Groove /UsersGuide/ 4
[11] Vgl. Udell et.al. /Security/ 7

Registrierte Identitäten(managed identitites) können in Unternehmen vom Administrator vergeben werden und legen gleichzeitig die Berechtigungen für den Anwender fest.[12]

2.3 Das Arbeitsgruppen-Konzept

Eine Arbeitsgruppe besteht aus Mitgliedern(Identitäten), Werkzeugen (Workspace Tools) und Daten, die durch die Zusammenarbeit eingestellt oder erstellt werden. Mitglieder einer Arbeitsgruppe werden einer der drei Benutzergruppen(Rollen) Manager, Teilnehmer(Participant) oder Gast(Guest) zugewiesen.[13] Die Rolle entscheidet letztlich über die Interaktionsmöglichkeiten eines Anwenders innerhalb einer Arbeitsgruppe. Eine Rolle repräsentiert eine Nutzergruppe, der Rechte auf Werkzeug- bzw. Arbeitsgruppenebene zugewiesen werden. Zur Auswahl stehen dabei die Rechte „Erstellen“, „Ändern beliebiger“, „Ändern eigener“, „Löschen beliebiger“, „Löschen eigener Einträge“ in Werkzeugen auf Werkzeugebene. Auf Arbeitsgruppenebene können die Rechte „Einladen“ bzw. „Ausladen von Identitäten“, „Hinzufügen“ und „Entfernen von Werkzeugen“, „Schließen der Arbeitsgruppe“ und „Arbeitsplatz nach Ausladen behalten“ vergeben werden.

3 Funktionen von Groove

3.1 Groove Transceiver

Der Groove Transceiver ist eine Art Hauptprogramm, mit dem sowohl administrative als auch konstruktive Aufgaben erledigt werden können. Mit dem Transceiver werden also einerseits Arbeitsgruppen verwaltet, Kontakte gepflegt und die Systemeinstellungen vorgenommen und andererseits mit Identitäten an Arbeitsgruppen teilgenommen. Der Transceiver unterscheidet sich vom Groove Explorer dahingehend, dass er zusätzlich über eine Task-Leiste verfügt, mit der auf die Groove-Systemdienste zugriffen werden kann. Außerdem verfügt er über einen Bereich, indem der Onlinestatus und der Authentifizierungsstatus anderen Groove-Identitäten sichtbar ist. Zur Ermittlung des Onlinestatus wird das Device Presence Protocol verwendet. Weiter Ausführungen folgen in Kapitel fünf der Arbeit.

[12] Vgl. Groove /Usersguide/ 129
[13] Vgl. Groove /Usersguide/ 85ff.

Abbildung 3-1: Groove Transceiver Beispiel

Der „Go To“-Button ist eines der Grundnavigationselemente mit dem man zu den so genannten Groove-Systemwerkzeugen gelangt. Diese Systemwerkzeuge sind „My Spaces“ zur Verwaltung von Arbeitsgruppen, „My Contacts“ zur Verwaltung von Kontakten, „My Account“ zur Verwaltung von Identitäten innerhalb eines Kontos und „My Messages“ zur Verwaltung von Nachrichten und Einladungen. Das Systemwerkzeug „My Communications“ ermöglicht die Überwachung der Datenübertragung. Es können sowohl einzelne Kommunikationsaktivitäten gestoppt und fortgesetzt, als auch ein Offline-Arbeiten eingestellt werden. Kommunikationsaktivitäten sind das arbeitsgruppenunabhängige übertragen von „Nachrichten und Einladungen“ und die Synchronisation einer Arbeitsgruppe.

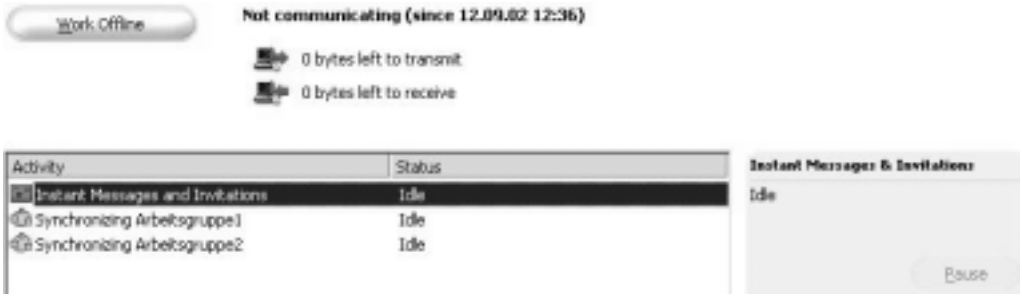

Abbildung 3-2: Ausschnitt - "My Communications"

Um gleichzeitig in mehreren Arbeitsgruppen aktiv zu sein, muss eine weitere Instanz des Transceivers gestartet werden. Jede weitere Transceiver-Instanz allokiert zusätzliche Systemressourcen. Die Werkzeuge einer Arbeitsgruppe können auch in einem neuen Fenster angezeigt werden. Sollen mehrere Groove-Systemwerkzeuge geöffnet werden („My Contacts“, „My Spaces“, „My Accounts“, ...), so muss ebenfalls eine weitere Transceiver-Instanz gestartet werden.
Die Funktion „Anzeigen neuer und geänderter Informationen“ ist eine weitere Kernfunktion der Groupware-Anwendung. Werden neue Inhalte durch ein Arbeitsgruppenmitglied generiert oder geändert, so werden die anderen Arbeitsgruppenmitglieder darüber in Kenntnis gesetzt, indem eine entsprechendes Icon angezeigt wird. Diese so genannte Groove-Awareness wird in Kapitel 5.3 genauer ausgeführt.

3.2 Arbeitsgruppenwerkzeuge

Die Groove Plattform in der Version 2.0 unterstützt die Zusammenarbeit einer Arbeitsgruppe mit bis zu 16 verschiedene Werkzeugen. Die Nutzungsmöglichkeiten der Werkzeuge sind von den Berechtigungen, die der Rolle des Nutzers zugewiesen wurden, abhängig. So kann einem Gast beispielsweise die Verwendung des Kalenders untersagt werden. Im folgenden werden alle in der Version 2.0 des Groove Workspaces verfügbaren Werkzeuge vorgestellt.

