iiitAccessServer

A rule-based authorization system

White Paper

May 9, 2003

Content

1 Overview

An authorization system makes it possible for an application to assign specific rights to actions or data elements.

The *iiitAccessServer* distinguishes itself by its capability to define the rules describing the rights independent of a specific application. The authorization system described herein gives the possibility to define any group of single elements or groups of groups. A group may also consist of an combination of other groups and single elements, which may be defined as an addition, subtraction or intersection (or any combinations of these operations) of its elements. It can be used to define rights for reading, writing or any other rights you need.

The rights are defined by expressions, which describe the group of users, who have a specific right, in an easy and flexible way. A very ingenious caching subsystem ensures an excellent performance despite the complex possibilities. The implementation of *iiitAccessServer* allows nearly unrestricted scalability, either by more powerful computers or by addition of further ones.

To meets all operational requirements, the system is designed to be intrinsic redundant and failure tolerant without the need for special hard- or software. It may also be included in disaster backup scenarios without any problems.

The *iiitAccessServer* is 100% pure Java for usage together with Linux and also only tested with Linux. Beside the Java runtime environment it uses only software products available for free, so there is no need to purchase any third party products as e.g. database servers.

2 Concepts

It is the intention of authorization systems, to give one or more applications the possibility to assign rights to users.[1] Important for the usability of such a system are the options to assign the rights to users in an easy way. Because there are many variations how to use a authorization system it must be designed to be very flexible.

Even the administration of the authorization rules needs a high level of flexibility. For example it could be necessary to let a department define the authorization rules for one or more applications while the system administrators define the lists of users.

2.1 Requirements to an authorization system

The requirements for definition of user groups and groups of groups are:

1. All settings and group definitions must be possible while the system is online.
2. It must be possible to assign rights to single users and to groups. Generally there shall be no difference between the assignment of users to groups and groups to groups.
3. It must be possible to link groups as a union of sets.
4. It must be possible to exclude distinct users or distinct groups from other groups. Hereby it is possible to dynamically exclude groups from a right irrespective of the configuration done by the administrator.[2] This will make it impossible to give a certain group of users a distinct right.
5. It must be possible to calculate the intersection of groups. Hereby it will be possible realize these examples within the authorization system:

[1] Generally it is possible to assign rights for other objects or functionalities to objects. Throughout this paper our examples will assign rights to users to show the possibilities, but this is not meant as a limitation of the more general possibilities.

[2] See also chapter 5.1.

(a) One may calculate a right that depends on a user being a member of two or even more groups at the same time.

(b) If there are high demands on security, one may force that two administrators must independently assign a user to a right. The user may use the belonging functions only if both administrators have assigned him to the groups. This will accord to internal security audits.

6. It must be possible to create any combination of above mentioned operations.
7. The user interface for all these functions shall be easy and comfortable to use.

2.2 Realized functions

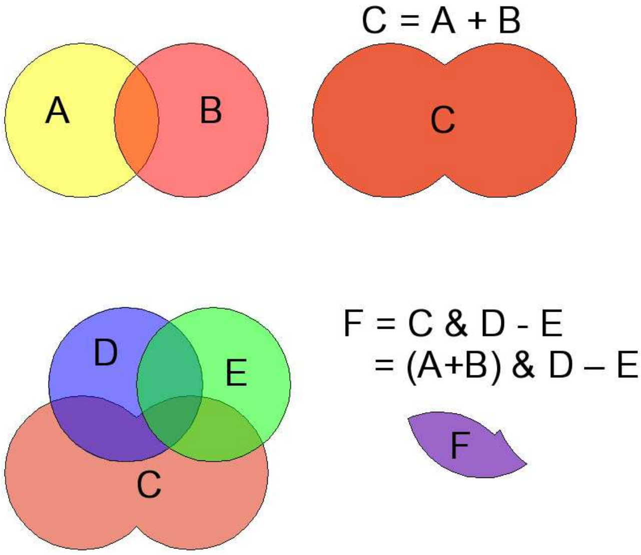

Illustration 1: Definition of Groups

All requirements listed in the previous chapter are completely implemented. For technical details see chapter 3. The user interface gives access to the authorization system by formula-like expressions (set operations called rights scheme or short formulas throughout this paper). The possibilities are shown in illustration 1.

