ISBN 978-981-11-3671-9
Proceedings of 2017 the 7th International Workshop on Computer Science and Engineering (WCSE 2017)
Beijing, 25-27 June, 2017, pp. 682-690
doi: 10.18178/wcse.2017.06.119

Context-Specific Modeling of IdM Workflows in a Federated Application Domain

Johannes Schick [1], Inge Koch [2] and Wolfram-Manfred Lippe [1 +]

[1] Dept. of Mathematics and Natural Science, Institute for Computer Science, University of Muenster, D-48149 Muenster

[2] Deutscher Wetterdienst, D-63067 Offenbach am Main

[1 +] Dept. of Mathematics and Natural Science, Institute for Computer Science, University of Muenster, D-48149 Muenster

Abstract. The context-specific approach allows project structures to be depicted across particular organizational boundaries. In this paper, we apply context-specific methods to model approval processes for identity management systems (IdM) in a federated application domain. This view reduces complexity and a model was created and implemented in our IdM. The modeling language has process-oriented elements and can be used for software-based implementation in the IdM. Communicational interactions between organizational units and technical systems were modeled for our application domain. The graph-based view of the modeling language can be used to make network analyses of the specified issue. These analyses are evaluated in this paper.

Keywords: Modeling, Identity management systems, System analysis and design.

1. Introduction

Identity management systems (IdM) are essential informational systems in IT infrastructures. This kind of system is used to realize authorization structures for web services or access rules for the use of hard- and software resources. IdMs connect different organizational units. Users submit applications, employees' superiors approve applications and service providers establish approved services for users.

Workflows in common modeling languages are designed with a focus on functional decomposition. Control flows link the functions and signal the direction. Process modeling languages [1] aim to depict organizational structures and only marginally show the interactions and integration of technical systems. Earlier models were complex, often with wallpapers of flow diagrams and in many cases not easy to read. Requirements for technical implementations cannot directly be derived from these models without any abstraction of the technical implementations. Organizational structures relate to their own organizational regulations. Interorganizational structures are in the sphere of interest of the involved participants. The formalization of these environmental factors helps to establish a homogeneous and coordinated working and application domain. This language was developed to model workflows and constraints in a simple way.

We use the context-specific approach [2] with some adaptions to model authorization processes and the sequential handling of applications in different organizational units. This approach allows a designer or a system specialist to describe organizational or interorganizational structures with an entity-based view [3].

[+] Corresponding author. Tel.: +49 (69) 8062-2235; fax: +49 (69) 8062-4162
E-mail address: schickj@uni-muenster.de
[+] Corresponding author. Tel.: +49 (69) 8062-4523; fax: +49 (69) 8062-4162
E-mail address: Inge.Koch@dwd.de

The interactions between the IdM, organizational units and approvers can be designed with this approach. Sociotechnical [4] systems can be modeled, even across organizational boundaries [5]. The concise design of this language enables a fast development with goal-oriented coordination rounds.

The main contribution of this paper is to show how to apply the context-specific approach with adaptions in a federal application domain. We use a case study to explain modeling and implementation with this approach, and applied the waterfall model for the realization. Additionally, we introduce adaptions to the common modeling technique. The paper is structured as follows: Section 2 provides a brief overview of our field of application. Section 3 explains the design of our model. Section 4 outlines the implementation. The graph-based structure of our approach makes it possible to perform system-specific analytics. These aspects are discussed in section 5. The conclusion can be found in section 6. Visions and work in progress are presented in section 7. An acknowledgment is given in section 8.

2. Case Study

The context-specific approach is commonly used to model organizational structures or to depict informational content and ties in social networks. The DWD (Deutscher Wetterdienst) has an IdM for the regulation of user access to technical, meteorological and administrative systems.

