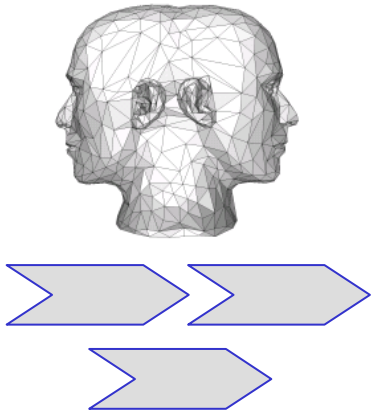
GenericIAM

generic processes for the
Identity- & Access Management



9th Meeting, 2008-02-08

at NIFIS e.V.,
Hanauer Landstraße 300, Frankfurt am Main

Version 0.3

agenda

- participants
  - confirmend
  - no participation
  - no answer
- housekeeping
- New members introduce themselves
  3 – 5 Minutes per Person
- 2007-10-12 meeting minutes & assignments
- Report from the WG Organisation
  work done during the last three months
  - guideline on membership
    who is to be counted as an (active) group member
  - List of votes
    guideline on membership
- Report from the WG Quality Assurance
  work performed during the last three months
- NIFIS-GenericIAM on the EIC 2008
- Members of the working groups
  each group determines a speaker (s) and his deputy (d)
- Additional topics
- NIFIS-GenericIAM-infrastructure
  we work and publish using the following sites ...
- NIFIS-members
  Who of those engaged in GenericIAM is a NIFIS-member?
- Links to NIFIS-GenericIAM
- ToDo‘s
  „Who will do what & until when?“
- Decisions
- Closing

confirmend participants

Name	participation	E-Mail-Adress	member status
Bernd Hohgräfe	Yes	bernd.hohgraefe@siemens.com	member
Henning Guder	Yes	Henning.Guder@sbi-ruhr.de	member
Holger Görz	Yes	Holger.Goerz@secu-sys.com	
Holger Weß	Yes	holger.wess@rwe.com	member
Horst Walther	Yes	horst.walther@gmail.com	Eigentümer
Jürgen Kühn	Yes	Juergen.Kuehn@trivadis.com	member
Marc A. Dierichsweiler	Yes	m.dierichsweiler@impulsit.de	member
Marko Vogel	Yes	mvogel@kpmg.com	member
Martina Hendricks	Yes	martina.hendricks@dekra.com	invited
Oliver Belikan	Yes	oliver.belikan@doubleslash.de	member
Roland Stahl	Yes	roland.stahl@henkel.com	member
Stephan Vogtland	Yes	svogtland@kpmg.com	invited
Thomas Felder	Yes	Thomas.Felder@secude-consulting.com	member
Vanessa Hennig (ImpulsIT)	Yes	v.hennig@impulsit.de	member
Volker Ludwig	Yes	VolkerL@InterXion.com	invited

no participation

Name	participation	E-Mail-Adress	member status
Andreas Netzer	No	netzer@ic-compas.de	member
Andreas Schmidt	No	Andreas.Schmid1@swisscom.com	invited
Angelika Steinacker	No	asteinac@csc.com	member
Ashokkumar Muthu	No	ashokpearl@gmail.com	member
Denis Royer	No	denis.royer@m-lehrstuhl.de	member
Edward Bertsch	No	bertsch@gmail.com	member
Erich Krahmer	No	erich.krahmer@rsd.rohde-schwarz.com	invited
Gerco Kanbier	No	gerco.kanbier@gmail.com	member
Hans-Jürgen Stritter	No	hjstt@edv-auditconsult.de	invited
Holger Nahrgang	No	Holger.Nahrgang@googlemail.com	member
Jan Schallaböck	No	Jan.Schallaboeck@gmail.com	member
Jens Petersen	No	Jens.Petersen@firstattribute.com	member
Maarten Stultjen	No	m.stultjens@bholdcompany.com	invited
Martin Kuppinger	No	mk@kuppingercole.de	member
Michael Lang	No	michael.lang@myrealbox.com	member
Michael Ohgami	No	michael.ohgami@gmail.com	member
Nicole Kleff	No	nk-consulting@t-online.de	invited
Peter Weierich	No	peterw@voelcker.com	member
Sargasso	No	thomas.moss@bell.ca	member
Steve Stewart	No	steve.f.stewart@gmail.com	member
Tino Kanngiesser (cgi)	No	tino.kanngiesser@cgi.com	member

no answer

1. Ads, adityabhushan@yahoo.com, member
2. **Arslan Broemme, broemme@consecur.de, member**
3. Barbara Lange, bl@blkst.de, member
4. Britta Hilt, Britta.Hilt@ids-scheer.com, invited
5. Christian Patrascu, christian.patrascu@oracle.com, member
6. Dörte Neundorf, Doerte.Neundorf@bmw.de, invited
7. EG, egnala@gmail.com, member
8. Erich Vogel, Erich.Vogel@computacenter.com, invited
9. Ernst Liniger, eliniger@ipg-ag.com, invited
10. Ernst Liniger, ernst.liniger@ipg-ag.com, member
11. Frank Jahn, Frank.Jahn@t-systems.com, member
12. Franz-Josef Noelke, franz-josef.noelke@siemens.com, member
13. Friedel Vogel, fvogel@covisint.com, invited
14. Gerd Rossa, Gerd.Rossa@secu-sys.com, member
15. Gerd Rossa, rossagerdrossa@googlemail.com, member
16. Gernot Achtermann, Gernot.Achtermann@firstattribute.com, invited
17. Giovanni Baruzzi, giovanni.baruzzi@syntlogo.de, member
18. Hans Nolan, hanns.nolan@siemens.com, member
19. Hans Wieser, hans.wieser@sun.com, invited
20. Hans-Jörg Kremer, hj.kremer@peak-solution.de, invited

1. Heike Jürgensen, heike.juergensen@oracle.com, member
2. Hermann Rueb, Hermann.Rueb@it-advisory.com, invited
3. Hübner Manfred, Manfred_Huebner@WestLB.de, invited
4. Ian Dobson, i.dobson@opengroup.org, invited
5. Ingrid Brunner, ingrid.brunner@post.at, invited
6. Isabell Conrad, isabell.conrad@ssw-muc.de, invited
7. Jacobshagen, Mareike, Mareike.Jacobshagen@de.compuware.com, invited
8. James Kirk, Agile HR, james.kirk@agilehr.co.uk, member
9. Jan Schallaböck, LD103@datenschutzzentrum.de, invited
10. Joe Ponder, joe.ponder@gmail.com, member
11. Jörg Resch, jr@kuppingercole.de, member
12. Jörg van gen Hassend, jvghassend@googlemail.com, member
13. Jörn Fischbach, joern.fischbach@togal.de, invited
14. Jürgen Skirde (DSK), juergen.skirde@dsk.de, member
15. Kirsten Bönisch, Kirsten.Boenisch@bmw.de, member
16. Kristof Kloeckner, kristof@us.ibm.com, invited
17. Lars Hansen, Lars.Hansen@secu-sys.com, invited
18. Maarten Stultjen, m.stultjens@bholdcompany.com, invited
19. Marco Kluge (StadtWolfsburg), Marco.Kluge@stadt.wolfsburg.de, invited
20. Marcus Schmid, Marcus.Schmid@de.ibm.com, member

