Incorporating Privacy Patterns into Semi-Automatic Business Process Derivation

Nikolaos Argyropoulos*, Christos Kalloniatis†*, Haralambos Mouratidis*, Andrew Fish*

*School of Computing, Engineering and Mathematics,
University of Brighton, Brighton, UK
{n.argyropoulos, h.mouratidis, andrew.fish}@brighton.ac.uk

†Department of Cultural Technology and Communication,
University of the Aegean, Lesvos, Greece
chkallon@aegean.gr

***Abstract*—The design of systems capable of protecting users' privacy is a challenging endeavour. Since users are becoming more concerned about the amounts of their personal data handled, stored and shared by such systems it is imperative to identify methods for developing privacy-aware information systems. Current approaches either focus on the elicitation of user requirements at an abstract high level or approach the issue of privacy exclusively from a technical point of view. As a result, privacy implementations are often misaligned with the overarching system goals. This work improves the current situation by presenting an approach for the design of privacy-aware business processes. Goal models are created as a first step, for privacy requirements elicitation, and are then transformed into process models, thus bridging the gap between high level goals and low level processes. Privacy process patterns are utilised for the final instantiation of process models, achieving the satisfaction of the identified privacy objectives through the integration of privacy enhancing technologies. The main advantage of the proposed approach is its ability to map privacy from the strategic to the operational level through a semi-automatic process while offering designers adequate guidance to its operationalisation via the use of process patterns.**

I. Introduction

Privacy has emerged as an important non-functional characteristic of information systems used to implement e-services. The volume and sensitive nature of user data handled and stored makes privacy a major concern for users of such services. According to recent research [1], [2], 92% of users of e-services are concerned about the amount of their personal data available online while 58% are troubled about the lack of control they possess regarding who uses their data and for what purposes. The same surveys showed that 59% of users value online anonymity but do not believe this can be realistically achieved. Therefore, the protection of their privacy has become an important factor which can influence the interaction of users with e-services.

The scientific community of the area also recognises the importance of privacy as a criterion to be considered during the early design stages of information systems. Nevertheless, privacy is often grouped with other security concerns and treated as another type of security requirement by existing requirements elicitation approaches. However, for the development of trustworthy information systems it is critical that privacy is addressed separately as it is a multifaceted concept which encompasses a variety of requirements [3].

A common approach for dealing with the privacy needs of users when developing information systems is by using requirements engineering methods to identify potential issues during the early design stages of the development lifecycle. A major drawback of such an approach is the inability to link the identified requirements with actual solutions at the operational level [4]. On the other hand, purely implementational solutions to privacy concerns fail to take into account contextual information and the overarching organisational strategy under which they will operate. Therefore, an approach that would guide the design of privacy-aware information systems from the highly abstract strategic level up to specific implementations at the operational level, would be an effective way to address the current issues concerning privacy.

In this work we introduce an approach for linking high level organisational goal models, able to capture privacy constraints, to business process models at the operational level. To maintain a mapping between high level goals and privacy controls, we transform goal models, created using the well-established Secure Tropos notation [5], as it provides concrete syntax able to capture both goal and security related concepts, to BPMN business process models. This transformation is facilitated by the use of intermediate hybrid process skeletons, introduced in our previous work [6], [7], which bridge the gap between goal and process models, and privacy-oriented process patterns which provide process fragments to be integrated into process models to address privacy concerns. Thus, our approach is able to derive privacy-aware process models, beginning from abstract organisation goals and producing flexible operational level solutions.

The rest of this paper is structured as follows: Section II discusses related work in the area of privacy and business process modelling. Section III introduces privacy-oriented process patterns and the approach for the goal-to-process model transformation. Section IV presents a case study, applying the proposed approach at the design of a real life e-voting system, while Section V provides conclusions and discusses future work.

II. Related Work

A. Privacy Requirements Engineering

As a design criterion, privacy needs to be considered early during the system design phase. Thus, a number of software engineering methods supporting the elicitation and modelling of privacy issues have been proposed. Most of them deal with privacy as a security concept or constraint like Secure Tropos, an extension of Tropos methodology proposed in [5], which employs the concepts of security constraint, and secure dependency in order to model and analyse security issues during the requirements engineering phase. Similarly, the SecReq approach introduced in [8] describes a systematic approach to derive security requirements from system security objectives. In [9] misuse cases are used in order to represent security threats and to identify "security use cases", i.e., countermeasures that mitigate the threats. Privacy patterns have been used as a way to model privacy issues. In [10] privacy patterns are used in the context of online activities, aiming to convey privacy policies to end users during online interactions. In [11] a pattern language is proposed, containing 12 patterns for developing anonymity solutions for various domains including anonymous messaging, anonymous voting and location anonymity.

From the legal compliance perspective of privacy, the work of [12] uses natural language patterns and makes use of the Hohfeld legal taxonomy, to extract security requirements from laws and combine them with the ISO/IEC policies. Finally it traces the identified requirements into secure system design. Work presented in [13] describes an approach for evaluating the legal compliance of existing security and privacy requirements, by establishing traceability links from requirements to legal texts. The emergence of cloud computing has raised the attention of researchers on the analysis and modelling of security and privacy requirements. Some works identify existing cloud technology vulnerabilities where various security incidents may occur. In [14] authors present ways that attackers can exploit data duplication techniques to access customer data through hash-code retrieval of stored files. In [15] the authors present ways in which side-channel attacks can instantiate new virtual machines in order to monitor the cached memory of adjacent virtual machines. Information or resource misuse through security and privacy incidents is also a very important area. In [16] authors argue that there is a variety of privacy threats based on the cloud scenario and lack of user control, potential unauthorized secondary usage and data proliferation. Finally, in [17] authors suggest the analysis of security and privacy risks as a decision-making criterion for migrating IT services to the cloud.

B. Business Process Modelling

Graphical standards have been broadly used for the purposes of business process modelling due the intuitive nature of capturing and visualising the sequence of activities and the flow of information within the organisational structure during the enactment of a business process [18]. BPMN 2.0 [19] is currently considered as the *"de-facto standard"* for graphical business process modelling and ha been has been used as the basis for a number of security and privacy-oriented extensions. For instance, annotated padlock symbols are introduced in [21] and special sets of symbols are introduced in [20] as part of the SecBPMN extension, to express security requirements. In such works, privacy is considered as just another type of security requirement and no further distinction between types of privacy requirements is made. Additionally, it is not within the scope of such extensions to capture the rationale behind security or privacy decisions or offer capabilities to further analyse them, as they are limited to simply annotating existing process models.