This case study considers IdMs in a federated context [5][6]. The agencies of the German Administration procure their goods and services independently. Framework agreements between four German Governmental Institutions and enterprises may be made to obtain better purchasing conditions. The governmental institutions are Bundesfinanzdirektion Südwest (BFD SW), Bundesanstalt für Materialforschung und -prüfung (BAM), Beschaffungsamt des Bundesministeriums des Innern and Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw). Framework agreements of this kind are available from the Kaufhaus des Bundes (KdB) [7], the central procurement portal of the German Federal Administration. The Beschaffungsamt des Bundesministeriums is the procurement office of the Federal Ministry of the Interior. We will call it Federal Procurement Office in this paper. It manages these contracts and maintains the KdB. The organization of the procurement portal's user administration is decentralized (see Fig. 1). All agencies using the portal have local administrators, who register internal users or make changes to existing accounts. We examined the following IdM workflows:

- Create account
- change credentials
- delete account
- delete access to the KdB (or delete several permissions)

These workflows map whole lifecycles in response to individual triggering events and were modeled and implemented. A new account is created whenever a new employee is taken on who needs access to the procurement portal. If an employee takes on new responsibilities, the DWD user account is extended and a new account is created in the KdB. Credentials can be changed if a user's competences are extended or reduced. The user can request different authorizations in the KdB as purchaser, with read only access or with special privileges.

Read only access allows a user to view contracts and items. The purchaser role authorizes users to purchase items. Users can only access specific contracts with configurations issue if they have special KdB privileges. Any application for a change in existing authorizations must be supported by a brief justification. Users who no longer require access to the KdB use a different kind of application for the deletion of a whole set of permissions. Users' complete accounts are deleted when their contracts are terminated or when they retire. In this case, the application is for the deletion of KdB access.

3. Modeling of the Application Domain

The starting point for implementation of the above-listed workflows in IdM is the development of a context-specific model. Within this model, the participating organizational units and the technical systems are specified and formalized as entities. All the model components and their semantics are explained in [2].

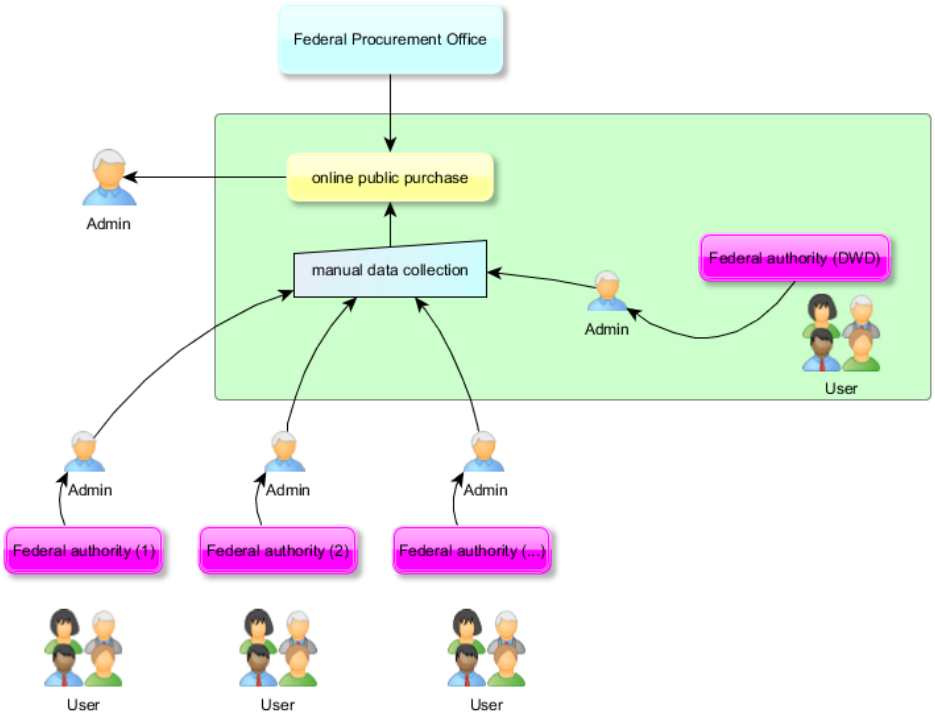

Fig. 1: Administration structure of the KdB with institutions using the procurement portal

The relations between the entities are assigned during this specification phase. These relations are called Contextdomains and are intended to model activities in a communicational context. All components are depicted in the Communicationgraph (see Fig. 2). The Communicationgraph gives a complete overview of all the relations and communication in a system of communicators. There are the following entities:

- User
- Procurement Department
- Superior

The applications are submitted by the users and are subject to the approval of the superiors. The DWD procurement department performs local user administration for the KdB. Subsequent procurements are transacted by the procurement department. Technical systems are: IdM, KdB, daccord.