no answer

1. Maria Specht, Maria.Specht@wwk.de, invited
2. Markus Kunkel, Markus.Kunkel@ibsolution.de, member
3. Maruthi, maruthigsr@gmail.com, member
4. Matthias Hain, M.Hain@DeutschePost.de, invited
5. Matthias Neher, Matthias.neher@web.de, member
6. Matthias Schabl, matthias.schabl@gmail.com, member
7. Matthias Schabl, matthias@schabl.com, member
8. Michael Boley, michael.boley@gmail.com, member
9. Michael Buerger, michael.buerger@oracle.com, invited
10. Michael Ohgami, michael.ohgami@gmail.com, member
11. Murat Firat, Murat.Firat@axa.de, invited
12. Murat Firat, murat.firat@gmx.net, member
13. Netzer Andreas, netzer@ic-compas.de, member
14. Nicole Chemnitz, mail@nicole-chemnitz.de, member
15. Nicole Kleff, email@nkleff.de, member
16. Nientimp Axel, Axel.Nientimp@karstadt.de, invited
17. Norbert Boß, bossno01@googlemail.com, member
18. Norbert Zessel, Norbert.Zessel@bmw.de, invited
19. Oliver Belikan, oliver.belikan@doubleslash.de, member
20. Patrick Rempel, Patrick.Rempel@oxfordcomputergroup.com, member
1. Peter Knapp, PeterK@InterXion.com, invited
2. Peter Weierich, peter@weierich.de, member
3. Rainer Hasenstein, rainer.hasenstein@thoranet.de, member
4. Rainer Knorpp, Rainer.Knorpp@danet.de, invited
5. Raj, nagarajan.mv@gmail.com, member
6. Robert Hannemann, robert.hannemann@freenet.de, invited
7. Roland Awischus, roland.awischus@betasystems.com, member
8. Roland Blomer, roland@blomer.de, invited
9. Ron Rymon, rrymon@eurekify.com, member
10. Ruediger Weyrauch, Ruediger.Weyrauch@Sun.COM, invited
11. Sabine Burba, Sabine.Burba@it-advisory.com, invited
12. Sabine Winklmeier, winklmeier@gmail.com, member
13. Sabrina Sommer (Linde), sabrina.sommer@linde-mh.de, member
14. Sagiv Tamary-Amir, sagivt@gmail.com, member
15. Sebastian Weber, sebastian.weber@daimlerchrysler.com, member
16. seshu, rajesh.seshu@gmail.com, member
17. Stefan Sulistyo, stefan.sulistyo@accenture.com, member
18. Yash Vartak, yashvartak@gmail.com, member
19. Stefanie Winklmeier, s.winklmeier@mmkh.de, member
20. Stephan Holler, shfirma@gmx.net, member

no answer

1. Stephan Holler, stephan.holler@eds.com, member
2. Sujit, sujit2c@gmail.com, member
3. Suresh, igsureshkumar@gmail.com, member
4. Suresh Botta, suresh.botta@gmail.com, member
5. Thomas Schmidt, Thomas.Schmidt@Thoranet.com, invited
6. Thorsten Schroeter, Thorsten.Schroeter@trivadis.com, invited
7. Tim Cole, tc@kuppingercole.de, invited
8. Tino Kanngiesser (cgi), tino.kanngiesser@cgi.com, member
9. Tobias Mateika, Tobias.Mateika@rwe.com, member
10. Vipin Jain, Vipin_Jain@satyam.com, member
11. Vipin Jain, vipin17in@yahoo.com, member
12. Werner Schönenkorb, w.schoenenkorb@identity-management-consulting.de, invited

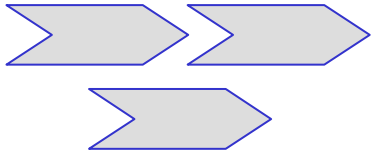
housekeeping

- agenda
- breaks,
- smoking,
- Mobiles,
- minutes,
- Presented contributions, results,
- Workshop nature,
- ...

The (new) members introduce themselves
3 – 5 Minutes per Person

- Who I am?
- Where I come from?
- What exposure I have to IAM?
- Why I came here?
- What I may contribute?

Organisation Group – Quarterly Report



Version 0.4

2008-02-07, Dr. Horst Walther

Report from the WG Organisation / next steps
(Horst Walther)

- phone call and mail-invitation to Dr. Martin Kuhlmann / Omada
- Martin Kuhlmann, Omada joined
- reworking 1st paper on top down approach (Arslan Brömme, Andreas Netzer)
- Updating GenericIAM-Webpage
- polling for a volunteer, serving as a speaker for the presentation group
- Friedel Vogel left covisint
- Deputy function in validation open
- Covisint inactive now

- Further contacts to international standardisation bodies had been put on hold due to **lack of substantial results**.

guideline on membership
who is to be counted as an (active) group member

1. Everybody who shows up at our quarterly meetings and / or **actively contributes** to our mission will be considered as a GenericIAM-member.
2. If he does not meet these criteria **for one year** we don't consider him / her as a GenericIAM-member any longer.
3. Not-Members may stay registered in the GenericIAM Google group in order to receive relevant information further on. They should also maintain their NIFIS-membership. We consider them as "**friends of GenericIAM**".
4. Whenever anyone out of the group "friends of GenericIAM" **resumes his volunteering activities** or starts them for the first time, we will count him / her as a member again.
5. Members will be listed on our **NIFIS-Generic-IAM-Webpage** with their company and full name and logo.

➔ **to take into account the volatile environment of our members and friends, so that they can flexibly invest more or less effort into our joint initiative.**

List of votes
guideline on membership

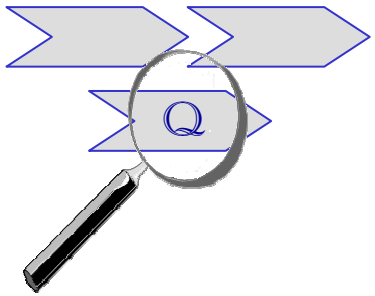
votes in total

20	yes
1	yahbut
0	no

accepted

No.	date	Name	vote
1	03.12.2007	Jens Petersen	yes
2	03.12.2007	Marcus Schmid	yes
3	03.12.2007	Nicole Kleff	yes
4	04.12.2007	Andreas Netzer	yes
5	04.12.2007	Angelika Steinacker	yes
6	04.12.2007	Bernd Hohgräfe	yes
7	04.12.2007	Holger Nahrgang	yes
8	04.12.2007	Marc Dierichsweiler	yes
9	04.12.2007	Peter Weierich	yes
10	04.12.2007	Roland Awischus	yes
11	04.12.2007	Thomas Felder	yes
12	05.12.2007	Jürgen Kühn	yes
13	05.12.2007	Oliver Belikan	yes
14	05.12.2007	Thomas Felder	yes
15	05.12.2007	Yash Vartak	yahbut (issue solved)
16	06.12.2007	Denis Royer	yes
17	06.12.2007	Marko Vogel	yes
18	07.12.2007	Vanessa Henning	yes
19	10.12.2007	Holger Görz	yes
20	11.12.2007	Norbert Boss	yes
21	12.12.2007	Martina Hendricks	yes