One proposed approach for providing rationale for design choices at the process level, is linking organisational strategy and business processes via the transformation of goal into process models [22]. This approach has also been applied in the context of security, for instance in [23] legacy business processes are used to extract functional and security requirements, which are then expressed via SI* organisational goal models and, finally, transformed into BPMN specifications. In the BP&SLA methodology [24] abstractly defined organisational needs and executable business processes are linked via goal models, to facilitate the selection of secure services for the process implementation. Finally, [22] presents a framework for designing secure socio-technical systems beginning with the specification of security requirements, with privacy being considered as one of them, via goal models. Next the goal models are transformed into secure process designs modelled in SecBPMN2. A work specialising in the area of privacy requirement is the PriS framework [4], which incorporates privacy requirements into business process designs via goal models. However, the output of the framework is limited to a "black-box" definition of privacy-constraint processes and it does provide further guidance on the implementation of privacy controls at the operational level.

The majority of the above works focus on security and regard privacy solely as another type of security requirement. Moreover, even if similar goal-to-process transformation techniques are utilised by them, the means of security analysis they offer are rather one-dimensional, as they are limited to either a social or a technical point of view. They also provide a static process model as output, which needs to be readjusted by repeating the application of such approaches, when the context under which it operates is slightly altered. The approach proposed in this work aims to overcome such limitations by: i) supporting the elicitation and operationalisation of all aspects of privacy requirements, ii) allowing input during decision making both at the organisational and operational level and iii) allowing for an adaptable approach to process model instantiation where a number of similar but slightly different process designs can be derived from the same reference model, according to specific situational needs of each implementation.

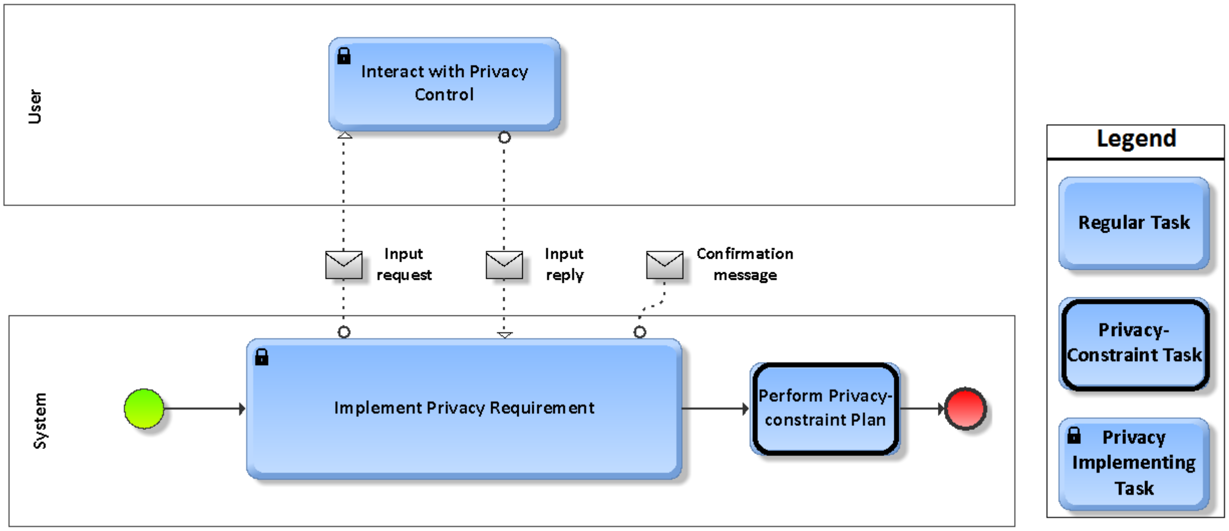
User
Interact with Privacy Control
Input request
Input reply
Confirmation message
System
Implement Privacy Requirement
Perform Privacy-constraint Plan
Legend
Regular Task
Privacy-Constraint Task
Privacy Implementing Task

Fig. 1: General privacy implementing process pattern template.

III. Proposed Framework

The two main building blocks of our proposed framework will be presented in this section. Initially a number of generic privacy process patterns will be presented and discussed. Every proposed process pattern realises one specific privacy concern. These patterns will be integrated into the second build block, a goal-to-process transformation approach. This approach is capable of supporting the elicitation of privacy requirements at a high level of abstraction through the use of goal models and transform these to hybrid reference process models, which by connecting privacy and process oriented concepts forms a privacy-annotated process skeleton. Finally, this process skeleton can be instantiated by integrating the aforementioned patterns into it and refining it to a complete process model.

A. Privacy-related Process Patterns

In this section, process patterns will be introduced for each of the main types of privacy requirements which, according to [4], are the following: *authentication, authorisation, identification, data protection, anonymity, pseudonymity, unlinkability* and *unobservability*.

Each privacy-related process pattern contains a task which implements one of the available privacy techniques, followed by the task during which the privacy constraint activity is performed. As illustrated in Fig. 1, both the task implementing the privacy technique and the corresponding task at the user's lane interacting with it, are marked with a padlock symbol at their top left corner, while the privacy-constraint task is annotated with a bold line margin in order to be visually distinguishable from regular, non-constraint tasks of the process. Messages are also typically exchanged between the user and the privacy control, and at the end of the interaction a confirmation message is sent to notify the user. For each type of privacy requirement, a different process fragment is introduced into the template of Fig. 1 thus creating a discrete process privacy pattern.

Figure 2 presents the process pattern for addressing the authentication requirement, which describes the relevant activities needed to realize that process. In particular, every time a user submits a request to the system, the system should check that request and if authentication is needed the user should provide the appropriate authentication data or else his access will be denied.

The authorisation process pattern is presented in Fig. 3. When a user requests specific services or access to data that need authorisation then he/she should pass the authentication process and then, according to his/her rights, get the privileges for allowing or denying the access to a specific service or data.

The pattern corresponding to the identification requirement is presented in Fig. 4. The role of identification is twofold. Firstly to protect both the user that accesses a resource or service and the user's data that are stored in the system and secondly to allow only authorized people to access them. When a user submits a request related to accessing private information or accessing personalized services then the process of authorization is triggered and once it is successfully completed the user is matched with an identity with specific privileges and access rights.

The aim of the data protection pattern, presented in Fig. 5, is to ensure that every transaction with personal data is realized according to the system's privacy regulations. When a user tries to access protected data, an identification process is triggered for identifying the user and for granting the rights of reading, processing, storing, or deleting private data. On the other hand, if the data to be accessed is not restricted, no identification is required.

The pattern presented in Fig. 6, addresses the anonymity and pseudonymity requirements. These two are joined in one pattern since pseudonymity could be considered as part of anonymity. First, the user's request is checked in order to decide whether or not identity is needed. If there is a need for knowing user's identity, the identification process is triggered.

