Überblick über Aufbau und Funktionsweise von CIDAS*

Friedrich-L. Holl
holl@fh-brandenburg.de

Jan Tobias Mühlberg
muehlber@fh-brandenburg.de

Fachhochschule Brandenburg
Magdeburger Straße 50
14770 Brandenburg, Germany

Brandenburg an der Havel, 4. Juli 2005

Inhaltsverzeichnis

*Configurable Internet Directory and Authentication Service

1 Problemstellung

Das Internet hat sich von einem Informationsmedium für Wissenschaftler zu einem weltumspannenden Wirtschafts- und Unterhaltungsbetrieb gewandelt. In Deutschland hatten im April 2002 fast die Hälfte der Haushalte einen Internet-Zugang[1]. Damit waren zu diesem Zeitpunkt mehr als 34 Millionen Menschen (vgl. [4, S. 15]) in Deutschland „online“ und verwendeten verschiedenste Internet-Anwendungen um sich zu informieren, Geschäfte abzuwickeln oder Kontakte zu knüpfen.

Zu den größten Herausforderungen in einem offenen IT-System gehört die korrekte und zweifelsfreie Legitimation seiner Benutzer. Sie ist von grundlegender Bedeutung für einen verbindlichen elektronischen Geschäftsverkehr und die Verwaltung von Zugriffsrechten auf physikalische Ressourcen und Informationen in Rechnernetzen.

Die Betreiber von Anwendungen[2] im Internet müssen wissen, wer der Benutzer ist, der Informationen abruft oder ein Produkt bestellt. Aus diesem Grund implementiert ein großer Teil der Anwendungen eine Benutzerverwaltung. Mit der Vielzahl von Speicherungsorten personenbezogener Daten ergeben sich erhebliche Probleme für Datensicherheit und Datenschutz. Der einzelne Benutzer kann den Schutz seiner persönlichen Daten kaum beeinflussen, geschweige denn kontrollieren.

Die Vielzahl der Anwendungen erfordert vom Benutzer, dass er sich eine Vielzahl von Passworten und Benutzerkennungen merken muss. Die Benutzer wählen oft einen einfachen Weg aus diesem Dilemma: Sie verwenden bei jeder Internet-Anwendung das gleiche oder nur sehr einfache Passworte, die dementsprechend auch einfach zu brechen sind. Nicht anders ist die Situation in lokalen Netzwerken bei Unternehmen oder Institutionen – auch hier sind die Passworte der Benutzer eine große Sicherheitslücke.

Viele existierende Benutzerverwaltungssysteme können vor allem die Probleme der Benutzer nur unzureichend lösen: Nur der Betreiber des Systems kann festlegen, welche Sicherheitseinstellungen gelten. Der Benutzer hat keinen Einfluss auf die Sicherheit des Systems. Er kann nicht beeinflussen, wo seine Daten gespeichert werden, ob sie verschlüsselt sind und wer auf die Daten zugreifen kann. Besonders bei Web-Applikationen bemängeln viele Be-

[1] Entsprechend [4, Seite 10] etwa 44%.

[2] Kostenlos bereitgestellte und frei zugängliche Informationen werden an dieser Stelle nicht berücksichtigt.

nutzer den unzureichenden Schutz ihrer persönlichen Daten. Obwohl manche Anwender bereits eigene Sicherheitsinfrastrukturen auf Basis von Chipkarten, Zertifikaten oder biometrischen Sicherheitseinrichtungen aufgebaut haben, können sie diese bisher nur für spezielle Applikationen, beispielsweise beim Home-Banking, benutzen. Für allgemeinere Anwendungen ist die teilweise kostenintensiv aufgebaute Infrastruktur nicht verwendbar.

Daneben würden auch viele Betreiber von Web-Applikationen gern höhere Sicherheitsstandards einführen, haben dafür aber oftmals nicht genügend Know-How. Auch ergeben sich Schwierigkeiten dadurch, dass potentielle Benutzer durch die komplizierte Sicherheitstechnik verschreckt werden könnten. Letztlich kann auch die Frage, ob das eingesetzte System sicher ist von den Betreibern nicht beantwortet werden. Sie müssen sich auf die Zusicherungen der Hersteller und Anbieter verlassen.

