FIDIS

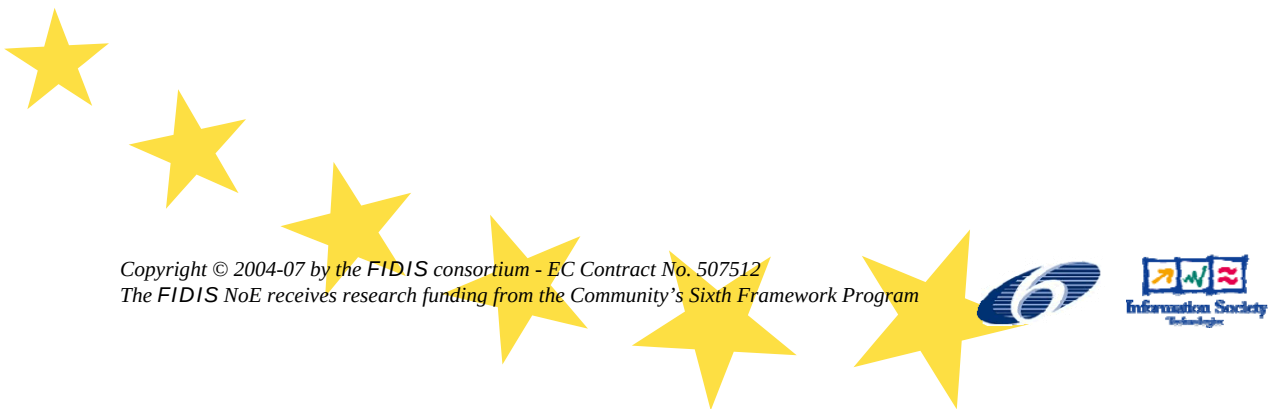
Future of Identity in the Information Society

Title:	"D3.11: Report on the Maintenance of the IMS Database"
Author:	WP3
Editors:	Martin Meints (ICPP, Germany)
Reviewers:	Denis Royer (University of Frankfurt, Germany)
	Sabine Delaitre (IPTS, Spain)
Identifier:	D3.11
Type:	[Report]
Version:	1.0
Date:	Tuesday, 24 April 2007
Status:	[Final]
Class:	[Public]
File:	20070418_Report_IMS_Database_final.doc

Summary

This document is a report summarising the maintenance work carried out for the database on Identity Management Systems (IMS database) in the context of D8.6 and D3.11.

This report covers the third FIDIS period (April 2006 to March 2007).



Copyright © 2004-07 by the FIDIS consortium - EC Contract No. 507512
The FIDIS NoE receives research funding from the Community's Sixth Framework Program

Copyright Notice:

This document may not be copied, reproduced, or modified in whole or in part for any purpose without written permission from the FIDIS Consortium. In addition to such written permission to copy, reproduce, or modify this document in whole or part, an acknowledgement of the authors of the document and all applicable portions of the copyright notice must be clearly referenced.

The circulation of this document is restricted to the staff of the FIDIS partner organisations and the European Commission. All information contained in this document is strictly confidential and may not be divulged to third parties without the express permission of the partners.

All rights reserved.

PLEASE NOTE: This document may change without notice – Updated versions of this document can be found at the FIDIS NoE website at www.fidis.net.

Members of the FIDIS consortium

1. Goethe University Frankfurt	Germany
2. Joint Research Centre (JRC)	Spain
3. Vrije Universiteit Brussel	Belgium
4. Unabhängiges Landeszentrum für Datenschutz	Germany
5. Institut Europeen D'Administration Des Affaires (INSEAD)	France
6. University of Reading	United Kingdom
7. Katholieke Universiteit Leuven	Belgium
8. Tilburg University	Netherlands
9. Karlstads University	Sweden
10. Technische Universität Berlin	Germany
11. Technische Universität Dresden	Germany
12. Albert-Ludwig-University Freiburg	Germany
13. Masarykova universita v Brne	Czech Republic
14. VaF Bratislava	Slovakia
15. London School of Economics and Political Science	United Kingdom
16. Budapest University of Technology and Economics (ISTRI)	Hungary
17. IBM Research GmbH	Switzerland
18. Institut de recherche criminelle de la Gendarmerie Nationale	France
19. Netherlands Forensic Institute	Netherlands
20. Virtual Identity and Privacy Research Center	Switzerland
21. Europäisches Microsoft Innovations Center GmbH	Germany
22. Institute of Communication and Computer Systems (ICCS)	Greece
23. AXSionics AG	Switzerland
24. SIRRIX AG Security Technologies	Germany

Versions

Version	*Date*	*Description (Editor)*
0.1	12.02.07	• Initial Version (Martin Meints, ICPP)
0.2	13.03.07	• Content by Sabine Delaitre (IPTS) and Denis Royer (JWG) integrated
1.0	18.04.07	• Review remarks integrated

Foreword

FIDIS partners from various disciplines have contributed as authors to this document. The following list names the main contributors for the chapters of this document:

Chapter	*Contributor(s)*
1 (Management Summary)	Martin Meints (ICPP)
2 (Intorduction)	Martin Meints (ICPP)
3 (Quality Assurance Measures and additional Content)	Sabine Delaitre (IPTS), Christian Krause (ICPP)
4 (Integration in the FCI, Redesign and Functional Enhancements)	Denis Royer (JWG), Martin Meints (ICPP)
5 (Future Plans for the Maintenance)	Martin Meints (ICPP)
7 (Annex 1: Overview of the feed back by the vendors)	Sabine Delaitre (IPTS)
8 (Annex 2: Feed Back in Detail)	Sabine Delaitre (IPTS)

Table of Contents

1 Executive Summary

This report describes the maintenance carried out for the database on Identity Management Systems (IMS) in the context of FIDIS deliverable D8.6 and D3.11. In the third project period (April 2006 to March 2007), which is covered by this report, the maintenance work mainly contained:

- Quality assurance by integrating feed back from 26 contacted vendors and editorial work carried out by ICPP leading to substantial updates of 14 records
- Adding of seven additional records (the database had 38 records by end of March 2007)
- Integration of the IMS database in the FIDIS Communication Infrastructure (FCI)
- Redesign of the layout and adaptation of the presentation system for the new FCI platform
- Development of a simplified editing front end in preparation of content management functions
- Public deployment of the database (http://imsdb.fidis.net) on 30th of March 2007

Based upon the original maintenance plan, it is planned to enhance the maintenance of the content of the database in future by using content management functions. These functions will enable vendors of IMS to maintain their own content in the database. To stimulate this vendor supported maintenance dissemination work for the database will be carried out using dissemination activities of FIDIS, FIDIS partners and other EU funded projects, such as PRIME.

2 Quality Assurance Measures and additional Content

2.1 Quality Assurance by Vendors

In the context of D8.6, quality feed-back the vendors of different IMS's was planned. To achieve this, 26 vendors were contacted via ground-mail and e-mail. Twelve vendors responded to the mail, seven sent usable feed-back, which was integrated into the existing records in the database on IMS. An overview of the feed back can be found in chapter 5 (Annex 1). The detailed feed-back is listed in chapter 6 (Annex 2).

2.2 Quality Assurance carried out by the editing team

As feed back from the developers of IMS seemed to be limited, additional maintenance work was carried out by ICPP until March 2007. These activities covered general feedback from vendors, which needed further search and editing of seven additional existing records. Mainly this work covered the check and correction of:

- Current versions of the IMS
- Identity management functions of the product and related descriptions in the database
- External links
- Adding screenshots and flow charts

Currently (end of March) the IMS database contains 38 records of different types of IMS. The database is publicly available via http://imsdb.fidis.net.

3 Integration in the FCI, Redesign and Functional Enhancements

Until May 2006 the content of the IMS database was moved to the internal FIDIS web site (internal.fidis.net). A first preliminary layout was developed and the integrated content management function used to maintain the content. In total the layout functions were limited by the version of the technical platform (Typo 3) used at that time.

From October 2006 until December 2006 a new version of the platform Typo 3 was developed and introduced by WP1 (JWG). This version enabled enhanced functionality, such as front-end editing functionality, search functions, etc. Based on the work carried out by the FCI Steering Group[1] (with respect to the public layout of the FCI) a new layout for the presentation of the content of the database was developed and tested in January and February 2007.

