Bewertungskriterien und ihre Anwendung zur Evaluation und Entwicklung sicherer Sync&Share-Dienste

Kevin Koerner[1] Holger Kuehner[3] Julia Neudecker[2]
Hannes Hartenstein[3] Thomas Walter[1]

[1] vorname.nachname@uni-tuebingen.de
[2] vorname.nachname@student.uni-tuebingen.de
[3] vorname.nachname@kit.edu

Abstract:
Der Schutz der Vertraulichkeit von Daten, die in Sync&Share-Systemen vorgehalten werden, ist für viele Anwendungen im Umfeld von Hochschulforschung und -lehre unerlässlich. Um die Anforderungen an einen sicheren Sync&Share-Dienst spezifizieren zu können, der möglicherweise hochschulübergreifend betrieben wird, ist es unverzichtbar, sich des Vertrauensmodells zwischen den unabhängig betreibbaren Systemkomponenten bewusst zu sein. Eine zentrale Fragestellung hinsichtlich des Vertrauensmodells ist die Frage der Zugriffskontrolle auf die einzelnen Systemkomponenten. Anforderungen an diese müssen zum genauen Verständnis und somit zur Fehlervermeidung möglichst feingranular definiert werden. Bisherige Arbeiten haben diese Aspekte nicht hinreichend betrachtet. Im vorliegenden Dokument stellen wir einen von uns erstellten Anforderungskatalog für die Evaluation und Entwicklung sicherer Sync&Share-Dienste vor, der insbesondere die Definition von Zugriffsberechtigungen zum Schwerpunkt hat. Als Grundlage für diesen führen wir eine Sync&Share-Systemarchitektur inklusive deren Vertrauensmodell ein. Abschließend präsentieren wir die Ergebnisse einer anhand des Katalogs durchgeführten Produktevaluation.

1 Einleitung

Durch die Etablierung der Cloud-Technologien sind Sync&Share-Dienste im privaten sowie im geschäftlichen Umfeld zu Werkzeugen für die verlustfreie Datenaufbewahrung und zum Datenaustausch geworden (vergleiche [ZCB10]). Der Nutzung eines Sync&Share-Dienstes steht im akademischen Umfeld entgegen, dass Forscher, Lehrende und Studierende angesichts der Sensibilität von zum Beispiel unveröffentlichten Forschungsdaten, Finanzierungsanträgen oder Abschlussarbeiten das Risiko ungewollter Preisgabe der Daten immer wieder bewerten und im Zweifelsfall auf die Nutzung von Sync&Share-Diensten verzichten müssen. In einem Projekt des Landes Baden-Württemberg befassen wir uns deshalb mit der Entwicklung eines Sync&Share-Dienstes, der sicheren kollaborativen Datenaustausch in wissenschaftlichen Projekten und in der (Hochschul-)Lehre ermöglichen soll. Ziel dieses Dienstes ist es, die Vertraulichkeit der Daten mit Hilfe von standardisierten kryptografischen Methoden sicherzustellen und gleichzeitig existierende Systeme mit geringem Aufwand einbinden zu können.

Während der Analysephase des Projekts haben wir uns intensiv mit den Anforderungen an Sync&Share-Systeme allgemein und im Hinblick auf den sicheren Datenaustausch beschäftigt. Das Ergebnis ist ein Anforderungskatalog, den wir im vorliegenden Dokument erörtern. Da das Projekt zum Ziel hat, die an den verschiedenen Hochschulen bereits vorhandenen Infrastrukturdienste wie beispielsweise eine Public-Key-Infrastuktur (PKI) wann immer möglich zu nutzen, wurden zunächst einzelne, getrennt voneinander betreibbare Komponenten eines sicheren Sync&Share-Dienstes identifiziert und in eine abstrakte Architektur eingeordnet. Der Katalog formuliert Anforderungen an das Zusammenspiel dieser Komponenten und mögliche Vertrauensannahmen in diese Komponenten. Insbesondere das Zusammenspiel der Komponenten zur Daten- und zur Schlüsselhaltung gestaltet sich komplex, da die Zugriffskontrolle auf Daten über mannigfaltige Kombinationen von Verschlüsselung und vertrauensbasierten Zugriffskontrolllisten auf Seiten der Datenhaltung implementiert werden kann. Deshalb wurde der Schwerpunkt des Katalogs auf die Trennung von Daten- und Schlüsselorganisation und feingranulare Betrachtung der jeweiligen Zugriffsberechtigungen gelegt. Diese Trennung bringt zusätzlich den Vorteil, dass uneinheitliche, unscharfe oder missverständliche Begriffsinterpretationen, wie wir sie in einigen anderen Katalogen vorgefunden haben, vermieden werden. Der Katalog ist sowohl für die Evaluation existierender Systeme geeignet, als auch für die Festlegung der Anforderungen bei Neuentwicklungen.

Um die praktische Anwendbarkeit des Anforderungskatalogs zu validieren, haben wir eine Evaluation existierender Produkte durchgeführt. Dazu haben wir die existierenden Sync&Share-Anwendungen PowerFolder (www.powerfolder.com/de/) und OwnCloud (owncloud.com/de/) - jeweils in Verbindung mit Boxcryptor (www.boxcryptor.com/) - und TeamDrive (https://www.teamdrive.com/de/) anhand des von uns aufgestellten Katalogs analysiert und bewertet. Bei der Auswahl der Anwendungen war für uns der entscheidende Faktor, dass die Datenhaltung für die Anwendung von einer Hochschule selbstständig betrieben werden kann. Die Ergebnisse dieser Evaluation stellen wir ebenfalls im verlauf dieses Schriftstücks vor.