2 Potenziale und Ziele von CIDAS

An der Fachhochschule Brandenburg soll der „Configurable Internet Directory and Authentication Service“ CIDAS als ein modernes Identity Management System entwickelt werden, das für viele gängige Betriebssysteme und eine Vielzahl von Internet-Anwendungen unterschiedliche und differenziert nutzbare Authentifizierungsdienstleistungen erbringt. Damit ist es möglich, Authentifizierung[3] und Benutzerverwaltung von den eigentlichen Aufgaben der Anwendungen abzukoppeln. Die Grundlagen hierfür wurden von Schäfer in [5] sowie Mühlberg in [3] beschrieben.

Da CIDAS als ein freies Open-Source-Projekt entwickelt wird, ist es für jeden und weltweit[4] einsetzbar. Firmen, aber auch Institutionen wie Hochschulen und Verwaltungseinrichtungen, sollen durch den Einsatz von CIDAS in die Lage versetzt werden, dem zu verwaltenden Personenbestand – also Kunden, Studenten oder Einwohnern – Möglichkeiten zur Selbstverwaltung bzw. zur selbstständigen Pflege ihrer Daten zu geben und gleichzeitig den heute geltenden hohen Ansprüchen an den Schutz personenbezogener Daten und der eingesetzten Systeme gerecht zu werden.

[3] Unter dem Begriff Authentifizierung wird die Verifikation der vorher festgestellten Indentität eines Benutzers verstanden.

[4] In Bezug auf die verwendeten kryptographischen Verfahren zur Benutzerauthentifizierung wird der Einsatz von CIDAS unter Umständen durch die jeweils geltenden rechtlichen Bestimmungen eingeschränkt.

Für den verwalteten Personenbestand soll die Situation überschaubarer gestaltet werden: Benutzer sollen, natürlich immer in Abhängigkeit von der Art der Anwendung, jederzeit Auskunft bezüglich der über sie gespeicherten Informationen erhalten können und werden auch die Möglichkeit haben, die Nutzung und Weitergabe von Informationen zu verweigern.

3 Speicherung personenbezogener Daten

Viele Anwendungen und auch der Identifikations[5]- und Authentifizierungsdienst selbst kommen nicht ohne Zugriffe auf personenbezogene Daten aus. Deren Speicherung und vor allem der oftmals aus Sicht des Benutzers nicht nachvollziehbare Umgang mit diesen Daten ist einer der primären Kritikpunkte an bestehenden Anwendungen. Mit CIDAS wird versucht, eine aus Sicht des Benutzers maximal transparente Datenerfassung und sichere Datenspeicherung zu realisieren. Das bedeutet zum primär, dass von CIDAS immer nur unbedingt notwendige personenbezogene Daten erfasst werden. Zum anderen kann der Benutzer jederzeit Auskunft über die gespeicherten Daten erhalten und hat zudem die direkte Kontrolle über seine Daten. Er kann dadurch beispielsweise explizit entscheiden, welche Informationen an welche Dienstanbieter weitergegeben werden, wo er als Person erkannt werden möchte oder wo er unter einem nur dem CIDAS-Server bekannten Pseudonym agiert. Damit kann ein größtmöglicher Schutz gegen die eventuelle Kompromittierung des Datenbestandes realisiert werden.

Bezogen auf die zur Identifikation bzw. zur Abwicklung von Transaktionen mit einem Benutzer benötigen Daten, werden vorrangig dessen Name, die Postanschrift, unter Umständen sein Alter sowie seine Bankverbindung verwendet. Die Speicherung dieser Daten kann benutzerbedingt selbstverständlich auch verschlüsselt[6] erfolgen.