The following screen shots show the current layout:

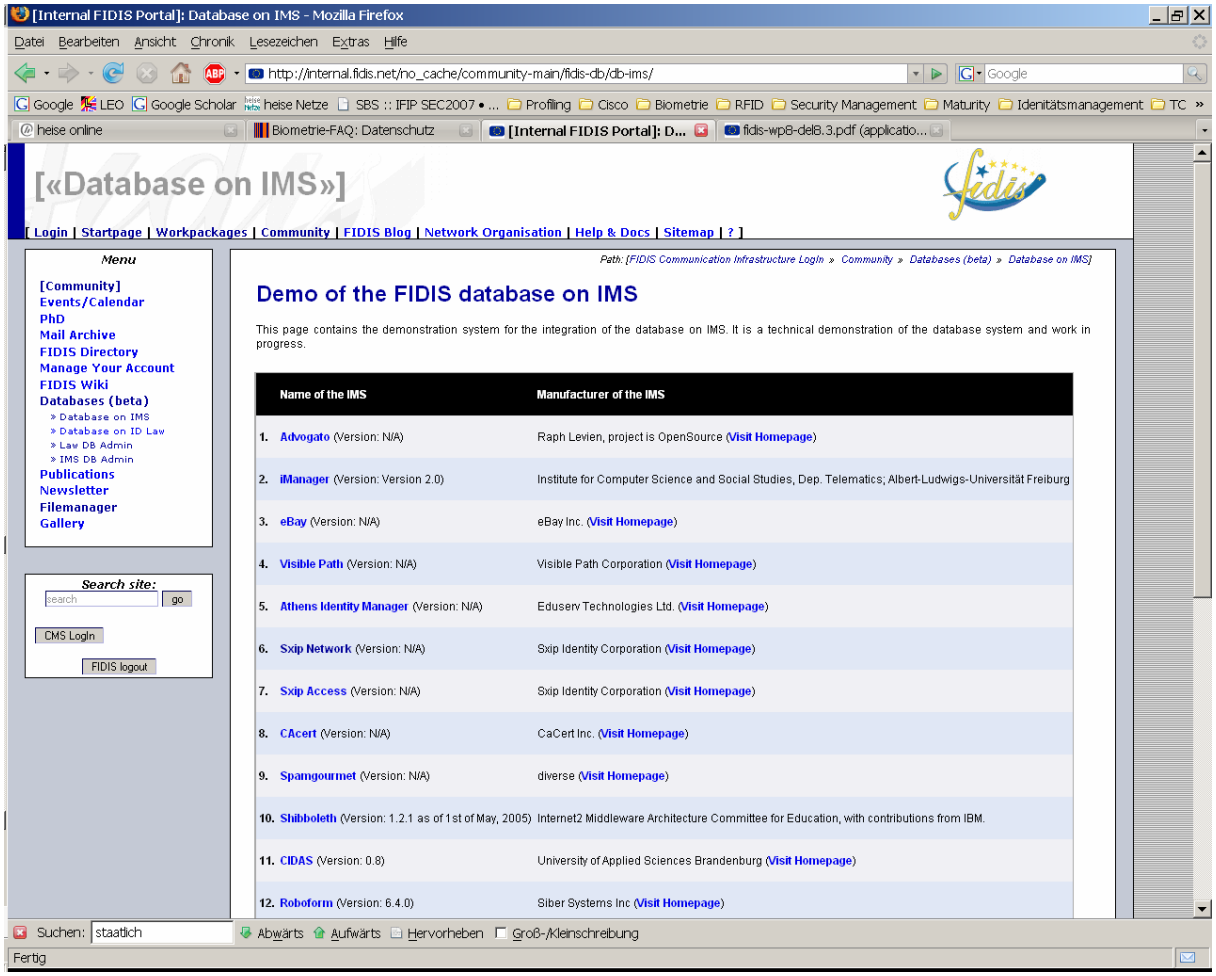


Figure 1: Overview of the available database records

[1] The FCI Steering Group was set up in the research plenary in 2006 with the mandate to co-ordinate the future development of the FCI.

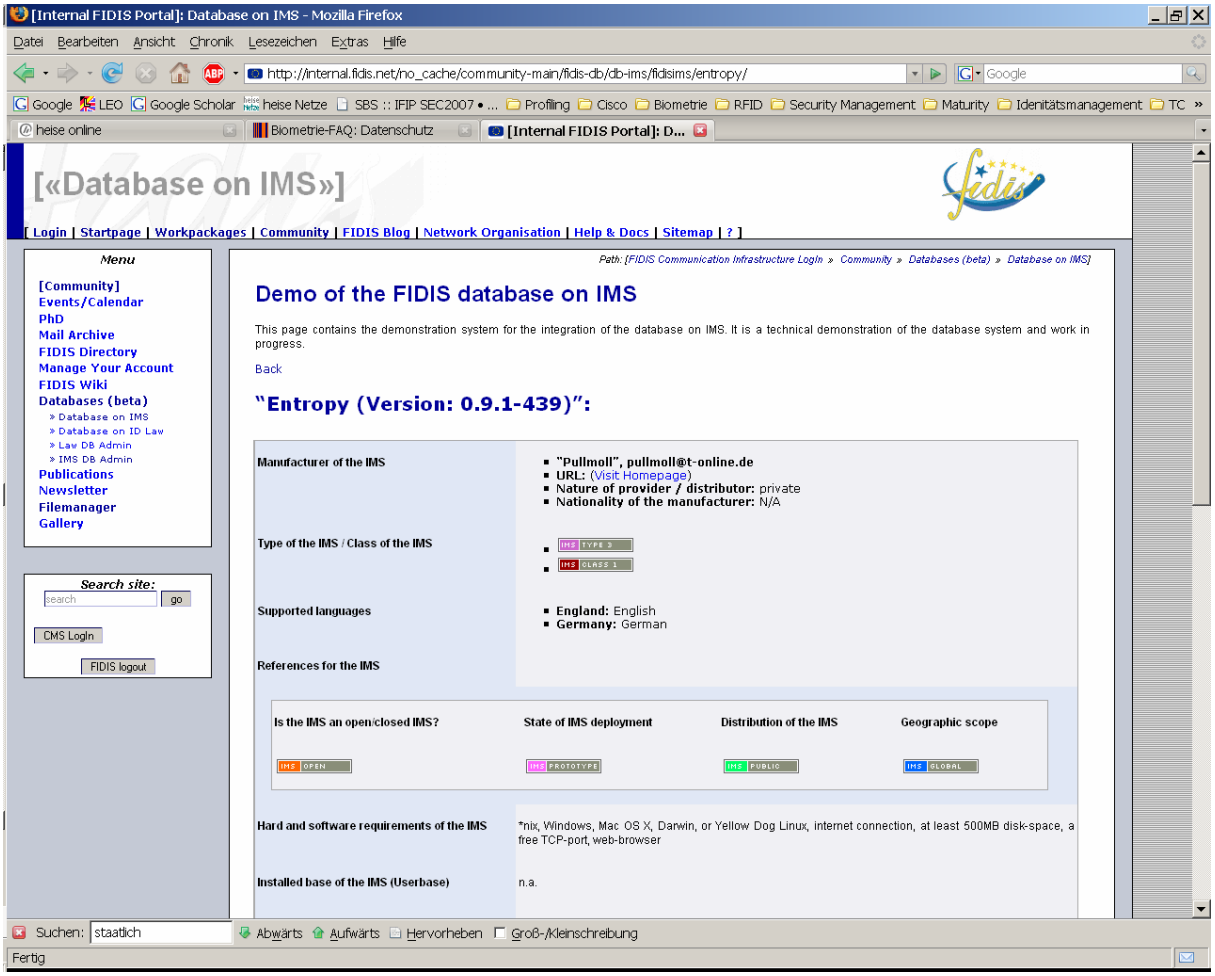


Figure 2: Example of a sample database record (1/4)

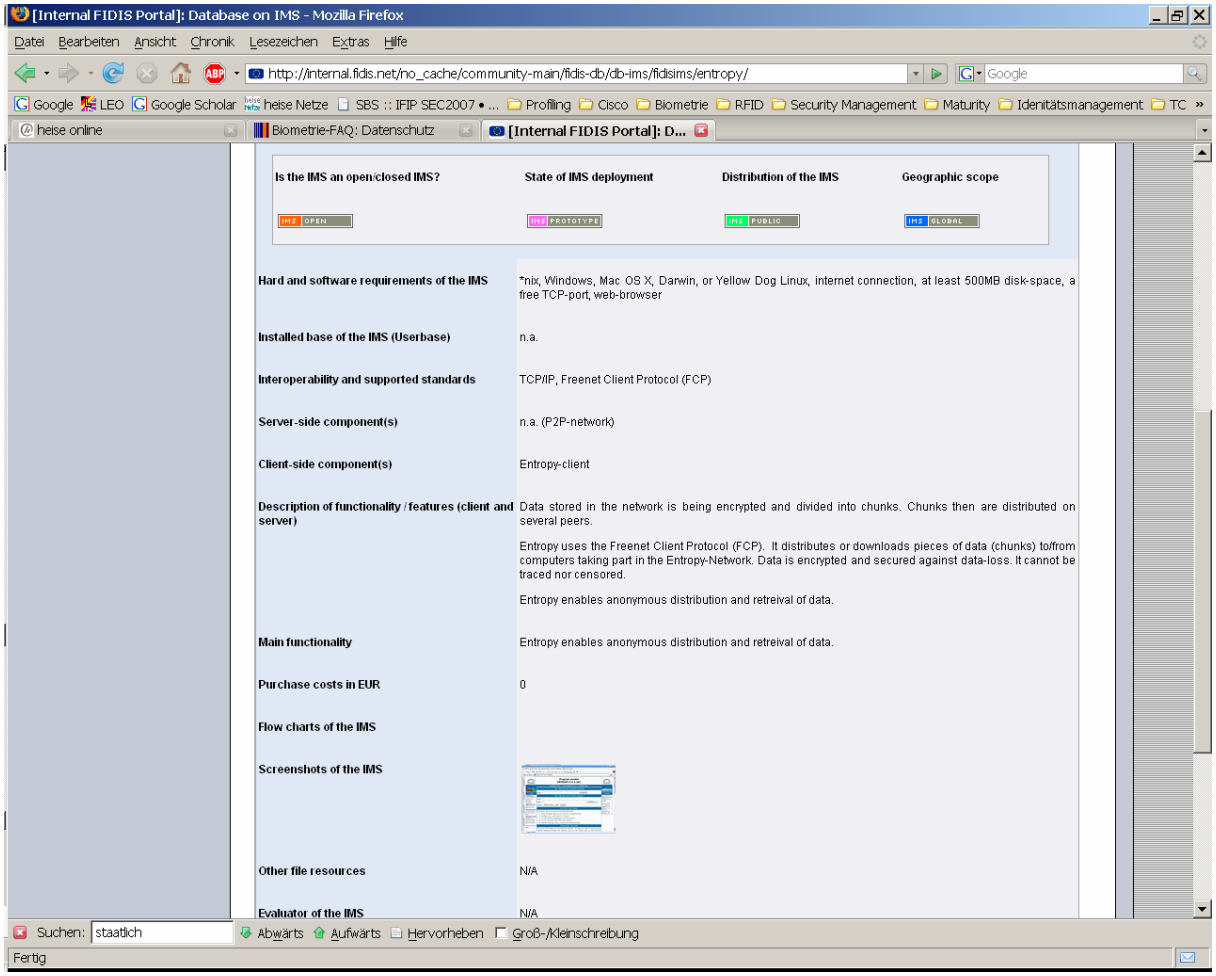


Figure 3: Example of a sample database record (2/4)