Calendar Tool

Mit dem Kalender können ausschließlich Gruppentermine verwaltet werden, d.h. persönliche Termine können nicht vor anderen Arbeitsgruppenmitgliedern versteckt werden.[14]
Der Kalender bietet die Ansichten Tag, Woche und Monat. Termine können mit Drag’n’Drop verschoben, bzw. Anfang und Ende geändert werden. Neue Elemente werden mit dem entsprechenden Piktogramm versehen und können nach dem Lesen wieder auf den Ungelesen-Status zurückgestellt werden.
Mit einer „Copy as Link“ - Funktion können Termine als Verweise in Textwerkzeuge wie Outliner, Notepad, Discussion oder Chat eingefügt werden.
Der Export ausgewählter oder aller Termine bzw. Import erfolgt mittels verschlüsselter XML-Dateien. Ein erneuter Import führt zur Duplizierung der Einträge.

[14] Alle Abschnitte dieses Kapitel Vgl. Groove /UsersGuide/ 155ff.

Contact Manager Tool

Dieses Werkzeug versteht sich als virtuelles Adressbuch. Die hier hinterlegten Kontakte sind nicht identisch mit den Groove-Kontakten, welche mit dem Transceiver verwaltet werden. Mit diesem Hilfsmittel lässt sich der Onlinestatus von Identitäten ermitteln, Namenskonflikte über die Vergabe von Aliasen auflösen, vCards anschauen, der digitale Fingerabdruck einsehen, Netmeeting-Verbindungen öffnen, Nachrichten(inkl. Voice Memo) versenden und private Chats organisieren.

Discussion Tool

Groove stellt Diskussionen in einer übersichtlichen, zusammenklappbaren Baumstruktur dar. Diskussionsbeiträge enthalten neben Text und Titel auch die Metainformationen Autor und Erstellungsdatum. Dateien können angefügt werden und eine Vorschau ist verfügbar.
Mit der bereits oben beschriebenen „Copy as Link“ – Funktion lassen sich in entsprechenden Textwerkzeugen Verweise auf Diskussionsbeiträge anlegen.

Document Review Tool

Ein Dokumentenkorrekturprozess kann nur von einem Nutzer der Rolle „Manager“ definiert und verwaltet werden. Standardberechtigungen finden bei diesem Werkzeug keine Anwendung. Das zu korrigierende Dokument wird dupliziert und die Veränderungen können mit der „Korrektur verfolgen“-Funktion von Microsoft Word bzw. Excel verfolgt werden.

Files Tool

Mit dem Dateiwerkzeug können gemeinsame Dateien entsprechend der Berechtigungen hinzugefügt, verändert und gelöscht werden. Bei diesem Werkzeug kann auch die Berechtigung zum Ändern der Berechtigungen an andere Benutzergruppen vergeben werden. Groove startet zum Lesen bzw. Bearbeiten von Dokumenten die verknüpften Anwendungen. Weitere Ausführungen zu dieser Komponente folgen in Kapitel 5.4.

Dashboard Tool

Das Dashboard Tool ist nur in der Professional Edition von Groove Workspace verfügbar. Es enthält die zwei Ansichten Persönliches (Personal) und Projekt (Project),

dabei werden hauptsächlich Informationen aus den Werkzeugen Meeting und Projekte übernommen. In der Projektansicht sollen Zeitpläne, kritische Projektaufgaben(Meilensteine), Zielstellungen sowie Risiken und Probleme wiedergegeben werden. Die persönliche Ansicht enthält eine Übersicht von Meetings, in denen der Nutzer Teilnehmer ist, Kurznachrichten von Projektleitern und eine „to do“-Liste mit Aufgaben, die mit dem Meeting Tool bzw. Project Management Tool erstellt wurden.

Meeting Tool

Das Meeting Tool unterstützt die Organisation und das Durchführen von Meetings sowie das Festhalten der Ergebnisse. Eine Agenda kann mit Dateianhängen und Zeitvorgaben erstellt und die Aufgabe der Protokollführung delegiert werden. Aufgaben können sowohl vor einem Meeting als auch während des Verlaufes festgelegt, mit einer Priorität versehen, Personen zugewiesen und mit Anhängen versehen werden. Die Rahmendaten des Meetings, Agenda und Protokoll können nach Microsoft Outlook exportiert werden.
Die Benutzergruppenberechtigungen für dieses Werkzeug können nicht verändert werden und sind im Handbuch nicht weiter dokumentiert.

Project Manager Tool

Mit diesem Werkzeug sollen anfallende Aufgaben festgehalten und überwacht werden. Neben dem Zuweisen von Aufgaben an Verantwortliche, der Vergabe von Prioritäten und dem Verfolgen des Status einer Aufgabe ist auch die Formulierung von logischen Abhängigkeiten möglich. Das Werkzeug verfügt über verschiedene Ansichten, um die Anzeige der Aufgaben nach Verantwortlichen und/oder Status zu filtern. Der Import und Export von Daten der Projektmanagementkomponente funktioniert nur, wenn auf dem Rechner eine Installation von Microsoft Project der Version 98 oder neuer vorhanden ist. Das Berechtigungskonzept dieser Komponente wurde erweitert. Es können bei diesem Werkzeug auch Berechtigungen zum Ändern der Projektinformation und des Zeitplanes zugewiesener Aufgaben vergeben werden.

Notepad Tool

Mit dem Notepad Tool können Notizen mit einigen Formatierungsmöglichkeiten erstellt werden. Änderungen an einem Dokument werden erst nach dem Speichern der „Seite“ an die anderen Arbeitsgruppenmitglieder gesendet. Eine Benachrichtigung

beim Öffnen eines Dokumentes, das bereits durch andere Teilnehmer bearbeitet wird, weist auf das Entstehen von persönlichen Kopien hin. Mechanismen zum Zusammenfügen derart verwandter Dokumente sind nicht beschrieben, es wird allerdings eine Verknüpfung zum ursprünglichen Dokument angelegt.
Das Berechtigungskonzept unterscheidet nur zwischen dem Erstellen, Bearbeiten und Löschen von Notizen sowie der Berechtigung zur Benutzung des Werkzeuges.

Outliner Tool

Das Outliner Tool unterstützt Brainstorming-Sitzungen, indem es als zeilen- bzw. stichwortorientierter Texteditor das Verschieben, sowie Ein- und Ausrücken von Einträgen ermöglicht. Neben diesen Strukturierungsmöglichkeiten sind die grundlegenden Formatierungsmöglichkeiten(**F**, *K*, U) vorhanden. Die hierarchische Struktur lässt sich zur besseren Übersicht falten.
Das Berechtigungkonzept dieser Komponente umfasst lediglich das Bearbeiten von Einträgen und Verwenden der Komponenten.