The IdM manages all DWD identities. It starts with a new employee joining the DWD. User credentials, domain accounts, e-mail addresses and accesses needed for work, are applied. Applications are stored and archived in daccord. Data is provisioned from IdM to daccord and can be viewed for further analyses. Except for the creation or the deletion of an account the IdM is a self-service system. A new account authorizes the user to use the IdM for future applications. After the application is placed in IdM, the next steps are approval and quality assurance, followed by moving the application to the unit that is liable for the technical realization of the application. Finally, the user is informed about the successful implementation of the application. Subsystems represent organizational boundaries in a model. Every entity or relation defined in the subsystem of Fig. 2 is part of the DWD.

3.1. The environment in a model

A Communicationgraph is embedded in its environment, which is defined by environmental factors. The system boundary [8] is specified with this type of model component. The environmental factors are the workspace and the Federal Procurement Office. Relations between environmental factors and entities are Informationdomains. Environmental factors define the aspects influencing [9] the interactions between entities. These environmental factors can affect the entities of one or more organizations. Boundaries between organizations are usually depicted and modeled by subsystems.

In our case study, the environmental factors have no direct impact on the technical implementation of the workflows, but give a description of the organizational surroundings and regulations.

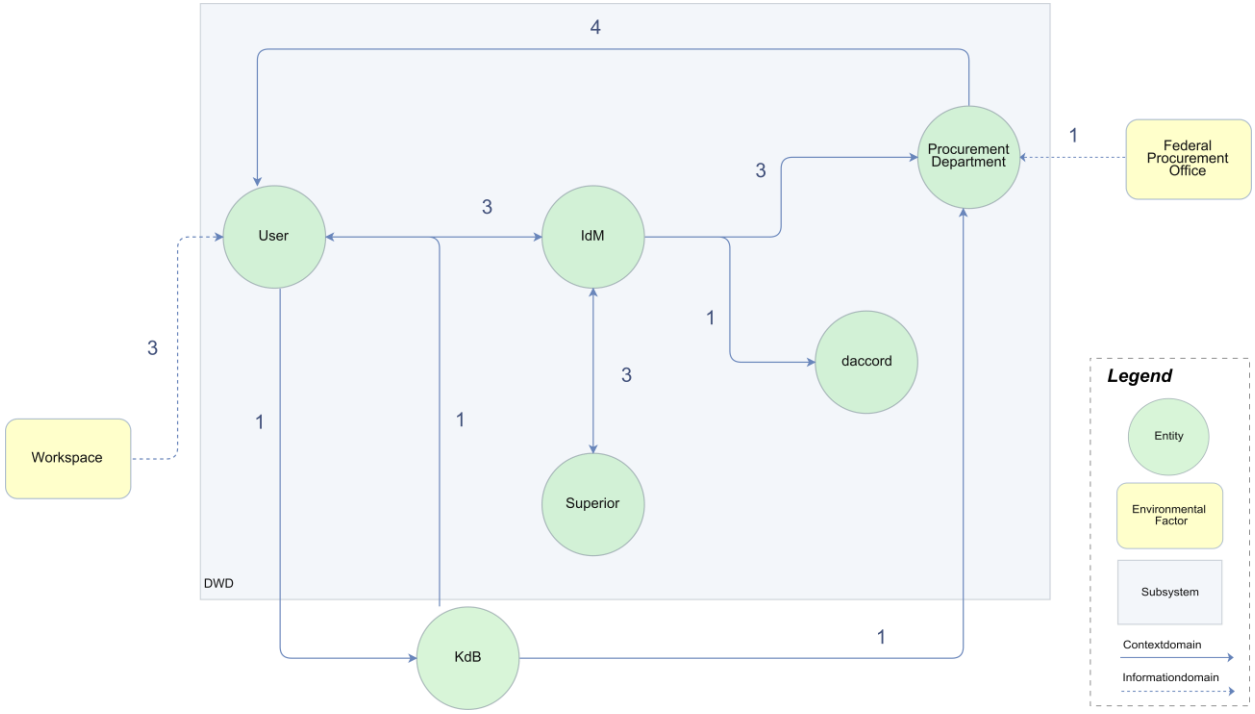

Fig. 2: Communicationgraph of the model showing the technical and non-technical entities as well as its environment

Tab. 1: Context- and Informationdomains of the Communicationgraph with communicators, used mediums and environmental factors

