Designdokument: Software Challenge

Stand: 31. Mai 2009 17:07 Uhr
Version: 1.0a

Autoren:

Christian Wulf

Florian Fittkau

Marcel Jackwerth

Raphael Randschau

Inhaltsverzeichnis

1. Einleitung

Dieses Dokument stellt eine Dokumentation bezüglich des Designs von Software Challenge dar. Es richtet sich in erster Linie an Personen, von denen weiterentwickelt werden soll, da hier das Verständnis des bestehenden Designs essenzieller Natur ist. Es existiert bereits ein Pflichtenheft, welches die grundlegenden Features des zu erstellenden Systems zusammenfasst. Des Weiteren sind verschiedenste Use Cases notiert, welche einen genaueren Überblick über die geplanten Programmabläufe geben.

1.1. Verweise

Um eine möglichst einfache Entwicklung insgesamt zu gewährleisten, wurde Eclipse als IDE verwendet. Eclipse1 ist eine kostenfreie Plattform, welche nativ die Sprache Java unterstützt. Da in Java 1.5 realisiert wurde, wird angenommen, dass der Leser vertraut im Umgang mit Java allgemein und im speziellen mit den Features der Version 1.5. Java ist eine freie Programmiersprache, welche von Sun entwickelt wird. Java und weitere Informationen können von der Internetpräsenz von Sun2 bezogen werden. Zur Erstellung und Visualisierung des Designs wurde Omondo3 verwendet. Omondo ist ein Plug-In für Eclipse, welches auf die Erstellung und Darstellung von UML-nahen Inhalten spezialisiert ist. In dem häufig referenzierten Buch „Design Patterns: Elements of Reusable Object-Oriented Software“ von den Autoren Erich Gamma, Richard Helm, Ralph Johnson und John Vlissides werden alle verwendeten Patterns ausführlich erläutert. Bezüglich der Verschlüsselungs- und Signierungsalgorithmen baut auf eine Crypto-Bibliothek namens „FlexiProvider“ auf. „FlexiProvider“ ist ein Produkt des Fachgebiets Theoretische Informatik an der Technischen Universität Darmstadt. Ausführlichere Informationen über diese Bibliothek können auf der Internetseite4 eingesehen werden. Da FlexiProvider ausschließlich eine Implementierung der von der JCA/JCE (Java Cryptographic Architecture/Extension) definierten Schnittstellen ist, lohnt ein Blick auf die Entsprechenden Ausschnitte der umfangreichen Dokumentation5 von Sun. Um die Verwendung der PKCSs (Public Key Cryptographic Standards) zu gewährleisten wird ein Codec Package des Fraunhofer Instituts für graphische Datenverarbeitung verwendet. Dieses kann ebenfalls von 1 bezogen werden. Im Zuge der Sicherung der sensiblen Daten wird auf den Java KeyStore6 zugegriffen. Dies ist ein System, welches auf die sichere und persistente Speicherung von Schlüsseln und Zertifikaten spezialisiert ist. 1

1.2. Überblick

Kapitel 2 wird einen kurzen Abriss über die Gesamtstruktur des Systems geben. Hier wird das bestehende Design in seiner Gesamtheit und sehr abstrakt analysiert. In Kapitel 3 wird genauer auf das Design eingegangen. Die wichtigsten Abstraktionsebenen und Designentscheidungen werden hier ausführlich behandelt. Dies bedeutet, dass auch Alternativen vorgestellt und kritische betrachtet werden. In Kapitel 4 folgt eine Kurzbeschreibung der eingesetzten Patterns. Kapitel 5 rundet dieses Dokument mit einer konkreten Analyse der Mechanismen ab, welche das Design von Crypt2Go ausmachen.

2. Systemüberblick

Allgemeine Systemübersicht. zB Packageabhängigkeit über die Interfaces oder ähnliches.