Pictures Tool

Mit diesem Bildwerkzeug können Grafiken der Formate BMP und JPEG angezeigt und verwaltet werden. Bilder können, entsprechend der eingestellten Benutzergruppenrechte hinzugefügt, umbenannt und gelöscht werden.

Text Tool

Das Text Tool ist ein „Echtzeit“-Editor. Der eingegebene Text wird unmittelbar an die anderen Arbeitsgruppenmitglieder versendet. Folglich ist der Protokoll- und Verwaltungsanteil einer Delta-Mitteilung umso größer, je langsamer geschrieben wird. Es wird im schlimmsten Fall nur ein Eingabezeichen übertragen, wofür allerdings mehrere Zeichen benötigt werden, um die Delta-Mitteilung als XML-Objekt darzustellen.
Neben den grundlegenden Formatierungsmöglichkeiten(**F**, *K*, U) sind Ausrichtungsfunktionen (linksbündig, zentriert, rechtsbündig sowie Anführungen und Ein- und Ausrücken) vorhanden.
Zur Benutzerrechteverwaltung können nur die Lese- und Schreibzugriff vergeben werden.

Sketchpad Tool

Um Skizzen anzufertigen, die verschiedene Formen, Farben und Text enthalten, kann das Sketchpad-Werkzeug verwendet werden. Objekte können beispielsweise verschoben, vergrößert, verkleinert oder in Ebene angeordnet werden. Jeder Skizze kann ein Name gegeben werden.
Benutzerrechte für Arbeitsgruppenmitglieder können für die Interaktion mit dem Werkzeug (Erstellen, Ändern und Löschen) und das Betrachten der Komponente eingestellt werden.

Web Browser Tool

Die Web Browser Komponente verfügt über die üblichen Navigationselemente, eine strukturierte Favoritenverwaltung und eine Option zum gemeinsamen Browser von Webseiten. Diese kann entweder durch Auswählen des entsprechenden Kontrollkästchens aktiviert werden oder wird zusätzlich eingeschaltet, wenn das Kontrollkästchen „gemeinsame Navigation“ aktiviert wird.
Für diese Komponente ist keine Einschränkung von Berechtigungen möglich.

Welcome Page

Auf der Willkommen-Seite können eine Beschreibung der Arbeitsgruppe sowie aktuelle Nachrichten(Notizen) hinterlegt werden. Während die Beschreibung nur nach Beendigung von Eingabe/Änderung des Textes aktualisiert wird, wird die Änderung der Notizen sofort an die anderen Arbeitsgruppenmitglieder versendet. Die Willkommen-Seite enthält zusätzlich eine Übersicht aller eingebundenen Werkzeuge und deren Versionen. Die Versionsinformationen sind beispielsweise zu berücksichtigen, wenn ein neues Arbeitsgruppenmitglied bereits Groove verwendet, aber seine Komponenten nicht der Version der Arbeitsgruppe entsprechen.

Groove Games

Zur kurzweiligen Unterhaltung sind die Spiele Schach und Tac-Tac-Toe als Komponenten verfügbar. Bei dem Schachspiel sind allerdings keine Regeln hinterlegt, sodass sich die Beteiligten selbstständig auf Regeln einigen und deren Einhaltung überwachen müssen.

Das Spiel Tic-Tac-Toe bietet hingegen keine Betrugsmöglichkeiten, da X und O abwechselnd von den Spielern zu setzen sind und der andere Mitspieler keine „Manipulationen“ vornehmen kann.

4 Sicherheit und Groove

4.1 Taxonomie der Schlüssel in Groove

Grundlage für das Verständnis der Sicherheitsarchitektur von Groove ist die Kenntnis der eingesetzten Schlüssel bzw. Verschlüsselungen[15]. Im Folgenden ist eine Übersicht der in Groove verwendeten Schlüssel mit Angabe der Verschlüsselungsalgorithmen, Verwendungszweck und Dauer der Gültigkeit dargestellt.

a) Eine Passphrase pro Nutzerkonto (Account)

Verschlüsselung: Keine Angabe zur Verschlüsselung. Unicode Zeichenkette beliebiger Länge und Gestalt, die auf dem Rechner gespeichert werden kann, was allerdings nicht empfohlen wird.
Verwendung: Ein Passwortsatz(mehrere Wörter) sichert den Zugriff auf das Nutzerkonto auf einem Endgerät und dient der Ableitung eines symmetrischen Schlüssels.
Gültigkeit: Bis geändert wird oder entsprechend der Unternehmensrichtlinien regelmäßig geändert werden muss. Ist ein Nutzerkonto auf mehreren Geräten verfügbar, „muss“ die Passphrase überall von Hand geändert werden.

b) Ein symmetrischer Schlüssel pro Nutzerkonto

Verschlüsselung: MARC4 Schlüssel generiert aus der Passphrase mittels PBKDF2-Algorithmus.
Verwendung: Schützt Nutzerkonto, genauer gesagt, den „storage key“ für die Nutzerkonto-Datei.
Gültigkeit: Ist direkt von der Passphrase abhängig.

c) Erstes asymmetrisches Schlüsselpaar pro Identität

Verschlüsselung: ElGamal/RSA[16]
Verwendung: Signatur und Verifikation; Identifizierung von Einladungen, Kurznachrichten und öffentlichen Diffie-Hellman Schlüsseln
Gültigkeit: keine Angabe

[15] Vgl. Udell et. al. /Security/ 20
[16] Vgl. Groove /Security Bulletin/ 1

Aufbewahrung: Wird im Nutzerkonto gespeichert und kann nicht geändert werden. Öffentlicher Schlüssel wird in Kontaktinformationen(Adressbuch) der Identität hinterlegt.

d) Zweites asymmetrisches Schlüsselpaar pro Identität

Verschlüsselung: ElGamal

Verwendung: Ver- und Entschlüsselung symmetrischer Schlüssel, die zur Verschlüsselung von Einladungen und Instant Messages verwendet werden.

Gültigkeit: keine Angabe

Aufbewahrung: Wird im Nutzerkonto gespeichert und kann nicht geändert werden. Öffentlicher Schlüssel wird in Kontaktinformationen der Identität hinterlegt.

e) Ein digitaler Fingerabdruck

Verschlüsselung: Hash der beiden obigen öffentlichen Schlüssel.