Validation Group – Quarterly Report



Approved by
Arslan Brömme, <Arslan.broemme@aviomatik.de>
Jürgen Kühn (Trivadis), <Juergen.Kuehn@trivadis.com>
Marko Vogel (KPMG), <mvogel@kpmg.com>
Martin Kuppinger (KCP), <mk@kuppingercole.de

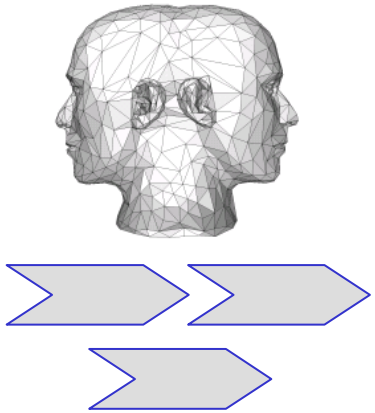
Version 1.0

2008-01-30, Dr. Angelika Steinacker

Quality Assurance

Work performed during the last three months

- Paper on
  „Modeling the ‘Generic Identity and Access Management approve-request Process’ V0.93“
  - Review – finished
  - Review – sent to modeling group
  - Review Meeting / Conference Call – tbd



GenericIAM

generic processes for the
Identity- & Access Management

Modelling Workshop, 2007-12-04

at Impuls IT Beratungsgesellschaft mbH

Wilhelm-Theodor-Römheld-Str. 14 , 55130 Mainz

2008-01-06, Andreas Netzer

Version 1.0

Agenda

- welcome - new members introduction
- Introduction actual status of modelling group
  - Important, because mostly new members were on site
- Presentation of first generic process (publishing)
- Discussion about next ToDos / Steps

Actual status

- Explanation what we have made up to now
- Showing all the materials we collected till now and short explanation of the

Results discussion “1st generic process”

- The described process is complete and consistent
- No shorter and more compact process description is known to anybody
- A detailed explanation “how the handle the recursion“ was necessary
  - → Probably this should be described deeper at a later stage
- Petri-Net needs explanation

- → With the description of process in two different ways we are on the right track

Next Steps / ToDo's

- Verify and complete the nomenclature
  - Take the wiki-content and put it into a word-document
  - Round-Trip of the doc, so that each member can add / change
  - After finishing discuss the new publishing
- Search a second additional process an define it as the first one
- Define the IAM-landscape (inspired by the BMW-modell) (next slide)
- Minor adjustments in the graphic of the petri-net modell to make some things easier to understand
- For a better support of the member collaboration impuls IT suggest to use a online platform for project working (www.projectplace.de) (better parallel working possible.
  - They offered to sponsor that.

IAM landscape

- Brainstroming result – Input for the next steps for defining this
  - Identitätsmanagement
  - Organisationsmanagement (Strukturmanagement)
    - Projekte / Standorte / etc
  - Rollenmanagement (Services and Roles Definition Process)
  - Bereitstellungsmanagement (Service Delivery Process and Assignment)

NIFIS-GenericIAM on the EIC 2008

- NIFIS-GenericIAM booth on the **European Identity Conference** (EIC) 2008
- Who will attend?
  - **Oliver Belikan**: Für den Donnerstag den 24.04.2008 bin ich sehr gerne ganztätig auf dem Stand und vermarkte GenericIAM so gut es geht. Auch helfe ich gerne bei Abbau und Aufräumen.
  - **Angelika Steinacker**: ich bin gerne bereit, ein paar Stunden "Dienst" zu schieben. planen sie mich ruhig ein.
  - **Thomas Felder**: ich würde an einem Tag ein paar Stunden übernehmen.
  - **Michael Lang**: Ja, gerne, planen Sie mich ein.
  - Who else?
- **NIFIS GenericIAM Meeting,** 22.04.2008, 09:00-11:00 and 11:30-13:00, **Moderator: Dr. Horst Walther**, Kuppinger Cole + Partner
- Yearly NIFIS-GenericIAM-meeting as a EIC pre-conference?
- Booking Code for NIFIS-Members (not booth attendance): 20% reduction using the Booking code **nifis208**

http://www.id-conf.com/eic2008

Members of the working groups
each group determines a speaker (s) and his deputy (d)

Modelling
- Roland Awischus
- Giovanni Baruzzi
- Oliver Belikan
- Norbert Boss
- Marc Dierichsweiler
- Thomas Felder
- Holger Görz
- Henning Guder
- Vanessa Henning
- Matthias Neher
- Andreas Netzer (S)
- Peter Weierich
- Roland Stahl
- no (D)

Validation
- Jürgen Kühn
- Martin Kuppinger (D)
- Gerd Rossa
- Angelika Steinacker (S)
- Marko Vogel

Presentation
- Martin Kuppinger
- Denis Royer (D)
- Horst Walther
- Peter Weierich (S)

Organisation
- Horst Walther (S)
- no (D)

Additional topics

- Modelling progress
- Using the ARIS-Licences?
- election of speakers of the working Group “Modelling”
  - For 2008: Andreas Netzer resigns due to work overload
- Links to NIFIS-GenericIAM?
- IAM survey of the KPMG (in German). Invitation and Link to the questionaire: http://link.nifis.de/archive.php?p=111907095_86504
- NIFIS-Membership?
- Enrich your profile at http://groups.google.com/group/GenericIAM/
- We will put more emphasis on the virtual interaction in our work for GenericIAM.
  - We need more personal and professional member information about in the profile.
  - Please fill in your full name and professional picture, Location, Title, Industry, Email address, Website and / or Blog, Quote and About me in your profile properly.
  - This additional information will help us to work more confidently in the virtual space.
  - It makes clear, that there are real humans acting and contributing behind the electronic representations.
- Next meeting in 2008 Q2 – 2009 – or never? How to proceed efficiently?

NIFIS-GenericIAM-infrastructure
we work and publish using the following sites ...