Sollte ein Benutzer besonders viel Wert auf den Schutz seiner persönlichen Daten legen, kann es je nach Applikation sogar akzeptiert sein, dass an Stelle der eigentliche Benutzerdaten lediglich Daten gespeichert werden, mit denen sich zwar die Korrektheit eingegebener Benutzerdaten nachweisen

[5] Während der Identifizierung wird die Identität eines Benutzers festgestellt. Benutzer übergeben hierfür ein eindeutiges Identifizierungsdatum wie eine E-Mail-Adresse oder eine insgesamt eindeutige Menge von Identifizierungsdaten, beispielsweise bestehend aus dem Namen und der Postanschrift, an den Authentifizierungsserver.

[6] CIDAS sieht verschiedene Möglichkeiten zur Speicherung des zum Schutz von personenbezogenen Daten verwendeten Schlüsselmaterials vor. Dieses kann zum einen vom CIDAS-Server, zum anderen aber vom Benutzer selbst verwaltet werden.

lässt, aus denen jedoch selbst keine Rückschlüsse auf den Benutzer gezogen werden können. In diesem Falle bliebe die sichere Speicherung der eigentlichen personenbezogenen Daten dem Benutzer selbst überlassen.

Neben den vorrangig zur Identifizierung eines Benutzers benötigten Daten können in CIDAS auch weitere personenbezogene Daten abgelegt werden. Dies geschieht üblicherweise in explizit dafür vorgesehenen und besonders geschützten Datenbanken. Auch hier können kryptographische Verfahren als Sicherheitsmechanismen eingesetzt werden. Insbesondere durch das Verwenden von nur innerhalb von CIDAS bekannten Datensatzidentifikatoren wird ein Ausspähen, vor allem aber die Zuordnung der Daten zu den zugehörigen Benutzern durch dazu nicht berechtigte Personen zusätzlich erschwert.

4 Authentifizierung

CIDAS bietet neben der Unterstützung von textuellen Authentifizierungsmethoden[7], die in vielen Anwendungsbereichen den an die Sicherheit gestellten Anforderungen immer noch genügen, auch die Authentifizierung mittels asymmetrischer Verschlüsselung und die Verwendung biometrischer Merkmale an. Der Einsatz kryptographischer und biometrischer Authentifizierungsverfahren ist insbesondere bei Zugriffen auf sensible Daten und sicherheitsrelevante Applikationen anzuraten.

Bei einer auf asymmetrischer Verschlüsselung basierenden Authentifizierung kann das Schlüsselmaterial auf verschiedenste Art und Weise bereitgestellt werden. Sowohl als Datei[8] auf einem vom Benutzer als sicher betrachteten Arbeitzplatz-Computer, als auch auf einem transportablen Datenträger. Speziell ist die Unterstützung von USB-Flash-Speicher und CD-ROMs geplant. Diese sind insbesondere preiswert, aber auch hinsichtlich der gebotenen Sicherheit ausreichend (vgl. Mühlberg, [3]). Die Nutzung derartiger Speichermedien für Authentifizierungszwecke stellt eine Neuheit auf dem Markt dar.

Zusätzlich wird es natürlich auch möglich sein, bereits etablierte kryptographische Authentifizierungsgeräte wie Smart-Cards heranzuziehen.

[7] Textuelle Authentifizierungsmethoden sind solche, bei denen ein Benutzer seine Identität durch die Eingabe textueller Informationen beweist. Zufällig abgefragte Daten und Passworte gehören hierzu.

[8] Denkbar sind beispielsweise X.509-Zertifikat entsprechend [2] oder OpenPGP-Schlüssel nach [1].