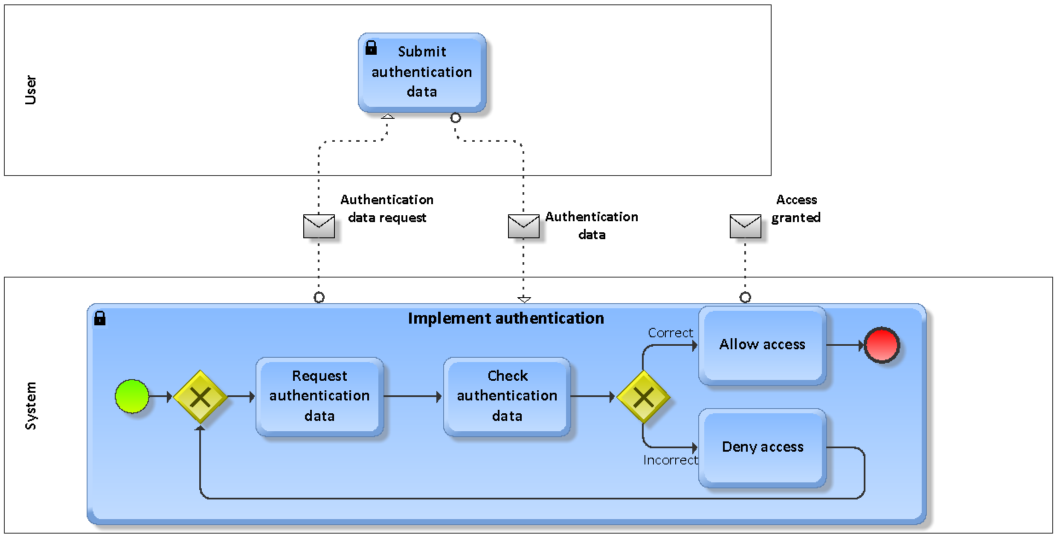

Fig. 2: Authentication pattern.

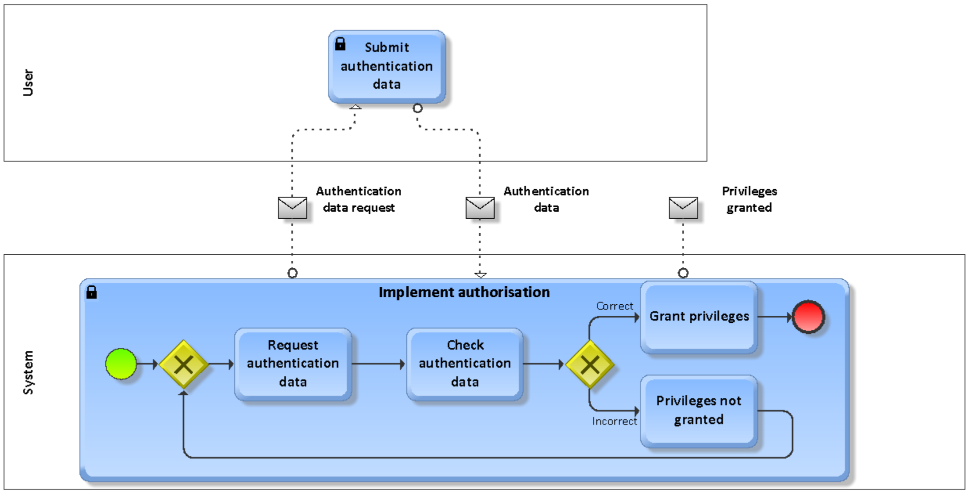

Fig. 3: Authorisation pattern.

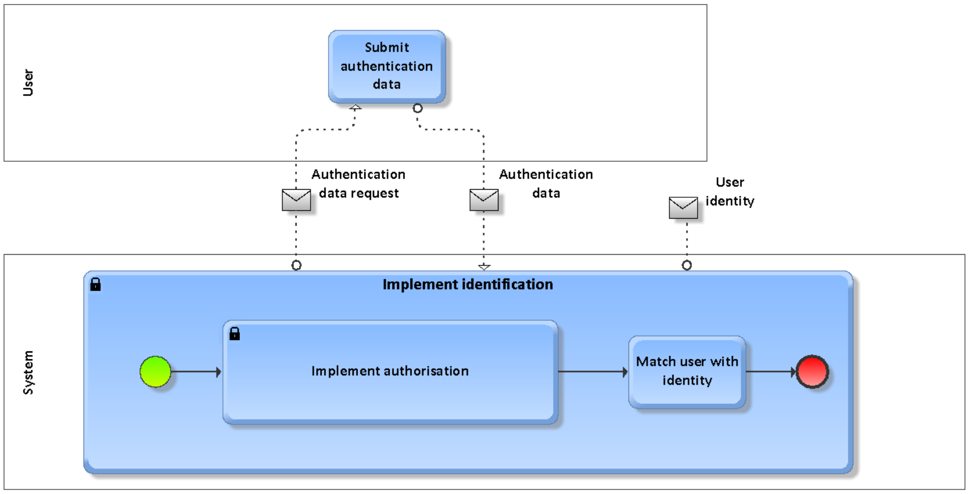

Fig. 4: Identification pattern.

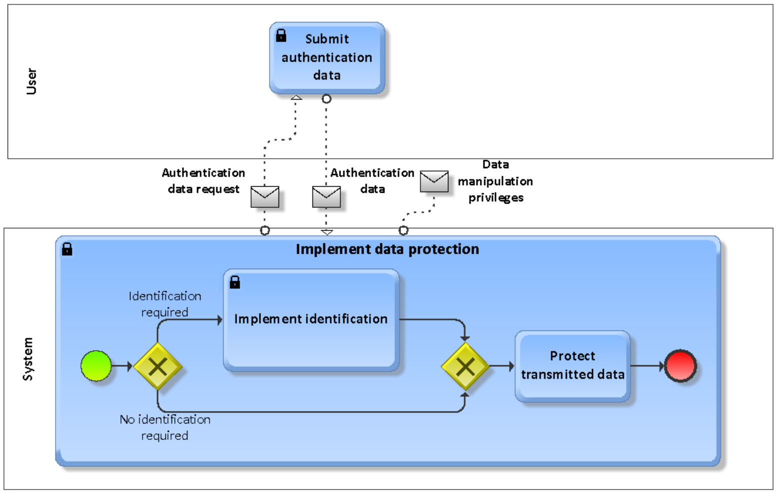
User
Submit authentication data
Authentication data request
Authentication data
Data manipulation privileges
System
Implement data protection
Identification required
Implement identification
No identification required
Protect transmitted data

Fig. 5: Data protection pattern.