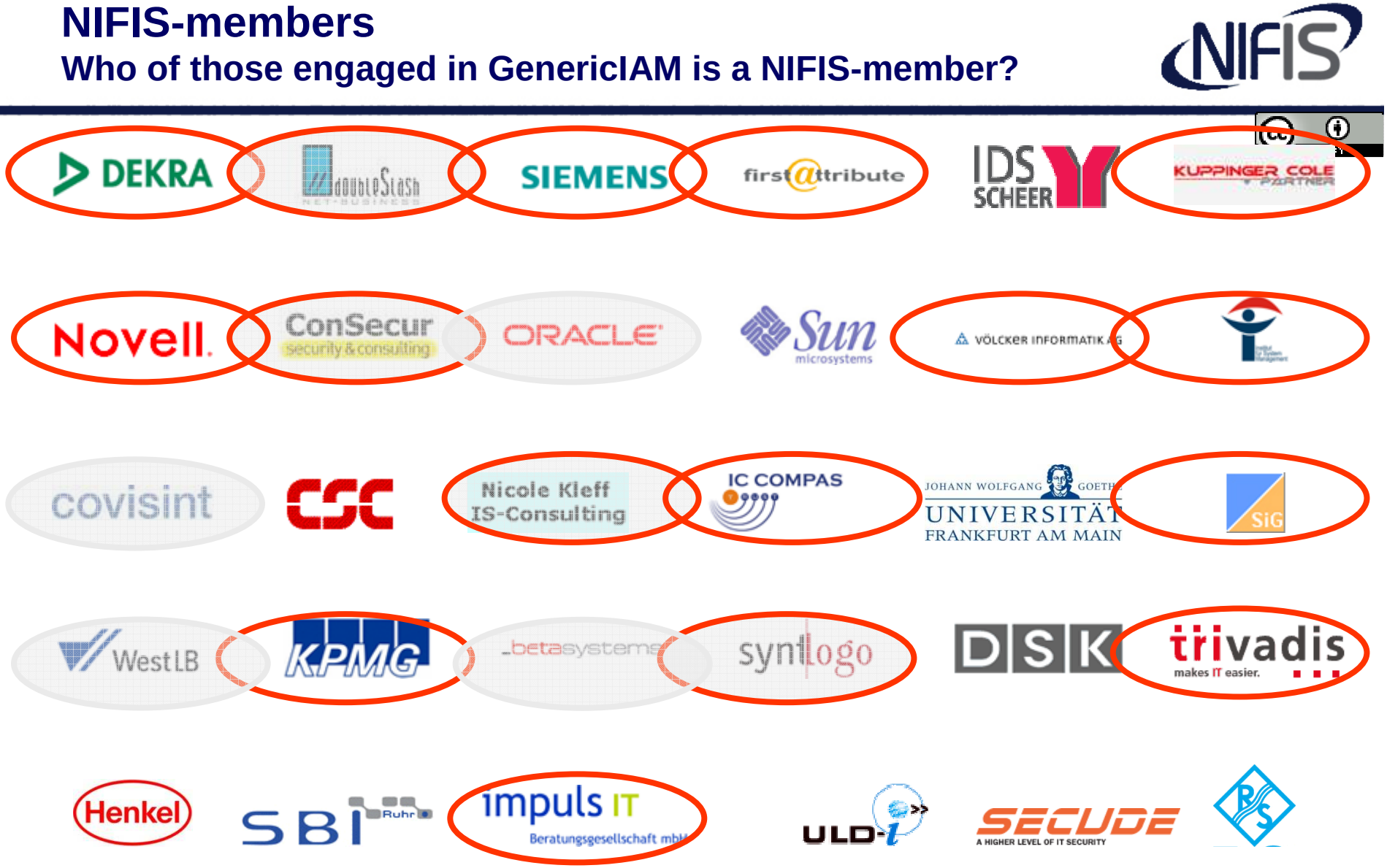
- The GenericIAM-Homepage: http://www.GenericIAM.org/
- The NIFIS-Homepage: http://www.nifis.org/
- The GenricIAM-Blog: http://blog.genericiam.org/
- The GenericIAM-Calendar
- This Discussion group: http://groups.google.de/group/GenericIAM/

and …

- The IAM-Wiki: http://www.iam-wiki.org/?

NIFIS-members

Who of those engaged in GenericIAM is a NIFIS-member?



Links to GenericIAM

- DoubleSlash http://www.doubleslash.de/de/Unternehmen/News/genericIAM_initiative.html
- iC Compas: http://www.ic-compas.de/ueber-uns/memberschaften/index.html
- Nicole Kleff http://www.nkleff.de/Aktuelles.htm
- Peak Solution http://www.peak-solution.de/index.php?content=content/statisch/index&navlink=60&gewaehlterBereich=59&session=&langID=1
- Gesellschaft für Prozessmanagement http://www.prozesse.at/gp/kooperationen/netzwerkpartner.html
- SiG http://www.si-g.com/HTML/archive_de.htm?lang=de

Closing

- Feedback
  - How did you enjoy the Meeting?
    - contents - schedule – Location – Moderation - Participation
  - Are we still on the right way?
  - Are there modifications necessary to our direction?
  - Do you believe, that we will be successful in the end?
  - Which changes should we apply to our approach?

Questions - comments – suggestions?

Lunch break

Caution Appendix

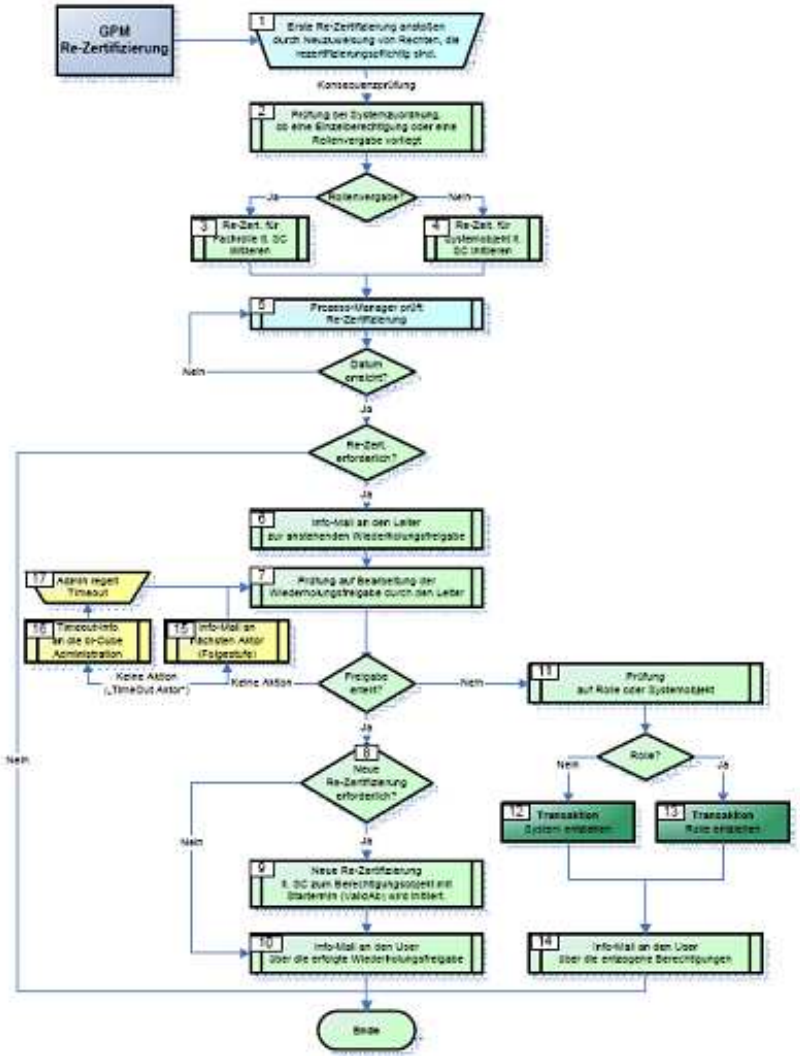
Here the notorious back-up-slides follow ...