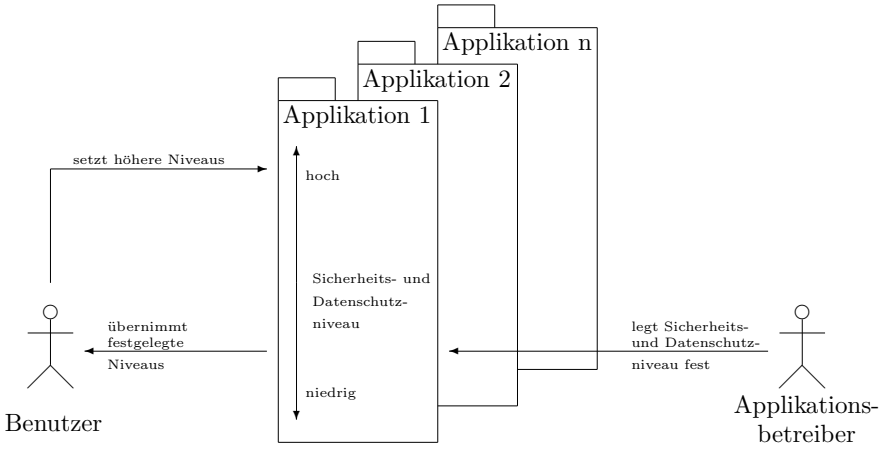

Abbildung 1: Benutzer und Applikationsbetreiber beeinflussen das geltende Sicherheitsniveau.

Neben diesen generischen Authentifizierungsmethoden ist es bei Nutzung von CIDAS auch möglich, kombinierte Verfahren einzusetzen. So bietet sich beispielsweise im Bereich der sicherheitskritischen Anwendungen die Nutzung einer Kombination an, die auf asymmetrischer Kryptographie und der Verwendung biometrischer Merkmale basiert.

Die Festlegung, welche Kombinationen von Authentifizierungsverfahren zum Einsatz kommen, kann auf verschiedene Weise erfolgen. Zum einen kann der Betreiber des CIDAS-Servers entsprechende Mindestanforderungen bezüglich der für den Zugriff auf einzelne Datenbestände oder Applikationen notwendigen Sicherheit bestimmen. Darüber hinaus ist es auch Benutzern und Applikationsbetreibern möglich, im Rahmen dieser Festlegung ihr eigenes Sicherheitsbedürfnis durch die Auswahl gleich- oder höherwertigerer Authentifizierungsverfahren umzusetzen (siehe auch Abbildung 1 auf Seite 7). Unterschreitet ein Benutzer die Sicherheitsanforderungen einzelner Applikationen, kann er diese entweder nicht nutzen oder muss sich mit einem höherwertigeren Verfahren erneut authentifizieren.

Betreiber legen immer nur den für sie unbedingt notwendigen minimalen Schutzbedarf fest, so dass von den Benutzern jederzeit höherwertigere Verfahren eingesetzt werden können. Ist der notwendige Schutz ein sehr hoher, erübrigt sich diese Option natürlich.

5 Systemarchitektur von CIDAS

Zum besseren Verständnis der Struktur des Gesamtsystems ist auf Seite 9 die Abbildung 2 zu finden. Gezeigt werden zwei Clients, ein Benutzer und eine Anwendung, die auf einen CIDAS-Server zugreifen. Die einzelnen Komponenten des Systems werden im Folgenden erläutert.

5.1 Authentifizierungsserver und -clients

Zur Realisierung der Authentifizierung ist CIDAS als ein Server-basiertes System konzipiert: Es gibt einen Authentifizierungsserver und zugehörige Clients. Die Kommunikation zwischen Server und Clients läuft über gesicherte Verbindungen und nach einem frei verfügbaren Protokoll[9] ab.

Implementierungen der CIDAS-Client-Software sind für gängige Betriebssysteme wie moderne Unixe, MacOS 10 und Windows geplant. In Abhängigkeit von der von diesen Systemen unterstützten Hardware gibt es unter Umständen Einschränkungen hinsichtlich der Funktionalität des Clients.

5.2 Single-Sign-On

Bei Verwendung von CIDAS meldet sich ein Benutzer im Gegensatz zu herkömmlichen Systemen nicht mehr bei jeder Anwendung einzeln an, vielmehr muss er sich lediglich einmal bei einem CIDAS-Server authentifizieren. Anwendungen, die diesen Server unterstützen, können über ein ihnen vom Benutzer übergebenes Sicherheits-Token[10] die Authentizität des Benutzers prüfen. Analog bekommen beteiligte Anwendungen automatisch eine Benachrichtigung, wenn sich ein Benutzer beim CIDAS-Server abmeldet.