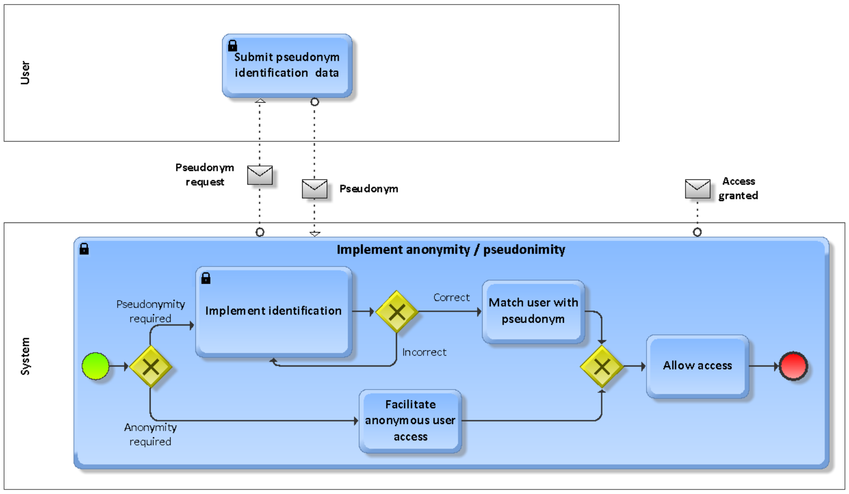

Fig. 6: Anonymity and Pseudonymity pattern.

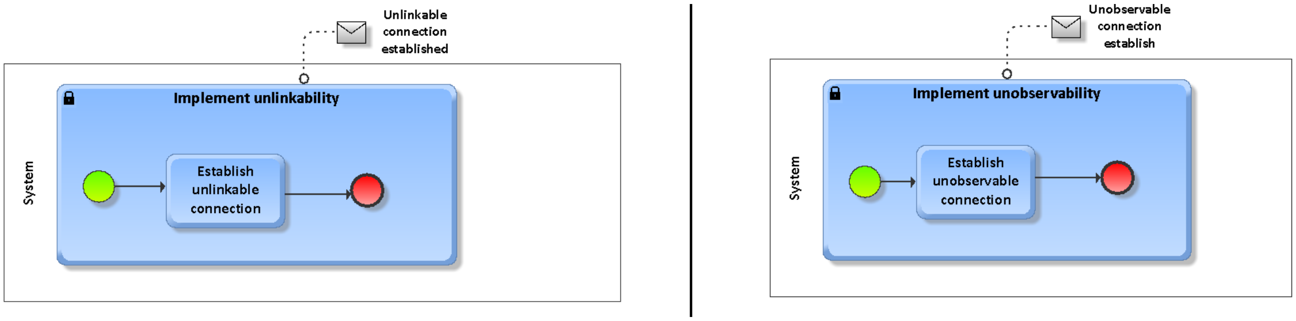
Unlinkable connection established
System
Implement unlinkability
Establish unlinkable connection
Unobservable connection establish
System
Implement unobservability
Establish unobservable connection

Fig. 7: Unlinkability and Unobservability pattern.

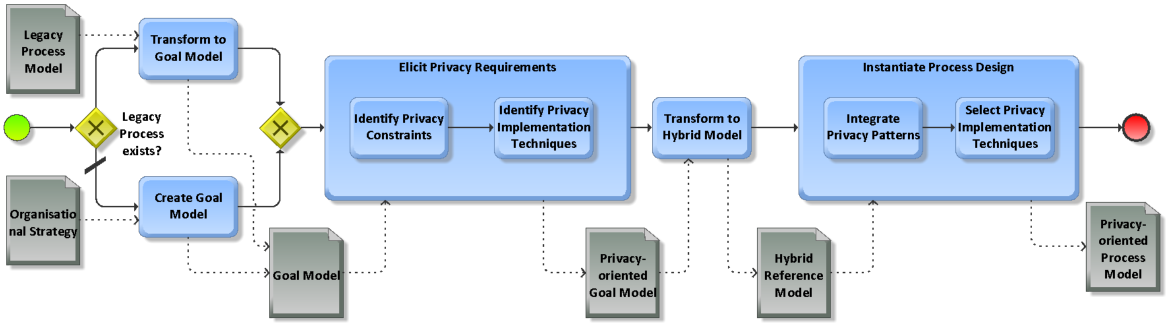
Legacy Process Model
Transform to Goal Model
Legacy Process exists?
Organisational Strategy
Create Goal Model
Goal Model
Elicit Privacy Requirements
Identify Privacy Constraints
Identify Privacy Implementation Techniques
Privacy-oriented Goal Model
Transform to Hybrid Model
Hybrid Reference Model
Instantiate Process Design
Integrate Privacy Patterns
Select Privacy Implementation Techniques
Privacy-oriented Process Model

Fig. 8: Proposed framework for the derivation of privacy-oriented business process designs

If not, the user not only receives his information without providing any personal data, but also specific techniques for protecting his anonymity are realized. Thus, identification may be a subpart of anonymity depending on whether or not specific data of user's identity are asked for processing. On the other hand, anonymity is a privacy requirement that needs to be protected and specific technologies should be used to realize users anonymisation while accessing the system and also during the whole communication. Pseudonymity is used when complete anonymity cannot be provided but the user's identity needs to be protected.

Finally, the patterns for unlinkability and unobservability requirements are presented in Fig. 7. The two patterns have a similar structure. User asks for a request. Based on system's requirements if one or both of these requirements need to be realized, then appropriate unlinkability or unobservability techniques are used for connecting the user to the system.

B. Model Transformation

The framework presented in this work aims to produce business process designs sourcing from high level stakeholder requirements. Using this framework, the process design that best fits the situational needs of the stakeholders can be instantiated from a reference hybrid model. This hybrid model contains process elements and privacy related concepts inherited by the privacy-oriented goal model from which it is transformed. Since the transformation process for the derivation of the hybrid model has been covered in our previous work [6], [7], this work will elaborate on instantiation of the hybrid model for the production of privacy-oriented process designs. The overall steps to be followed for the derivation of such business process instances are illustrated in Fig. 8.

The default first step is to begin from scratch and create a goal model of the system to be designed by taking into account the overall organisational strategy and the input of system stakeholders. This goal model will be the main artefact for the identification of the system's privacy requirements. The alternative option requires a legacy business process to be redesigned, the process model of which is transformed into a goal model by following a series of transformation steps [7].

During the second step privacy requirements are elicited and linked with the various elements of the goal model, using the concepts of constraints, objectives and implementation techniques, as introduced by the Secure Tropos approach [5]. The choice of Secure Tropos, as goal-oriented security requirements engineering method, was based on its ability to provide flexible concepts able to capture both security and privacy concerns and connect them to specific goals and potential solutions. The input of organisational stakeholders and security experts is essential for this step.