agenda

- GPM Re-Zertifizierung
  Beitrag des ism zu den generischen IAM-Prozessen
- GPM Re-Zertifizierung
  Erläuterungen
- Antrag auf Zuteilung einer Rolle
  Beitrag des ism zu den generischen IAM-Prozessen
- Antrag auf Zuteilung einer Rolle
  Erläuterungen
- Links to GenericIAM
- NIFIS – how to get there

GPM Re-Zertifizierung

Beitrag des ism zu den generischen IAM-Prozessen



1 Ziel

Abhängig von der Security-Classification (SC, nach X509) der beim User zugeordneter Rollen und Einzelberechtigungen wird in regelmäßigen Abständen eine Wiederholungsfreigabe (Re-Zertifizierung) eingefordert. Diese Prozesse werden automatisch initiiert

Mit der Re-Zertifizierung werden folgende Funktionen realisiert:

1. Berechtigungsobjekte (Rollen, Systeme), die in bi-Cube einer SC mit Re-Zertifizierungszeitraum unterworfen sind, werden in regelmäßigen Abständen einer Wiederholungsfreigabe durch den Leiter des Users unterworfen.
2. Die SC regelt den Re-Zertifizierungsrhythmus, wenn zur SC ein Zeitraum > 0 (null Monate) eingestellt ist. Eine SC gilt dann als ***rezertifizierungspflichtig***. In der Standard-Konfiguration sind folgende Re-Zertifizierungszeiträume definiert:
   - SC = 5 (top secret) → 6 Monate
   - SC = 4 (secret) → 6 Monate
   - SC = 3 (confidential) → 12 Monate

   Die vordefinierten Zeiträume können nach Einsatzfall geändert werden. Für die SC 0 bis 2 sind im Standard keine Re-Zertifizierungszeiträume definiert, können aber bei Bedarf jederzeit eingerichtet werden.
3. Existieren Systemobjekte mit rezertifizierungspflichtiger SC in einer Rolle, wird nur die Wiederholungsfreigabe lt. SC der Rolle eingefordert, die Re-Zertifizierung des Systems ist dabei inkludiert.
4. Stimmt der Leiter der Re-Zertifizierung zu, wird die nächste Freigabe lt. SC mit entsprechendem Startzeitpunkt für das Berechtigungsobjekt in bi-Cube automatisch initiiert.
5. Lehnt der Leiter die Re-Zertifizierung einer Rolle oder eines direkt zugewiesenen Systems (Einzelberechtigung) ab, werden die Rolle bzw. das Systemobjekt automatisch durch bi-Cube entzogen bzw. deaktiviert.
6. Zum Abschluss des Prozesses erhält der betroffene User eine Information zum Prozess-Verlauf und Ergebnis.

Änderungen zu den Einstellungen der Re-Zertifizierungsrhythmen der einzelnen SC werden wie folgt wirksam:

- Wird für eine SC nachträglich der Zeitraum verlängert oder verkürzt, wirkt sich dies nur für Neuzuweisungen und die automatische Initiierung von Re-Zertifizierungen aus. Bereits initiierte, aber noch nicht gestartete Prozesse laufen zum berechneten Starttermin an.
- Wird für eine SC der Zeitraum nachträglich auf 0 (null) gesetzt (also keine Re-Zertifizierung erforderlich), werden noch nicht gestarteten Prozesse nicht mehr ausgeführt. Bereits laufende Prozesse müssen über den Prozess-Manager im IPM Web-Portal gecancelt werden.
- Wird ein Berechtigungsobjekt, das bereits in bi-Cube verwendet wird (Zuweisungen bei den Usern bereits vorhanden), erstmalig einer SC mit Re-Zertifizierung unterworfen, können die erforderlichen Wiederholungsfreigaben über eine Mengenoperation mit V 7.X.X initiiert werden (verfügbar in einem späteren Release in V7).

2 Modellierungsrichtlinien

Folgende Richtlinien für die Modellierung der Re-Zertifizierung sind zu beachten:

- Die Re-Zertifizierungszeiträume werden kleiner, je höher die ausgewählte SC!
- Die SC im Rollenmodell erfolgt für die Fachrollen.
- Die SC zu den Berechtigungsobjekten (Rolle, System) muss so gesetzt werden, das eine Rolle immer mindestens die gleiche SC aufweist wie das am höchsten eingestufte Systemobjekt in der (Fach-) Rolle. Das bedeutet gleichzeitig, dass eine Rolle immer einer SC unterworfen werden muss, sobald ein Systemobjekt mit rezertifizierungspflichtiger SC zur Rolle gehört. Diese Regel gilt natürlich auch für SC in Systemobjekt-Hierarchien, die in Rollen verwendet werden.
- SC in Systemobjekthierarchien können derart gesetzt werden, das ein untergeordnetes Objekt eine höhere SC besitzt als das Wurzelobjekt (z.B. eine Software innerhalb win, die höher eingestuft ist als Windows selbst).

GPM Re-Zertifizierung
Erläuterungen

1 **Erste Re-Zertifizierung anstoßen:**
Bei Zuweisung rezertifizierungspflichtiger Berechtigungsobjekte (Rollen, Einzelberechtigungen) wird über die Konsequenzprüfung die Re-Zertifizierungs-Schleife für das Objekt angestoßen, siehe Punkt 2.

2 **Prüfung auf Rolle oder Einzelberechtigung:**
Die Konsequenz prüft, ob es sich bei Neuzuweisung eines Systems mit Re-Zertifizierungspflicht um eine Einzelberechtigung oder eine Rollenzuweisung handelt. Je nach Prüfergebnis wird in Punkt 3 oder 4 verzweigt.
Hinweis: Punkt 3 muss nur durchlaufen werden, wenn für die betroffene Rolle noch keine Re-Zertifizierung beim User initiiert ist!

3 **Re-Zert. für Fachrolle:**
Die Prüfung in 2 hat ergeben, das die Systemzuweisung über eine Rolle erfolgt ist. Die Re-Zertifizierung wird ausgehend von der SC der Rolle initiiert, nicht auf Grund der SC des Systems.

4 **Re-Zert. für Einzelberechtigung (Systemobjekt):**
Die Prüfung in 2 hat ergeben, das die Systemzuweisung als Einzelberechtigung (ohne Rolle) erfolgt ist. Die Re-Zertifizierung wird ausgehend von der SC des Systems initiiert.