Communicator	Communicator	Direction	Name	Mediums
User	IdM	Unidirectional	Create New Application	Web-Frontend IdM
User	IdM	Unidirectional	Create Change Application	Web-Frontend IdM
User	IdM	Unidirectional	Create Deletion Application	Web-Frontend IdM
IdM	Superior	Bidirectional	Confirm New Application	Web-Frontend IdM
IdM	Superior	Bidirectional	Confirm Modification Application	Web-Frontend IdM
IdM	Superior	Bidirectional	Confirm Deletion Application	Web-Frontend IdM
IdM	Procurement Department	Unidirectional	Approved Access Authorization	E-Mail
IdM	Procurement Department	Unidirectional	Approved Change	E-Mail
IdM	Procurement Department	Unidirectional	Approved Deletion	E-Mail
IdM	daccord	Unidirectional	Archiving	LDAP-Connector
User	KdB	Unidirectional	New Application	Webinterface
KdB	User	Unidirectional	Confirmation Application Request	E-Mail
KdB	Procurement Department	Unidirectional	Information for User Request	E-Mail
Procurement Department	User	Unidirectional	Confirmation of Access Authorization	E-Mail
Procurement Department	User	Unidirectional	Confirmation of Change	E-Mail
Procurement Department	User	Unidirectional	Demand Application Request in IdM	E-Mail
Procurement Department	User	Unidirectional	Confirmation of Deletion	E-Mail
Environmental Factor	**Communicator**	**-**	**Name**	**-**
Workspace	User	-	Adopt Substitution	-
Workspace	User	-	New Responsibilities	-
Workspace	User	-	New Adjustment	-
Federal Procurement Office	Procurement Department	-	User Regulations	-

In our case, environmental factors may, for example, be of a technological or organizational nature. A typical case is the Informationdomain `User Regulations` from the environmental factor Federal Procurement Office to the procurement department of the DWD. The regulations provide the framework for the usage of the KdB.

3.2. Modeling behavioral aspects

Interactions are depicted by other model components. Behavioral aspects are formalized implicitly with Contextdomains. IF-THEN rules are more detailed forms of behavioral modeling. These rules extend an entity. Approval of an application is modeled as a bidirectional Contextdomain for each workflow and with a corresponding IF-THEN rule. The IF-THEN rule for a superior to approve these workflows is:

IF *(Provided Application)* **THEN** *(Quality Check and Approvement)*

A model can cover different organizations. Therefore, organizational boundaries are crossed and interactions between particular institutions are specified. The scope is defined according to the user regulations of the central procurement portal of the Federal Administration and the given technical interfaces. Other tasks are undertaken inside our own organization in line with our regimentations and technical issues.

3.3. Workflow modeling

For a better depiction of the technical dependencies, the Contextdomains in a process contain the communication mediums within the labels (see Fig. 3). In contrast to the usual practice, the readability is improved. The communicational and informational content of relations are modeled in Contexttrees. It is up to the modeler to create a Contexttree for a relation. This is useful if the information exchanged has to fulfill security restrictions or if the parameters are used to implement them in a software system, e.g. as input parameters in a form.

The Contexttree consists of a root node and the leaf nodes represent the exchanged information. An example of a Contexttree is illustrated in Fig. 5. To provide a rough overview of a modeled issue, models without Contexttrees are possible. A model has to be aligned with domain-specific knowledge of the stakeholders involved [10]. On the basis of the Communicationgraph, process diagrams or Contextscenarios can be modeled. In principle, it is possible to specify only processes or to compose them as a Communicationgraph, for a complete model, however, every entity or relation used must finally be depicted in the Communicationgraph.

There are two different processes for requesting an account for the KdB. These processes are depicted in Fig. 3. Process `a)` is the short way of applying for an account. If a user contacts the KdB directly via the web interface as depicted in `b)`, the process is longer with more participants. The first process is more effective and faster. The KdB offers the opportunity to contact the local administrators. In fact, both processes must be implemented. The structure of the first process is applied as a template for the other workflows. The applicant uses the self-service function of the IdM and the superior approves applications in a one-step procedure. After that, the local administrator will make the changes and inform the user.

4. Realization of the model

Our model was transposed taking account of organizational regulations and technical implementations in the IdM. Before we implemented the processes in our IdM, the workflows had been done manually. The IdM allows a standardized working method. As a consequence, we modeled the workflows for their implementation in the IdM. The context-specific approach gives an intuitive and generalized view of the parties involved. Complexity is reduced and only relevant information is depicted in a model without syntactic overhead.