Next, the transformation of the privacy-oriented goal model to a hybrid process reference model is performed. The rules followed for this transformation, listed in Tab. I and introduced in [6], are based on concept mappings between Secure Tropos [5] and BPMN 2.0 [19] concepts, sourcing from conceptual similarities identified by their definitions and meta-models. Essentially, the rules describe how concepts from the initial goal model can be transformed into equivalent BPMN concepts at the process level, while maintaining the information and interrelations between them (e.g., the structure of a goal decomposition to plans is transformed into a sub-activity implemented by tasks). As shown in transition #1 of Fig. 9, by following these steps a hybrid reference model is created which includes process elements (lanes, activities and data objects) sourcing from similar concepts of the goal model (actors, goals and resources respectively), linked with privacy related concepts (constraints, objectives, implementation techniques) directly inherited from the same model.

TABLE I: Goal-to-Hybrid Transformation steps

Step 1	*For each* **actor** (a) of the goal model: *Create* a corresponding **lane** $l(a)$ in the hybrid model.
Step 2	*For each* **plan**(p) of the goal model: *Create* a corresponding **task** $t(p)$ in the hybrid model.
Step 3	*For each* **resource** (r) of the goal model: *Create* a corresponding **data object** $d(r)$ in the hybrid model.
Step 4	*For each* **constraint** (c), **objective** (o) or **mechanism** (m) connected to a plan (p) or resource (r) of the goal model: *Transfer* it to the hybrid model and *connect* it to the corresponding **tasks** $t(p)$ or **data objects** $d(r)$.

Once a hybrid process model has been created, it is used as a reference model from which different business process designs can be instantiated, as illustrated by transition #2 of Fig. 9. In the final process model, the privacy constraint activities are preceded by privacy implementing activities, as illustrated in

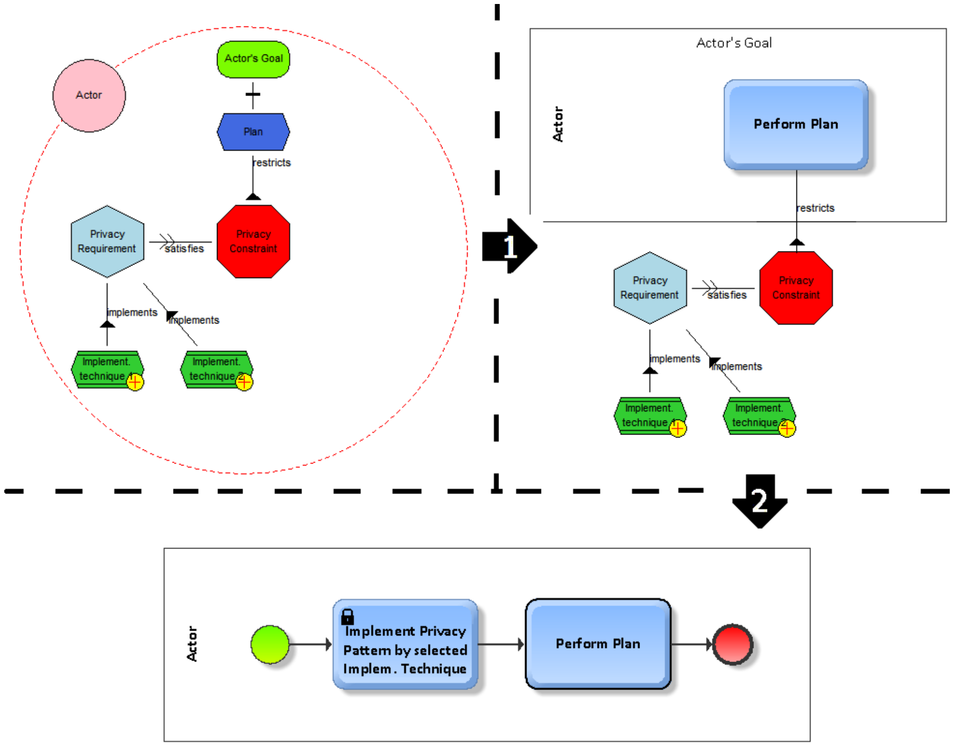

Fig. 9: Transition from goal model to business process instance

Fig. 1. The privacy implementing activities are structured by operationalising one of the privacy implementation techniques, identified at the goal model level, by inserting it as an activity of one of the previously introduced privacy process patterns. During this operationalisation different combinations of the proposed privacy implementation techniques are selected according to the specific needs of the process instance. The analysis required for the selection of the appropriate implementation techniques will be left to the discretion of the system's stakeholders and the privacy experts. To finalize the process model, the activities are manually ordered and connected to each other and to start and end events.

IV. Case Study

This section demonstrates a case study applying our methodology on an electronic voting system (e-VOTE). A detailed description of the e-VOTE project can be found in [25]. The main scope of the e-VOTE system is to provide eligible citizens the right to cast a vote over the Internet rather than visiting an election district, aiming to simplify the election process thus increasing the degree of citizens participation during elections. The e-VOTE system is described by four main principles that form the four primary organisational goals namely: Generality, Equality, Freedom and Directness.

Specifically, generality implies that all citizens above a certain age should have the right to participate in the election process. Equality implies that both political parties - that participate in the election process - and voters have equal rights before, during and after the election process and neither the system nor any other third party is able to infringe on them. Freedom implies that the entire election process is conducted without any violence, coercion, pressure, manipulative interference or other influences, exercised either by the state or by one or more individuals. Finally, directness implies that no intermediaries chime in on the voting process and that each and every ballot is directly recorded and counted. Based on three of the four primary goals of the e-VOTE system, the Secure Tropos approach was applied for constructing a partial goal model of the system and for identifying the relevant privacy requirements and plans that realize the operationalised sub-goals, as illustrated in Fig. 10.