Das vorliegende Dokument beinhaltet die Präsentation unserer Abstraktion einer sicheren Sync&Share-Architektur, eine Einführung in den Aufbau und die Interpretationsweise des Anforderungskatalogs und die Darlegung von ausgewählten Ergebnissen der Evaluation. Wir haben die Arbeit dafür folgendermaßen strukturiert: In Abschnitt 2 werden verwandte Arbeiten vorgestellt. Abschnitt 3 beschreibt zunächst die von uns zugrunde gelegte Systemarchitektur inklusive ihrer Teilkomponenten und führt anschließend Aufbau und Interpretationsweise des Anforderungskatalogs ein. Auszugsweise stellen wir in Abschnitt 4 die anhand des Katalogs ermittelten Ergebnisse der Evaluation dar. Abschließend fassen wir unsere Ergebnisse in Abschnitt 5 zusammen und geben einen Ausblick auf zu erledigende Aufgaben.

2 Verwandte Arbeiten

Die Notwendigkeit eines sicheren Sync&Share-Dienstes wird beispielsweise durch eine Studie von Microsoft [MT12] unterstrichen. Im Rahmen der Studie wurde evaluiert, wie

die Menschen mit Sync&Share-Diensten und der Cloud im Generellen umgehen. In der Studie wird das Verständnis unerfahrener Nutzer im (technischen) Umgang mit der Cloud als Datenspeicher analysiert. Ein wichtiger Teilbereich der Studie befasst sich mit der Wahrnehmung der Nutzer bezüglich Datensicherheit und Datenschutz im Cloud-Umfeld. Das Ergebnis dieses Teilbereichs lässt sich mit den Worten eines der Probanden zusammenfassen: „The convenience just outweighs the concerns“ (aus [MT12]).

Das erreichte Sicherheitsniveau eines Sync&Share-Dienstes bleibt jedoch unklar, solange nicht für jede der Komponenten die jeweiligen notwendigen Vertrauensannahmen und Berechtigungen systematisch festgelegt wurden. Dies zeigen die Autoren von [WA14], welche die Sync&Share-Anwendungen Wuala, Tresorit und Spider Oak hinsichtlich Sicherheitsaspekten analysiert haben. Diese Dienste werben mit Sicherheit durch Client-seitige Verschlüsselung. Hauptkritikpunkt stellt nach Erachten der Autoren der eigenverantwortliche Betrieb der PKI durch den Betreiber des jeweiligen Dienstes dar. Die Autoren argumentieren, dass der Betreiber selbst damit Schreibrechte auf die öffentlichen Schlüssel aller Benutzer hat und diese durch beliebige andere öffentliche Schlüssel ersetzen könnte, deren privates Gegenstück er selbst kennt. Auch wenn beispielsweise der Betreiber von Wuala dieser Darstellung widerspricht[1], zeigt dies dennoch die Notwendigkeit der Betrachtung aller Komponenten.

Im Vorfeld der Erstellung des in dieser Arbeit präsentierten Anforderungskatalogs haben wir Arbeiten recherchiert, die mögliche Sicherheitsanforderungen sowohl an das Auslagern von Daten im Allgemeinen, als auch an Sync&Share-Dienste im Speziellen diskutieren. Unsere Recherchen ergaben insbesondere, dass die gefundenen Paper sich zwar mit Datensicherheit im Allgemeinen befassen, jedoch Anforderungen an das Schlüsselmanagement nur rudimentär formulieren. Insbesondere bleibt unklar, welche Möglichkeiten zur Zugriffskontrolle die Komponente, die die Schlüssel verwaltet, bieten muss. Gerade die uns bekannten Arbeiten, die sich mit der Sicherheit von Cloud Computing im Allgemeinen befassen (zum Beispiel [SK11]), bleiben in diesem Aspekt sehr unklar.

Wesentlich detailliertere Anforderungskataloge für sicheres Cloud Computing werden von einigen Industriekonsortien oder öffentlichen Einrichtungen als Empfehlungen für sicheres Cloud Computing erarbeitet und veröffentlicht. Exemplarisch sei hier die Cloud Security Alliance genannt, die umfangreiche Richtlinien und Best pratices [All14] bereitstellt. Der Umfang dieses Anforderungskatalog geht wesentlich über den Anwendungsfall Sync&Share hinaus: unter anderem werden auch nicht dateibasierte Speicherarten und die Server-seitige Verarbeitung von Daten betrachtet. Obwohl auch Anforderungen an das Schlüsselmanagement genannt werden, sind diese zu grobgranular und zu wenig an den notwendigen Berechtigungsstrukturen orientiert, um als Basis für den Entwurfsprozess dienen zu können. Selbiges gilt für die Common Criteria, in deren Rahmen aktuell zwar Schutzprofile für einzelne Teilsysteme der von uns vorgeschlagenen Architektur definiert sind, beispielsweise für eine CA[2], die aber weder ein Schutzprofil für das Gesamtsystem anbieten, noch mögliche Berechtigungsstrukturen für die Schlüsselverwaltung vorschlagen. Ähnlich sind das Eckpunktepapier des BSI [BSI11] und die Empfehlungen des NIST [JG11] einzuordnen, die Sicherheitsanforderungen an die gesamte IT-Landschaft -

[1] https://support.wuala.com/2014/04/haben-sichere-cloud-dienste-doch-zugriff-auf-user-daten/

[2] https://www.commoncriteriaportal.org/files/ppfiles/cert-issu-v15-sec-eng.pdf

angefangen beim Rechenzentrum über Virtualisierung und Netze bis hin zur Datenhaltung - und die notwendigen Prozesse formulieren, aber Anforderungen bezüglich der Berechtigungen auf Daten und Schlüssel nur knapp anreißen.