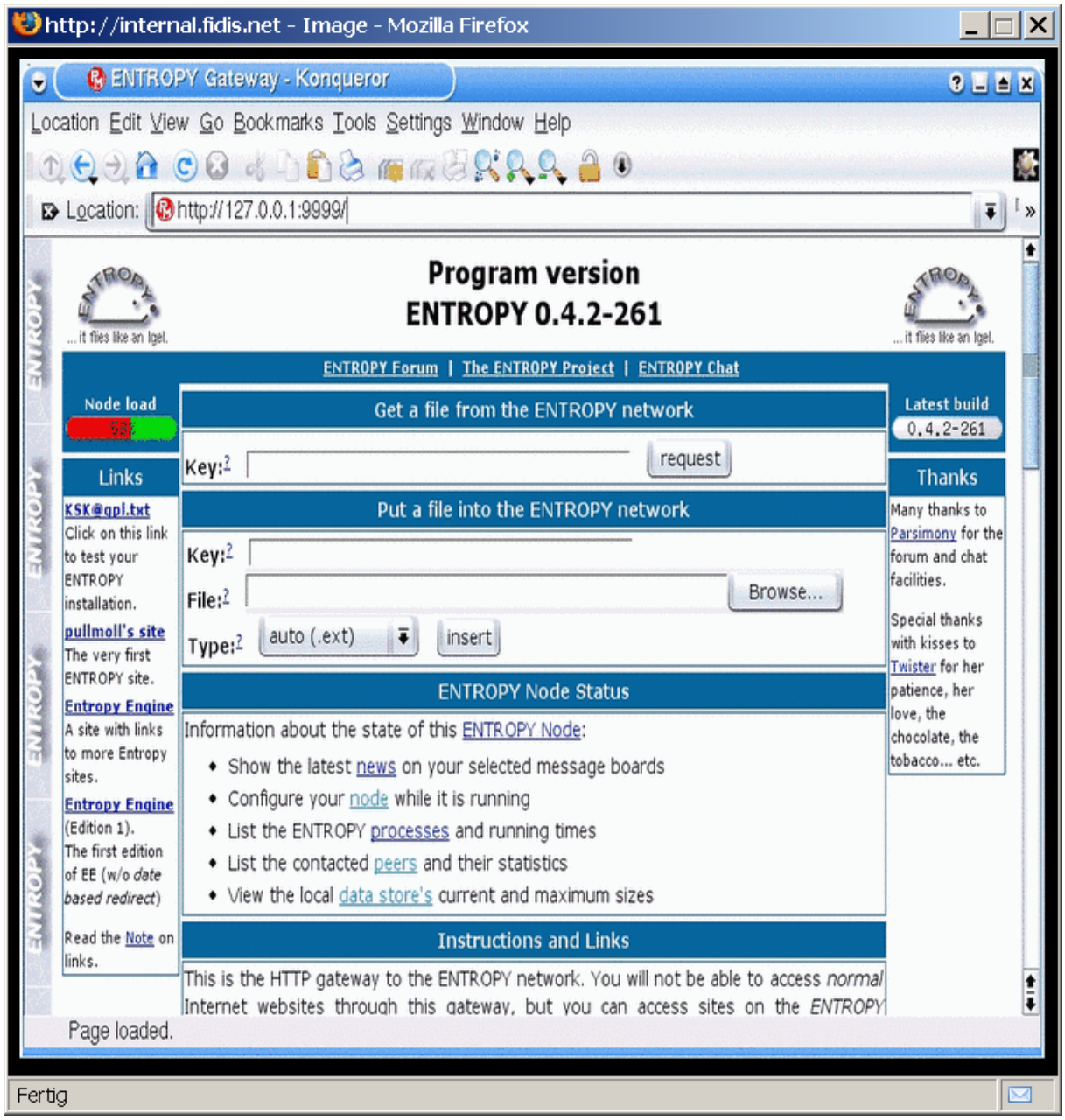


Figure 4: Example of a sample database record (3/4), zoomed view on a screenshot in a database record

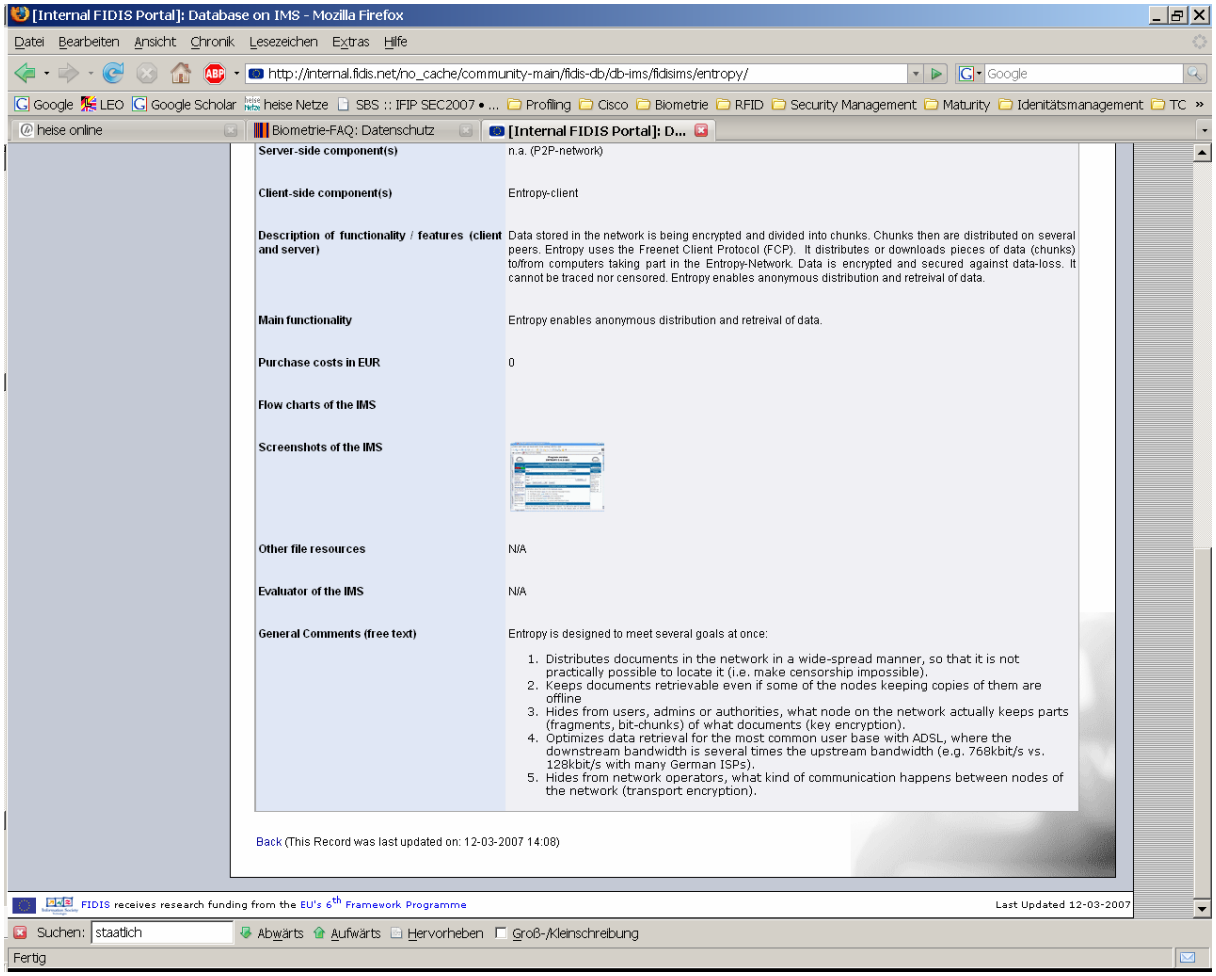


Figure 5: Example of a sample database record (4/4)

This layout is used for the public deployment of the database on IMS end of March 2007.

For a permanent maintenance structure of the IMS database a content management system is needed. This should support editing of existing records by vendors and the creation of new records. As authentication of vendors and quality of content may be a problem, an editorial check of the content by ICPP is planned. The editing interface needs to support a corresponding workflow to facilitate checking, approving and deployment of new content.