During the requirement elicitation phase, privacy constraints have been identified by referring to relevant legislation regarding the voting process and performing stakeholder analysis. The identified constraints denote certain privacy-related restrictions which need to apply during the realisation of the plans in order to satisfy the overall privacy objectives of the system. As a result, the plans included in the goal model of the system were analysed in order to determine which should be linked to the identified privacy constraints. An overview of the identified constraints and the overarching privacy objectives they satisfy is provided in Tab. II. Additionally, by referring to privacy enhancing technologies (PETs) repositories and matching each PET to one of our privacy objectives, we have obtained a number of implementation techniques for

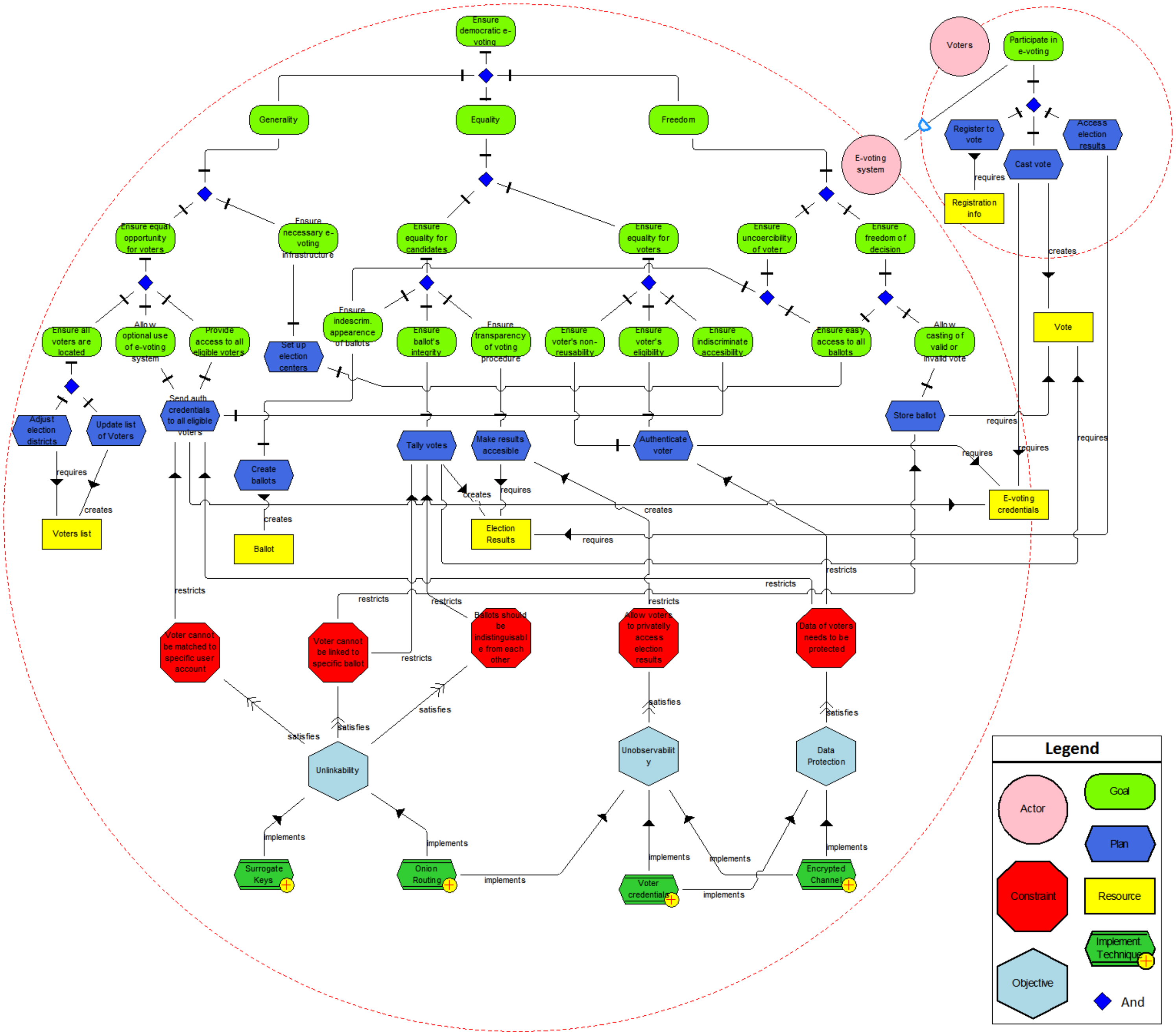
Voters
Participate in e-voting
Register to vote
Cast vote
Access election results
Registration info
Vote
E-voting credentials
E-voting system
Ensure democratic e-voting
Generality
Equality
Freedom
Ensure equal opportunity for voters
Ensure necessary e-voting infrastructure
Ensure equality for candidates
Ensure equality for voters
Ensure uncoercibility of voter
Ensure freedom of decision
Ensure all voters are located
Allow optional use of e-voting system
Provide access to all eligible voters
Set up election centers
Ensure indescrim. appearence of ballots
Ensure ballot's integrity
Ensure transparency of voting procedure
Ensure voter's non-reusability
Ensure voter's eligibility
Ensure indiscriminate accesibility
Ensure easy access to all ballots
Allow casting of valid or invalid vote
Adjust election districts
Update list of Voters
Send auth credentials to all eligible voters
Create ballots
Tally votes
Make results accesible
Authenticate voter
Store ballot
Voters list
Ballot
Election Results
Voter cannot be matched to specific user account
Voter cannot be linked to specific ballot
Ballots should be indistinguisable from each other
Allow voters to privately access election results
Data of voters needs to be protected
Unlinkability
Unobservability
Data Protection
Surrogate Keys
Onion Routing
Voter credentials
Encrypted Channel
requires
creates
restricts
satisfies
implements
Legend
Actor
Goal
Plan
Constraint
Resource
Objective
Implement Technique
And

Fig. 10: Secure Tropos goal model of the e-voting system.

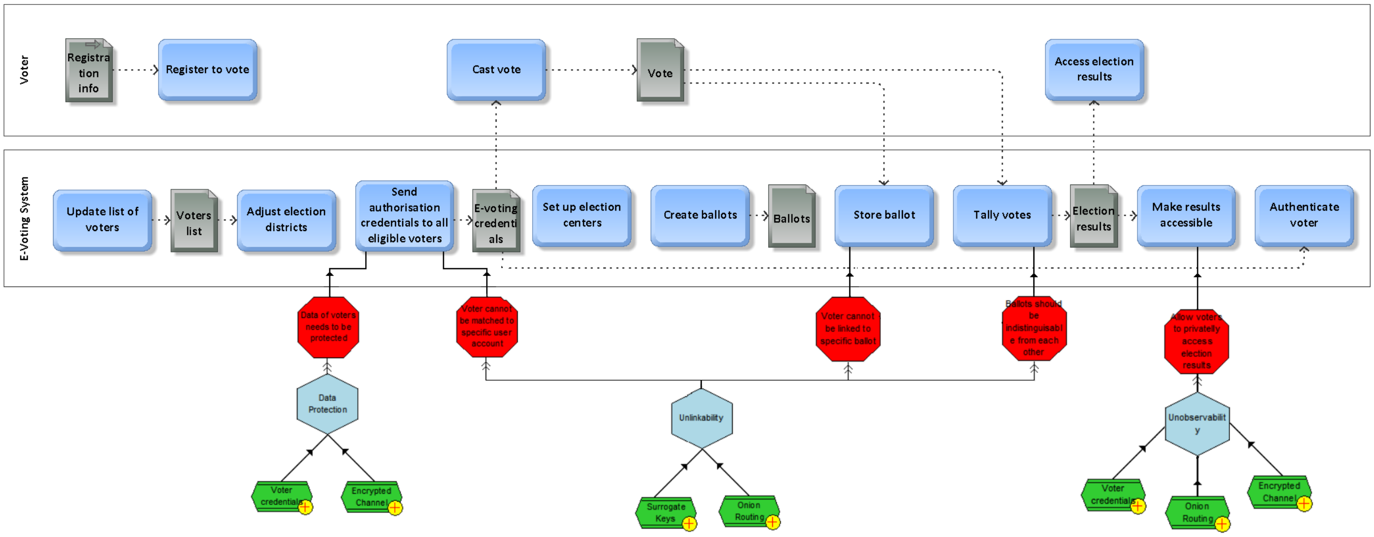

Fig. 11: Hybrid reference model of the e-voting system

satisfying our privacy constraints (e.g., encrypted channels, onion routing).