Verwendung: Ermöglicht Groove-Anwender (Idenitäten) sich zu authentifizieren.

Gültigkeit: Da aus den unveränderlichen Schlüsseln einer Identität berechnet, ist der Fingerabdruck für die Dauer der Existenz einer Identität gültig.

Aufbewahrung: Wird im Nutzerkonto gespeichert und ist der Visitenkarte einer Identität einsehbar.

f) Ein Diffie-Hellman Schlüsselpaar pro Identität und Arbeitsgruppe

Verschlüsselung: Wird deterministisch berechnet aus den zwei privaten asymmetrischen Schlüsselhälften und einer GUID (24Byte zufällige global eindeutige ID) der Arbeitsgruppe.

Verwendung: Erzeugung von paarweisen Schlüsseln aus den Diffie-Hellman-Schlüsseln der Beteiligten.

Gültigkeit: keine Angabe

g) Paarweiser Schlüssel K_{ij} pro Arbeitsgruppenmitgliederpaar

Verschlüsselung: MARC4 aus zwei Diffie-Hellman Schlüsseln, klassisches „authentic Diffie-Hellman key agreement“(Zitat).

Verwendung: Sichern der Verteilung von Gruppenschlüssel, wenn diese erneuert werden.

h) Paarweiser Schlüssel L_{ij} pro Arbeitsgruppenmitgliederpaar

Verschlüsselung: HMAC-SHA1 aus zwei Diffie-Hellman-Schlüsseln

Verwendung: Sicherung der Authentizität und Integrität von Mitteilungen

Gültigkeit: von Gültigkeit der Diffie-Hellman-Schlüsseln abhängig

i) Erster Gruppenschlüssel K_G

Verschlüsselung: MARC 4

Verwendung: Sicherung des Vertrauens – in Arbeitsgruppenkopie gespeichert

Gültigkeit: Wird in der Arbeitsgruppenkopie gespeichert und erneuert, wenn ein Mitglied die Arbeitsgruppe verlässt.

j) Zweiter Gruppenschlüssel L_G

Verschlüsselung: HMAC-SHA1

Verwendung: Sicherung der Mitteilungsintegrität im Modus „vertrauenswürdige Umgebung“.

Gültigkeit: Wird in Arbeitsgruppenkopie gespeichert und erneuert, wenn ein Mitglied die Arbeitsgruppe verlässt.

k) Master Key

Verschlüsselung: MARC 4

Verwendung: Im Nutzerkonto gespeichert und daher durch Passphrase geschützter Schlüssel, der wiederum „storage keys“ schützen soll.

Gültigkeit: keine Angabe

l) Storage Key

Verschlüsselung: keine Angabe

Verwendung: Verschlüsselung der Daten auf Festplatte, Storage Keys für Arbeitsgruppen sind durch Master Key geschützt und in Arbeitsgruppendatei gespeichert, Storage Key für Nutzerkonto ist in Nutzerkontodatei gespeichert und durch Passphrase geschützt.

Gültigkeit: keine Angabe

Die Passphrase soll bei dieser Konzeption zum schwächsten Glied der „Kette“ werden.

In einer neueren Veröffentlichung über die Sicherheitsarchitektur werden die kryptographischen Algorithmen und Schlüssellängen in einer weniger detaillierten Übersicht wie folgt dargestellt:[17]

Kryptografische Operation	Algorithmus (default)	Schlüssellänge (default)
(asymmetrische) Public Key Signatur	RSA	2048 bit
(asymmetrische) Public Key Verschlüsselung	ElGamal	2048 bit
(asymmetrische) Public Key Signatur innerhalb von Arbeitsgruppen	ESIGN	1536 bit
(symmetrische) Secret Key Verschlüsselung	AES	192 bit
(symmetrischer) Secret Key Integritätsschutz	HMAC-SHA1	192 bit
(symmetrische) Passphrase basierte Verschlüsselung	PBE-MARC4	2048 bit
Passphrase-Schlüssel-Herleitung	PBKDF2 / SHA-1	N/A
Schlüsselverteilung (Key Agreement)	Diffie-Hellman	2048 bit

Die Algorithmen und Schlüssellängen können mittels XML-Templates verändert werden, ohne Änderungen in der Programmlogik vornehmen zu müssen.[18]
In den ersten Versionen von Groove wurde noch zwischen „vertrauenswürdiger Umgebung“ und „nicht-vertrauenswürdiger Umgebung“ unterschieden. [19] Dies ist jetzt nicht mehr der Fall. Es wird nun immer von einer „nicht-vertrauenswürdigen Umgebung“ ausgegangen. Entsprechend sind einige Schlüssel obsolet geworden, bzw. es kommen nun andere Verschlüsselungen zum Einsatz.

4.2 Sicherheitsaspekte aus verschiedenen Perspektiven

4.2.1 Vertraulichkeit, Authentizität und Integrität der Daten

Unter Vertraulichkeit der Daten wird die ausschließliche Lesbarkeit durch den Empfänger verstanden.[20]
Authentizität bedeutet Echtheit, Zuverlässigkeit bzw. Glaubwürdigkeit[21] und steht folglich für die Gewissheit, dass eine Nachricht wirklich von dem anscheinenden Absender stammt.
Integrität der Daten heißt, dass die Daten während der Übertragung nicht durch Dritte geändert werden können, ohne das dies bemerkt wird.[22]

[17] Groove /Security Bulletin/ 1
[18] Vgl. Groove /Security Bulletin/ 1
[19] Vgl. Groove /Security Bulletin/ 2f.
[20] Vgl. Lowell /Secure Internet Communications/ 4
[21] Vgl. Duden /Fremdwörterbuch/ 94

4.2.2 Sicherheitsaspekte auf Benutzerebene

Basierend auf den zwei öffentlichen Schlüsseln (ElGamal und RSA) wird für jede Identität ein digitaler Fingerabdruck berechnet, der für die manuelle Authentifizierung von Personen genutzt werden kann. Neben dieser so genannten „out-of-band"-Authentifizierung(„authenticated icon") sind seit der Version 1.2 der Groove Software weitere Authentifizierungsmechanismen verfügbar.
Es wurde eine Groove-spezifische Public Key Infrastruktur entwickelt. Zentrales Element einer PKI ist die Zertifizierungsstelle(CA). Diese Aufgabe wird vom Groove Enterprise Management Server übernommen. Innerhalb einer Management-Domäne können Zertifikate erstellt und verwaltet werden. Die Zertifikate werden im Adressbuch der „managed users" hinterlegt, sodass sich andere Nutzer über deren Identität versichern können. Nach diesem Verfahren authentifizierte Groove-Identitäten werden in der Anwendungssoftware mit einem entsprechenden Symbol(„intra-organization certification") versehen.[23]
Die Vertrauenswürdigkeit von Zertifikaten anderer Management-Domänen kann innerhalb der eigenen Domäne genutzt werden, indem die Administratoren auch Zertifikate von anderen Enterprise Management Servern zulassen. Somit kann ein Handelsvertreter beispielsweise auf das Zertifikat vertrauen, das einem Zulieferer oder Kunden durch ihr Unternehmen ausgestellt wurde(„inter-organization certification").