As shown there, two groups can be combined. Mathematically spoken, the set *C* is a union of sets $C = A \cup B$. Because set operations can not be expressed with the common ASCII character set, it will be written as $C = A + B$ inside *iiitAccessServer.*

The second example shows the intersection of the sets *C* and *D* with the exclusion of set *E*. The mathematically correct representation of this operation $F = C \cap D \setminus E = (A \cup B) \cap D \setminus E$ can also not be written with the ASCII characters. Therefore it will be written as $F = C \,\&\, D - E = (A + B) \,\&\, D - E$ inside *iiitAccessServer*. The result will include all users which are members of groups *C* and *D* but not members of group *E*.

All these formulas can be written as Strings this way:[3]

- $(x + y + z)$ — A set consisting of the elements *x*, *y, and z*.
- $A + B$ — The union of the sets *A* and *B*. The result will include all elements of the sets *A* and *B*.
- $A - B$ — The difference of the sets *A* and *B*. The result includes all elements of *A*, which are not included in *B*.
- $A \,\&\, B$ — The intersection of the sets *A* and *B*. The result will include all elements which are included in *A* and included in *B*.
- $((x + y + z) + A) - (b + e + f) \,\&\, C$ — Expression can be grouped with braces. They are resolved from left to right. „&“ has a higher priority than „+“ and „-“.

[3] For clarification we will use lower-case (*x*,*y*,*z*) characters for atomic element and upper-case characters for groups (*A*,*B*, *C*).

The definition of formulas will be assisted by the possibility to create groups consisting of other groups or atomic elements. This makes it possible to create an administration system with low effort, which is able to assign the rights in very different granularity. Administration rights can then be assigned with a predefined group name while the belonging group can be configured inside the authorization system.

3 Implementation

The authorization system currently consists of a modular Java application, which can easily be extended by plug-ins.

The base version includes a TCP/IP interface implementing an easy to use ASCII protocol to request rights. Therefore a unique user name and the name of the right or an equation describing the authorized group will be passed to the server. The server answers with true if the user is a member of the group or false otherwise. The base version uses a Java property file as its data source, which is easily editable with a simple text editor.

Beside this, the package includes a plug-in acting as an interface to LDAP. This plug-in uses most of *iiitAccessServer's* capabilities. The LDAP database will be used to store all user groups and the expressions describing the combined groups. They may be edited with any LDAP front end while the authorization system is running. A specialized front end to edit groups and expressions will be published in the near future. Because the operations on the data stored in the LDAP database will consume a great amount of time, esp. when there are many users and complicated expressions, the data will be cached in a MySQL database using an optimized data structure. Changes in the LDAP database will be recognized and written to the cache database by a background process – the so called *CacheManager*. The *CacheManager* may be installed on its own somewhere inside the local network, but it must run only once at a time. Currently there exists an interface to OpenLDAP only but we think of developing interfaces to other LDAP servers, too. While reading the expressions from the LDAP database, all expressions are tested whether they are valid. If there are any errors, the system administrator can be notified by e-mail.

On the first start-up, the *CacheManager* will create all needed database tables and it will read all groups and expression from LDAP and write them into the cache databases.

The authorization system is designed to be scalable, redundant and error tolerant on its own. To improve performance the cache database can be distributed over up to 257[4] database servers. When one of the cache databases crashes, a reconnect will be tried automatically. Meanwhile the LDAP database will be used as the main data source, however this may cause performance impacts. The *iiitAccessServer* itself without the *CacheManager* can be installed and run on any number of servers. If one of them crashes, the application must recognize this error and connect to another instance. This can be achieved easily with DNS.