4.1. Technical implementation

The workflows relevant for the KdB were specified using process diagrams. Following the waterfall model, we applied the common annotation form and adopted it including the description of the communication mediums in the Contextdomains. A process diagram provides an instant overview of the parties involved, their mutual tasks and the technologies and communication mediums used. The workflows were implemented at different levels in the following steps:

- implementation of the application forms
- implementation of the workflows in IdM
- storage/archiving of credentials and applications

The web-frontend as well as the workflows were implemented in the development suite (see Fig. 4) of our IdM. The users and the superiors use the web-frontend of the IdM to create, change and approve applications.

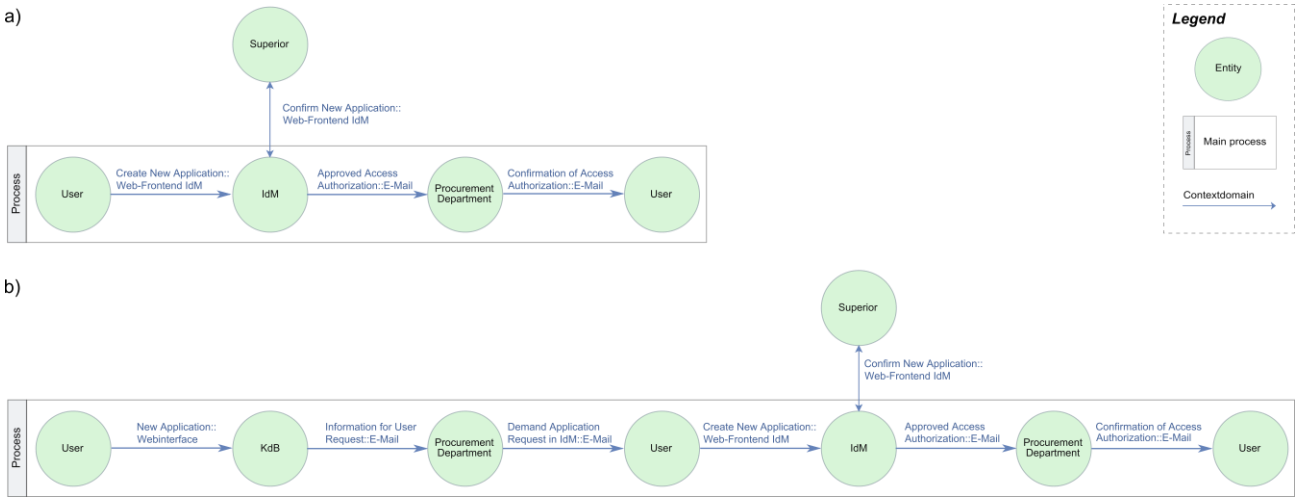

Fig. 3: Process diagrams for creating a new account in the KdB. (a) Workflow without the KdB. (b) Workflow using the KdB to get in contact with the local administrators

The relations between the entities of our model were specified with Contextdomains and Contexttrees. The Contexttrees of the model are implemented in different ways. Values of a Contexttree are realized as input parameters of the web-frontend. The grouping of parameters in a web-frontend can be depicted with sub-branches of a Contexttree. It is exemplified by the Contexttree for the Contextdomain `Create New Application :: Web-Frontend IdM`. The sub-branches of the Contexttree are implemented as tabs in the application form.

Workflows are configured in the IdM designer in a graph-based way, which includes, e.g., e-mail data of the parties concerned which is sent for a specific transaction. In the designer, the applications are realized as projects. In projects, multiple models are possible. The main page of the designer is divided into different parts, with various options for creating or changing a workflow. First of all, the user has to choose the project and model he/she would like to complement. After this step, the view in the designer shows, e.g., the properties and data item mapping belonging to the present model. The menu provides several icons, which can be used to design changes or additional branches for the existing workflow as well as to generate a new model. An icon can be added to the model simply by clicking on the icon in the palette window of the IdM designer, dropping it at the right place in the model and adding the needed connections. E-mail addresses can then be added in the properties window of the icon to provide the information of the concerning parties. An example is the Contextdomain `Approved Access Authorization :: E-Mail`. After approving an application, the IdM sends an e-mail to the procurement department, giving the user-related information for the access to the KdB.