TABLE II: Identified Privacy Constraints and Objectives

Privacy Constraint	Privacy Objective
Voter cannot be matched to specific user account, when authentication means are send	Unlinkability
Voter cannot be linked to specific ballot	Unlinkability
Ballots should be indistinguishable from each other	Unlinkability
Allow voters to privately access the election results	Unobservability
Data of voters needs to be protected	Data protection

By following the transformation steps of Tab. I the hybrid reference model of Fig. 11 is created. This model captures the skeleton of the e-voting process and connects individual tasks with the privacy related concepts and their potential implementation techniques, directly inherited from the goal model. As a result, it encompasses both process and privacy information thereby linking the organisational goals with the operational level. Nevertheless, certain information required for a complete process model (e.g., ordering of activities, start/end events) cannot be captured in the goal models, therefore it is not included in the derived hybrid model and needs to be manually added to the final process model during the instantiation phase.

The last step of our approach is the instantiation of the hybrid model to complete process models. To better illustrate the full extent of the e-voting process we decided to split it into three process models illustrating the activities before (see Fig. 12), during (see Fig. 13) and after (see Fig. 14) the casting of an electronic vote. Each privacy-constraint activity is preceded by a privacy implementing activity, denoted by a padlock symbol at its top left corner. Each of the privacy implementing activities integrate one of the previously presented privacy patterns and operationalise it by selecting, using appropriate selection criteria (e.g., cost, effectiveness, complexity), one or many of the privacy implementation techniques proposed during the initial requirement elicitation phase. For instance, in the process model describing the process prior to the casting of a vote (see Fig. 12) the privacy constraint regarding the data of the voters, satisfying the data protection objective is implemented by the corresponding pattern (i.e. data protection pattern, Fig. 5), operationalised by the user credentials technique. A more detailed view of this process fragment is presented in Fig. 15 illustrating the integration of the appropriate process patterns within the completed process model.

Based on the aforementioned analysis we are able to draw conclusions regarding the applicability and effectiveness of the proposed approach at the identification and integration of privacy-oriented solutions at the process level. The proposed privacy-oriented process patterns achieved a high degree of generality allowing their smooth integration with the rest of the activities of the business process. Additionally, the interconnected nature of privacy requirements was successfully captured by the patterns used to implement them at the process level, which are composed by connecting other privacy-oriented patterns with new activities. This was made evident by the example process fragment presented in Fig. 15 where the data protection pattern included the identification pattern, which, in turn, included the authorisation pattern. Moreover, the proposed patterns allowed us to better position PETs at the operational level by indicating during which step of a business process such implementations can be positioned. This can facilitates the selection of appropriate PETs as knowing their exact position within the process, eliminates one of the many criteria which can influence the decision making process.

V. Conclusion

Privacy is an important aspect which needs to be considered during the early stages of the design of business processes. It is also important to align the implementation of privacy controls at the operational level with high level organisational strategy

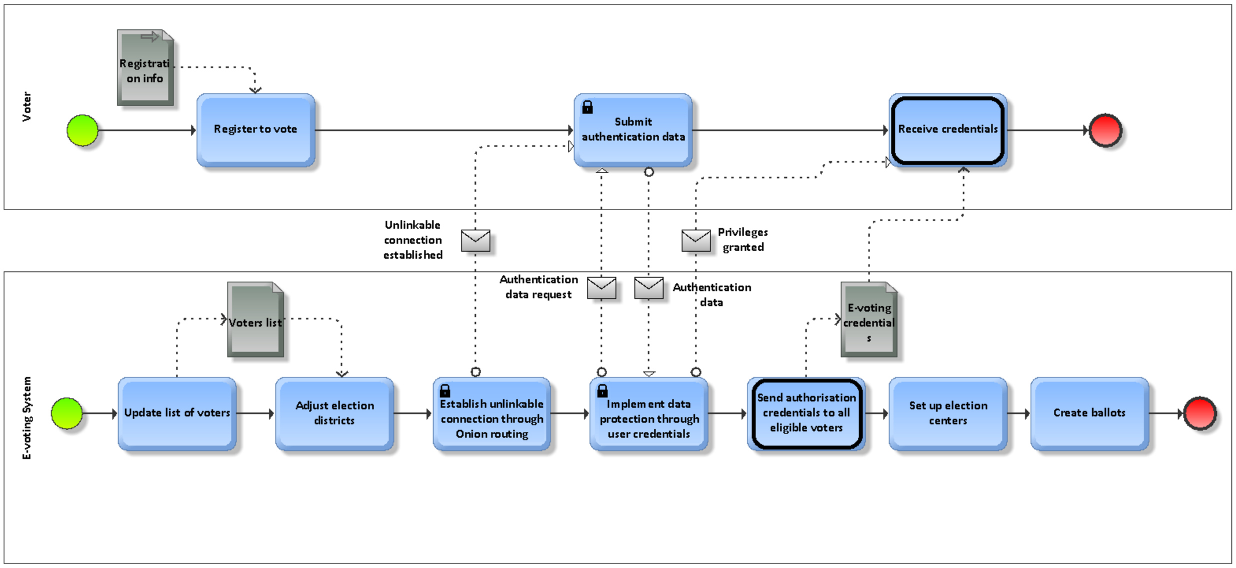
Voter
Registrati on info
Register to vote
Submit authentication data
Receive credentials
Unlinkable connection established
Privileges granted
Authentication data request
Authentication data
E-voting System
Voters list
E-voting credential s
Update list of voters
Adjust election districts
Establish unlinkable connection through Onion routing
Implement data protection through user credentials
Send authorisation credentials to all eligible voters
Set up election centers
Create ballots