Auch die Bereitstellung eines universell einsetzbaren Authentifizierungs-Frameworks, das neben textuellen Authentifizierungsmethoden auch hochwertige kryptographische und biometrische Verfahren gekoppelt mit Single-Sign-On Funktionalität anbietet, stellt eine zukunftsträchtige Innovation im IT-Sektor dar.

[9] Bei dem Protokoll handelt es sich um eine Eigenentwicklung. Die Spezifikation ist in [3] zu finden.

[10] Der CIDAS-Client unterstützt diesen Prozess derart, als dass vom Benutzer lediglich eine Bestätigung der Aktion gefordert wird.

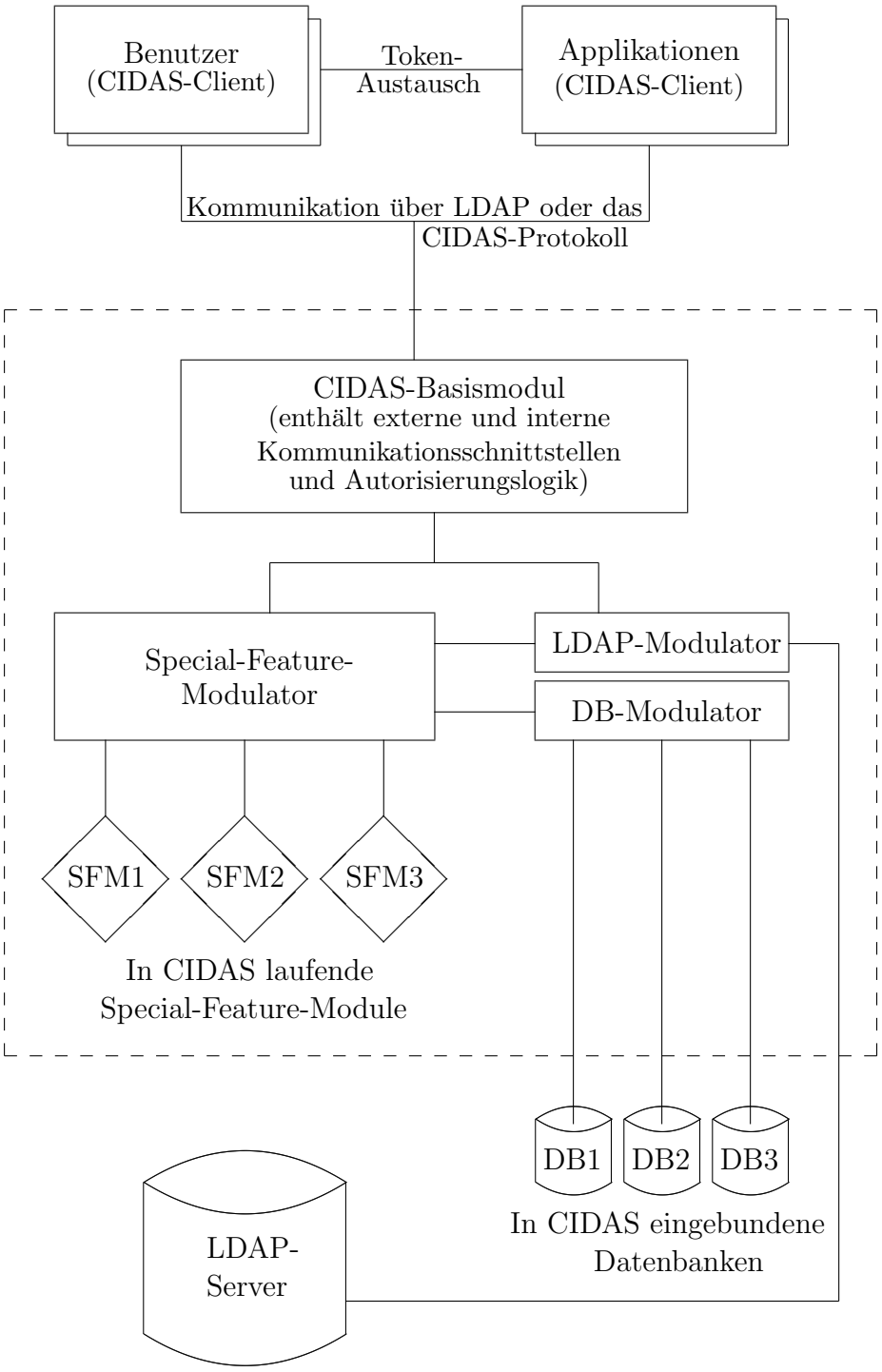

Abbildung 2: Modularisierung einer CIDAS-Infrastruktur nach [3]

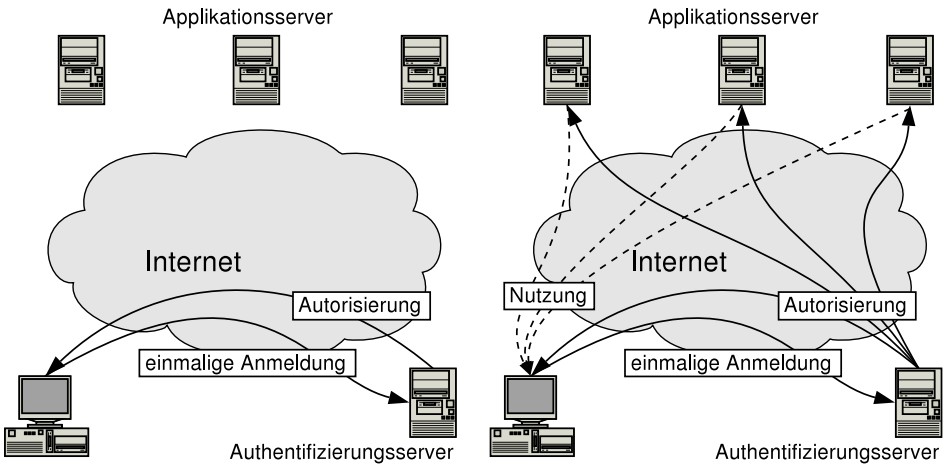

Abbildung 3: Single-Sign-On in CIDAS: Ein Benutzer meldet sich einmalig bei einem CIDAS-Server an (links) und kann anschließend, ohne weitere Anmeldeprozeduren zu durchlaufen, auf weitere Applikationen zugreifen. Autorisierungsinformationen werden dafür nach Rückfrage beim Benutzer vom CIDAS-Server verbreitet (rechts).

5.3 Special-Feature-Module