In the data item section data types are associated with expressions, e.g. the given name or the last name is specified as a string. Applications are approved within the IdM and privileges are stored in a related LDAP system. The data structures of stored data can, e.g., be modeled with LDAP trees. This kind of data has to be specified with a modeling language related to the technology being used in order to depict the complexity of the data and to optimize it for use in the targeting software system. This can be annotated in the Communicationgraph. Data is transmitted in LDAP specific formats and is loaded into the IdM. New privileges or further information contribute to an extension of the LDAP structure. The main - and possibly the most important - tab is the first in the application form. It shows the data that is necessary in order to confirm the identity of the applicant (see Fig. 6). This data is modeled in the sub-branch User Data of the Contexttree. It is possible for the user to set the application for another user as well. The application is used to request more access authorizations, each realized in an own tab. The tab called KdB contains all the possibilities needed for the access to the KdB. The different rights are chosen by selecting attributes on a panel. More information or reasons for the selected rights can be inserted in the additional text box. In order to archive all the application information, the data is provisioned to daccord using a LDAP connector as depicted in the Communicationgraph.

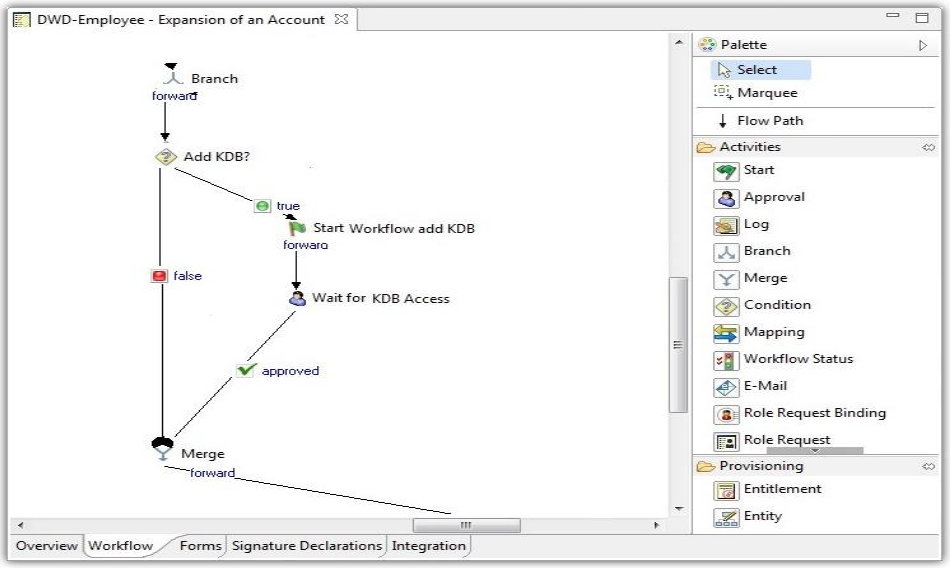

Fig. 4: Development suite with the workflow modeling module to create a KdB access with the modeling panel, possible activities and functions