„authenticated icon"	
„intra-organization certification"	
„inter-organization certification"	

Wie der Tabelle unter 4.1 zu entnehmen ist, werden zwei Public Key - Schlüsselpaare zum Austausch von Nachrichten außerhalb von Arbeitsgruppen verwendet. Die RSA-Schlüssel werden zur Signatur und Verifizierung der Signatur verwendet und die Verschlüsselung bzw. Entschlüsselung erfolgt mit den Schlüsseln des ElGamal-Verfahrens. Damit ist nach einem sicheren Austausch der Schlüssel für Vertraulichkeit, Authentizität und Integrität der Kommunikation gesorgt.

[22] Vgl. Lowell /Secure Internet Communications/ 4
[23] Vgl. Groove /Security Bulletin/ 3f.

4.2.3 Sicherheitsaspekte auf Arbeitsgruppenebene

Einleitend soll die Abfolge des Schlüsselaustausches beschrieben werden, wenn eine neue Person(Identität) in eine Arbeitsgruppe eingeladen wird.[24]
Alice ist bereits Mitglied einer Gruppe und möchte Dave einladen. Dazu versendet Alice eine Einladung, die neben einer Nachricht an Dave auch den öffentlichen Schlüssel von Alice sowie die kryptographischen Arbeitsgruppeneinstellungen enthält. Dave kann die Einladung akzeptieren und sendet damit seine öffentlichen Schlüssel und seinen soeben generierten öffentlichen Schlüssel für die Arbeitsgruppe mit. Als nächstes werden durch Alice's Client die anderen Mitglieder der Arbeitsgruppe über das neue Arbeitsgruppenmitglied informiert. Sie erhalten die persönlichen und den arbeitsgruppenspezifischen öffentlichen Schlüssel von Dave. Schließlich sendet Alice eine Kopie des Arbeitsplatzes an Dave, welche neben allen öffentlichen und arbeitsgruppenspezifischen Schlüsseln der Arbeitsgruppenmitglieder auch den geheimen symmetrischen Arbeitsgruppenschlüssel enthält.
Die Übertragung zwischen Alice und Dave ist von Beginn an geschützt, wenn sie innerhalb des Groove Systems stattfindet, da die öffentlichen Schlüssel von Dave in den Kontaktinformationen enthalten sind
Allen Mitgliedern einer Arbeitsgruppe ist folglich ein geheimer symmetrischer Gruppenschlüssel (Secret Space Key) bekannt.[25] Dieser wird zur Verschlüsselung der Übertragung von Nachrichten und Deltas verwendet. Um die Authentizität der Nachricht zu sichern, unterzeichnet der Sender die verschlüsselte Nachricht mit seinem privaten Schlüssel(ESIGN). Der Empfänger kann sich mittels des öffentlichen Schlüssels von der Integrität der Nachricht vergewissern. Der Austausch(Key Agreement) des Gruppenschlüssels erfolgt über das Diffie-Hellman-Verfahren.

4.2.4 Sicherheitsaspekte der Nutzerdatenspeicherung

Wie bereits erwähnt, stellt die Passphrase das schwächste Glied der Verschlüsselung in Groove dar. Um keine zusätzlichen Schwachstellen einzubauen, werden die Schlüssel zur Datensicherung auf dem Endgerät von der Passphrase abgeleitet.[26]
Die Übersicht unter 4.1 führt unter b) einen symmetrischen Schlüssel an, der aus der Passphrase abgeleitet wurde. Folglich muss und sollte die Passphrase nicht auf dem Rechner gespeichert werden. Nach Eingabe der Passphrase wird entsprechend des

[24] Vgl. Lowell /Secure/ 11
[25] Vgl. Groove /Security Bulletin/ 2
[26] Vgl. für ganzen Absatz Udell et. al. /Security/ und Groove /Security Bulletin/ 1

PBKDF2 od. SHA-1 Algorithmus ein symmetrischer Schlüssel berechnet. Sind der berechnete Schlüssel und der gespeicherte Schlüssel identisch, so kann als nächstes auf den Master Key zugegriffen werden. Dieser Schlüssel basiert ebenfalls auf der Passphrase und dient der Ver- / Entschlüsselung der Storage Keys. Die Nutzerdaten und die Arbeitsgruppendaten sind in verschiedenen Dateien bzw. Speicherobjekten abgelegt und durch einen eigenen Storage Key gesichert.

4.3 Zusammenfassung

Wie bereits oben ausgeführt, wird bei der Verschlüsselung der Übertragung zwischen Arbeitsgruppenbeziehungen und Nicht-Arbeitsgruppenbeziehungen unterschieden.
Bei der Kommunikation innerhalb von Arbeitsgruppen erfolgt die Verschlüsselung zuvorderst durch einen geheimen symmetrischen Schlüssel (AES) der Länge 192 Bit. Indem jede Nachricht mit dem arbeitsgruppenspezifischen privaten Schlüssel unterschrieben wird, ist die Authentizität der Information gewährleistet.
Außerhalb von Arbeitsgruppen werden die beiden Public Key-Schlüsselpaare verwendet, um die Kommunikation zwischen Identitäten zu sichern. Die Schlüsselpaare werden automatisch nach dem Anlegen der Identität generiert und deren öffentliche Schlüssel in den Kontaktinformationen für die Clients veröffentlicht.
Außerdem ist festzustellen, das innerhalb der Arbeitsgruppen eine symmetrische Verschlüsselung verwendet wird, die im allgemeinen schneller funktioniert und die Sicherheit durch Geheimhaltung eines gemeinsamen Schlüssels und Signatur der Nachricht gewährleistet wird. In welcher Weise die angeführte symmetrische Verschlüsselung zur Integritätswahrung[27] verwendet wird, konnte im Detail nicht festgestellt werden.