As a first step with respect to described enhanced functionality, an administrative interface for the database was integrated at internal.fidis.net. This interface allows the editing and approving of content by selected editors and supports notification of a selected database manager to stimulate further actions. The notification currently is carried out via e-mail.

The following screen shots show the admin interface.

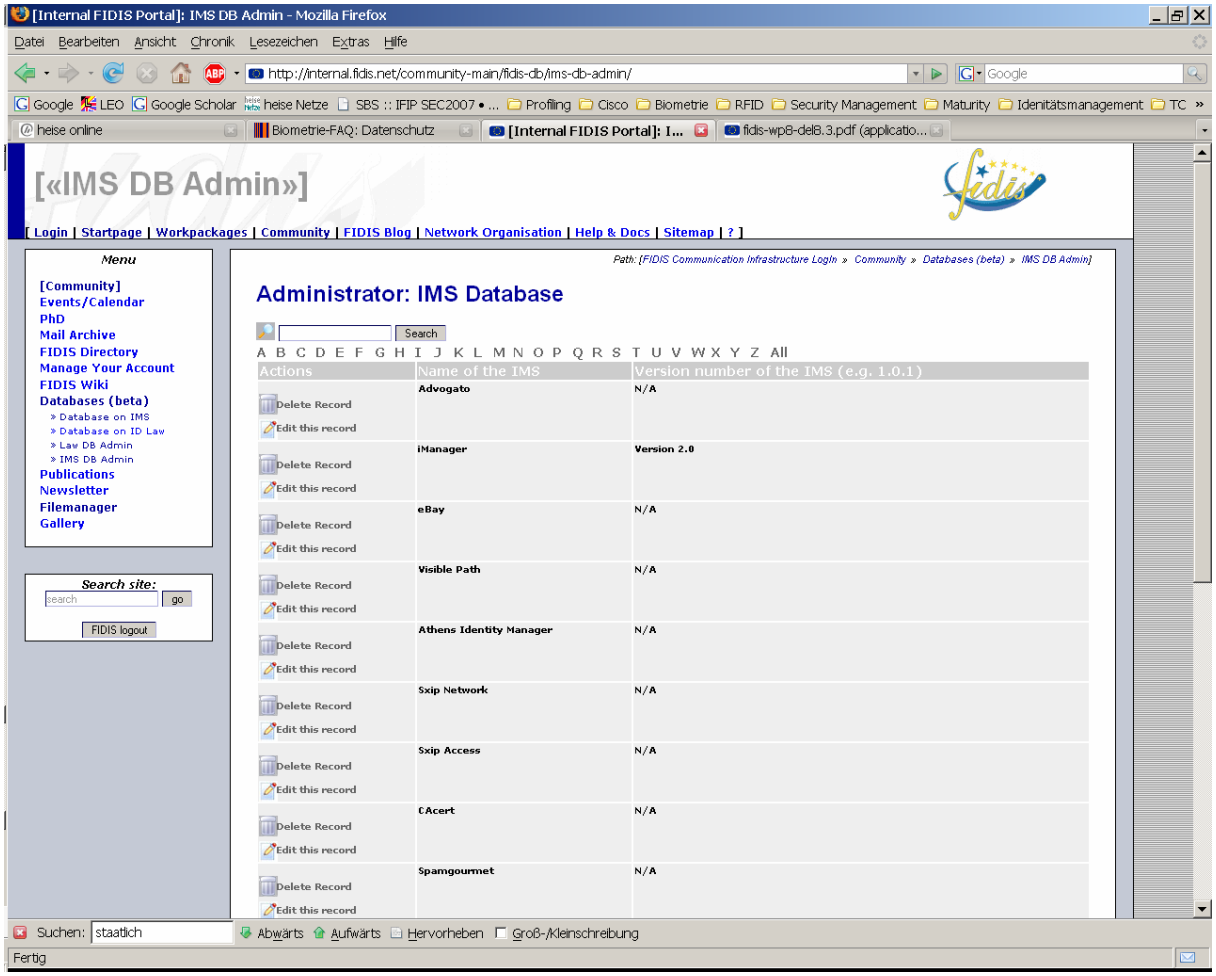


Figure 6: Record overview

The admin interface starts with an overview of existing records. Records can be searched for, edited or deleted. When choosing “Edit a record”, the following editing form is displayed (partial view only):

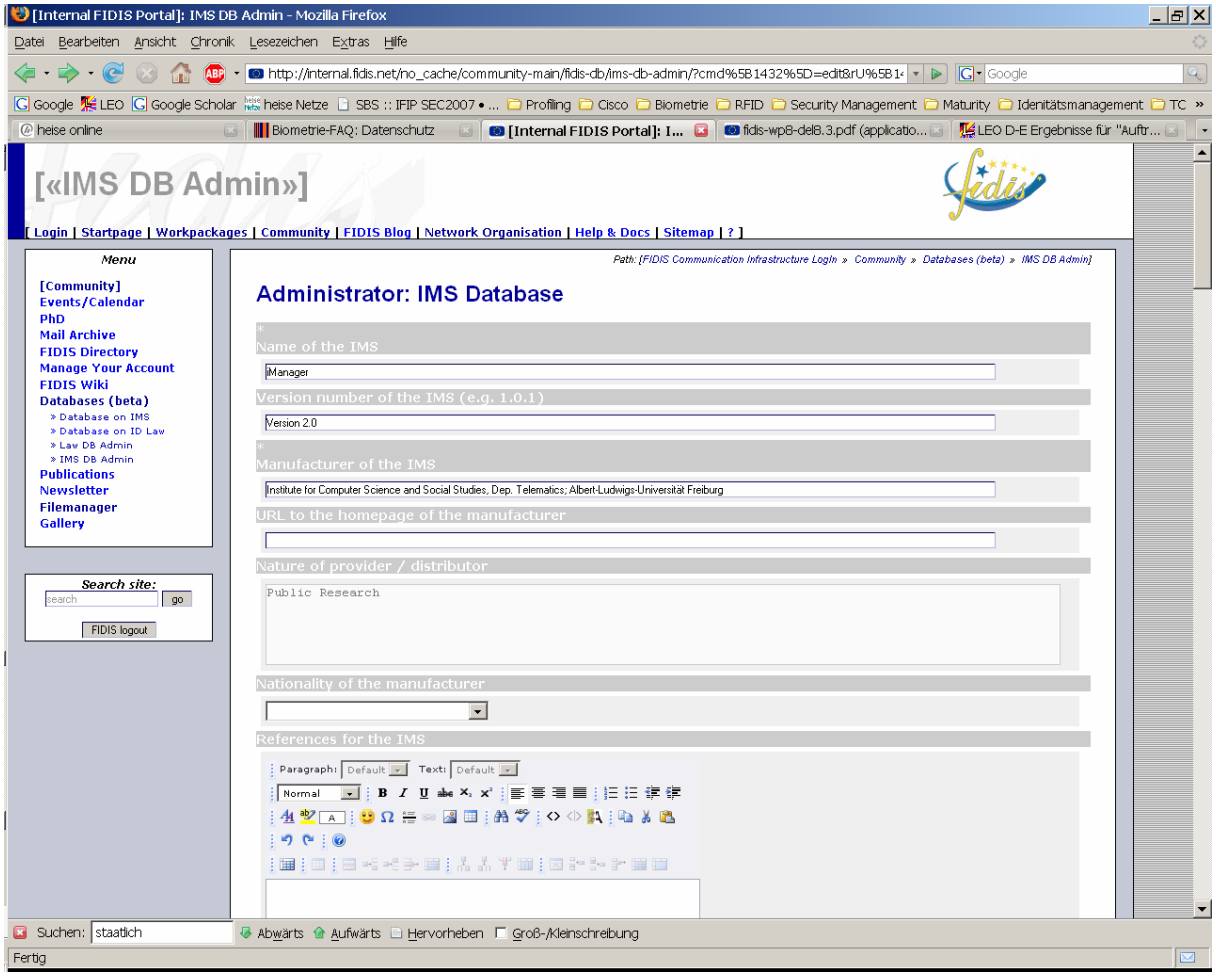


Figure 7: Editing form (1/2)