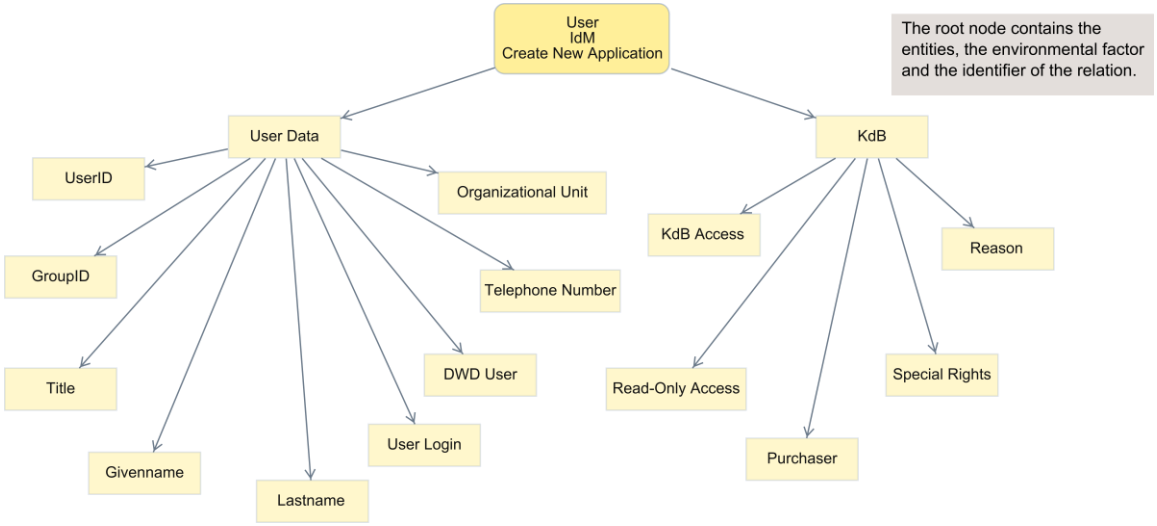

Fig.5: Contexttree “Create New Application“ for the implementation of exchanged information

The Contextdomain `Archiving :: LDAP-Connector` specifies this data transfer. With daccord, information can be accessed in a user-friendly way. It comes with a web-frontend and shows the single applications as well as the access rights granted to the user. It is also possible to see the status of an application. If an error is made, this feature gives the user the chance to repeat the application.

4.2. Organizational regulations

The organizational rules for using the IdM and integrating the KdB in the workflows are also important. The technical realization corresponds with organizational rules. The IdM is an existing system and the basic legal rules for data protection and their terms of use were already in place. These were mandatory for the implementation and the daily use of the IdM.

Apart from these aspects, we also had to extend the existing regulations for the approvers and the local administrators of the KdB for the purpose of inclusion of the requested data and assurance of process quality. The approvers have to authorize applications with the IdM, the local administrators have to ensure that the workflows are performed in the correct manner. The procurement department has regulations on how to use the KdB which clearly defines the scope of use. The procurement department informs the internal users of

the DWD about how to place an application for the use of the KdB. Basic aspects are committed and endorsed in an internal transaction document.

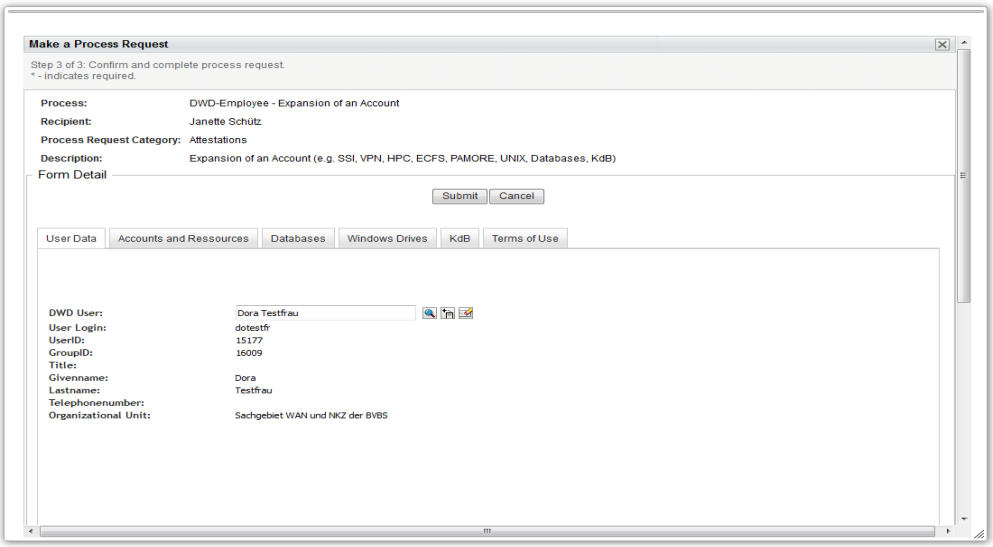

Fig. 6: Implemented web-frontend for a new application as a result of a specified Contexttree

5. Network Analytics

The Communicationgraph depicts all entities, environmental factors and relations in a weighted multigraph. It provides a structural overview and a starting point for further quantitative analytics. An entity with various Contextdomains to other entities has a central position. With a total amount of ten Contextdomains to four entities, the IdM hold the central position in the model. The whole system depends strongly on the IdM with a high level of cohesion [11]. Fewer relations are evidence for a minor role.