5 **Re-Zertifizierung starten:**
Der Prozess-Manager startet den eigentlichen Prozess der Re-Zertifizierung genau dann, wenn das Re-Zertifizierungsdatum (ValidAb der Message) erreicht ist. Dabei wird geprüft, ob die SC zum Berechtigungsobjekt noch rezertifizierungspflichitg ist.
D.h. wurde nachträglich der Re-Zertifizierungszeitraum im Customizing für die SC auf 0 (null Monate) gesetzt, wird der Prozess ohne weitere Aktion beendet. Ansonsten stößt der Prozess-Manager die Info-Aktion zur Bearbeitung an, siehe Punkt 6.

6 **Info-Mail an den Leiter:**
Der Aktor (z.B. der Leiter) zur Genehmigung der Wiederholungsfreigabe erhält eine Info per Email, das eine Re-Zertifizierung zur Bearbeitung vorliegt verbunden mit der Aufforderung, diesen Antrag zu bearbeiten.

7 **Prüfung auf Bearbeitung der Re-Zertifizierung:**
Der Aktor (z.B. der Leiter) meldet sich im IPM Web-Portal an und bearbeitet den Antrag zur Wiederholungsfreigabe. Die Überwachung durch den Prozess-Manager kann folgende Ergebnisse erbringen:
Wiederholungsfreigabe bestätigt: Der Leiter hat die Wiederholungsfreigabe für das Berechtigungsobjekt im IPM Web-Portal bestätigt. Der Prozess-Manager leitet weiter zur Initiierung der Folgefreigabe (nächste Re-Zertifizierung des Berechtigungsobjekts), siehe Punkt 8.
Wiederholungsfreigabe abgelehnt: Der Leiter hat die Freigabe abgelehnt. Der Prozess-Manager leitet weiter zum Entzug der Berechtigungen, siehe Punkt 11.
Keine manuelle Aktion: Die Bearbeitung des Auftrags durch den Aktor erfolgte nicht im dafür vorgesehenen Zeitraum. Der Prozess-Manager leitet weiter zur Erinnerung, siehe Punkt 15.

8 **Neue Re-Zertifizierung erforderlich?**
Für das Berechtigungsobjekt wird auf Grundlage der SC geprüft, ob eine erneute Re-Zertifizierung initiiert werden muss:
Ja: Die beim Objekt (Rolle, System) eingestellte SC ist immer noch rezertifizierungspflichtig. Der Prozess-Manager leitet weiter zur Initiierung der Re-Zertifizierung, siehe Punkt 9.
Nein: Lt. SC ist das Berechtigungsobjekt nicht (mehr) rezeritfizierungspflichtig. Der Prozess-Manager leitet weiter zur Abschluss-Info, siehe Punkt 10.

9 **Neue Re-Zertifizierung lt. SC initiieren:**
Nach erfolgter Re-Zertifizierung wird die nächste Wiederholungsfreigabe automatisch initiiert, das auf Grundlage der aktuellen Einstellung für den Re-Zertifizierungszeitraum für die SC am Berechtigungsobjekt. Ist zwischenzeitlich die Definition für die SC auf 0 (null Monate) gesetzt worden, wird keine neue Re-Zertifizierung für das Berechtigungsobjekt (Rolle, System) initiiert. Danach leitet der Prozess-Manager weiter zur Abschluss-Info für die Re-Zertifizierung, siehe Punkt 10.

10 **Info-Mail an den User über Wiederholungsfreigabe:**
Zum Abschluss der erfolgten Re-Zertifizierung wird der betroffene User per Mail über das Ergebnis informiert.

11 **Prüfung auf Rolle oder Systemobjekt:**
Nach Ablehnung der Wiederholungsfreigabe wird geprüft, ob es sich bei dem Berechtigungsobjekt um eine Rolle handelt.
Ja: Das Berechtigungsobjekt ist eine Rolle, es wird weitergeleitet zum Sub-Prozess *Rolle entziehen*, siehe Punkt 13.
Nein: Bei dem Berechtigungsobjekt handelt es sich um eine Einzelberechtigung (Systemobjekt), es wird weitergeleitet zum Sub-Prozess *System entziehen*, siehe Punkt 12.

12 **Transaktion System entziehen (siehe auch Beschreibung der Transaktionen):**
Das zum Entzug vorgesehene System und alle dazu gehörenden Berechtigungen werden dem User entzogen.
Handelt es sich um ein Zugangssystem, dann wird das Zugangssystem gesperrt und je nach Customizing-Einstellung zum Systemobjekt nach einer Nachlaufzeit gelöscht.
Die Transaktionen werden vom Transaktionsmonitor überwacht und Fehlermeldungen aus den Schnittstellen (Connectoren) an die bi-Cube Administration gemeldet. Nach erfolgreichem Abschluss der Transaktionen wird intern zur nächsten Aktion weitergeleitet (siehe Punk 14).

13 **Transaktion Rolle entziehen (siehe auch Beschreibung der Transaktionen):**
Die zum Entzug vorgesehene Rolle und alle dazu gehörenden Berechtigungen werden unter Berücksichtigung der Rollenkonfliktauflösung entzogen.
Befindet sich in der Rolle ein Zugangssystem, das durch keine andere Rolle mehr beim User zugewiesen ist, dann wird das Zugangssystem gesperrt und je nach Customizing-Einstellung zum Systemobjekt nach einer Nachlaufzeit gelöscht.
Die Transaktionen werden vom Transaktionsmonitor überwacht und Fehlermeldungen aus den Schnittstellen (Connectoren) an die bi-Cube Administration gemeldet. Nach erfolgreichem Abschluss der Transaktionen wird intern zur nächsten Aktion weitergeleitet (siehe Punkt 14)

14 **Info-Mail an der User über Berechtigungsentzug:**
Zum Abschluss der nicht bestätigten Re-Zertifizierung wird der betroffene User per Mail über das Ergebnis und den Entzug der Berechtigungen informiert.