Besides the database cache there is an additional 1st-level cache inside the *iiitAccessServer* storing the determined rights for a configurable amount of time. After that, the data will be deleted from the cache to assure that changes in the database will be recognized.

4 Considerations on the assignment of rights

Illustration 2 shows the relations between all instances concerned in the assignment of rights:

- A user is member of one or more groups. Through the membership, right are assigned to the user.
- A group consists of users and/or other groups. Groups are used to evaluate the rights users have inside an application.

[4] 256 cache databases plus one database for temporary data needed by the *CacheManager*.

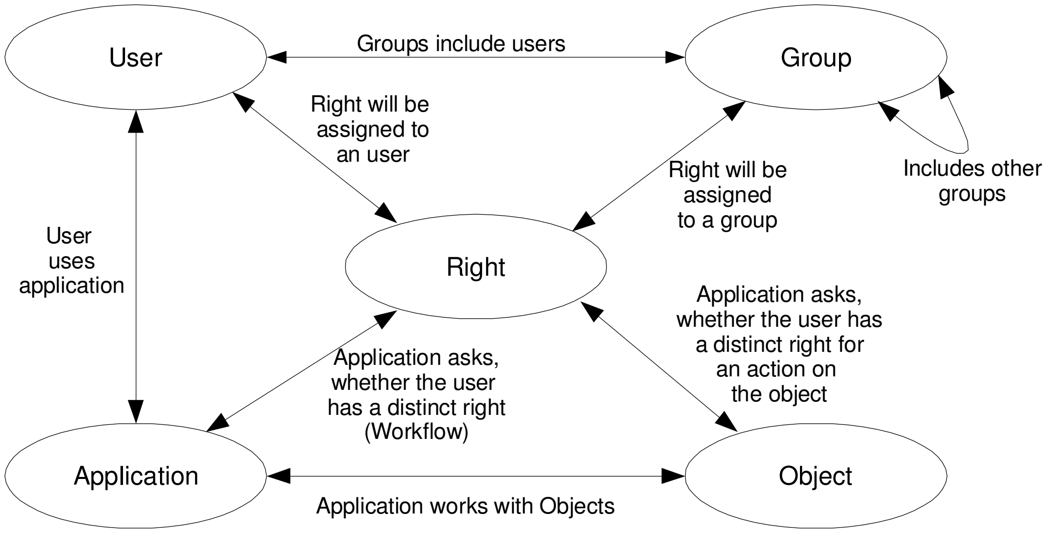
User
Group
Groups include users
Right will be assigned to an user
Right will be assigned to a group
Includes other groups
User uses application
Right
Application asks, whether the user has a distinct right for an action on the object
Application asks, whether the user has a distinct right (Workflow)
Application
Object
Application works with Objects

Illustration 2: Integration of the authorization system

- A user uses an application. The application asks, whether a user has a distinct right or which users have a distinct right. The application may generate the rule describing the right dynamically at run time, to let it be evaluated by the *iiitAccessServer*.
- The application may work with objects. These objects contain references to groups or dynamically generated rules describing the rights at run time.

5 Examples

5.1 Realizing a four eyes principle

For the realization of the four eyes principle there a two possibilities:

1. On the side of administration, the *iiitAccessServer* can assure, that two administrators independently assign rights to the users. It is fully realized inside the *iiitAccessServer*, you do not need to take it into consideration while developing the applications. The needed groups are created twice. One set is managed by administrator a, and the other by administrator b. If the right requested by the application is called Right1, these are the expressions describing the right:

   Right1 → Right1AdminA & Right1AdminB
   Right1AdminA → [jim joe bob] managed by administrator a
   Right1AdminB → [jim joe] managed by administrator b

   Here only the users Jim and Joe have the right but not Bob, because administrator b did not assign him to the group Right1AdminB.

