An Experimental Study on the Design and Modeling of Security Concepts in Business Processes

Maria Leitner, Sigrid Schefer-Wenzl, Stefanie Rinderle-Ma, Mark Strembeck

An Experimental Study on the Design and Modeling of Security Concepts in Business Processes

Maria Leitner[1], Sigrid Schefer-Wenzl[2,3],
Stefanie Rinderle-Ma[1], and Mark Strembeck[3]

[1] University of Vienna, Austria
Faculty of Computer Science
{maria.leitner,stefanie.rinderle-ma}@univie.ac.at
[2] University of Applied Sciences Campus Vienna, Austria
Competence Center for IT-Security
sigrid.schefer-wenzl@fh-campuswien.ac.at
[3] Vienna University of Economics and Business (WU Vienna), Austria
Institute for Information Systems, New Media Lab
mark.strembeck@wu.ac.at

Abstract. In recent years, business process models are used to define security properties for the corresponding business information systems. In this context, a number of approaches emerged that integrate security properties into standard process modeling languages. Often, these security properties are depicted as text annotations or graphical extensions. However, because the symbols of process-related security properties are not standardized, different issues concerning the comprehensibility and maintenance of the respective models arise. In this paper, we present the initial results of an experimental study on the design and modeling of 11 security concepts in a business process context. In particular, we center on the semantic transparency of the visual symbols that are intended to represent the different concepts (i.e. the one-to-one correspondence between the symbol and its meaning). Our evaluation showed that various symbols exist which are well-perceived. However, further studies are necessary to dissolve a number of remaining issues.

Key words: BPMN, Business Processes, Empirical Evaluation, Icons, Modeling, Security, Visualization

1 Introduction

Over the last three decades, organizations moved towards a process-centered view of business activities in order to cope with rising complexity and dynamics of the economic environment (e.g., [1]). Business processes consist of tasks which are executed in an organization to achieve certain corporate goals [2]. Business process models represent these processes of organizations. Typically, the business process models are executed via process-aware information systems

(PAIS) (e.g., [3]). Today, various business process modeling languages exist that support graphical representations of business processes such as the Business Process Model and Notation (BPMN) [4], Unified Modeling Language (UML) Activity Diagrams [5] or Event-driven Process Chains (EPC) [6, 7].

To protect sensitive organizational data and services, information systems security is constantly receiving more attention in research and industry (e.g., [8]). In many organizations, process models serve as a primary vehicle to efficiently communicate and engineer related security properties (e.g., [9]). However, contemporary process modeling languages, such as BPMN, EPCs or UML Activity diagrams, do not provide native language support to model process-related security aspects [10, 11]. As a consequence, while business processes can be specified via graphical modeling languages, corresponding security properties are usually only defined via (informal) textual comments or via ad hoc extensions to modeling languages (e.g., [12, 13]). For example in [13], we outlined current research and practice of security modeling extensions in BPMN. In addition, we conducted a survey to evaluate the comprehensibility of these extensions. The study showed that a mix of visual representations of BPMN security extensions (e.g., use of different shapes, use of text) exists. What is missing is a uniform approach for security modeling in BPMN.

Missing standardized modeling support for security properties in process models may result in significant problems regarding the comprehensibility and maintainability of these ad hoc models. Moreover, it is difficult to translate the respective modeling-level concepts to actual software systems. The demand for an integrated modeling support of business processes and corresponding security properties has been repeatedly identified in research and practice (e.g., [12, 14]).

In this paper, we present the preliminary results of an experimental study on the design and modeling of 11 security concepts on different abstraction levels in a business process context. In particular, we investigate the visualization of the following security concepts: Access control, Audit, Availability, Data confidentiality, Data integrity, Digital signature, Encryption, Privacy, Risk, Role and User. This study aims at designing symbols that are semantics-oriented and user-oriented (see Section 2) as outlined in [15]. Based on the suggestions and findings presented in [13, 16, 17], we designed two studies to obtain graphical symbols for 11 security concepts. Subsequently, we evaluated the symbol set via expert interviews. As most symbols were well-perceived, we plan to use these results and reexamine the symbols that were misleading in further studies. This will yield the basis to convey security-related information in business process models in a comprehensible way.

Our paper is structured as follows. Section 2 introduces background information on the visualization of business processes and security concepts. In Section 3, we outline the methods applied in this paper and corresponding research questions. Next, Sections 4 and 5 describe the design and results of the two experimental studies we conducted to obtain a symbol set for security concepts. The results of the evaluation of the symbols are presented in Section 6. Finally, in Section 7 we discuss results, preliminary options for integrating the symbols

into BPMN and UML and impact on future research. Section 8 concludes the paper.