Eine wichtige Eigenschaft von CIDAS ist die einfache Erweiterbarkeit des Servers. Durch so genannte Special-Feature-Module lässt sich auch sicherheitskritische Anwendungslogik in den Authentifizierungss-Server auslagern. Die von Special-Feature-Modulen gebotene Funktionalität ist entweder mittels eines konventionellen Internet-Browsers oder über den CIDAS-Client erreichbar. Auch sind aus einem Special-Feature-Modul heraus Zugriffe auf speziell geschützte Datenbanken möglich.

Die Anbindung von Special-Feature-Module erfolgt über eine CORBA-Schnittstelle. Dementsprechend können die Module in beliebigen Programmiersprachen entwickelt sein. Auch wird daduch eine hohe Skalierbarkeit des Gesamtsystems erreicht. Beim Einsatz von Special-Feature-Modulen ist insbesondere deren Korrektheit sicherzustellen um eine Gefährdung des Datenbestandes und der Gesamtsicherheit des Servers auszuschließen.

5.4 Unterstützte Anwendungen

CIDAS unterstützt auf Anwendungsseite jede Anwendung, die entweder LDAP[11] oder das CIDAS-eigene Protokoll verwenden bzw. einen CIDAS-Client bedienen kann. Dies schließt die Anmeldung an einem Arbeitsplatz-Rechner ebenso wie das Login bei parameterorientierten Anwendungen wie etwa Internet-Shopsystemen ein.