Richtet man den Fokus auf Arbeiten, die sich im speziellen mit der Sicherheit ausgelagerter Daten beschäftigen, so zeigt sich nach den uns bekannten Arbeiten zu urteilen ein ähnliches Bild. Der wesentlich breitere Fokus dieser Arbeiten wie beispielsweise „privacy risks“ [dVFS12] oder die Miteinbeziehung rechtlicher Aspekte [GEWS12] geht einher mit grobgranularen Beschreibungen der Anforderungen an das Daten- und Schlüsselmanagement. Einschlägige Standards und Best Practices zur Verarbeitung personenbezogener Daten in der Cloud wie beispielsweise ISO/IEC 27018:2014 oder das Trusted Cloud-Datenschutzprofil[3] referenzieren den ISO-Standard 27002 - „Code of practice for information security controls“ -, der jedoch ebenfalls keine konkreten Berechtigungsstrukturen für Schlüssel oder Daten diskutiert.

Dies zeigt sich auch an einer Fraunhofer-Studie aus dem Jahr 2012 [BHH+12], in der die Cloudspeicher CloudMe, CrashPlan, Dropbox, Mozy, TeamDrive, Ubuntu One und Wuala auf ihre Funktionalität und Sicherheit hin analysiert wurden. Bezüglich der Sicherheitsanalyse grenzen sich die Autoren auf die Punkte Registrierung, Login, Transportsicherheit, Verschlüsselung, sicheres Teilen und sichere Deduplikation ein. Auch hier wird allerdings die Schlüsselverwaltung nur grob beschrieben, nicht analysiert, wer bei asymmetrischen Verschlüsselungsansätzen die PKI betreibt, und nicht definiert, was für die Autoren Integrität der Daten bedeutet, auch wenn sie immer wieder als wichtig aufgeführt wird. Insbesondere der Punkt der Datenaktualität wird von den Autoren vollständig vernachlässigt.

Zusammenfassend stellen wir fest, dass die Vertrauensannahmen für jede einzelne Komponente eines verschlüsselnden Sync&Share-Dienstes systematisch aufgezeigt werden müssen, um Aussagen über dessen Sicherheit treffen zu können. Die uns bekannten Anforderungskataloge listen jedoch die Anforderungen an die verschiedenen Komponenten nicht feingranular genug auf, als dass sie direkt als Basis des Entwurfsprozesses genutzt werden könnten. Insbesondere gilt dies für Anforderungen an die Zugriffsberechtigungen auf Daten und Schlüssel.

3 Systemkomponenten und Anforderungskatalog

3.1 System-Architektur und Anwendungsszenarien

Im Folgenden beziehen wir uns auf eine Softwarearchitektur, wie sie in Abbildung 1 dargestellt ist. Sie besteht aus einer Client-seitig betriebenen Komponente und mehreren weiteren Komponenten, die auf Servern betrieben werden. Wir gehen davon aus, dass die Komponenten über standardisierte Netzwerk- oder Webprotokolle miteinander kommunizieren; beispielsweise HTTP/HTTPS, WebDAV oder FTP. Die Client-Komponente der Architektur besitzt uneingeschränktes Vertrauen seitens der Nutzer, da auf ihr die unverschlüsselten

[3] http://www.trusted-cloud.de/media/content/Publikation_TCDP.pdf

Daten bearbeitet werden. Beispiele für die Umsetzung sind native, ins Betriebssystem integrierte Anwendungen oder Webbrowser. Ebenfalls ist eine Client-Implementierung für mobile Endgeräte in der Architektur berücksichtigt. Wir gehen zudem davon aus, dass Mitglieder einer kollaborativen Gruppe sich gegenseitig vertrauen. Dementsprechend geben sie die Daten und verwendeten Schlüssel nicht an unberechtigte Dritte weiter, so lange sie lesenden Zugriff auf diese haben. Es ist jedoch sicherzustellen, dass Mitglieder, die eine Gruppe verlassen haben, weder neue Schlüssel noch aktualisierte Inhalte der Daten im Klartext lesen können.
Für den Datenaustausch zwischen unterschiedlichen Client-Installationen gibt es die Server-seitig zentral bereitgestellte Datenspeicher-Komponente. Diese ist für die Authentifizierung und Autorisierung von Zugriffen, für das Nutzermanagement sowie die Organisation von gespeicherten Dateien in ihrem Dateisystem verantwortlich. Wir gehen davon aus, dass diese Komponente nicht als vertrauenswürdig anzusehen ist. Systeme, deren Datenspeicher vertrauenswürdig ist, werden von uns deshalb nicht betrachtet.
In der Architektur findet sich die Verschlüsselungskomponente ENC. Diese kann in Abhängigkeit von den Anforderungen Client-seitig implementiert sein oder auf einem eigenen Server bereitgestellt werden. In letzterem Fall besitzt dieser Server ebenfalls das uneingeschränkte Vertrauen der Systemnutzer. Die Komponente ist verantwortlich für die Ver- und Entschlüsselung von Daten sowie im Falle des dedizierten Servers auch die Überführung der Daten zwischen Client und Server.
Ebenfalls Server-seitig zentral bereitgestellt wird die Schlüsselaustausch-Komponente. Diese ist verantwortlich für die Organisation von digitalen Schlüsseln, welche für die Verschlüsselung der Daten benötigt werden, sowie die Authentifizierung und Autorisierung von Zugriffen auf diese. So können unterschiedliche ENC-Instanzen auf sicherem Weg die benötigten digitalen Schlüssel für die Ver- und Entschlüsselung automatisierbar austauschen. Ebenfalls ist eine direkte Schnittstelle für die Nutzer denkbar, um die Schlüssel „von Hand“ zu bearbeiten; beispielsweise über eine HTTP-Schnittstelle. Mögliche Anforderungen an diese Komponente reichen von bloßen Verfügbarkeitsanforderungen bis zum vollständigen Vertrauen in die Vertraulichkeit, Integrität und Aktualität der abgelegten Schlüssel. In letzterem Fall muss sie auf einer, von allen Gruppenmitgliedern als vertrauenswürdig angesehenen Infrastruktur, betrieben werden. Im deutschen Hochschulumfeld kann dies beispielsweise das Deutsche Forschungsnetz (DFN) sein, analog zu bereits existierenden Diensten wie der DFN-PKI. Es ist ebenfalls denkbar, die Schlüsselaustausch-Komponente in den Datenspeicher zu integrieren, wenn über technische Mechanismen die Vertraulichkeit, Integrität und Aktualität der auszutauschenden Schlüssel gewährleistet wird. Durch die Entkopplung von Datenspeicher und Schlüsselaustausch können jedoch unterschiedliche Datenspeicher über dieselbe Schlüsselaustausch-Komponente gesichert werden.
Der Aktualitäts-Server ist eine optionale Systemkomponente. Er ist verantwortlich für die Organisation von eindeutigen Werten, welche die Aktualität von Objekten angeben, sowie die Authentifizierung und Autorisierung von Zugriffen auf diese. Für unsere Architektur sind Objekte von Interesse, wie beispielsweise die im Datenspeicher hinterlegten Daten sowie auszutauschende Schlüssel. Unter Zuhilfenahme des Aktualitäts-Servers können unterschiedliche Client-Instanzen auf sicherem und automatisierbarem Weg die Aktualität der vom Datenspeicher empfangenen Daten abspeichern und validieren; analog die Ak-