5 Kommunikation und Dateiarbeit

5.1 Protokolle zur Kommunikation und Benachrichtigung

Offene Standards und Protokolle

Groove verwendet zur Kommunikation die Protokolle HTTP, UDP und TCP/IP.[28]
Zur Beschreibung der Information wird XML als Metastandard verwendet. Die genaue Bezeichnung der Kodierung(Scheme) ist nicht bekannt, da die XML-Daten zumeist verschlüsselt sind.

[27] Vgl. Groove /Security Bulletin/ 1
[28] Vgl. Groove /Product Backgrounder/ 8

Zur anwendungsübergreifenden Verständigung werden die Standards SOAP und XML-RPC verwendet.
Die Verwaltung von Identitäten erfolgt im vCard-Standard. Dazu können bei der serverseitigen Erstellung der Identitäten Informationen aus LDAP oder dem Active Directory verwendet werden.[29]

Groove Protokolle

Um festzustellen, welche Mitglieder einer Arbeitsgruppe gerade online sind, bzw. wie der Online-Status von Groove-Kontakten ist, werden automatisch Nachrichten entsprechend des Device Presence Protocol (DPP) versendet. Diese Discoveryfunktion[30] wird sowohl vom Transceiver als auch von den Relay-Servern ausgeführt.
Der Transceiver meldet den Online-Status von Arbeitsgruppenmitgliedern im lokalen Netz auch dann zuverlässig, wenn der Zugriff auf das Internet vorübergehend unterbrochen ist.
„The Simple Symmetric Transport Protocol (SSTP) connects clients to clients, clients to relays, and relays to relays. It's SSTP that propagates information about a delta message, including its target endpoint.“[31] Mit diesem proprietären Protokoll werden die Informationen zwischen Clients ausgetauscht, egal ob direkt oder indirekt.

5.2 Kommunikationsmechanismen

Ob es zu einer direkten oder indirekten Kommunikation mit einem anderen Groove-Anwender kommt, hängt von mehreren Tatsachen ab. Befindet sich ein Nutzer beispielsweise hinter einer Firewall oder ist er nur über eine Wahlverbindung zum Internet verbunden, so kommt es zu einer indirekten Verbindung.
Groove-Anwender, die sich hinter einer Firewall befinden, kann es untersagt sein „Inbound“-Verbindungen aufzubauen. Die Groove-Clients können folglich nicht direkt miteinander kommunizieren. In solchen Fällen werden die SSTP-Pakete in HTTP-Pakete eingepackt und über einen Proxy(Relay-Server) versendet. Dieser entpackt das HTTP-Paket und schickt das SSTP-Paket entweder direkt oder indirekt an den Empfänger weiter.

[29] Vgl. Groove /Enterprise Management Server/ 1
[30] Vgl. Gupta /Platforms/ 3
[31] Udell et.al. /Security/ 11

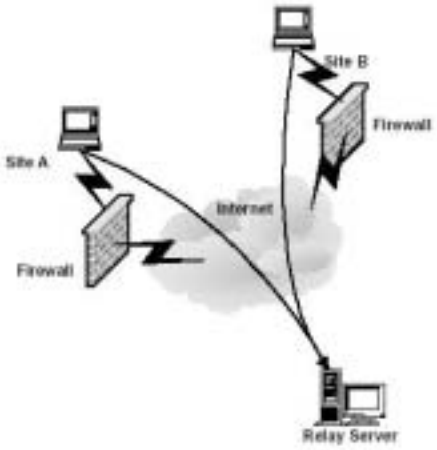

Abbildung 5-1: Groove Relay Server Mechanismus

Ist ein Groove-Anwender nur mit einer geringen Bandbreite an das Groove-Netzwerk angeschlossen, so wäre es aus Kosten- und Zeitgründen ungünstig, wenn er die Deltas an alle Arbeitsgruppenmitglieder selbstständig versenden müsste. Wird eine solche Situation von der Groove-Software festgestellt, so werden die Informationen nicht (mehrfach) direkt an alle Clients, sondern nur einmal an den Relay-Server gesendet und automatisch weiter verteilt. Dieser Mechanismus wird Fan-Out genannt.[32]

5.3 Benachrichtigungsmechanismen

Das Device Presence Protocol (DPP) stellt fest, ob eine Client erreichbar ist und auf welchen Endgeräten welche Identitäten gerade aktiv sind. Das Protokoll wird sowohl vom Transceiver als auch vom Relay Server verwendet. Falls einer der Groove-Anwender sich hinter einer Firewall befinden sollte, können die Clients nicht ohne die Hilfe eines Relay Servers kommunizieren und sich folglich auch nicht „sehen“.
Auf dem DPP basierend sorgt die „Groove-Awareness“ dafür, dass die Clients immer auf dem aktuellen Stand der Arbeitsgruppe bleiben. In Abhängigkeit von den Werkzeugen werden Änderungen sofort, wie beispielsweise bei dem Text Tool, oder erst nach dem Speichern einer Seite wie bei dem Notepad Tool, propagiert. Die Änderungen werden in den anderen Clients automatisch vorgenommen und an mehreren Stellen durch das Symbol in Abbildung 5-2 vermerkt.[33]

Abbildung 5-2: Ungelesen-Icon

[32] Vgl. Udell et. al. /Security/ 11
[33] Anm.: Vermerke erfolgen in direkter Nähe der Änderung, an der Werkzeugauswahlleiste und in Arbeitsgruppenübersicht

5.4 Dateiaustausch und -abgleich

Der Groove Workspace hält drei Werkzeuge(Files Tool, Document Review Tool und Pictures Tool) bereit, mit denen Dateien „ausgetauscht“, bearbeitet bzw. betrachtet werden können. Ein Dateiaustausch findet derart statt, dass ein Nutzer ein Bild in das Archiv des „Picture Tool“ hinzufügt oder eine beliebige Datei in das Archiv des „File Tool“ aufnimmt. Die Dateien werden verschlüsselt im XML-Objekte-Speicher[34] abgelegt und sofort an die anderen Arbeitsgruppenmitglieder übertragen, insofern sie online sind. Während bei einer Kommunikationsbeziehung per Mail Änderungen und neue Versionen eines Dokumentes zur Übertragung der gesamten Datei führen, wird der Übertragungsaufwand in Groove schon mit der ersten Änderung gering gehalten, indem nur die binären Änderungen übertragen werden. Diese so genannten „Binary Differentials“ (Binary Diffs) sind gleichzeitig ein Argument gegen Sicherheitsbedenken, da es sich um verschlüsselte Dateiauszüge handelt.[35]