Applications are stored in daccord. The provisioning of the data from the IdM to daccord is modeled by the unidirectional Contextdomain `Archiving :: LDAP-Connector`. Applications can be approved even without this Contextdomain as the core data is stored in the IdM. This Contextdomain is therefore less important for operational issues. Either entities with a few relations can take key positions. It is therefore important to examine a model thoroughly before making any further analytics. All entities except daccord are senders and receivers of information. This indicates a high degree of mutual dependency in our model.

As a result of the creation of subsystems, interfaces are emphasized and depicted with relations. Basically, nested subsystems are possible but are not used in our model. If sequences in a process diagram are repeated, it is a sign that the process is not optimal or may be inefficient. To evaluate the enhancement, it should be verified that changes make work easier or reduce the workload.

6. Conclusion

The context-specific approach generalizes components and organizational units to entities and interactions of entities with the possibility of specifying the exchanged information and the environmental surroundings. This approach combines process modeling aspects and software engineering questions with the aim of integrating software-driven implementations in cross organizational structures.

We used this method to couple systems in the German Federal Administration. Organizational and environmental boundaries are modeled and complexity is reduced to essential factors. The context-specific approach is simple to use and models give a good overview of the specified issue. It results in a good relation between the time used for creating the model and its implementation in the IdM. The time scale for the implementation or comparable applications usually was some weeks. This approach enables to model and implement applications with few model components and small language knowledge.

The context-specific approach simplifies the documentation and the implementation of a model. Approval processes were depicted, which laid the basis for the planning and implementation in the technical systems involved. Information exchanged between organizational units and technical systems was modeled

using Contexttrees. This enables informational parameters to be specified in detail. The graph-based view enables analytics with conclusions on the modeled scenario.

7. Work in Progress

An interesting aspect is interrelation with other modeling languages. Technical aspects can be derived from a context-specific model and can be depicted in UML. Environmental factors influence a system of entities. New model components should be created to depict direct dependencies between environmental factors and entities with the ability to extend behavioral modeling.

8. Acknowledgements

This paper was supported by the DWD as a German Governmental Agency. The technical implementation was done by the Communication Division (TI 16) of the DWD, which is part of the DWD's IT department and is responsible for the IdM.

9. References

[1] D. Brain, P. Seltsikas, D. Tailor, *Process Modelling Notations for eGovernment: An Assessment of Modelling Notations for Identity Management.*18th Bled eConference eIntegration in Action, Slovenia, 2005.

[2] J. Schick, M. Kuboschek, W. M. Lippe, *Context Specific Entity based Modeling of Organizational Structures.* Proceedings of the 2014 IEEE International Conference on Behavioral, Economic, Socio-Cultural Computing (BESC 2014), Shanghai, 2014.

[3] P. Chen, *The Entity-Relationship Model - Toward a Unified View of Data.* ACM Transaction on Database Systems, vol. 1, number 1, pp. 9-36, 1976.

[4] A. Cherns, *The Principles of Sociotechnical Design.* Human Relations, vol. 29, number 8, pp. 783-792, 1976.

[5] S. Balasubramaniam, G. A. Lewis, E. Morris, S. Simanta, D. B. Smith, *Identity Management and its Impact on Federation in a System-of-System Context.* 3rd Annual IEEE International Systems Conference, Vancouver, Canada, 2009.

[6] A. Arabo, M. Kennedy, Q. Shi, M. Merabti, D. Llewellyn-Jones, K. Kifayat, *Identity Management in System-of-Systems Crisis Management Situation. Proceedings of the 6th International Conference on Systems of Systems Engineering,* Albuquerque, New Mexico, 2011.

[7] Beschaffungsamt des Bundesministeriums des Innern, *Kaufhaus des Bundes.* Bonn, 2016.

[8] E. M. Roger and R. Agarwala-Rogers, *Communication in Organizations.* The Free Press, New York, 1976.

[9] V. Gautam, S. K. Batra, *Organisation Development Systems. Including Essentials of Organisational Behaviour and Organisation Management.* Concept Publishing Company Pvt. Ltd., New Delhi, 2011.

[10] H. Klarl, C. Wolff, C. Emig, *Abbildung von Zugriffskontrollaussagen in Geschäftsprozessmodellen.* Modellierung 2008 - Workshop Verhaltensmodellierung: Best Practices und neue Erkenntnisse, Berlin, 2008.

[11] J. Scott, *Social Network Analysis,* SAGE Publications Ltd., London, 2013.