Grundsätzlich bietet CIDAS aufgrund seines modularen Aufbaus die Möglichkeit zur Integration wieterer Kommunikationsschnittstelen. Denkbar ist in diesem Sinne beispielsweise die Umsetzung einer Schnittstelle zum *Liberty Alliance Project*.

Gegenwärtig existiert ein Prototyp des Systems, der mit einem Hochschulinformationssystem[12] zusammenarbeitet. Eine vollständige Integration von CIDAS in den Apache-Webserver ist geplant. Damit ergeben sich dann vielfältige Möglichkeiten zur Anbindung von Internet-Anwendungen. Ebenfalls geplant ist eine Integration des Systems in die Authentifizierungs-Infrastruktur *PAM*, die von vielen Unix-ähnlichen Betriebssystemen genutzt wird.

6 Open-Source

Wie bereits weiter oben erwähnt, handelt es sich bei CIDAS um ein Open-Source-Produkt im Sinne der GPL[13]. Damit haben Entwickler und Anwender die Möglichkeit, alle Bereiche von CIDAS im Quellcode einzusehen, zu erweitern oder ihren eigenen Bedürfnissen anzupassen. Auch kann durch eine Offenlegung der Quellen garantiert werden, dass die von CIDAS gebotene Sicherheit nicht auf der Geheimhaltung von Verfahren und Implementierungsdetails basiert, sondern vielmehr auf einer nachprüfbaren Sicherheit der Verfahren bzw. des Systems an sich. Darüber hinaus wird auf diese Weise auch die Verifikation einer CIDAS-Implementierung durch Dritte hinsichtlich ihrer Korrektheit ermöglicht.

[11] LDAP: „Lightweight Directory Access Protocol“, siehe [6].

[12] Das *University Information System* erlaubt die Verwaltung von personalisierten Stundenplänen. Es wurde als Web-Applikation auf Basis von PHP entwickelt.

[13] Siehe hierzu `http://www.gnu.org`.

Literatur

[1] J. Callas, L. Donnerhacke, H. Finney, and R. Thayer. OpenPGP message format. RFC 2440, 1998. `http://www.faqs.org/rfcs/rfc2440.html`; visited on October 1st 2003.

[2] CCITT. The Directory-Authentication Framework. Recommendation X.509, Consultation Comittee, International Telephone and Telegraph, International Telecommunications Union, Geneva, 1989. can be purchased at `http://www.itu.int`; visited on January 24th 2004.

[3] Jan Tobias Mühlberg. Konzeption und prototypische Umsetzung von Authentifizierungsverfahren und Kommunikationsschnittstellen für das Identity Management System CIDAS unter besonderer Berücksichtigung mobiler identifizierbarer Datenträger. Diploma thesis, University of Applied Sciences in Brandenburg, Germany, March 2004.

[4] Olga Pötzsch, Birgit Korth, and Susanne Schnorr-Bäcker. *Informationstechnologie in Haushalten - Ergebnisse einer Pilotstudie für das Jahr 2002*. Statistisches Bundesamt, Frankfurt am Main, 2003.

[5] Ingo Schäfer. Konzeption und prototypische Umsetzung eines universellen Benutzermanagement-Systems mit Transaktionskomponente. Diploma thesis, University of Applied Sciences in Brandenburg, Germany, August 2003.

[6] W. Yeong, T. Howes, and S. Kille. Lightweight Directory Access Protocol. RFC 1777, 1995. `http://www.faqs.org/rfcs/rfc1777.html`; visited on December 22nd 2003.

GNU Free Documentation License

Preamble

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The **"Document"**, below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as **"you"**. You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A **"Modified Version"** of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A **"Secondary Section"** is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The **"Invariant Sections"** are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The **"Cover Texts"** are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A **"Transparent"** copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called **"Opaque"**.

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The **"Title Page"** means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License

requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section **"Entitled XYZ"** means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as **"Acknowledgements"**, **"Dedications"**, **"Endorsements"**, or **"History"**.) To **"Preserve the Title"** of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent

and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties–for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section

titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You

may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.