Die Binary Diffs, auch Delta genannt, werden nicht nur im Zusammenhang mit Dokumenten verwendet. Da sämtliche Inhalte in Groove als XML-Objekte formatiert und gespeichert werden, findet der Abgleich von Inhalten mittels dieser Delta-Nachrichten überall Anwendung und gestaltet die Nutzung der Übertragungskapazität effizient. Durch die sofortige Übertragung stehen allen Anwendern sämtliche Dateien zur Verfügung. Die Problematik der Discovery-Mechanismen[36] ist folglich kein Thema in einem Groove-Netzwerk. Dies liegt vor allem daran, dass bei einer Groupware-Anwendung eine begrenzte Anzahl von Personen gemeinsam an einem Thema arbeitet und folglich zumindest über Leserechte an den Dateien verfügen. Um den Nutzer auf neue und geänderte Dokumente hinzuweisen wird der bereits oben beschriebene Mechanismus zur Kennzeichnung neuer Inhalte verwendet.

Obwohl das Lesen von bestimmten Dokumenten auch ohne die verknüpften Anwendungen installiert zu haben möglich sein soll, können andererseits Projektdaten ohne eine „MS Project“-Installation weder importiert noch exportiert werden.[37]

[34] Vgl. Udell et. al. /Security/ 5
[35] Vgl. Groove /Bandwidth/ 2
[36] Im Sinne von Auffinden von Ressourcen innerhalb des Netzwerkes
[37] Vgl. Groove /Workspace/ 1 und Groove /UsersGuide/ 224f.

6 Groove Enterprise Server

6.1 Groove Enterprise Relay Server

Das Relaying als Umwandern einer Firewall und die Bandbreitenoptimierung wurden anfänglich als „Hosted Services“[38] von Groove zur Verfügung gestellt. Unternehmen haben aber durchaus ein Interesse, das Risiko der Verfügbarkeit dieser Dienste selbst zu tragen. Folglich hat Groove diese und weitere Funktionen zu einem eigenständigen Produkt entwickelt. Im folgenden werden die Hauptfunktionen der Serveranwendung „Groove Enterprise Relay Server“ vorgestellt.[39]

Asynchrone Kommunikation

Um das Senden und Empfangen von Informationen zu ermöglichen, wenn alle anderen Arbeitsgruppenmitglieder offline sind, wird ein „store-and-forward“-Mechanismus eingesetzt.

Bandbreitenoptimierung

Für jeden Nutzer wird individuell festgestellt, ob Daten direkt an andere Nutzer übertragen werden oder ob sie an den Relay Server gesendet werden und dieser die Informationen verteilt. Dies verbessert vor allem effizientes Arbeiten per Wahlverbindung.

Online-Offline-Status

Verfolgen des Online-Offline-Status entsprechend des DPP. Trifft vorwiegend auf Nutzer zu, die sich hinter einer Firewall befinden.

Firewall / Proxy Transparenz

Sollten eingehende Verbindungen aus dem Netzwerk zu dem Client gesperrt sein, so kann der Client mittels HTTP (z.B. Port 80) versuchen einen Relay Server als Proxy zu verwenden.

Reporting

Es können verschiedene Informationen auf dem Server über die verwalteten Verbindungen geloggt werden. Beispielsweise Volumen der Deltas, Anzahl der Instant Messages, Anzahl der aktiven Verbindungen.

Identity Handling

[38] Vgl. Groove /Hosted Services/ 1ff.
[39] Ganzer Abschnitt Vgl. Peer Development /GrooveServer/ 7ff., Groove /Enterprise Relay Server/ 1f.

Es können Nutzeridentitäten verwaltet werden, Abhängigkeiten von Identitäten und Endgeräten hinterlegt werden und registrierte und nicht-registrierte Benutzer unterschieden werden.

Quota

Es können Quotas für zu 'cachende' Datenmengen auf Benutzerebene festgelegt werden. Die individuelle Verwaltung erfolgt über den Management Server.

6.2 Groove Enterprise Management Server

Der Groove Enterprise Management Server dient der „zentrale(n) Administration und Management der Groove Infrastruktur innerhalb einer Unternehmung“[40]. Im folgenden sollen die Hauptaufgaben des Servers vorgestellt werden.[41]

User Management

Ermöglicht das Erstellen und Verwallten von Nutzeridentitäten, sowie das Einrichten von zeitlich beschränkten Nutzerkonten.

Policy Management

Unterstützung beim Erstellen von Regeln für Nutzer und Endgeräte. Festlegen von zulässigen Groove Komponenten und Servern, von denen die Komponenten geladen werden dürfen. Verwalten digitaler Signaturen von Software-Herstellern. Unterstützt das Festlegen von Regeln für Passphrase (Länge, Gültigkeitsdauer, Struktur).

Reporting

Erstellen von Berichten über die Domäne, enthält Informationen über Benutzer (-aktivitäten), Arbeitsgruppen und verwendete Werkzeuge.

LDAP Support

Auslesen von Nutzerinformationen mit LDAP zur Erstellung bzw. Überprüfung von Identitäten.

Relay Server Integration

Einbindung eines oder mehrerer Relay Server. Die Administration erfolgt im Management Server.

Verwalten von Groove Domänen

Abbilden von Nutzergruppenhierarchien und Zuweisen von Berechtigungen auf Nutzergruppenebene, um beispielsweise Unternehmenshierarchien abzubilden. Dient

[40] Peer Development /GrooveServer/ 18

[41] Ganzer Abschnitt Vgl. Peer Development /GrooveServer/ 18ff., Groove /Enterprise Management Server/ 1

als Zertifizierungsstelle(CA) für die Domäne und ermöglicht das Verwalten von Signaturen anderer Groove-Domänen-Server (Querzulassung).

SQL Datenbankintegration

Daten werden nicht auf dem Anwendungsserver, sondern in einer Datenbank gespeichert.