tualität der verwendeten Schlüssel. Nicht vertrauenswürdige Datenspeicher können somit nicht unbemerkt veraltete, korrekt signierte Daten ausliefern, obwohl aktuellere angefordert wurden. Selbiges gilt für nicht vertrauenswürdige Schlüsselaustausch-Komponenten. Das Vertrauen der Systemnutzer bezüglich der Datenaktualität verschiebt sich hierdurch vom Datenspeicher beziehungsweise Schlüsselaustausch auf den Aktualitäts-Server. Dieser kann jedoch mit geringerem Aufwand betrieben werden als die ersteren. In jedem Fall gehen wir davon aus, dass dieser Komponente von den Systemnutzern uneingeschränkt vertraut wird.
Abschließend gehen wir davon aus, dass es eine Komponente gibt, welche die Identitäten der Nutzer eindeutig nachweist: Den Identifikations-Server. Beispielsweise kann dieser eine PKI sein, welche digitale Zertifikate ausstellt und vertrauenswürdig verwaltet. Dieser Komponente muss von den Nutzern uneingeschränkt Vertrauen entgegengebracht werden, da ansonsten nicht sichergestellt ist, dass nur berechtigte Nutzer mit dem System arbeiten können.

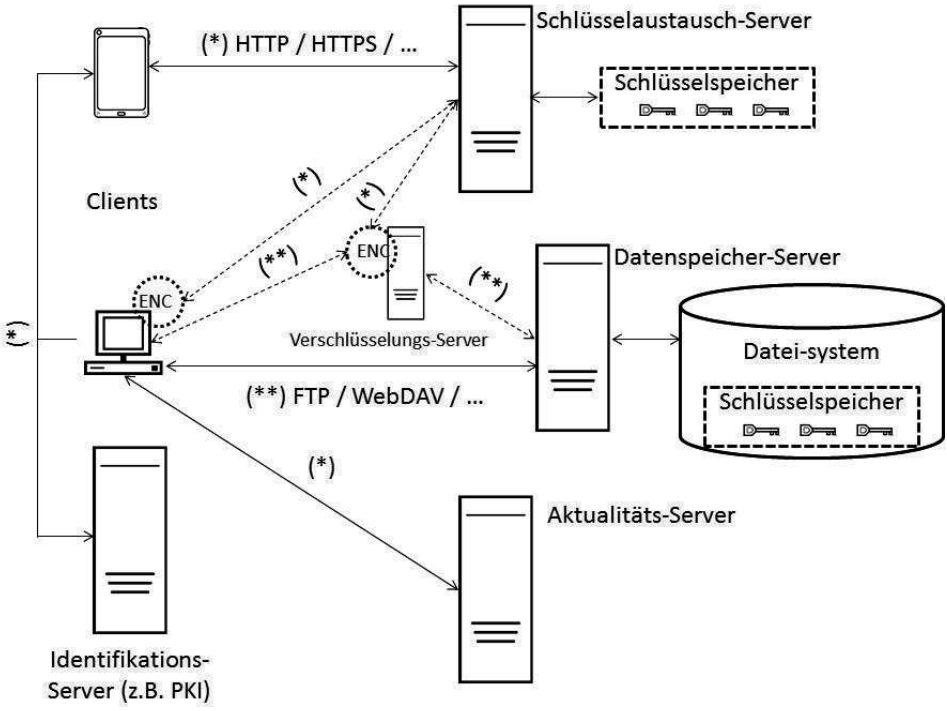

Abbildung 1: Komponenten einer sicheren Sync&Share-Architektur

Die erörterte Systemarchitektur ist geeignet, heterogen aufgebaute Systeme miteinander zu verbinden. Insbesondere im Hochschulumfeld, in dem oft einrichtungsübergreifend gearbeitet wird, hilft dies. Hochschulen, die eine umfangreiche Expertise mit einer spezialisierten Anwendung haben, können diese als Dienst für andere Hochschulen bereitstellen. Daraus resultieren Zeit- und Kosteneinsparungen sowie die Vermeidung der Wiederholung