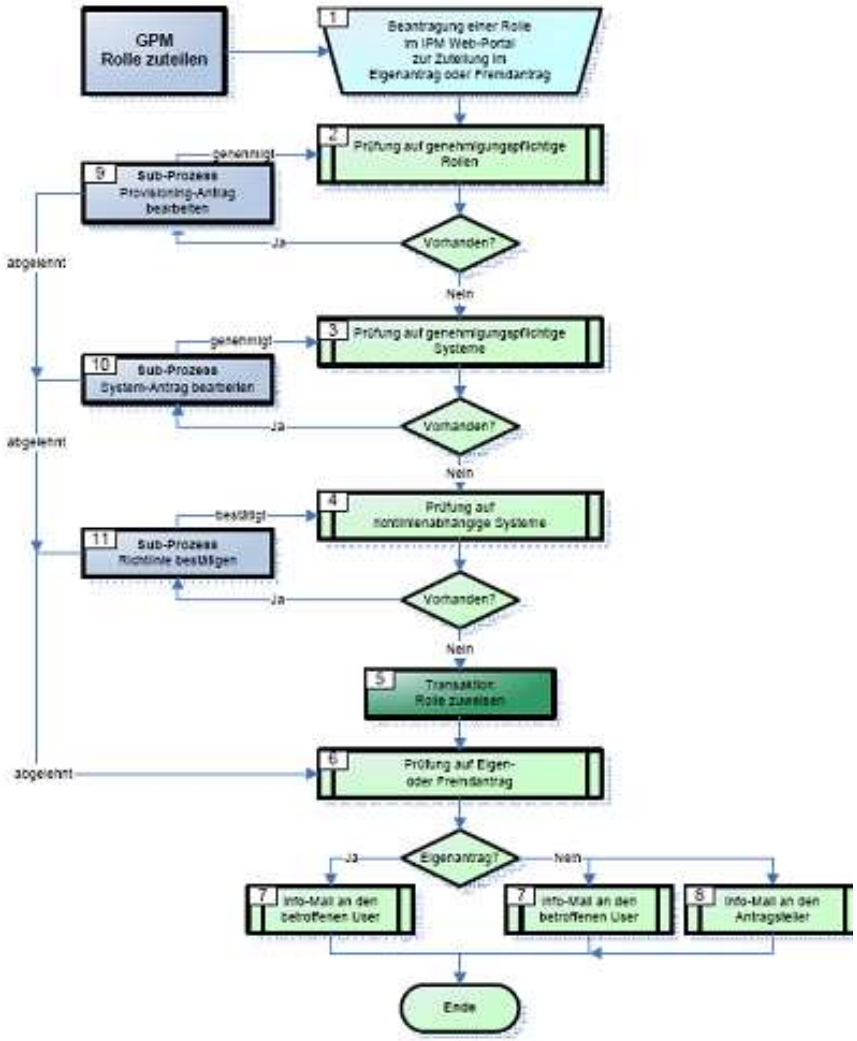
15 **Keine manuelle Aktion:**
Die Bearbeitung des Antrags durch den Aktor erfolgte nicht im dafür vorgesehenen Zeitraum. Es wird eine **Info-Mail** an die Stellvertretung des Aktors verschickt (nächste Stufe zur gleichen Aktion) verschickt, damit die die Bearbeitung des Auftrags erfolgt.

16 **Timeout-Info:**
Für die Bearbeitung des Antrags ist das Timeout eingetreten, d.h. es erfolgte keine manuelle Bearbeitung durch einen Aktor im Timeout Zeitfenster. Eine Timeout-Info wird per Email an die bi-Cube Administration verschickt. Diese Timeout-Info kann auch an eine andere Adressatengruppe verschickt werden, einzustellen in der Aktion im Prozess-Modell.

17 **Admin regelt Timeout:**
Bei Timeout-Info muss die bi-Cube Administration eingreifen und z.B. die zuständigen Aktoren auffordern, Ihren Job zu erledigen.

Antrag auf Zuteilung einer Rolle

Beitrag des ism zu den generischen IAM-Prozessen



1 Ziel

Beim Rollenantrag werden folgende Funktionen realisiert:

1. Im Antragsverfahren (bi-Cube Web-Portal) kann ein User für sich selbst (Eigenantrag) oder eine berechtigte Person (z.B. der Leiter) für andere (Fremdantrag) Anträge auf Zuteilung einer neuen Rolle stellen. Dabei sorgt die Attributindizierung der Fachrollen dafür, das jeder User nur die Rollen beantragen kann, die für ihn vorgesehen sind bzw. jeder Leiter nur die Rollen aus einem Pool beantragen kann, die für alle seine Mitarbeiter vorgesehen sind.
2. Sollte es im Mitarbeitereintritt zu Fehlern bei der automatischen Zuteilung von (Basis-) Rollen gekommen sein (diese wurden nicht zugeordnet), können die Rollen im Nachgang manuell beantragt werden.
3. Wenn in einer Rolle ein genehmigungspflichtiges System abgelehnt wird, dann werden die Rolle und damit alle zur Rolle gehörenden Systeme nicht zugeordnet.
4. Der User bestätigt vor der Zuweisung richtlinienabhängige Systeme in der Rolle. Lehnt er eine Richtlinie ab, dann werden die betroffene Rolle und damit alle zur Rolle gehörenden Systeme nicht zugeordnet.

Um den Rollenantrag als einen Prozess zu betrachten, werden alle beantragten Rollen intern verwaltet und die Zuordnungen werden komplett kontrolliert. Der Rollenantrag ist erst dann abgeschlossen, wenn alle beantragten Rollen zugeordnet sind. Aus dieser Liste fallen die nicht genehmigten Rollen heraus.

Zum Ende des Prozesses erhält der Antragsteller eine Aufstellung per Email:

- Rolle xy zugeordnet – Timestamp
- Rolle ab durch <Leiter> abgelehnt – Timestamp
- Rolle…

Weiterhin in der Info-Mail enthalten sind die Anmeldenamen (Accounts) für neu zugeordnete Systeme sowie die Erstanmeldepasswörter.

2 Modellierungsrichtlinien

Die Modellierung im Rollenmodell sollte so erfolgen, dass die sog. Zugangssysteme (LAN, Host) und das Mailsystem ohne Freigabe zugeordnet werden können und im manuellen Rollenantrag und damit in diesem GPM nicht betroffen sind. Sie sollten in einer so genannten Basisrolle enthalten sein, die unabhängig von anderen Rollen zugeordnet wird. Damit wird gesichert, dass zusätzliche Berechtigungen (z.B. Filespace im AD) in einer Systemrolle unter einer Fachrolle bereits einen entsprechenden Account vorfinden.

Systeme, die sogenannte technische Attribute beinhalten, die erst bei Antragstellung mit Werten befüllt werden können, sind als Zwang zu vereinbaren. Benötigt das System zusätzliche Userinformationen (Werte aus Userattributen), die für die Verwaltung der Userdaten nicht als Zwang definiert sind, sind diese Userattribute auf entsprechende Systemattribute zu referenzieren und die Systemattribute als Zwang zu vereinbaren. Damit wird bei Antragstellung letztendlich die Befüllung dieser Userattribute durch den Antragsteller sichergestellt.

Soll im Unternehmen ein gewisser Pool von Rollen uneingeschränkt für alle Teilnehmer am Antragsverfahren verfügbar sein (z.B. nicht lizenzpflichtige Grafik-Tools), dann werden diese Rollen im Rollenmodell unter einem Rollencontainer (Organisationsrolle) abgelegt. Diese Organisationsrolle wird im Customizing zum Antragverfahren als Container *Allgemein verfügbare Rollen* eingestellt und so kann sich jeder Teilnehmer aus diesem Pool bedienen.