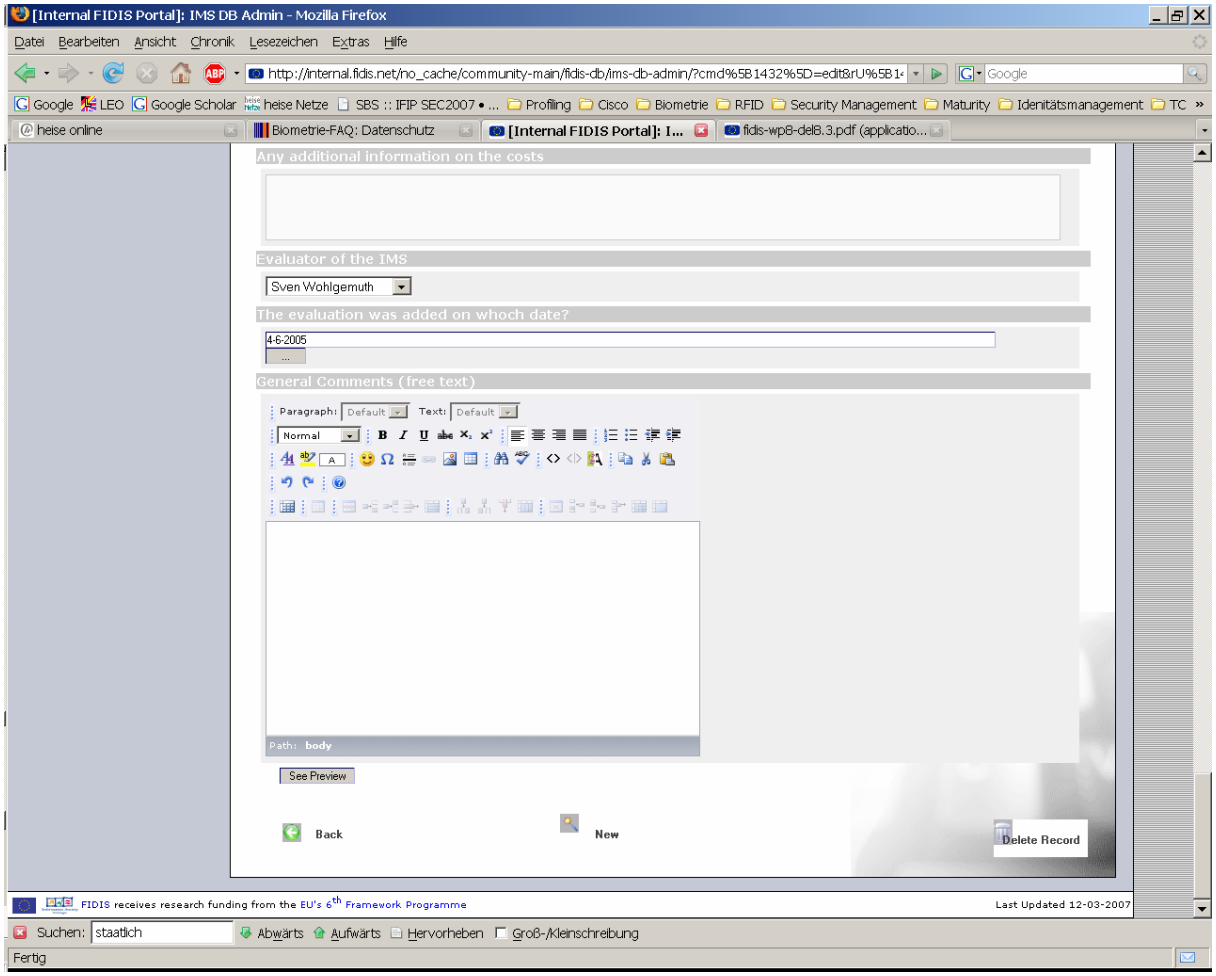


Figure 8: Editing form (2/2)

When this form is completed (or changed), a preview can be selected – cp. following screenshot.

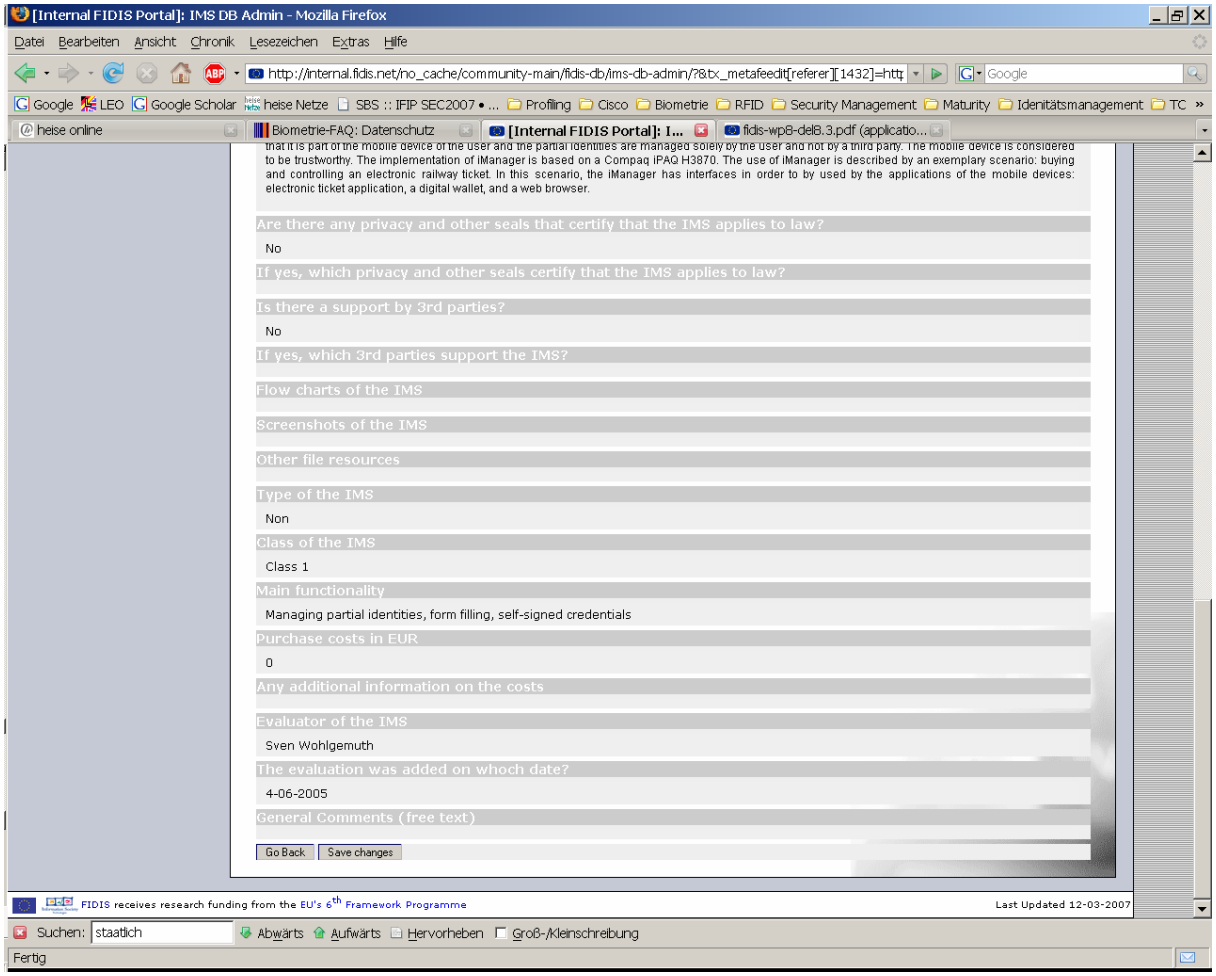


Figure 9: Preview of edited records

The administrative front end is available vial http://internal.fidis.net/community-main/fidis-db/ims-db-admin.

The FCI development work described in this chapter was carried out by JWG, supported by ICPP through description of requirements, testing and approving.

4 Future Plans for the Maintenance

In the long run, a maintenance concept is needed that is more resource efficient. For this reason vendors of IMS should have the opportunity to maintain their own content in the database. In order to facilitate this, content management functionalities are a possible solution. A first step in this direction was made in this period with the simplified admin interface in the front-end of the FCI.

In the next period it is planned to integrate this interface in an editing workflow:

1. Vendors can suggest modification in existing content or new records
2. A member of a team of an editors checks and approves the modified or newly added content
3. After approving, the content is published at www.fidis.net

As the current FCI does not support such a workflow for non members yet, additional programming is required, using existing libraries and functions of the FCI. As an intermediate solution an e-mail address of the editing team is offered (imsdb@fidis.net).

To stimulate feed back from vendor's dissemination is needed. For this purpose presentations on various conferences attended by FIDIS members will be used, supported by the FIDIS website, websites of FIDIS partners and a press release. In addition, co-operation with other EU funded projects, such as PRIME, are planned.

In addition it is planned to use the content of the database as a platform for a delta report, summarising the development in IMS during period 1 to 4 of FIDIS. This will be a separate deliverable in the context of the Work Package 3 on High-Tech ID (WP3) in the fifth Work Plan.

5 Annex 1: Overview of the feed back by the vendors

On 27 IMS, produced by 26 manufacturers (cf. sxip products), we obtained 12 answers

Color code:

Green : answer with feedback (completed questionnaire or email with information)

Blue : answer with intention to send feedback but no reception

Red : negative answer, no possibility to deliver feedback

Yellow: answer to obtain more detail on our survey

Nb	IMS name	Evaluator	Organism	Date	reference	version	manufacturer	contact and last contact- LC- (in case of various)	Date of questionnaire sending	Remark
1	Advogato	Christian Krause	ICPP	20-Jan-2006	http://www.advogato.org/	n.a.	Raph Levien, project is OpenSource	raph.levien@gmail.com	10/07/06 + doc	
2	Athens Identity Manager	M. Meints	ICPP	13-Jun-2005	http://www.athensams.net/		Eduserv Technologies Ltd.	http://www.athensams.net/contact.html	10/07/06 +doc	
5	Cookie Pal	Christian Krause	ICCP	13-Oct-2005	http://www.kburra.com/	1.7c	Kookaburra Software	info@kburra.com	10/07/06 + doc	
6	Friendster	Christian Krause	ICPP	05-Jan-2006	http://www.friendster.com/	n.a.	Friendster, Inc.	international@friendster.com	10/07/06 + doc	
8	HiPath SIcurity DirX	Christian Krause	ICPP	20-Jan-	http://www.siemens.de/directory	7.0	Siemens	psc-51296	contact 10/07/06	Feedback