von Fehlern beim Systembetrieb. Beispielsweise kann eine Hochschule den kostenintensiven Datenspeicher betreiben und warten, während die ihn verwendenden Hochschulen nur ihren eigenen Schlüsselaustausch-Server kostengünstig betreiben. Ebenfalls aus Kostengründen ist es somit denkbar, kostengünstige Speicherangebote aus der Wirtschaft abgesichert zu nutzen. Zudem ermöglicht die Architektur die einfache Integration bestehender Systeme, da sie auf standardisierten Protokollen basiert. Die Hochschule kann somit eigenständige Anwendungserweiterungen entwickeln und es den Hochschulmitglieder infolgedessen ermöglichen, die ihnen bekannten Umgebungen abgesichert zu verwenden. Ebenso kommt es zu einer Steigerung der Nutzerakzeptanz. Beide Aspekte stellen eine wichtige Argumentationsgrundlage für die Einführung in existierende Strukturen dar.

3.2 Übersicht über den Anforderungskatalog

Der komplette Anforderungskatalog ist online auf [KKHW14] zugänglich. Da dieser mehrere Seiten umfasst, haben wir ihn aus Platzgründen nicht mit in das vorliegende Dokument aufgenommen. Im folgenden geben wir eine Übersicht über den Katalog. Inhaltlich ist der Katalog auf die Fragestellungen Datenorganisation, Datensicherheit und Schlüsselorganisation ausgerichtet. Wir erheben keinen Anspruch darauf, den Katalog als allumfassend anzusehen. Dementsprechend lässt er sich je nach Bedarf um zusätzliche Anforderungen erweitern.

Datenorganisation		
Nutzerrechte		
□Datei erstellen	□Datei lesen	□Datei schreiben
□Datei ausführen	□Dateizugriff gewähren	□Dateizugriff widerrufen
□Ordner lesen[1]	□Ordnerdateien lesen[1]	□Ordner beschreiben[1]
□Ordnerdateien beschreiben[1]	□Ordnerdateien ausführen[1]	□Ordnerzugriff gewähren[1]
□Ordner anlegen	□Ordnerzugriff widerrufen[1]	

[1] Nur sinnvoll, wenn Dateisystem-basierte Datenorganisation.

Tabelle 1: Auszug aus dem Anforderungskatalog, Kategorie *Datenorganisation*

Der Katalog ist unterteilt in die Kategorien Datenorganisation, Datensicherheit, Schlüsselorganisation, Nutzerfreundlichkeit und Sonstiges. Die Kategorien unterteilen sich weiter auf entsprechende Teilaspekte; beispielsweise die Datenorganisation in Nutzerrechte und Gruppenrechte. Die unterste Ebene des Katalogs enthält die potentiellen Anforderungen. Bei diesen unterteilen wir voneinander unabhängige, voneinander abhängige und sich ausschließende Anforderungen. Sich innerhalb einer (Unter-)Kategorie ausschließende Anforderungen haben wir über das Symbol ○ gekennzeichnet. Wir gehen davon aus, dass in diesen Fällen nur genau eine Anforderung gewählt werden darf. Alle anderen Anforderungen werden durch das Symbol □ gekennzeichnet. Bei diesen ist es möglich mehrere Anforderungen zu einer (Unter-)Kategorie zu wählen. Sollten Anforderungen abhängig von anderen Anforderungen sein, so wird dies über eine Fußnote angegeben. Somit ist so-

fort visuell ersichtlich, dass die gestellte Anforderung tiefer gehender Betrachtung bedarf. Die Kategorie der Datenorganisation beschäftigt sich einerseits mit dem Nutzer- und Rechtemanagement bezüglich der Daten sowie der Client-seitigen Datenorganisation und der Server-seitigen Datenspeicherung. Hierbei haben wir uns stark an den Fragestellungen orientiert, die (netzbasierte) Dateisysteme zu lösen versuchen. Grundlegende Fragestellung ist hierbei beispielsweise, ob die Daten als einzelner großer Datenblock angesehen werden oder ob es eine hierarchische Ordner- und Dateistruktur gibt. Weiterhin sind typische Zugriffsberechtigungen auszuwählen, beispielsweise ob ein Nutzer- und Gruppenmanagement notwendig ist und welche Rechte Nutzer auf Ordner- und Dateiebene haben können. Letztere Fragestellung ist nur interessant, wenn zuvor festgelegt wird, dass Daten in einer Ordner- und Dateistruktur vorgehalten werden. Andererseits werden hier alle Anforderungen bezüglich des Datentransfers zwischen den Architekturkomponenten eingeordnet; beispielsweise geforderte Kommunikationsprotokolle und Schnittstellendefinitionen. Um Anforderungen an die Systemkomponenten möglichst voneinander zu entkoppeln, sind Datenorganisation und Schlüsselorganisation im Katalog explizit voneinander getrennt, obwohl es zur Optimierung der Nutzerfreundlichkeit Sinn macht, diese miteinander in Beziehung zu setzen; beispielsweise indem der Entzug des Dateirechts „Lesen“ auch den Entzug des entsprechenden Schlüssels einbezieht. Ein Auszug aus der Kategorie der Datenorganisation des Anforderungskatalogs findet sich in Tabelle 1.