2 Related Work

Visual representations have a strong impact on the usability and effectiveness of software engineering notations [17]. The quality of conceptual models is essential to, e.g., prevent errors and to improve the quality of the corresponding systems [18]. Several frameworks exist that provide guidelines on how to design and evaluate visual notations (e.g., [17, 19]). For example, the *Physics of Notations* in [17] consists of nine principles to design visual notations effectively. Further language evaluation frameworks include the cognitive dimensions of notations [19, 20] that provide a set of dimensions to assist designers of visual notations to evaluate these designs. A framework for evaluating the quality of conceptual models is presented in [21]. This approach considers various aspects such as learning (of a domain), current knowledge and the modeling activity. It also provides a dynamic view showing that change to a model might cause a direct change of the domain.

Visual Representations of Business Processes In the context of PAIS, recent publications show increased interest in the visual representation of process modeling languages. For example in [22], an evaluation of the cognitive effectiveness of BPMN using the *Physics of Notations* is performed. Further studies investigate certain characteristics such as routing symbols [23] or the usage of labels and icons [15]. In this paper, we use the terms *symbol* and *icon* synonymously as icons *are symbols that perceptually resemble the concepts they represent* [17, p.765]. In [15], the following guidelines for icon development are outlined based on research in graphical user interface design:

a Semantics-oriented: Icons should be natural to users, resemble to the concepts they refer to, and be different from each other (so that all icons can be easily differentiated).
b User-oriented: Icons should be selected based on user preferences and user evaluation.
c Composition principle: The composition of icons should be easy to understand and learn.
d Interpretation: The composition rules should be transferable to different models.

Modeling of Security Concepts in Business Processes Typically, process models are created by process modelers or process managers in an organization. These managers have an expertise in process modeling, but are often not experts in security. A security expert provides know-how and collaborates with the process modeling expert to enforce security concerns in a process. Hence, the integrated modeling of security aspects in a process model is intended to provide a common language and basis between different domain experts. Recent publications try to

provide a common language between domain experts (e.g., security experts) and process modelers by proposing process modeling extensions such as to the Unified Modeling Language (UML) (e.g., [24, 25, 26]) or to BPMN (e.g., [12, 13]).

3 Methodology

The main goal of this paper is to assess the design and modeling of security concepts in business processes. Thereby, we expect to obtain an initial set of symbols for security concepts. In contrast to existing security extensions, we do not design these symbols from scratch though. In order to obtain a set of symbols for selected security concepts, we conducted two studies (Experiment 1 and 2) and evaluated the results via expert interviews. In particular, our research was guided by the following questions (RQ):

1 Which symbols can be used to represent 11 different security concepts?
2 How can the drawings from RQ1 be aggregated into stereotype symbols?
  2.1 How do experts evaluate the one-to-one correspondence between the symbols and security concepts?
  2.2 How do experts rate the resemblance between the symbols and concepts?
  2.3 How can the stereotype symbols be improved?
3 How can the security symbols be integrated into business process modeling?
  3.1 Are the stereotype symbols suitable to be integrated into business process models?
  3.2 Which business process modeling languages are suggested for security modeling by experts?
  3.3 In BPMN, which symbols should be related to which process elements?
  3.4 Can color be useful to distinguish security symbols from BPMN standard elements?

Research question RQ1 investigates what kind of symbols people draw for 11 security concepts in Experiment 1. In the first experiment, we retrieved the symbols by setting up an experiment where the participants were asked to draw intuitive symbols for security concepts. Based on these drawings, we aggregate the drawings into stereotype symbols (RQ2) based on frequency, uniqueness and iconic character in Experiment 2. For evaluation, we analyze the stereotype symbols with expert interviews (see Section 6). In particular, we will evaluate the one-to-one correspondence between symbols and concepts, the rating of resemblance between symbols and concepts and if these symbols can be improved. With this expert evaluation, we hope to identify not only strengths and shortcomings of the symbols but also to gain insights on how to enhance the symbols such as with the use of hybrid symbols that combine graphics and text. Moreover, we investigate if security symbols can be integrated into business process modeling (RQ3). For example, we evaluate for each security concept which process elements in BPMN can be associated with it. Thereby, we expect to identify integration options for business process modeling languages.