				2006				LC: paulus.hovestadt@siemens.com	sending doc(13/07/06)	24/07/06
9	Hushmail	Christian Krause	ICCP	13-Oct-2005	http://www.hushmail.com/	n.a.	Hush Communications Inc.	No e-mails available in the web-site LC: ben.cutler@hush.com	contact 10/07/06 contact request	Willingness but no reception
10	Jabber	Christian Krause	ICPP	05-Jan-2006	http://www.jabber.org	n.a.	diverse, protocol by Jabber Software Foundation		10/07/06 + doc	
12	KeePass Password Safe	C. Krause	ICPP	06-Jun-2005	http://keepass.sourceforge.net	1.0	Dominik Reichi	**LC:** dominik.reichl@t-online.de	contact email 10/07/2006	Feedback 12/07/06
13	Kerberos	M. Meints	ICPP	07-Jun-2005	http://web.mit.edu/kerberos/www/	5-1.4.1	MIT Massachusetts Institute of Technology	<kerberos@mit.edu> ..http://web.mit.edu/kerberos/contact.html After 5 contacts, **LC**: Paul B hill pbh@MIT.EDU	10/07/06 + doc	New contact 22/08/06 Feedback 23/08/06
14	Leverage Software	Christian Krause	ICPP	01-Mar-2006	http://www.leveragesoftware.com/	n.a.	Leverage Software, San Francisco, CA	No e-mails available in the web-site -->> no, contact us	contact email 10/07/06	
15	Liberty Alliance	Christian Krause	ICPP	13-Oct-2005	http://www.projectliberty.org	1.1	Liberty Alliance Project	info@projectliberty.org	10/07/2006 +doc	
16	Light-Weight IDentity (LID)	Martin Meints	ICPP	04-Jun-2005		N/A	NetMesh Inc.	info@netmesh.us **LC**: Johannes Ernst, jernst@netmesh.us	10/07/2006 +doc	Feedback 12/07/06
17	LOAF	Christian Krause	ICPP	13-Oct-2005	http://loaf.cantbedone.org/	0.03	Maciej Ceglowski, Joshua Schachter	maciej @ceglowski.com	contact email 11/07/06 +doc	
18	Mozilla Firefox	C. Krause	ICPP	06-Jun-2005	http://www.mozilla.org/products/firefox	1.0.x	Mozilla Organisation	webmaster (1st)	10/07/06 + doc	
19	Norton Password Manager	Christian Krause	ICPP	30-Nov-2005	product evaluation	1.03	Symantec Corporation		contact email 10/07/06 ref: 2277051	

20	OpenID	M. Meints	ICPP	07-Jun-2005	http://www.danga.com/openid/	In development	Brad Fitzpatrick	brad@danga.com	10/07/06 + doc	
21	OpenPrivacy	Christian Krause	ICPP	13-Oct-2005	http://www.openprivacy.org/	0.7 (Whitepaper)	OpenSource, Founders: Fen Labalme fen@openprivacy.org, Kevin Burton burton@openprivacy.org	fen (burton failure of delivery message)	10/07/06 + doc	
22	Opera	Christian Krause	ICPP	13-Oct-2005	http://www.opera.com/	8	Opera Software ASA		contact email 10/07/06	
23	Orkut	M. Meints	ICPP	04-Jun-2005		beta	Google, Inc		contact email 10/07/06 ref: #64899783	
24	PayPal	Christian Krause	ICPP	05-Jan-2006	http://www.paypal.com/	n.a.	PayPal (Europe) Ltd., registered in GB	leen (10/07/06) lisa (12/07/06) LC: rebecca: negative answer (security reasons unable to view attached doc) webform@paypal.com	contact 10/07/06 +doc (11/07)	Request for information
25	Roboform	Christian Krause	ICPP	13-Oct-2005	http://www.roboform.com/	6.4.0	Siber Systems Inc	ask@robofrom.com	10/07/06 + doc ref:88791 Bill Carey	**10/07/06 it is an old version the new version is 6,7,4**
26	Shibboleth	M. Meints	ICPP	04-Jun-2005		1.2.1 as of 1st of May, 2005	Internet2 Middleware Architecture Committee for Education, with contributions from IBM.	shib-info@internet2.edu LC: Steve Olshansky steveo@internet2.edu	10/07/06 + doc	Feedback 12/07/06
27	Spamgourmet	Christian Krause	ICPP	14-Oct-2005	http://www.spamgourmet.com/	-	diverse, team contact info@spamgourmet.com	Josh Hamilton With the mail: info@spamgourmet.com	10/07/06 +doc	feedback 10/07/06 :)

28	Sxip Access	Christian Krause	ICPP	14-Oct-2005	http://www.sxip.com/	n.a.	Sxip Identity Corporation, info@sxip.com	lori@sxip.com	10/07/06 +doc (2)	first answer 10/07/06
29	Sxip Network	Christian Krause	ICPP	14-Oct-2005	http://www.sxip.net/	n.a.	Sxip Identity Corporation		see sxip.com	
30	Visible Path	Christian Krause	ICPP	01-Mar-2006	http://www.visiblepath.com/	n.a.	Visible Path Corporation, lradosevich@visiblepath.com		10/07/06 +doc	
31	eBay	Christian Krause	ICPP	13-Oct-2005	http://www.ebay.de	n.a.	eBay Inc.		contact email 10/07/06 +doc	

6 Annex 2: Feed Back in Detail

6.1 HiPath SIcurity DirX Feedback

HiPath SIcurity Identity Management System

Verification of data – Instructions

Please indicate with a Yes/No in the respective field of the following table the correctness / completeness of the data held in our database. If you find that the data is not correct and/or complete, please proceed with making the appropriate corrections / additions by appropriately filling in the next field ("Correction / Completion").

For a description / definition of each field, you can refer at Table B.

TABLE A – VERIFICATION OF DATA				
Data held in database			Yes / No	Correction / Completion
1.	**Evaluation of IMS**			
1.1.	**Evaluator:**	Christian Krause		
1.2.	**Organisation:**	ICCP		
1.3.	**Date of evaluation:**	20-Jan-2006		
2.	**Identification of IMS**			
2.1.	**Sources of information:**	http://www.siemens.de/directory	Yes	http://www.siemens.com/hipath-sicurity
2.2.	**Version:**	7.0	Yes	
2.3.	**Manufacturer:**	Siemens	No	Siemens AG
2.4.	**Nature:**	international	Yes	
2.5.	**Country:**	Germany	Yes	
2.6.	**Regions:**	Global	Yes	
2.7.	**Language:**	ENGLISH,GERMAN	Yes	
2.8.	**State:**	Available	Yes	

TABLE A – VERIFICATION OF DATA				
Data held in database			**Yes/No**	**Correction / Completion**
2.9.	**Open/Closed:**	Closed IMS: the scope of the identities is restricted to the IMS context.	Yes	
3.	**Platform & Environment**			
3.1.	**Requirements:**	Intel Server Platform or SPARC, 1GB RAM, 700+MB HD, Windows, Solaris, Red Hat, SuSE	Yes	
3.2.	**Number of users:**	n.a.	Yes	
3.3.	**Standards:**	LDAPv3, DSMLv2, DAP, DSP, DISP, IDM, X.500, X.509, X521	Yes	
3.4.	**Description of Server - Side components:**	DirX is a meta directory allowing interoperability between directory services. To achieve this the directory service's data is reproduced in the meta directory.	No	Server components are: Identity Server, Agents and Connectors, Identity Store. The Identity Server provides a comprehensive runtime environment for event-triggered and scheduled provisioning workflows. Agents and connectors provision and synchronize accounts/groups in target systems. The Identity Store is an LDAPv3 directory server.
3.5.	**Description of methods:**	n.a.	No	DirX Identity provides provisioning and synchronization based on a metadirectory technology.
3.6.	**Descriptor of Client - Side components:**	n.a.	No	The Identity Web Center is the component that enables user self-service and delegated administration from a Web browser.
3.7.	**Seals:**	No	Yes	
3.8.	**Which seal:**			
3.9.	**Third party:**	no	Yes	
3.10.	**Which third party:**			
3.11.	**Features:**	Among other identity management-features meta directories faciltate single sign-on.	No	Web-based user self-service and delegated administration, password management, user management, cross-platform provisioning and metadirectory functionality. The provisioning of users and their access rights

TABLE A – VERIFICATION OF DATA				
Data held in database			**Yes/No**	**Correction / Completion**
				in various target systems is driven by a powerful, centralized privilege management component which deals with the business roles, permissions, user groups, and includes a flexible policy and workflow engine. In addition, comprehensive scheduling, monitoring and auditing are available.
3.12.	**Screenshot picture:**	HiPath SIcurity dirx_screen.png		
3.13.	**Flowchart:**	HiPath SIcurity dirx-flow.png		
4.	**Cost**			
4.1.	**Price:**	0		
4.2.	**Comment to the Cost:**	depends on product	No	Product pricing depends on the number of managed identities
5.	**Type & Class of IMS**			
5.1.	**Type of IMS:**	Type 1: IMS for account management.	Yes	
5.2.	**Class of IMS:**	Class 1: Pure IMS which main objective is to support or implement identity management functionality.	Yes	
5.3.	**Functionality:**	metadirectory, account management, single sign-on	No	metadirectory, account management, password management
6.	**Suggestions:**	Meta directories in general connect different directory services. Data from one directory service is available for another. To achieve this, data is reproduced in a central database.		