Datensicherheit		
Verschlüsselungsbedarf[1]		
○ Ja	○ Nein	
Verschlüsselungsort		
○ Client	○ Vertrauenswürdiger Server	○ Datenspeicher
Verschlüsselungsart		
○ Symmetrische	○ Asymmetrische	○ Hybride

[1] Falls Nein, restliche Fragen zu Datensicherheit ignorieren.

Tabelle 2: Auszug aus dem Anforderungskatalog, Kategorie *Datensicherheit*

Folgend befasst sich der Abschnitt Datensicherheit mit den Anforderungen an Schutzmechanismen für die im Sync&Share-System vorgehaltenen Daten. In diesem Bereich werden grundlegende Entscheidungen festgelegt, beispielsweise welches Verschlüsselungssystem genutzt wird. Der Teilbereich umfasst zudem Anforderungen, die den beiden Teilbereichen Datenorganisation und Schlüsselorganisation zugeordnet werden können, sich jedoch auf die Sicherheit der Daten auswirken; beispielsweise ob sofortige Neuverschlüsselung bei Rechteentzug eines Zugriffsberechtigten gewünscht ist und ob die Notwendigkeit eines Aktualitäts-Servers besteht. Ebenfalls in diesen Bereich fällt die feingranulare Unterteilung von Datenintegrität. Er umfasst zudem die Fragen nach Vertrauen in die einzelnen Komponenten wie auch Fragen nach geforderter Aktualität von Daten und Schlüsseln. Tabelle 2 zeigt Auszüge aus der Kategorie Datensicherheit des Katalogs.
Der Bereich Schlüsselorganisation listet die Anforderungen bezüglich der digitalen Schlüssel auf, die für die Ver- und Entschlüsselung von Daten und zum Teil für den Integritätsschutz benötigt werden. Hierbei wird, ähnlich zur Datenorganisation, Nutzer- und Rechtemanagement festgelegt; in diesem Abschnitt jedoch bezüglich des Schlüsselmaterials.

Eine zentrale Fragestellung bezüglich des Schlüsselaustauschs ist das Austauschmedium. Hierbei gehen wir in der vorgestellten Architektur davon aus, dass digitale Schlüssel entweder auf einem eigenständigen Schlüsselaustausch-Server vorgehalten werden, um somit eine möglichst geringe Kopplung der Systemkomponenten zu erreichen, oder alternativ der Schlüsselaustausch über den unsicheren Datenspeicher erfolgt. In letzterem Fall ist auf jeden Fall sicherzustellen, dass die Schlüssel vor dem Zugriff Unberechtigter geschützt werden; beispielsweise indem sie mit den öffentlichen Schlüsseln aller Zugriffsberechtigter oder einem verteilten Gruppengeheimnis verschlüsselt werden. Dies gilt ebenfalls, wenn der Schlüsselaustausch-Server nicht vertrauenswürdig ist. Ebenfalls in diesen Teilbereich fällt die Frage, wie feingranular die Schlüssel angewandt werden. Hierbei reicht das Spektrum von einem einzelnen „Superschlüssel“, der für jede Dateiverschlüsselung verwendet wird, bis zu einem neuen Schlüssel bei jeder Dateiänderung.
Der Abschnitt Nutzerfreundlichkeit befasst sich mit den Rahmenbedingungen der Nutzbarkeit aus Nutzersicht. Hier werden insbesondere Anforderungen bezüglich der Interaktion zwischen Nutzer und der Systemfunktionen aufgelistet. Ebenfalls in diesen Teilbereich fällt Systemverhalten, welches den Nutzer direkt beeinflusst; beispielsweise Versionsverwaltung, Backup-Strategien und Fehlerbehandlung. Der Bereich ist nur grundlegend ausgearbeitet, da sich unsere Aufgabenstellung hauptsächlich mit Datensicherheit befasst.
Für Anforderungen, die sich nicht in die vorgestellten Kategorien eingliedern lassen, gibt es die Kategorie *Sonstiges*. Dies gilt zum Beispiel für die technische Frage, ob und welche existierenden Produkte eingebunden werden sollen.

4 Evaluation existierender Sync&Share-Lösungen

In diesem Abschnitt präsentieren wir die Ergebnisse der Evaluation existierender Sync&Share-Lösungen, die wir basierend auf dem in Abschnitt 3 dargelegten Anforderungskatalog durchgeführt haben. Die Evaluation dient im Kontext der vorliegenden Arbeit in erster Linie zur Demonstration der praktischen Einsetzbarkeit des Anforderungskatalogs.

Die Auswahl der zu evaluierenden Sync&Share-Lösungen wurde anhand von zwei Kriterien getroffen: Zum einen verlangt die Zielsetzung des eingangs erwähnten Landesprojekts, dass der Betreiber des Dienstes „Datenspeicher“ (vergleiche Abbildung 1) frei wählbar ist beziehungsweise eine „on-premise“-Installation dieses Dienstes möglich ist. Zum anderen beschränken wir uns, um dem Sicherheitsfokus des Anforderungskatalogs gerecht zu werden, auf Lösungen, die Ende-zu-Ende-Verschlüsselung ermöglichen. Zu diesem Zweck werden für die Evaluation ownCloud 6.0 und PowerFolder 9.0 - die keine Ende-zu-Ende-Verschlüsselung anbieten - jeweils mit Boxcryptor 2.0 kombiniert. Zusätzlich wird TeamDrive 3 evaluiert, das Ende-zu-Ende-Verschlüsselung mitbringt.

Der Sync&Share-Dienst ownCloud entstand 2010 aus einem Projekt von Frank Karlitschek und wird aufgrund des Verbleibs der Kontrolle der Daten beim Nutzer mit ihrer Datensicherheit beworben. Diese Kontrolle soll dadurch ermöglicht werden, dass ownCloud Open Source ist und somit auf einem privaten Server betrieben werden kann. Weiterhin ist in ownCloud eine Anwendung integriert, welche bei Aktivierung die vom Nutzer abge-

speicherten Daten mittels AES-256 Server-seitig verschlüsselt.