4 Experiment 1: Production of Drawings

The first experiment addresses research question RQ1 to identify which symbols can be used to represent security concepts (see Section 3). For this purpose, we adapted the experiment design of the first experiment presented in [16].

4.1 Participants and Procedure

In our first experiment, we used a paper-based questionnaire to conduct a survey. In total, 43 Bachelors' and Masters' students in Business Informatics at the University of Vienna and the Vienna University of Economics and Business filled out the questionnaire. Most participants had beginner or intermediate knowledge of business processes and/or security. We expect to find this setting also in research and industry where experts from different domains (e.g., process modelers, security experts and business process managers) interact with each other to discuss and define security in business processes.

The survey contained 13 stapled, one-sided pages and completing the survey took about 30 minutes. It consisted of two parts. The first part, 2 pages long, presented the aim and collected demographic data of the participants, such as knowledge of business processes, knowledge of business process modeling languages and security knowledge. The second part consisted of 11 pages; one for each security concept. At the top of each page, a two-column table was displayed. Its first row contained the name of the security concept in English (see Table 1). Additionally, we displayed the name of the respective concepts in German. In the last row, a definition of the concept was given. All definitions were taken from the internet security glossary [27] except for *Role* and *User* which were taken from the RBAC standard in [28]. Please note that a definition of *Role* is not given in [27] and the *User* definition in [27] and [28] are very similar. *Role* is important as it is an essential concept for access control in PAIS (see [9]). The selection of the security concepts to be included in the survey was based on literature reviews and research projects. The aim was to consider concepts on different abstraction levels, including abstract concepts such as data integrity or confidentiality but also to include its applications (e.g., digital signature (integrity) and encryption (confidentiality)). In the middle of each page, a (3 inch x 3 inch) frame was printed. Participants were asked to draw in the frame what they estimate to be the best symbol to represent the name and the definition of a security concept. At the bottom of each page, we asked the participants to rate the difficulty of drawing this sketch. Additionally, the participants were asked to describe the symbol with one to three keywords in case they want to clarify the sketch.

4.2 Results

In total, we received 473 drawings (blank and null drawings included). We observed that participants often did not only draw a single symbol for a concept

Table 1. Names and Definitions of Security Concepts in Experiment 1

Name	Definition
Access control	Protection of system resources against unauthorized access.
Audit	An independent review and examination of a system's records and activities to determine the adequacy of system controls, ensure compliance with established security policy and procedures, detect breaches in security services, and recommend any changes that are indicated for countermeasures.
Availability	The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system.
Data confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
Data integrity	The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner.
Digital signature	A value computed with a cryptographic algorithm and appended to a data object in such a way that any recipient of the data can use the signature to verify the data's origin and integrity.
Encryption	Cryptographic transformation of data (called "plaintext") into a form (called "ciphertext") that conceals the data's original meaning to prevent it from being known or used.
Privacy	The right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share information about itself with others.
Risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
Role	A role is a job function within the context of an organization with some associated semantics regarding the authority and responsibility conferred on the user assigned to the role.
User	A user is defined as a human being. The concept of a user can be extended to include machines, networks, or intelligent autonomous agents.

but a combination of several symbols e.g., a desk in front of a matchstick man. These drawings often included signs or symbols that resembled the majority drawings.

As can be seen in Figure 1, most participants stated that the task to draw a symbol for *User*, *Encryption*, *Risk* and *Access control* was easy or fairly easy. On the other hand, it was fairly difficult or difficult for many participants to draw *Audit*, *Data confidentiality*, *Digital signature* and *Role*.

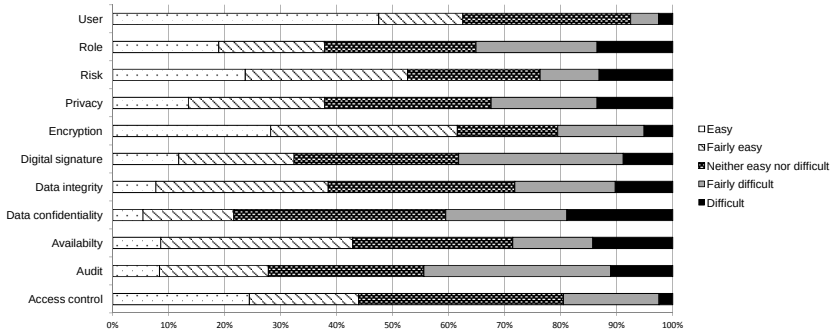

Fig. 1. Participant Rating of Difficulty of Drawing a Sketch

5 Experiment 2: Selection of Stereotypical Drawings

To answer research question RQ2, Experiment 2 is concerned with *producing stereotypical symbols* out of the sketches of Experiment 1 (adapted from [16]).