6.3 Groove Enterprise Integration Server

Der Groove Enterprise Integration Server ermöglicht den Zugriff auf externe Anwendungssysteme und Datenquellen.[42]

Informationsaustausch mit externen Systemen

Der Integration Server als Bestandteil der Groove Architektur greift auf externe Datenquellen zu. Dies sind beispielsweise SQL-Datenbanksystem, Notes-Server oder ERP-Anwendungen. Der Server ermöglicht autorisierten Nutzern(Agenten) einen bidirektionalen Zugriff auf andere serverbasierte Systeme. Die Informationen werden dann der ganzen Arbeitsgruppe zur Verfügung gestellt.

Agenten (Bots)

So genannte Agenten dienen der Single-Point Integration von externen Systemen in die Groove Umgebung. Mehrere Bots mit elementaren Aufgaben können zu einem Dienst zusammengefasst werden. Diese Dienste können als Identität eingeladen werden und funktionieren zeit- und/oder ereignisgesteuert. Die Bots laufen in der „Integration Server“-Umgebung und werden dort auch verwaltet. Dabei sind neben der Lebensdauer auch die Zugriffsberechtigungen auf die externen Systeme und Informationen konfigurierbar.

[42] Ganzer Abschnitt Vgl. Peer Development /GrooveServer/ 28ff. und Groove /Enterprise Integration Server/ 1f.

6.4 Fazit

Obwohl sich Groove als P2P-Anwendung sieht, geht der dezentrale Charakter streng genommen durch die Integration der Server verloren und es handelt sich eher um eine hybride Architektur. Dies ist zum einen dem Relay-Mechanismus geschuldet, zum anderen den fortgeschrittenen Funktionen(Public Key Technologie, punktuelle Integration externer Systeme), welche das System mittlerweile bietet.
Einige der Funktionen waren schon von Beginn an als „Hosted Services“ verfügbar, andere sind im Laufe der Zeit entstanden und haben das Anwendungsspektrum erweitert(Integration Server) oder auf eine professionelle Ebene geführt(Management Server).

7 Zusammenfassung

Die Kommunikationsarchitektur basiert auf einer Objektbeschreibung in der Metasprache XML und geht schonend mit Netzwerkressourcen um, indem nur Änderungsdaten(Delta) übertragen werden. Groove ist als P2P-Anwendung konzipiert und umgesetzt worden. Die angeführten Serveranwendungen dienen der Funktionserweiterung in einem professionellen Umfeld bzw. erhöhen die Reichweite einer Arbeitsgruppe, indem Firewall-Anwendungen umgangen werden können.
Das Sicherheitskonzept wird ständig weiterentwickelt und besteht aus bekannten Verschlüsselungskonzepten(PKI) und Verschlüsselungsalgorithmen.
Groove Workspace besitzt die Vorteile einer dezentralen Anwendung und bietet in bezug auf Sicherheitsaspekte und Nutzer-Management einige interessante Ansätze.

8 Literaturverzeichnis

Duden /Fremdwörterbuch/

Wissenschaftlicher Rat der Dudenredaktion (Hrsg.): Duden Fremdwörterbuch. 5. Aufl. Mannheim u.a. 1990

Groove /Bandwidth/

Groove Networks Inc.: Decentralized Collaboration: Good for Bandwidth. http://www.groove.net/pdf/Groove_and_Bandwidth.pdf, Abruf am 30.07.2002

Groove /Enterprise Integration/

Groove Networks Inc.: Enterprise Integration – Groove Brief. http://www.groove.net/pdf/brief-ent_integration.pdf, Abruf am 23.07.2002

Groove /Enterprise Integration Server/

Groove Networks Inc.: Groove Enterprise Integration Server Datasheet. http://www.groove.net/pdf/ds_geis.pdf, Abruf am 30.07.2002

Groove /Enterprise Management Server/

Groove Networks Inc.: Groove Enterprise Management Server Datasheet. http://www.groove.net/pdf/ds_gems.pdf, Abruf am 30.07.2002

Groove /Enterprise Relay Server/

Groove Networks Inc.: Groove Enterprise Relay Server Datasheet. http://www.groove.net/pdf/ds_gers.pdf, Abruf am 30.07.2002

Groove /Hosted Services/

Groove Networks Inc.: Groove Hosted Services – Groove Brief. http://www.groove.net/pdf/brief-hosted_services.pdf, Abruf am 23.07.2002

Groove /Product Backgrounder/

Groove Networks Inc.: Product Backgrounder. http://www.groove.net/pdf/backgrounder-product.pdf, Abruf am 23.07.2002

Groove /Security Bulletin/

Groove Networks Inc.: Groove Security Bulletin.
http://www.groove.net/pdf/security_bulletin.pdf, Abruf am 30.07.2002

Groove /UsersGuide/

Groove Networks Inc.: User's Guide – Groove 2.0.
http://www.groove.net/pdf/usersguide.pdf, Abruf am 30.07.2002

Groove /Workspace/

Groove Networks Inc.: Groove Workspace Datasheet.
http://www.groove.net/pdf/ds_workspace.pdf, Abruf am 30.07.2002

Gupta /Platforms/

Nitin Gupta, Peer to Peer Computing-Platforms.
http://netserver.cerc.wvu.edu/classes/cs491h_summer2_2001/gupta_platforms/termpaper.doc, Abruf am 27.08.2002

Lowell /Secure Internet Communications/

Abbott Lowell: Secure Internet Communications.
http://conferences.oreillynet.com/presentations/p2pweb2001/Lowell_A_1748.ppt, Abruf am 21.08.2002

Minar /Topologies/

Nelson Minar: Distributed Systems Topologies: Part1.
http://www.openp2p.com/pub/a/p2p/2001/12/14/topologies_one.html, Abruf am 30.07.2002

Ozzie /GrooveSystemsIntegration/

Jack Ozzie: Systems Integration with Groove.
http://www.groove.net/developers/presentations/groovesystemsintegration.ppt, Abruf am 23.07.2002

Peer Development /GrooveServer/

Peer Development GmbH: Groove Enterprise Server. http://www.she.de/images/SHE/Internet/GrooveServerAlle.pdf, Abruf am 27.08.2002

Suthar, Ozzie /GrooveSharedSpaceArchitecture/

Paresh Suthar, Jack Ozzie: The Groove Shared Space Architecture. http://www.groove.net/developers/presentations/GrooveSharedSpaceArchitecture.ppt, Abruf am 23.07.2002

Udell et. al. /Security/

Jon Udell, Nimisha Asthagiri, Walter Tuvell: Chapter 18 – Security: in Peer-to-Peer: Harnessing the Power of Disruptive Technologies. http://www.groove.net/pdf/chapter18-security.pdf, Abruf am 30.07.2002