PowerFolder ist eine Sync&Share-Lösung, die seit 2009 von der Firma dal33t GmbH entwickelt wird und die Möglichkeit bietet, die Software auf einem eigenen Server als private Cloud zu nutzen. Der PowerFolder Kern ist Open Source verfügbar und alle in der Cloud abgespeicherten Daten werden Server-seitig mittels AES verschlüsselt. Ende-zu-Ende-Verschlüsselung ist nativ nicht integriert, hierfür nutzbare Lösungen von Drittanbietern werden jedoch auf der Webseite vorgestellt.

Boxcryptor 2.0 ist selbst kein eigenständiger Sync&Share-Dienst, sondern ergänzt diese um Ende-zu-Ende-Verschlüsselung. Zu diesem Zweck stellt Boxcryptor ein virtuelles Laufwerk bereit, das Zugriff auf bereits existierende Ordner ermöglicht und die Daten bei Zugriff transparent ver- beziehungsweise entschlüsselt. Die Komponente „Schlüsselaustausch“ (vergleiche Abbildung 1) wird hierbei von den Entwicklern von Boxcryptor selbst bereitgestellt, teilweise werden verschlüsselte Schlüssel auf dem Datenspeicher hinterlegt.

TeamDrive 3 bietet Ende-zu-Ende-Verschlüsselung bei freier Wahl des Datenspeicher-Betreibers. Die Schlüsselaustausch-Komponente wird auch hier zum Teil durch die Entwickler betrieben.

Aus Platzgründen werden im folgenden lediglich die Besonderheiten und Unterschiede der evaluierten Lösungen in den einzelnen Kategorien des Anforderungskatalogs dargestellt. Das vollständige Evaluationsergebnis kann in [KKHW14] eingesehen werden.

In der Kategorie *Datenorganisation* fällt zunächst auf, dass die Kombination von Boxcryptor mit ownCloud beziehungsweise PowerFolder in einer zweistufigen, „seriellen“ Zugriffskontrolle resultiert. Folglich ist das Erteilen von Berechtigungen auf Daten nur möglich, wenn diese Berechtigungen sowohl im zugrundeliegenden Sync&Share-Dienst als auch in Boxcryptor erteilt werden können. Für den Entzug von Berechtigungen hingegen reicht es aus, wenn die Berechtigungen entweder im Sync&Share-Dienst oder in Boxcryptor entzogen werden können. Aus diesem Umstand ergibt sich konkret, dass ownCloud in Kombination mit Boxcryptor den Benutzern die Möglichkeit bietet, das Recht zum Entzug von Zugriffsrechten auf Ordner und Dateien an andere Benutzer zu delegieren; ownCloud alleine bietet lediglich die Möglichkeit, das Recht zum Einräumen von Zugriffsrechten zu delegieren. Weiterhin ergibt sich daraus, dass Boxcryptor das Berechtigungsmodell von PowerFolder - das Rechtezuweisungen nur auf Ordnerebene zulässt - um die Möglichkeit zur Rechtezuweisung auf Dateiebene erweitert; ownCloud erlaubt dies von Hause aus. TeamDrive unterscheidet sich von den anderen evaluierten Lösungen dahingehend, dass Rechte auf der Ebene sogenannter „Spaces“ vergeben werden, die zwar beliebige Ordner- und Dateistrukturen enthalten, aber nicht ineinander verschachtelt werden können. Im Gegensatz zu den anderen Lösungen können in TeamDrive Berechtigungen nicht an zuvor definierte Gruppen von Benutzern vergeben werden. Sämtliche evaluierte Lösungen bieten den Zugriff auf die Daten ausschließlich über einen nativen Client an, der auch für mobile Plattformen verfügbar ist. Der Zugriff über einen Webbrowser ist somit nicht möglich; weiterhin kann auch nicht über standardisierte Protokolle wie zum Beispiel WebDAV auf die Daten zugegriffen werden.

Die Kategorie *Datensicherheit* zeigt keine wesentlichen Unterschiede zwischen den evaluierten Produkten auf: die Verschlüsselung der Daten wird auf dem Gerät des Benutzers

„on-the-fly“ vorgenommen und bleibt vor dem Benutzer weitestgehend verborgen. Ein Verschlüsselungsserver (vergleiche Abschnitt 3) kommt nicht zum Einsatz. Auffällig ist, dass von allen möglichen Anforderungen, die zusätzliche Sicherheitsaspekte darstellen, die evaluierten Lösungen keine einzige erfüllen. So wird bei Entzug von Zugriffsrechten keine Neuverschlüsselung der betroffenen Daten mit einem neuen Schlüssel vorgenommen. Auch ist die Integrität der Daten, Schlüssel und Zugriffsrechte nicht überprüfbar, ebensowenig deren Aktualität.

Die Evaluation der Kategorie *Schlüsselorganisation* ergab für alle Lösungen, dass auf Schlüsselverwaltungsebene keine Administratorenrechte vergeben werden können. Die einzige Ausnahme stellt hier die Rolle des Firmenadministrators bei Nutzung des Boxcryptor Company Packages dar, die in Notfällen den Zugriff auf alle Schlüssel innerhalb einer (virtuellen) Firma erlaubt. Die Granularität von Schlüsseln unterscheidet sich dahingehend, dass in TeamDrive ein Schlüssel für die Verschlüsselung eines kompletten „Spaces“ verwendet wird, während Boxcryptor für jede Datei einen eigenen Schlüssel benutzt. Der Schlüsselaustausch gestaltet sich bei allen evaluierten Lösungen vergleichbar: Er läuft automatisiert ohne Zutun des Benutzers ab, Schnittstellen für den Schlüsselaustausch werden nicht angeboten beziehungsweise geöffnet. Der Schlüsselaustauschserver selbst wird auf Infrastruktur der Entwickler von Boxcryptor beziehungsweise TeamDrive betrieben.