Antrag auf Zuteilung einer Rolle
Erläuterungen

1 **Rollenantrag im Web-Portal stellen:**
Der Antrag kann durch den User selbst oder eine berechtigte Person (z.B. den Leiter) für den betroffenen User gestellt werden. Die Prüfung und Befüllung der Userattribute und der technischen Attribute werden bei Antragstellung durchgeführt. Dabei sind die zu befüllenden Userattribute an dieser Stelle Systemzwangsattribute, die auf Userattribute referenziert sind und damit bei Antragstellung durch den Antragsteller ausgefüllt werden müssen.

2 **Prüfung auf genehmigungspflichtige Rollen:**
Ja: Bei positivem Prüfergebnis wird in den Subprozess *Provisioning-Antrag bearbeiten* verzweigt (siehe Punkt 9)
Nein: Sind keine genehmigungspflichtigen Rollen im Antrag vorhanden bzw. ist die Genehmigung erteilt, wird intern zur nächsten Aktion weitergeleitet (siehe Punkt 3).

3 **Prüfung auf genehmigungspflichtige Systeme:**
Ja: Bei positivem Prüfergebnis wird in den Subprozess *Systemantrag bearbeiten* verzweigt (siehe Punkt 10)
Nein: Sind keine genehmigungspflichtigen Systeme vorhanden bzw. die Genehmigungen erteilt, wird intern zur nächsten Aktion weitergeleitet (siehe Punkt 4).

4 **Prüfung auf richtlinienabhängige Systeme:**
Diese Prüfung findet auf Systemebene statt. Werden richtlinienabhängige Systeme gefunden, wird der betroffene User aufgefordert, die Richtlinie nachweislich zur Kenntnis zu nehmen.
Ja: Bei positivem Prüfergebnis wird in den Subprozess *Richtlinie bestätigen* verzweigt (siehe Punkt 11)
Nein: Sind keine richtlinienabhängigen Systeme vorhanden bzw. alle erforderlichen Richtlinien bestätigt, wird intern zur nächsten Aktion weitergeleitet (siehe Punkt 5).

5 **Transaktion Rolle zuweisen (siehe auch Beschreibung der Transaktionen):**
Die Berechtigungen werden automatisch zugewiesen. Der Logon-Name für die Subsysteme wird über eine Bildungsregel pro Subsystem automatisch vergeben und wenn erforderlich ein Passwort generiert. Die Zuweisungen (Transaktionen) werden vom Transaktionsmonitor überwacht und Fehlermeldungen aus den Schnittstellen (Connectoren) an die bi-Cube Administration gemeldet. Nach erfolgreichem Abschluss aller Transaktionen wird intern zur nächsten Aktion weitergeleitet (siehe Punkt 6).

6 **Prüfung auf Eigen- oder Fremdantrag:**
Durch diese Prüfung soll die Verteilung Abschluss-Mail gesteuert werden. Dabei wird ermittelt, ob der User für sich selbst einen Antrag gestellt hat (Eigenantrag) oder ob eine berechtigte Person für andere einen Antrag gestellt hat (Fremdantrag).
Eigenantrag: Die Abschluss-Information wird nur an den User verschickt (siehe Punkt 7).
Fremdantrag: Die Abschluss-Mail wird an den User und zusätzlich an den Antragsteller verschickt (siehe Punkt 8).

7 **Info-Mail an den betroffenen User:**
Sind alle Berechtigungen zugewiesen, wird der User über den Abschluss des Rollenantrags informiert. Er erhält die Zugangsdaten (Accounts mit Passwörtern für Erstanmeldung) neu vergebener Systemzugänge per Email.

8 **Info-Mail an den Antragsteller:**
Sind alle Berechtigungen zugewiesen, wird der Antragsteller zusätzlich zum User über den Abschluss des Rollenantrags informiert, wenn Antragsteller nicht gleich betroffener User (Fremdantrag). Er erhält per Email die Informationen über zugeteilte Rollen.

9 **Sub-Prozess Provisioning-Antrag bearbeiten (siehe auch Beschreibung der Sub-Prozesse):**
Sind genehmigungspflichtige Rollen für den betroffenen Mitarbeiter zur Zuweisung vorgesehen, wird in diesem Subprozess die Freigabe der Rollen vom zuständigen Leiter eingeholt. Lehnt der Leiter eine Rolle ab, wird diese nicht zugewiesen. Im Sub-Prozess werden definierte Bearbeitungszeiträume überwacht und ggf. Vertreter benachrichtigt bzw. Timeout-Informationen verschickt.'
Sind alle genehmigungspflichtigen Rollen freigegeben, leitet der Prozess-Manager intern zur nächsten Aktion lt. Modell weiter.

10 **Sub-Prozess Systemantrag bearbeiten (siehe auch Beschreibung der Sub-Prozesse):**
Sind lt. der freigegebenen Rollen genehmigungspflichtige Systeme für den betroffenen Mitarbeiter zur Zuweisung vorgesehen, wird in diesem Subprozess die Freigabe der Systeme vom jeweiligen System-Owner (auch Applikationsverantwortlichen) und / oder vom System-Admin (technisch Verantwortlichen) eingeholt. Lehnt ein Genehmiger ab, dann werden die übergeordnete Fachrolle und damit alle zu dieser Rolle gehörenden Systeme nicht zugeordnet.
Im Sub-Prozess werden definierte Bearbeitungszeiträume überwacht und ggf. Vertreter benachrichtigt bzw. Timeout-Informationen verschickt.
Sind alle genehmigungspflichtigen Systeme freigegeben, leitet der Prozess-Manager intern zur nächsten Aktion lt. Modell weiter.

11 **Subprozess Richtlinie bestätigen (siehe auch Beschreibung der Sub-Prozesse):**
Sind richtlinienabhängige Systeme in der Rolle vorhanden, wird der User per Email aufgefordert, die Richtlinie zu lesen und die Kenntnisnahme zu bestätigen. Lehnt er die Richtlinie ab bzw. bestätigt er nicht innerhalb eines vorgegebenen Zeitraums, dann werden die betroffene Rolle und damit alle zur Rolle gehörenden Systeme nicht zugeordnet.

NIFIS – how to get there

From:	Frankfurt Hauptbahnhof station	Edit
Drive:	3.9 km – about 10 mins	
1.	Head **southeast** on **Am Hauptbahnhof** toward **Im Hauptbahnhof**	0.1 km
2.	Continue on **B44/Baseler Straße**	0.2 km
3.	Turn **right** at **Gutleutstraße/K818**	0.2 km
4.	Turn **left** at **K818/Stuttgarter Straße**	40 m
5.	Turn **left** to stay on **K818/Stuttgarter Straße** Continue to follow K818	0.7 km
6.	Turn **left** at **K818/Mainluststraße**	73 m
7.	Slight **right** at **K818**	1.9 km
8.	Continue straight onto **Allerheiligentor/K818** Continue to follow K818	0.6 km
9.	Slight **right** at **Hanauer Landstraße**	0.1 km
To:	Hanauer Landstraße 300 60314 Frankfurt	Edit

NIFIS e.V., Hanauer Landstraße 300, Frankfurt am Main, Germany