2. If you need the four eyes principle inside an application to assure that two persons independently confirm to an transaction, you could realize it this way:

Confirm → [jim joe bob]

The first request of the application would be:

“Is user Jim member of the group *Confirm*”

The application must then store the name of this first confirming user together with the transaction. For the second confirmation the request to the *iiitAccessServer* would be:

“Is user Joe member of the group *(Confirm – jim)*”

This rule is created dynamically by the application and assures that one user can not confirm twice and therefore is not able to confirm the transaction on his own.

5.2 Cascading groups

You may have groups of users authorized to confirm transactions up to a distinct amount of money.

One group may be authorized to confirm up to 10,000 €, a second one up to 20,000 € and a third one up to 50,000 €. There will be one group for each level of authorization, but you have to consider, that users authorized to confirm 50,000 € may also confirm 10,000 € or 20,000 €. Therefore you create the groups *Group10000*, *Group20000* and *Group50000*. You may define the rights as:

Right50000 → Group50000

Right20000 → Group20000 + Group50000

Right10000 → Group10000 + Group20000 + Group50000

or

Right50000 → Group50000

Right20000 → Group20000 + Right50000

Right10000 → Group10000 + Right20000

6 System architecture

In illustration 3, an exemplary assembly is shown. The two network segments connected to the *iiitAccessServer* are only drawn for clearness. The are not necessary for a real installation. Also for clearness every server has only one functionality.

The server CM (*CacheManager*) represents the authorization system's connection to the LDAP database. This server initializes and refreshes the data stored in the cache databases.

The applications – represented by the computers AP1 - AP3 – distribute their requests to the authorization servers AS1, AS2 and AS3. To use the 1st-level cache inside *iiitAccessServer*, every application should send all requests regarding one user to the same *iiitAccessServer*. If one of the servers AS*n* crashes, the applications using it must connect to one of the remaining. If the crashed one is available again, it can be used again automatically.

The *iiitAccessServer* (e.g. AS1) uses persistent caches stored in databases to answer the requests. The servers DB1 and DB2 represent those databases. If one of them crashes, the *iiitAccessServer* must use the LDAP databases for its evaluations, which may result in impacts on performance.

To simplify the drawing the *CacheManager* is installed together with the admin database and the LDAP server on the same computer. This is not a necessary requirement for the operation of the *CacheManager*! The *CacheManager* uses the admin database as a temporary but persistent storage. If the *CacheManager* or the admin database crashes, the update of the persistent 2nd-level cache will be interrupted, but the authorization system itself will still be operational.