In der Kategorie *Nutzerfreundlichkeit* zeigt sich, dass sämtliche Lösungen keine Nutzung klassischer digitaler Zertifikate vorsehen, sondern den Austausch öffentlicher Schlüssel über Schlüsselaustauschserver vornehmen, der von den jeweiligen Anbietern betrieben wird; das Aufsetzen oder Integrieren einer eigenen PKI zur Nutzeridentifizierung ist nicht möglich. Die Problematik von Sync&Share-Diensten mit potentiell nicht vertrauenswürdiger PKI wurde bereits in Abschnitt 2 erläutert. Weiterhin führt der Verlust des Passworts in den kostenfreien Versionen von TeamDrive und Boxcryptor dazu, dass auf Daten, die der jeweilige Benutzer exklusiv besitzt, nicht mehr zugegriffen werden kann.

5 Zusammenfassung und Ausblick

In dieser Arbeit haben wir den Aufbau und die Interpretationsweise eines Anforderungskatalogs für sichere Sync&Share-Dienste eingeführt. Dieser basiert auf einer im vorliegenden Dokument vorgestellten abstrakten Systemarchitektur, welche eine Einteilung potentieller Systemkomponenten zu ihrer Funktionalität erlaubt. Inhaltlich befasst sich der Katalog sehr intensiv mit den Fragestellungen des Vertrauensmodells hinsichtlich der Komponenten sowie der Datensicherheit, dem Datenmanagement und dem Schlüsselmanagement, bei letzteren vertiefend mit der Zugriffskontrolle auf im System vorgehaltene Objekte. Der Katalog soll Projekten bei der Definition ihrer Anforderungen bei der Einführung, Evaluation und Entwicklung von Sync&Share-Anwendungen helfen. Wir haben seine praktische Anwendbarkeit anhand einer Evaluation der Systeme PowerFolder und ownCloud in Verbindung mit Boxcryptor und TeamDrive gezeigt sowie die Ergebnisse präsentiert.
Weitere Arbeit sehen wir zum einen in der Verfeinerung und Erweiterung des Anforde-

rungskatalogs selbst, insbesondere in den Bereichen Benutzerfreundlichkeit sowie hinsichtlich der Evaluationsunterstützung. Zum anderen werden wir den Katalog künftig heranziehen, um das angemessene IT-Sicherheitsniveau für verschiedene Nutzungsszenarien von Sync&Share-Diensten bestimmen und formulieren zu können.

6 Danksagung

Diese Arbeit entstand mit freundlicher Unterstützung des Ministeriums für Wissenschaft, Forschung und Kunst Baden-Württemberg im Rahmen der IQF-Förderung des Projekts „*CollabFuL*: Sichere soziale Kollaboration für Forschung und Lehre“.

Literaturverzeichnis

[All14] Cloud Security Alliance. Security Guidance for Critical Areas of Focus in Cloud Computing V3.0, 2014.

[BHH+12] Moritz Borgmann, Tobias Hahn, Michael Herfert, Thomas Kunz, Marcel Richter, Ursula Viebeg und Sven Vowé. On the Security of Cloud Storage Services. Bericht, Fraunhofer Institute for Secure Information Technology, Darmstadt, 2012.

[BSI11] BSI. Sicherheitsempfehlungen für Cloud Computing Anbieter - Mindestanforderungen in der Informationssicherheit. Bericht, Bundesamt für Sicherheit in der Informationstechnik, 2011.

[dVFS12] Sabrina De Capitani di Vimercati, Sara Foresti und Pierangela Samarati. Managing and Accessing Data in the Cloud: Privacy Risks and Approaches. In *7th International Conference on Risk and Security of Internet and Systems (CRiSIS)*, Seiten 1–9, 2012.

[GEWS12] Sebastian Graf, Jörg Eisele, Marcel Waldvogel und Marc Strittmatter. A Legal and Technical Perspective on Secure Cloud Storage. In *5. DFN-Forum Kommunikationstechnologien*, Seiten 63–72, Bonn, 2012. Gesellschaft für Informatik.

[JG11] Wayne Jansen und Timothy Grance. Guidelines on Security and Privacy in Public Cloud Computing. *NIST Special Publication*, 800(144), 2011.

[KKHW14] Kevin Koerner, Holger Kuehner, Hannes Hartenstein und Thomas Walter. Usecase catalog for sync and share systems. `http://ceres.zdv.uni-tuebingen.de/forschung/collabful.html`, 2014. [Online; letzter Aufruf 10.12.2014].

[MT12] Cathy Marshall und John C. Tang. That syncing feeling: Early user experiences with the cloud. In *Designing Interactive Systems (DIS) 2012*. ACM, June 2012.

[SK11] S. Subashini und V. Kavitha. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, 34(1):1–11, Januar 2011.

[WA14] Duane Wilson und Giuseppe Ateniese. To Share or Not to Share in Client-Side Encrypted Clouds. *CoRR*, abs/1404.2697, 2014.

[ZCB10] Qi Zhangi, Lu Cheng und Raouf Boutaba. Cloud computing: state-of-the-art and research challenges. In *Journal of Internet Services and Applications*, Seiten 7–18, 2010.