5.1 Procedure

A stereotype is the best median drawing, i.e. the symbol which is most frequently used by people to depict a concept [16]. The resulting set of stereotypes then constitutes our first proposed set of hand-sketched symbols for visualizing security concepts. However, as mentioned in [16], the drawing that is the most frequently produced to denote a security concept is not necessarily expressing the idea of the respective concept best. Thus, we subsequently evaluated the set of stereotypes via expert interviews (see Section 6).

In accordance with [16], we applied a judges' ranking method in Experiment 2 to identify the stereotypes. We started by categorizing the drawings obtained from Experiment 1. We evaluated (a) the idea it represented, (b) whether it is a drawing or a symbol and (c) the uniqueness and dissimilarity between the drawings. Thereby, each author associated a keyword (i.e. category) that represented the idea with each drawing. Drawings representing the same idea for a particular security concept form a category. Each author performed the categorization independently. Subsequently, we analyzed each categorization and reviewed and agreed on a final categorization in several rounds (see column Experiment 2 in Table 2 for the final number of categories).

To select the stereotypes, we applied the following three criteria to determine the symbol that best expressed the idea of the respective security concept: (1) Frequency of occurrence: For each security concept, we chose a drawing from each category that contained the largest number of drawings. (2) Distinctiveness and uniqueness: To avoid ambiguities and symbol overload [22, 17], we tried to select symbols which are not too similar and can be easily distinguished from each other. (3) Iconic character: According to [17], users prefer real objects to abstract shapes, because iconic representations can be easier recognized in a diagram and are more accessible to novice users (see [29]).

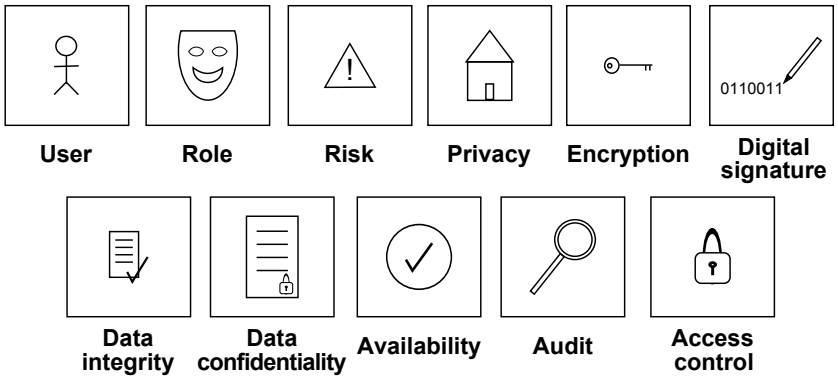

Fig. 2. Stereotype Drawings for Security Concepts

5.2 Results

The outcome of this experiment is a set of 11 stereotypes as visualized in Figure 2. For 9 out of the 11 concepts, the categorization and identification of the stereotypes was clear and straightforward. Even though the concepts *Access control* and *Data confidentiality* delivered a wide range of drawings which did not lead to a clear majority, we selected the most frequent symbol which represented an idea that could be found in many other drawings. We assume that this is due to the high level of abstraction of the terms which leads to difficulties in their visual representation. The results also indicate that the participants prefer real objects for representing security concepts (e.g., a house for *Privacy*).

6 Evaluation

This evaluation is concerned with validating the results retrieved form Experiments 1 and 2 via expert interviews and also to initially assess the use of the security symbols for business process models.

6.1 Participants and Procedure

For evaluation, a series of semi-structured interviews were conducted. A paper-based questionnaire served as the basis for these interviews. Moreover, one of the authors observed each expert while filling out the questionnaire. In addition to the questionnaire, a sheet with a list of security concepts and definitions (see Table 1) was provided to the expert. In total, we interviewed 6 experts from the security (2), process modeling (3) and visualization (1) domain. All experts have a high or intermediate expertise in both areas, process modeling and security.