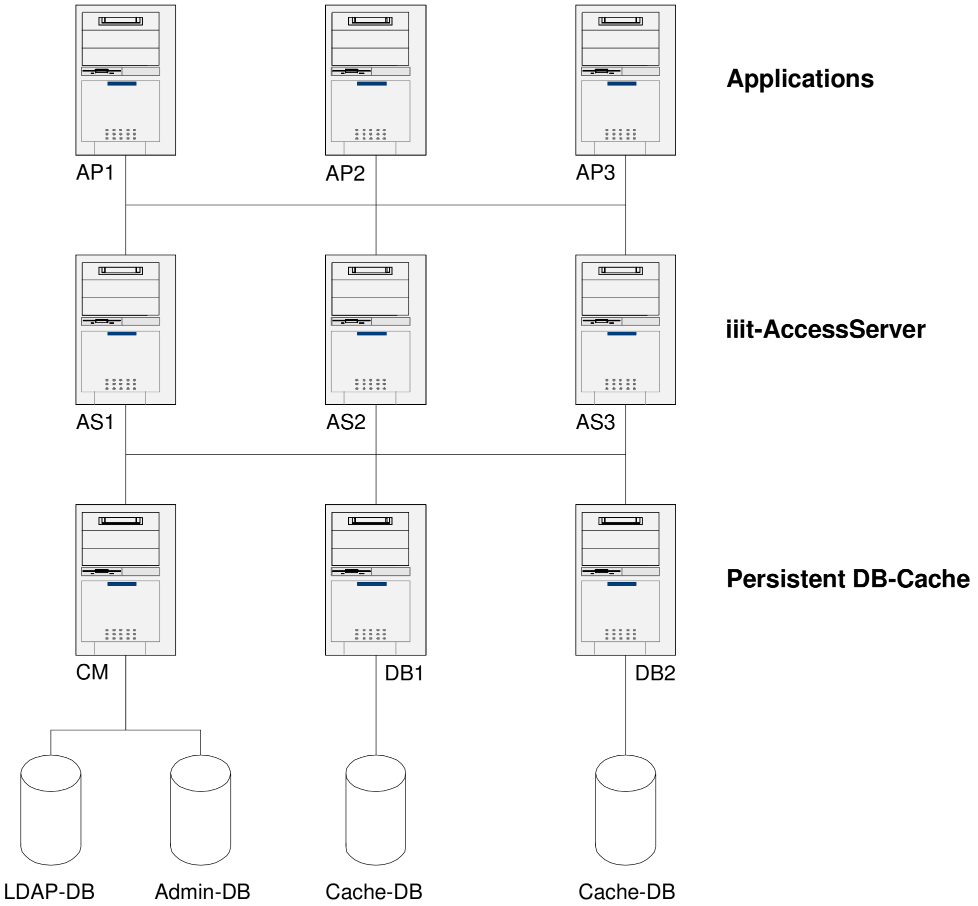

Illustration 3: System Architecture

6.1 Scalability and Availability

All design decisions concerning the components of the authorization system have been checked for their influence on availability.

1. Software packages like Linux-Failsafe of heartbeat can be used to to reach High-Availability for the required databases. Even if you do not install the databases this way, in case of a crash of one or all databases the authorization system stays fully operational. Only the performance will decrease.
2. The *iiitAccessServer* realizes error tolerance by the n+1 principle. This means, that you need n servers to handle the load, and one acts as a spare part. If one of them crashes, the load will be shared by the remaining ones.
3. The *CacheManager* is only needed to refresh the cache databases in case of changes in the LDAP database. If it crashes it does not hamper normal operation of the authorization system. If you have high demands on the cache to be current, you may lay out the *CacheManager* for High-Availability.

The system is scalable through load balancing:

1. You may use DNS-Round-Robin or IP load balancing to distribute the requests over all instances of the *iiitAccessServer*. The *iiitAccessServer* can be installed and run on any number of servers at the same time.
2. For load balancing purposes, the cache database can be distributed over up to 256 separate database servers.

7 Performance

Through several optimizations and multilevel caching, we achieved a response time of about 3 ms.[5] Under unfavorable conditions we measured response times of about 60 ms with 26,000 defined users and more than 2,500 predefined groups. If you use dynamically created expression, which can not be cached in the persistent cache, this response time will be needed for every part of the formula. E.g. a dynamic request like $A + B \& C$ consisting of three parts will cause a response of about 9 ms rsp. up to 180 ms under unfavorable conditions.

Further requests with expressions consisting of the same parts will have a response time of about 9 ms, even if the request is done for another user.

If an application sends the same requests several times, the *iiitAccessServer* will use its built-in 1st-level cache to answer the questions. The response time will be less than 1 ms then. Dynamically created requests will take advantage from the 1st-level cache also.

The databases are used to hold the group information in an optimized form. Through the use of databases it is possible to process a great amount of data with high performance. The CacheManager will need less than five minutes to initialize the databases in an environment with 26,000 defined users and more than 2,500 groups and expression.

8 GNU Free Documentation License

Version 1.2, November 2002

Copyright (C) 2000,2001,2002 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

0. 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.

[5] To do the tests, we used standard PCs (800 MHz Pentium III, 256 MB RAM) with Linux.

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' susers 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' sCover 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.