6.2 KeePass Password Safe feedback

Keepass Identity Management System

Verification of data – Instructions

Please indicate with a Yes/No in the respective field of the following table the correctness / completeness of the data held in our database. If you find that the data is not correct and/or complete, please proceed with making the appropriate corrections / additions by appropriately filling in the next field ("Correction / Completion").

For a description / definition of each field, you can refer at Table B.

TABLE A – VERIFICATION OF DATA

	Data held in database		Yes / No	Correction / Completion
1.	**Evaluation of IMS**			
1	**Evaluator:**	Christian Krause		
1	**Organisation:**	ICCP		
1	**Date of evaluation:**	06-Jun-2005		
2.	**Identification of IMS**			
2	**Sources of information:**	**http://keepass.sourceforge.net**	Yes	
2	**Version:**	1.0	No	1.05 is the latest version.
2	**Manufacturer:**	Dominik Reichl	Yes	
2	**Nature:**	private	Yes	
2	**Country:**	Germany	Yes	
2	**Regions:**	Global	Yes	
2	**Language:**	CZECH,DANISH,DUTCH,ENGLISH,ESTONIAN,FRENCH,GERMAN,HUNGARIAN,ITALIAN,POLISH,PORTUGUESE,SLOVAK,SPANISH	Yes	Also in Bulgarian, Catalan, Finnish, Greek, Hebrew, Japanese, Korean, Lithuanian, Macedonian, Norwegian, Russian, Chinese, Swedish, Turkish, Ukrainian

TABLE A – VERIFICATION OF DATA				
Data held in database			Yes / No	Correction / Completion
2	**State:**	Available	Yes	
2	**Open / Closed:**	Open IMS: the identities work with several systems or applications.	Yes	
3.	**Platform & Environment**			
3	**Requirements:**	MS Windows 95 or higher	Yes	
3	**Number of users:**	237365 Downloads in May 2005	No	860.442 downloads up to July 2006
3	**Standards:**	Interoperability is mainly achieved via clipboard-functions of Windows Operating System. This Software is OpenSource, so it can theoretically ported to other systems.	Yes	Interoperability also through Auto-Type, Drag-and-Drop and automatic form filling.
3	**Description of Server - Side components:**	n.a.	Yes	
3	**Description of methods:**	KeePass is a password manager with an AES/Twofish encrypted database.	Yes	
3	**Descriptor of Client - Side components:**	KeePass	Yes	
3	**Seals:**	No	Yes	
3	**Which seal:**		Yes	
3	**Third party:**	no	Yes	
3	**Which third party:**		Yes	
3	**Features:**	Users can store passwords and add meta-data such as URLs, expiry-dates and comments. Passwords are copied to clipboard via double-click and are deleted from clipboard automatically after ten seconds.	Yes	
3	**Screenshot picture:**	http://keepass.sourceforge.net/screenshots.php	Yes	
3	**Flowchart:**	n.a.	Yes	
4.	**Cost**			
4	**Price:**	0	Yes	
4	**Comment to the Cost:**		Yes	
5.	**Type & Class of IMS**			
5	**Type of IMS:**	Type 3: IMS for user-controlled context-dependent role and pseudonym management.	Yes	

TABLE A – VERIFICATION OF DATA				
Data held in database			Yes / No	Correction / Completion
5.	**Class of IMS:**	Class 1: Pure IMS which main objective is to support or implement identity management functionality.	Yes	
5.	**Functionality:**		Yes	
6.	**Suggestions:**		Yes	

6.3 Kerberos feedback

Kerberos Identity Management System

Verification of data – Instructions

Please indicate with a Yes/No in the respective field of the following table the correctness / completeness of the data held in our database. If you find that the data is not correct and/or complete, please proceed with making the appropriate corrections / additions by appropriately filling in the next field ("Correction / Completion").

For a description / definition of each field, you can refer at Table B.

TABLE A – VERIFICATION OF DATA				
Data held in database			Yes / No	Correction / Completion
7.	Evaluation of IMS			
7	Evaluator:	M. Meints		
7	Organisation:	ICCP		
7	Date of evaluation:	07-Jun-2005		
8.	Identification of IMS			
8	Sources of information:	http://web.mit.edu/kerberos/www/		
8	Version:	5-1.4.1		
8	Manufacturer:	MIT Massachusetts Institute of Technology		
8	Nature:	Private		
8	Country:	USA		
8	Regions:	Global		
8	Language:			
8	State:	Available		
8	Open / Closed:	Open IMS: the identities work with several systems or applications.		

TABLE A – VERIFICATION OF DATA				
Data held in database			**Yes / No**	**Correction / Completion**
9.	**Platform & Environment**			
9	**Requirements:**	Almost any modern hardware/software		
9	**Number of users:**	Widely used, distributed with various Microsoft and Apple products		
9	**Standards:**	Kerberos employs a standardized protocol of the same name. There are several partially interoperable implementations by MIT, Kungliga Tekniska Hoegskoln Stockholm, Microsoft, Apple and Transarc		The Transarc implementation only supports version 4 of the protocol and should be considered obsolete. I do not recommend including it in this document. The Kerberos standard is defined by the IETF. The current controlling documents are RFC 4120 and RFC 4537 Suggest that you change "partially" to "mostly".
9	**Description of Server - Side components:**	The main component is the Key Distribution Center (KDC) which authenticates the users and supplies them with so-called tickets. These in turn allow the use of other resources. The KDC shares secrets with every service and user in the installation.		
9	**Description of methods:**	The only data kept about a user is her username and a hash of her password. The password can be changed by the user.		
9	**Descriptor of Client - Side components:**	The client needs Kerberos-enabled clients for the services it wants to use with Kerberos.		
9	**Seals:**	No		
9	**Which seal:**			
9	**Third party:**	yes		
9	**Which third party:**			

TABLE A – VERIFICATION OF DATA				
Data held in database			**Yes / No**	**Correction / Completion**
9	**Features:**	Kerberos authentication perimeters are called Realms. Inside a realm, the Kerberos setup consists of clients, application servers and the Ticket Granting Service (TGS). A user authenticates herself by password on her local machine (which must be known to the TGS and share a secret with it). After successful authentication the user can request tickets for services from the TGS. A ticket states that the user is authenticated and is allowed to use the service. Services on the application servers check if the user sent a valid ticket with her request, and allows access if valid. Tickets are valid only for pre-defined periods of time. Newer versions of Kerberos allow cross-realm authentication. In this setup, the TGSs of the several realms have pairwise shared secrets and forward requests to remote services. The forwarded tickets are authenticated with the shared secrets.		There are many other standards that extend the functionality of Kerberos. For example some implementations currently support PKINIT so that public keys can be used for initial authentication instead of a username / password. Please see http://www.ietf.org/html.charters/krb-wg-charter.html You make no mention that many organizations use Kerberos as a key component of their single sign-on (SSO) strategy. That is probably more useful than the features that you are pointing out. There are also products that use Kerberos for web authentication. Using http-spnego. Examples include: IE, IIS, Apache, Firefox, Safari, ...
9	**Screenshot picture:**	n.a.		
9	**Flowchart:**	kerberos-flow.gif		
10	**Cost**			
1	**Price:**	0		
1	**Comment to the Cost:**	Open Source		

TABLE A – VERIFICATION OF DATA				
	Data held in database		Yes / No	Correction / Completion
11.	**Type & Class of IMS**			
1	**Type of IMS:**	Type 1: IMS for account management.		
1	**Class of IMS:**			
1	**Functionality:**	Authentication and Single Sign-On		
12.	**Suggestions:**			

6.4 LID feedback

LID has made substantial progress since the time of your evaluation. Depending on the goal of your table, what we filled in may or may not be sufficient; there are substantial other features as well.

NetMesh InfoGrid LID (Light-Weight Identity) Identity Management System

Verification of data – Instructions

Please indicate with a Yes/No in the respective field of the following table the correctness / completeness of the data held in our database. If you find that the data is not correct and/or complete, please proceed with making the appropriate corrections / additions by appropriately filling in the next field ("Correction / Completion").

For a description / definition of each field, you can refer at Table B.

TABLE A – VERIFICATION OF DATA				
Data held in database			**Yes / No**	**Correction / Completion**
13.	**Evaluation of IMS**			
13.1	**Evaluator:**	Martin Meints		
13.2	**Organisation:**	ICCP		
13.3	**Date of evaluation:**	04-Jun-2005	N	substantially extended since
14.	**Identification of IMS**			
14.1	**Sources of information:**			
14.2	**Version:**	N/A		
14.3	**Manufacturer:**	NetMesh Inc.		