The questionnaire consisted of three different parts. In the first part of the interview, goals and purpose of the interview were presented. Then, demographic data of the experts were collected such as general level of knowledge of process

Table 2. Quantitative Evaluation Results for each Security Concept

	Experiment 1	Experiment 2	Evaluation
Security Concept	No. of Drawings (out of 43)	No. of Categories	Correct Matchings (out of 6)
Access control	42	15	3
Audit	38	16	6
Availability	38	15	6
Data confidentiality	39	18	4
Data integrity	41	9	5
Digital signature	37	11	2
Encryption	42	5	5
Privacy	40	20	4
Risk	40	14	6
Role	38	15	4
User	43	5	6

modeling and security. The second part of the interview was concerned with investigating the stereotype symbols (see Figure 2). First, the experts matched the 11 security (stereotype) symbols with corresponding 11 security concepts using thinking aloud techniques (see [30]). With this setting, we expect to gain insight into how the symbols are matched by experts. After the matching, the interviewer pointed out his/her matching. Subsequently, the experts were specifically questioned for the one-to-one correspondence between the symbols and their security concepts to evaluate the semiotic clarity of the symbols (see [17]). Furthermore, the experts were asked to rate the resemblance of the symbols with the concepts they represent. Additionally, we asked if the use of shapes (e.g., triangles or circles), "document" shapes or hybrid symbols (a combination of graphics and text) can be helpful for the stereotype symbols. The third part addressed the icons' suitability to be integrated into a business process modeling language. Therefore, we asked if the stereotype symbols are suitable to be integrated into business process models and more specifically into which business process modeling languages. For example, we analyzed to which BPMN elements the symbols could be related to and if color can be helpful to distinguish security symbols from standard BPMN elements.

6.2 Results

In the following, we will summarize the results according to each research question (see Section 3). Table 2 displays the quantitative results of the study: the number of collected drawings by concept in Experiment 1, the number of assigned categories per concept in Experiment 2 (see Section 5) and the number of correct matches of the one-to-one correspondence of the experts for evaluation (RQ2a).

RQ2a: How do experts evaluate the one-to-one correspondence between the symbols and security concepts? In general, all experts could relate most stereotype symbols to the list of security concepts (see Table 2). For example, all (6) experts could identify the stereotype symbols *Audit*, *Availability*, *Risk* and *User* (see Figure 2). However, *Digital signature* (2 of 6) and *Access control* (3) were the least recognized symbols.

In case of *Digital signature*, two experts related the pen symbol with the act of writing and signing. However, all other experts could not identify the symbol as pen and binary code. Two security experts could not relate the symbol to any concept or at least to the *Data confidentiality* symbol (see Figure 2). Furthermore, two experts related the padlock symbol for *Access control* to the key symbol for *Encryption* as referring to locking and unlocking something. One expert assigned the concept encryption to the padlock symbol. One could not interpret the symbol at all. In addition, two experts pointed out that the padlock symbol used for *Access control* is also part of the *Data confidentiality* symbol, which might lead to differentiation problems.

RQ2b: How do experts rate the resemblance between the symbols and concepts? All experts agreed on a good resemblance of the symbols *Encryption*, *Risk* and *User*. Four of the experts assessed a good resemblance of the symbols *Availability*, *Data confidentiality* and *Data integrity*. The expert opinions for *Access control*, *Audit*, *Digital signature* and *Role* varied and therefore no clear statement can be made. In the case of *Audit*, at first, experts often associated the magnifier to searching for something. After the interviewer referred to the definition of *Audit*, the expert could link the symbol to review and examine.

RQ2c: How can the stereotype symbols be improved? There were only few suggestions on how to improve the symbols. One important note, however, was the similarity of the *Access control* and *Data confidentiality* symbol (due to the use of the padlock symbol) and of the *Availability* and *Data integrity* symbol (due to the check mark). Also, the relation of the padlock and the key symbol were associated with something that is in a locked or unlocked state. Hence, these symbols need to be reexamined in future studies.

Shapes The use of additional shapes such as triangles or circles around the symbols can be slightly or moderately helpful. Some experts pointed out that the complexity of most symbols should not be increased by additional shapes. However, the shapes in symbols *Risk* and *Availability* were well-perceived.

Document Shapes In the first experiment, many participants draw symbols using a "document" shape (e.g., symbol *Data confidentiality* in Figure 2). The experts pointed out that these document shapes should be primarily used to display concepts in relation to data such as data integrity or confidentiality. Additionally, the size of the symbol integrated in the document shape should be large enough to recognize the symbol.

Hybrid Symbols Most experts found that hybrid symbols combining graphics and text can be very and extremely helpful to display security concepts. However, it is important to use common abbreviations or the full name to display the security concepts.