3. Designüberlegungen

3.1. Annahmen und Vorüberlegungen

Allgemeine Annahmen zB nur 1000 Knoten im Netz oder ähnliches

3.2. Allgemeine Vorgaben und Bedingungen

Performance:

3.3. Designziele

Erweiterbarkeit:

4. Systemarchitektur

4.1. Beschreibung der Interaktion zwischen Paketen/Komponenten

5. Pakete

Beschreibung der Pakete

5.1. GUI

5.1.1. Transfer

5.2. Logic

6. Entwurfsmuster

Verwendete Entwurfsmuster (kurze Vorstellung dieser)

6.1. Singleton

7. Klassen

Beschreibung der Klassen nach Packagereihenfolge

7.1. GUI

7.1.1. FactoryCreater

8. Dynamik

Beschreibung der Dynamik für ausgewählte Aufrufe (zB Benutzer Use Cases)

8.1. Identifikation

8.2. Datei hochladen

8.3. Datei herunterladen

8.4. Speicherplatz freigeben

A. Anhang

A.1. evtl Klassendiagramme/Paketdiagramme

Glossar

Backup
Sicherungskopie einer Datei oder eines ganzen Ordners.

BaseTorrent file
Eine Datei (oder ein Ordner), die auf irgendeine Art und Weise im BTN bekannt ist.

BaseTorrent file part
Ein Daten-Teil bzw. Stück einer BTF.

BaseTorrentApplikation
Das Programm, welches den Zugang zum BTN ermöglicht und Benutzereingaben verarbeitet.

BaseTorrentNetzwerk
Peer2Peer Netzwerk aus Rechnern in verschiedenen Netzwerken.

Daten
Dateien sowie ganze Ordner, die wiederum Ordner und Dateien enthalten können.

Hash
Eine Zahlen und Buchstabenfolge, die aus einer Datei zur Identifikation und Validierung gebildet wird.

IP
Eine Adresse, die zur Identifikation im Netzwerk verwendet wird.

Meta-Daten
Informationsdaten über bestimmte Daten, z.B. ”Teil x von yöder der Dateiname.

Node
Im Allgemeinen eine andere Bezeichnung für einen Peer, die in den Vordergrund stellt, dass andere Peers über diesen Peer erreichbar sind.

Orgware
Rahmenbedingungen bei IT-Projekten, die nicht unter Hardware oder Software fallen.

Part-Passwort
Bei Backups wird neben dem Autorennamen im Klartext dieser zusätzlich nochmal in verschlüsselter Form gespeichert, um den Ersteller eindeutig zu identifizieren. Dieses Passwort wird Part-Password genannt und ist Teil der verschlüsselten Meta-Daten, aus denen nur der Inhaber das Passwort rekonstruieren kann.

Peer
Ein Rechner im Netzwerk, der sowohl als Client als auch als Server fungiert.

Peerliste
Die Liste von allen Nodes im BTN.

Port
Ein Tor, um den richtigen Dienst auf dem Zielrechner anzusprechen.

Redundanzqualität
Die Redundanzqualität k ist der Grad bzw. die Anzahl der Verteilungen eines BTFP im BTN. $k = min(\lceil 3 \cdot \log |\text{Peerliste}| \rceil, |\text{Peerliste}|)$, d.h. ein fester Wert, damit alle Benutzer gleichberechtigt verteilen.

TCP
Ein Protokoll zur Nachrichtenübertragung in einem Netzwerk; speziell zur Übertragung von großen Datenmengen geeignet.

Tracker
Ein Server-Programm, dass den Clients Informationen über die im BaseTorrent-Netzwerk verteilten Dateien liefert, insbesondere den Aufenthaltsort der einzelnen Teile einer konkreten Datei.

UDP
Ein Protokoll zur Nachrichtenübertragung in einem Netzwerk.

XML
Eine spezielles Dateiformat mit <tag></tag> Struktur.

Acronyms

BTA
BaseTorrentApplikation.

BTF
BaseTorrent file.

BTFP
BaseTorrent file part.

BTN
BaseTorrentNetzwerk.