TABLE A – VERIFICATION OF DATA				
Data held in database			**Yes/No**	**Correction / Completion**
14.4	**Nature:**	Private company		
14.5	**Country:**	USA		
14.6	**Regions:**	Global		
14.7	**Language:**	ENGLISH		
14.8	**State:**	Prototype	No	Beta; deployed both on the public internet and inside corporate enterprises today
14.9	**Open/Closed:**	Open IMS: the identities work with several systems or applications.	No	Not just "several" but LID has been constructed explicitly with the goal of "internet scale": thousands or millions of systems and applications from a variety of vendors, open-source projects etc. LID functionality can be extended and augmented by implementers / deployers.
15.	**Platform & Environment**			
15.1	**Requirements:**	Hardware: any; Software: Web Server, Perl, Open Source components	No	Hardware: any; Software: Web Server or Application Server, either Perl or PHP or Java/J2EE (recommended)
15.2	**Number of users:**	unknown - because of decentralised approach	addition	More than 10 million enabled users
15.3	**Standards:**	The protocol and the reference implementation are open (and quite concise), so interoperable implementations should be easy.	addition	Supports the Yadis, OpenID, PGP, VCard, XML, XPath, HTML standards. Interoperable implementations exist from vendors such as Six Apart, Jan Ran and

TABLE A – VERIFICATION OF DATA				
Data held in database			**Yes/No**	**Correction / Completion**
				Verisign.
15.4	**Description of Server - Side components:**	CGI-script (The user runs the server-side-component. It is assumed, that he/she has control over the server.)	No	In the PHP and Perl implementations, this is correct. In the Java/J2EE implementation, the server-side component is a collection of Servlets. Persistence in a relational database (e.g. MySQL)
15.5	**Description of methods:**		Addition	Encryption through PGP and Diffie-Hellman shared secrets. RESTful. Rich and thin clients. Availability, integrity and confidentiality through standard web methods (e.g. server mirroring, SSL, public key encryption etc.)
15.6	**Descriptor of Client - Side components:**		Addition	Can be used in thin-client and rich-client environments. No requirements in case of thin clients.
15.7	**Seals:**	No		
15.8	**Which seal:**			
15.9	**Third party:**	no	Yes	
15.1	**Which third party:**		Yes	Versign, Six Apart, Jan Rain, RSS, Atom etc.
15.1	**Features:**	The salient idea behind LID is to use the URLs of CGI scripts as "smart pointers" to personal information. URLs are commonly accepted identifiers on the Internet, and the script referred to by the URL can actively check requests for the data before returning any. The architecture is totally decentralized and relies on HTTP as the only means of communication. Creation of accounts/IDs: The user creates an	Addition	Through the additional Yadis protocol, LID services may run at URLs other than the identity URL. That way, a simple HTML markup in the HTML HEAD section is sufficient to turn any URL into a LID

TABLE A – VERIFICATION OF DATA				
Data held in database			Yes / No	Correction / Completion
		identity by installing a perl-script on a web server maintained by him/her or a trusted party. The personal information is stored in vcard (RFC2425) format on the web server and can only be accessed by the script. Social links to other people and another set of personal information can expressed in a FOAF (http://xmlns.com/foaf/0.1/) file, again only accessable for the script. LID allows to have arbitrarily many IDs (Pseudonyms). To make this easier, the pseudonymous scripts may delegate requests opaquely to other scripts that process the personal information. Web Single-sign-on: The users gives a website his/her LID-URL. The website then sends a redirect to the LID-URL, together with a cookie to tie the browser to the LID-Id. The redirect gives the script behind the URL additional parameters like the URL of the website, a nonce, the action requested from the script (authentication in this case) and the type of authorization accepted at the website. The user's browser follows the redirect and calls the LID-URL with the parameters. The script signs the nonce, URL and action strings using public key cryptography (gnupg) and returns it through another redirect to the website. The public key is bound to the LID-URL, not an e-mail address as suggested by the OpenPGP standard. The website can request the public key directly from the LID-script, and check if the signature on the authentication data is valid. If so, the browser proved that it exerts control over the script behind the LID-URL, which can then be used as identity for further transactions. No PKI is necessary for LID itself, the script returns its own key on request. To secure transmission of keys, HTTPS can be employed with the partial PKI already employed there. Personal Information: Personal information (vCard or FOAF) can be requested by simply calling the LID-script of the ID (the URL of the scrit _is_ the ID). The user may configure the script to act differently when given additional parameters, for example the LID-ID of the requesting party. A possible application is to give only general information by default and give selected information (phone numbers, e-mail		URL (without the need to run CGI scripts at that URL) There are also now additional features such as authenticated messaging (similar to e-mail, but from identity URL to identity URL, without the ability to spam)

TABLE A – VERIFICATION OF DATA				
Data held in database			**Yes / No**	**Correction / Completion**
		address) only to a set of configured LID-IDs.		
15.1	**Screenshot picture:**	http://lid.netmesh.org/		
15.1	**Flowchart:**	TBAL		
16.	**Cost**			
16.1	**Price:**	0	No	NetMesh InfoGrid LID is distributed under two licenses: open-source and commercial
16.2	**Comment to the Cost:**			The idea is a “tit for tat”: if a developer open-sources all of their code, InfoGrid LID is free and open-source, too; if not, it isn’t either.
17.	**Type & Class of IMS**			
17.1	**Type of IMS:**	Type 3: IMS for user-controlled context-dependent role and pseudonym management.	Addition	Also suitable for Type 1
17.2	**Class of IMS:**	Class 1: Pure IMS which main objective is to support or implement identity management functionality.	Addition	Class 1 is correct, but InfoGrid LID has many features not traditionally considered identity management (e.g. social networking)
17.3	**Functionality:**	decentralized SSO, Globally Unique Identifiers, "Smart Pointer", social networking functionality	Addition	Profile exchange, authenticated messaging, sessions, public key distribution, account management functionality, logging, access provisioning, filtering of incoming communication, single-sign-on
18.	**Suggestions:**			

6.5 Shibboleth feedback

We appreciate your interest in Shibboleth. I believe most or all of the information you are seeking is available on our website:

http://shibboleth.internet2.edu/

If you need more information, I would refer you to the folks at SWITCH, who are quite active and knowledgeable about Shibboleth:

http://www.switch.ch/aai/

http://www.switch.ch/aai/tech/

JISC is quite active and knowledgeable in this arena as well:

http://www.jisc.ac.uk/index.cfm?name=pub_shibboleth

http://www.jisc.ac.uk/index.cfm?name=programme_cminfrastructure

6.6 Spamgourmet feedback

Spamgourmet Identity Management System

Verification of data – Instructions

Please indicate with a Yes/No in the respective field of the following table the correctness / completeness of the data held in our database. If you find that the data is not correct and/or complete, please proceed with making the appropriate corrections / additions by appropriately filling in the next field ("Correction / Completion").

For a description / definition of each field, you can refer at Table B.

TABLE A – VERIFICATION OF DATA				
Data held in database			Yes / No	Correction / Completion
19.	**Evaluation of IMS**			
1	**Evaluator:**	Christian Krause	Yes	
1	**Organisation:**	ICCP	Yes	
1	**Date of evaluation:**	14-Oct-2005	Yes	
20.	**Identification of IMS**			
2	**Sources of information:**	http://www.spamgourmet.com/	Yes	
2	**Version:**		No	1.22
2	**Manufacturer:**	diverse	Yes	
2	**Nature:**	private	Yes	
2	**Country:**	n.a.	No	USA
2	**Regions:**	Global	Yes	
2	**Language:**	ENGLISH	No	Various (15 total for user interface)
2	**State:**	Available	Yes	
2	**Open / Closed:**	Open IMS: the identities work with	Yes	

TABLE A – VERIFICATION OF DATA				
Data held in database			**Yes / No**	**Correction / Completion**
		several systems or applications.		
21.	**Platform & Environment**			
2	**Requirements:**	Browser, E-Mail client	Yes	
2	**Number of users:**	>100.000 users. Server-software is OpenSource, but no installation-base apart from the developer's service is published.	Yes	(there are other installations, but not published)
2	**Standards:**	none	No	SMTP (but I may be misinterpreting this question – if it's referring to privacy standards, then yes, it's correct)
2	**Description of Server - Side components:**	software is written entirely in PERL	Yes	
2	**Description of methods:**	An account is created wherin the user's mail-address is being stored. After registration, users can generate one-time addresses connected to their account. Mails sent to this address are forwarded only for a specified period, e.g. four times.	No	Text is correct, but I would substitute the phrase "limited use" for the phrase "one-time"
2	**Descriptor of Client - Side components:**	Browser to register with the service, E-Mail client to receive one-time mail	No	Same comment as immediately above – substitute "limited use" for "one-time"
2	**Seals:**	No	Yes	
2	**Which seal:**		Yes	
2	**Third party:**	no	Yes	
2	**Which third party:**		Yes	
2	**Features:**	The service hides the original mail-address. Since the specific username appears in every generated one-time address, there is only pseudonymity given.	Yes	
2	**Screenshot picture:**	spamgourmet-screen.png	Yes	(will have to trust you on this one)
2	**Flowchart:**	none	Yes	
22.	**Cost**			

TABLE A – VERIFICATION OF DATA				
Data held in database			Yes/No	Correction / Completion
22.	**Price:**	0	Yes	
22.	**Comment to the Cost:**			
23.	**Type & Class of IMS**			
23.	**Type of IMS:**	Type 3: IMS for user-controlled context-dependent role and pseudonym management.	Yes	
23.	**Class of IMS:**	Class 2: Systems/applications with another core functionality.	Yes	
23.	**Functionality:**	Spamgourmet's main purpose is avoiding spam. Generating multiple addresses is used as an instrument.	Yes	
24.	**Suggestions:**	There are two ways spamgourmet can be operated: 1. Make up addresses like "someword.x.user@spamgourmet.com", where "someword" is a randomstring and x is the number of mails that shall be received. 2. The above structure can be combined with "watchwords". These are user-generated and stored in the service. Only mails to addresses containing one ore more watchwords are forwarded. This makes it harder for attackers to construct a valid address from scratch. The service allows to create arbitrary mail-addresses and thus avoid spam, although linkability of these created addresses is not averted due to identical unique strings (the username) in all generated addresses.	No	Text is correct, but there are other features, including the ability to send email as if it came from a disposable address