RQ3a: Are the stereotype symbols suitable to be integrated into business process models? In general, the experts agreed that the symbols are suitable for the integration into business processes. However, they noted that some symbols should be reevaluated or redrawn to avoid symbol redundancy as stated in research question RQ2c. Furthermore, they stated that the use of legends could be helpful to novices.

RQ3b: Which business process modeling languages are suggested for security modeling by experts? The experts proposed mainly BPMN and UML. The choice for BPMN was motivated by the experts as it serves as de facto standard for business process modeling. In addition, UML is suggested because it offers integrated languages for specifying software systems from various perspectives, which includes the process and security perspectives.

RQ3c: In BPMN, which symbols should be related to which process elements? In the following, we will list the experts opinions (of at least 3 or more experts) on the linkage of security symbols and BPMN process elements (events, data objects, lanes, message events, tasks and text annotations).

Tasks can be associated to *Access control*, *Audit*, *Privacy*, *Risk*, *Role* and *User*. Hence, not only the authorization of end users to tasks is an important factor but also the supervision of these. Furthermore, events can be related to *Audit* and *Risk*. Data objects can be linked to *Availability*, *Data confidentiality*, *Data integrity*, *Digital signature* and *Encryption*. This is not surprising as these security concepts are closely related to data. Moreover, message events are associated to *Data confidentiality*, *Data integrity*, *Digital signature* and *Encryption*. As messages represent a piece of data this seems conclusive. Lanes can be linked to *Role*. As lanes can represent job functions or departments it seems feasible that lanes could be also linked to *User*. Lastly, *Audit* was the only symbol associated to text annotations.

These suggestions provide an initial basis to further develop a security extension for BPMN. However, not only the semantic (semiotic) modeling but also the syntactic modeling is important and will be investigated in future work.

RQ3d: Can color be useful to distinguish security symbols from BPMN standard elements? Most experts state that color can be helpful to highlight the security symbols in BPMN. However, the use of color should be moderately handled such as using only one color or coloring the background of the symbol.

In conclusion, our evaluation showed that most symbols could be recognized by the experts. Some symbols such as *Data confidentiality* and *Access control*

should be reexamined to dissolve remaining issues (see RQ2b and RQ2c). Furthermore, the integration of security symbols into business processes was in general well-perceived.

7 Discussion

Threats of Validity In the first experiment, we analyzed the drawings of 43 students. One can argue that this number is not enough to discover stereotype symbols for security concepts. As depicted in Section 5, we evaluated the frequency, uniqueness and iconic character between the drawings to develop the stereotype symbols. Most symbols could be easily identified except for *Access control* and *Data confidentiality*. Our evaluation showed that even though we received a wide range of drawings, the experts rated the resemblance of symbols and their concepts in general positively.

Moreover, the 11 security concepts differ in their level of abstraction. For example, *Privacy* and *Availability* are highly abstract concepts, while *Digital signature* and *Encryption* are more low-level concepts (e.g., applications). In future studies, we need to investigate the need to translate the abstract concepts into further low-level (e.g., implementation relevant) concepts and their use in a business process context.

For evaluation, we interviewed six experts from the security and/or process modeling domain. The purpose of these interviews was to gain qualitative insights on the security symbols and to analyze the one-to-one correspondence matching of the symbols and concepts. Based on these interviews, we will further develop and evaluate the security symbols and continue our research centering on end user preferences.

Integration Scenarios for BPMN and UML The BPMN [4] metamodel provides a set of extension elements that assign additional attributes and elements to BPMN elements. In particular, the `Extension` element binds an `ExtensionDefinition` and its `ExtensionAttributeDefinition` to a BPMN model definition. This elements could be used to define, e.g., an encryption level or that a digital signature is required. Furthermore, new markers or indicators can be integrated into BPMN elements to depict a new subtype or to emphasize a specific attribute of an element. For example, additional task types could be established by adding indicators similar to the e.g., service task in the BPMN specification (see [4]). The BPMN standard already specifies user tasks; i.e. tasks executed by humans. However, this does not specify how the user is authenticated (*Access control*) nor how the task showed up in his worklist (resolved via *Role* or *User*). We will investigate further if the assignment of *Role* or *User* to tasks is really needed as lanes provide similar functionality in BPMN. For the BPMN symbols for data and message events, we would need to adapt these symbols and determine how to relate security concepts to them.

In case of UML, an integration of the security concepts is possible either by extending the UML metamodel or by defining UML stereotypes (see [5]).

In particular, UML2 Activity models offer a process modeling language that allows to model the control and object flows between different actions. The main element of an Activity diagram is an `Activity`. Its behavior is defined by a decomposition into different `Actions`. A UML2 Activity thus models a process while the Actions that are included in the Activity can be used to model tasks.

Several security extensions to the UML already exist, for example SecureUML [24]. However, this extension does not have any particular connection to process diagrams. In addition, several approaches exist to integrate various security aspects, such as role-based access control concepts [31, 32, 33] or data integrity and data confidentiality [25] into UML Activity diagrams. However, in contrast to the approach presented in this paper, all other security visualizations only represent presentation options. They are suggested by the authors and not evaluated with respect to the cognitive effectiveness of the new symbols. Based on the integration options for BPMN, we derive the following suggestions for integrating the security symbol set into UML. *Access control*, *Privacy*, *Risk*, *Role* and *User* may be linked to a UML Action. *Availablity*, *Data confidentiality*, *Data integrity*, *Digital signature* and *Encryption* can be assigned to UML ObjectNodes. *Audit* may be linked to EventActions or be integrated as a UML Comment.

Future Research Several opportunities for future research emerge from our paper. As this initial study aimed at a preliminary design and modeling of security concepts, further research is necessary to fully develop security modeling extensions for business processes that can be interpreted by novices and experts, that are based on user preferences and are easy to learn (see Section 2). For example, we plan to use the stereotype drawings as basis to develop icons that can be integrated in process modeling languages. Therefore, we will investigate the icons in business processes, i.e. evaluate icons in a specific context. Furthermore, an extensive survey could assess the end user preferences of security symbols and the interpretation of these symbols (in and out of business process context). This could lead to a general approach to model security in business processes which might be adaptable to various business process modeling languages.

8 Conclusion

This paper presented our preliminary results of an experimental study on the design and modeling of security concepts in business processes. In our first study, we asked students to draw sketches of security concepts. Based on these drawings, we produced stereotype symbols considering the main idea the drawings represented, the frequency of occurrence and the uniqueness and dissimilarity between drawings. For evaluation, we interviewed experts from the area of process modeling and/or security. This evaluation showed that most symbols could be recognized based on the idea they represented. We received an even stronger acceptance for the one-to-one correspondence during the interviews when using a list of symbols and its concepts. In future studies, we aim to further analyze how our symbol set affects the cognitive complexity of corresponding models.

In addition, we will evaluate different symbol integration options into process modeling languages.

Acknowledgements The authors would like to thank the participants of the survey and the experts for their support and contributions.

References

1. Zairi, M.: Business Process Management: A Boundaryless Approach to Modern Competitiveness. Business Process Management Journal **3**(1) (1997) 64–80
2. zur Muehlen, M., Indulska, M.: Modeling Languages for Business Processes and Business Rules: A Representational Analysis. Information Systems **35**(4) (2010)
3. Weske, M.: Business Process Management: Concepts, Languages, Architectures. Springer (2007)
4. OMG: Business process model and notation (BPMN) version 2.0. OMG Document formal/2011-01-03, Object Management Group (January 2011)
5. OMG: Unified Modeling Language (OMG UML): Superstructure version 2.4.1. OMG Document formal/2011-08-06, Object Management Group (August 2011)
6. Mendling, J.: Metrics for Process Models: Empirical Foundations of Verification, Error Prediction and Guidelines for Correctness. Volume 6 of Lecture Notes in Business Information Processing (LNBIP). Springer (2008)
7. Scheer, A.W.: ARIS - Business Process Modeling. 3 edn. Springer Verlag (2000)
8. Johnson, M.E., Goetz, E.: Embedding Information Security into the Organization. IEEE Security & Privacy **5**(3) (2007)
9. Strembeck, M.: Scenario-Driven Role Engineering. IEEE Security & Privacy **8**(1) (2010)
10. Leitner, M.: Security policies in adaptive process-aware information systems: Existing approaches and challenges. In: 2011 Sixth International Conference on Availability, Reliability and Security (ARES), IEEE (August 2011) 686–691
11. Leitner, M., Mangler, J., Rinderle-Ma, S.: SPRINT-Responsibilities: design and development of security policies in process-aware information systems. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA) **2**(4) (2011) 4–26
12. Wolter, C., Menzel, M., Meinel, C.: Modelling security goals in business processes. In: Modellierung. volume 127 of LNI, Berlin, Germany, 2008. GI (2008) 197–212
13. Leitner, M., Miller, M., Rinderle-Ma, S.: An analysis and evaluation of security aspects in the business process model and notation. In: 2013 Eighth International Conference on Availability, Reliability and Security (ARES), Regensburg, Germany, IEEE (2013) (accepted for publication).
14. Russell, N., Hofstede, A.H.M.T., Edmond, D.: Workflow Resource Patterns: Identification, Representation and Tool Support. In: Proceedings of the 17th Conference on Advanced Information Systems Engineering (CAiSE). (2005)
15. Mendling, J., Recker, J., Reijers, H.A.: On the usage of labels and icons in business process modeling. International Journal of Information System Modeling and Design **1**(2) (2010) 40–58
16. Genon, N., Caire, P., Toussaint, H., Heymans, P., Moody, D.: Towards a more semantically transparent i* visual syntax. In Regnell, B., Damian, D., eds.: Requirements Engineering: Foundation for Software Quality. Number 7195 in Lecture Notes in Computer Science. Springer Berlin Heidelberg (January 2012) 140–146

17. Moody, D.: The physics of notations: Toward a scientific basis for constructing visual notations in software engineering. IEEE Transactions on Software Engineering **35**(6) (December 2009) 756 –779
18. Moody, D.L.: Theoretical and practical issues in evaluating the quality of conceptual models: current state and future directions. Data & Knowledge Engineering **55**(3) (December 2005) 243–276
19. Blackwell, A.F., et al.: Cognitive dimensions of notations: Design tools for cognitive technology. In: Cognitive Technology: Instruments of Mind. Number 2117 in Lecture Notes in Computer Science. Springer (January 2001) 325–341
20. Green, T., Blandford, A., Church, L., Roast, C., Clarke, S.: Cognitive dimensions: Achievements, new directions, and open questions. Journal of Visual Languages & Computing **17**(4) (August 2006) 328–365
21. Krogstie, J., Sindre, G., Jørgensen, H.: Process models representing knowledge for action: a revised quality framework. European Journal of Information Systems **15**(1) (2006) 91–102
22. Genon, N., Heymans, P., Amyot, D.: Analysing the cognitive effectiveness of the BPMN 2.0 visual notation. In Malloy, B., Staab, S., Brand, M.v.d., eds.: Software Language Engineering. Number 6563 in Lecture Notes in Computer Science. Springer Berlin Heidelberg (January 2011) 377–396
23. Figl, K., Mendling, J., Strembeck, M., Recker, J.: On the cognitive effectiveness of routing symbols in process modeling languages. In: Business Information Systems. Number 47 in Lecture Notes in Business Information Processing. Springer Berlin Heidelberg (January 2010) 230–241
24. Lodderstedt, T., Basin, D., Doser, J.: SecureUML: a UML-Based modeling language for model-driven security. In: UML 2002 — The Unified Modeling Language. Volume 2460. Springer Berlin Heidelberg, Berlin, Heidelberg (2002) 426–441
25. Hoisl, B., Strembeck, M.: Modeling support for confidentiality and integrity of object flows in activity models. In: Business Information Systems. Volume 87. Springer (2011) 278–289
26. Sindre, G.: Mal-Activity Diagrams for Capturing Attacks on Business Processes. In: Proc. of the 13th International Working Conference on Requirement Engineering: Foundation for Software Quality. (2007)
27. Shirey, R.: Internet Security Glossary. Number 2828 in Request for Comments. IETF (May 2000)
28. Council, I.T.I.: Information technology - role based access control. Technical Report ANSI INCITS 359-2004, American National Standards Institute, Inc. (2004)
29. Petre, M.: Why looking isn't always seeing: Readership skills and graphical programming. Communications of the ACM **38**(6) (1995)
30. Boren, T., Ramey, J.: Thinking aloud: reconciling theory and practice. IEEE Transactions on Professional Communication **43**(3) (2000) 261–278
31. Strembeck, M., Mendling, J.: Modeling Process-related RBAC Models with Extended UML Activity Models. Information and Software Technology **53**(5) (2011)
32. Schefer-Wenzl, S., Strembeck, M.: A UML Extension for Modeling Break-Glass Policies. In: Proc. of the 5th International Workshop on Enterprise Modelling and Information Systems Architectures (EMISA), Springer (2012)
33. Schefer, S., Strembeck, M.: Modeling Support for Delegating Roles, Tasks, and Duties in a Process-Related RBAC Context. In: Proc. of the International Workshop on Information Systems Security Engineering (WISSE), Springer (2011)