Fig. 12: Privacy-enhanced view of the process prior to voting

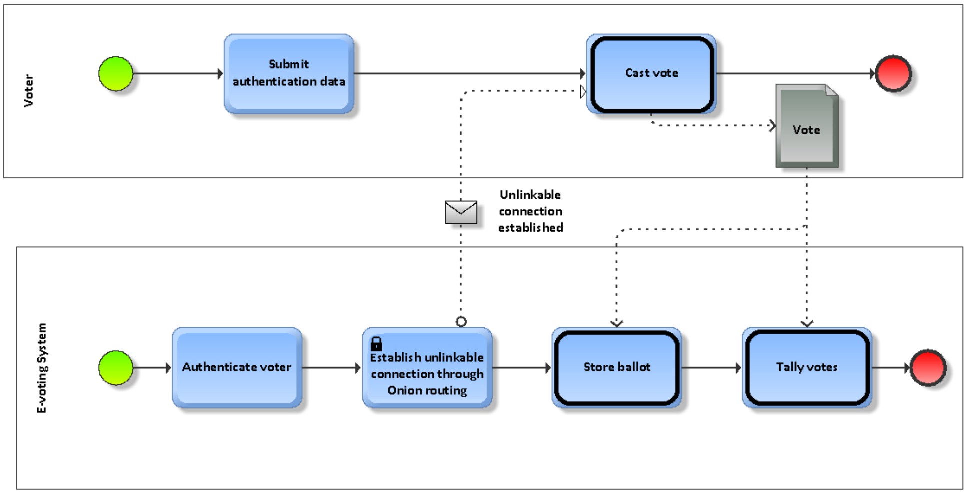
Voter
Submit authentication data
Cast vote
Vote
Unlinkable connection established
E-voting System
Authenticate voter
Establish unlinkable connection through Onion routing
Store ballot
Tally votes

Fig. 13: Privacy-enhanced view of the process of casting a vote

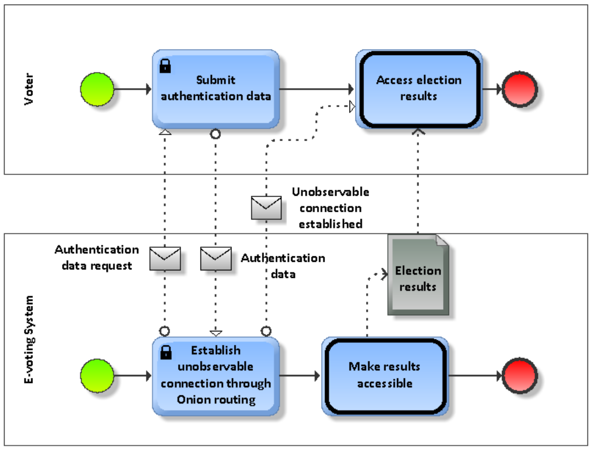
Voter
Submit authentication data
Access election results
Unobservable connection established
Authentication data request
Authentication data
Election results
E-voting System
Establish unobservable connection through Onion routing
Make results accessible

Fig. 14: Privacy-enhanced view of the process after voting

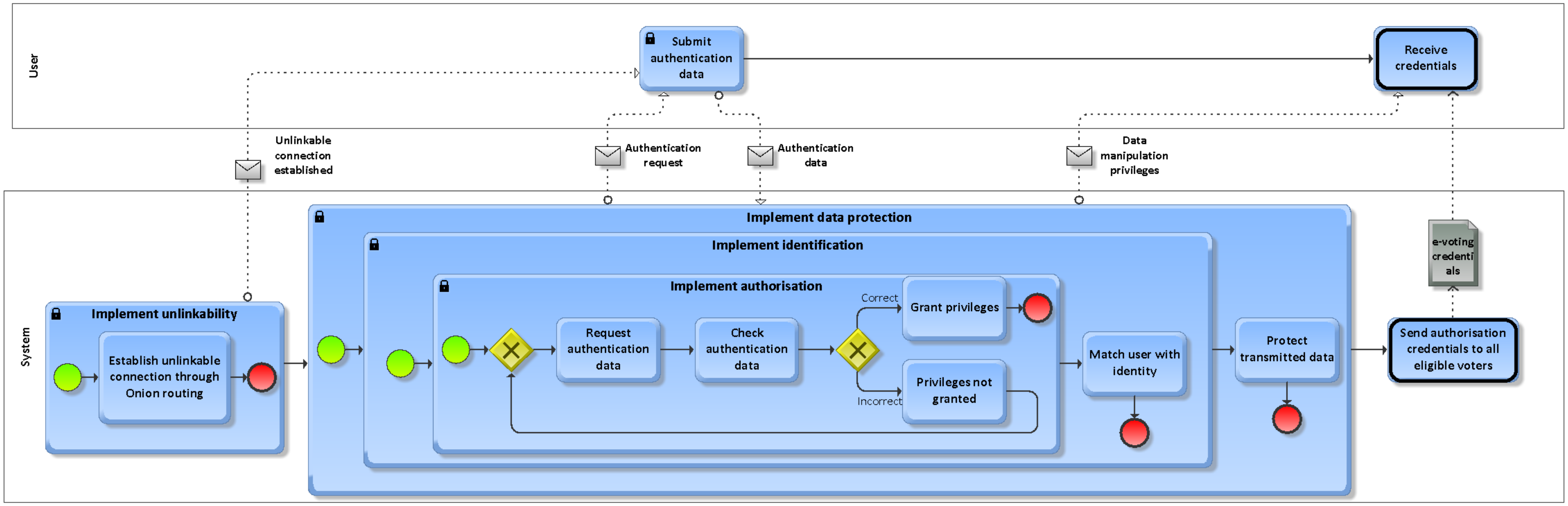
User
Submit authentication data
Receive credentials
Unlinkable connection established
Authentication request
Authentication data
Data manipulation privileges
System
Implement unlinkability
Establish unlinkable connection through Onion routing
Implement data protection
Implement identification
Implement authorisation
Request authentication data
Check authentication data
Correct
Incorrect
Grant privileges
Privileges not granted
Match user with identity
Protect transmitted data
e-voting credentials
Send authorisation credentials to all eligible voters

Fig. 15: Detailed view of privacy patterns within process fragment

in order to be able to capture the rationale behind implementation choices. This alignment can also allow designers to easily assess how strategic changes, captured at the goal model could affect the operational level, captured by the process model, and vice versa. Current literature in the area of business process modelling handles privacy as just another security requirement without being able to differentiate and express the variation of the different types of privacy requirements. On the other hand, approaches designed specifically for privacy focus on the requirements level and do not provide guidance for the operationalisation of privacy controls at the business process level of abstraction.

To cover this gap, this work introduced an approach for addressing privacy-related concerns of business process designs, which are created by transforming organisational goal models. It also introduced a series of process patterns covering the basic types of privacy requirements thus providing some guidance on the integration of privacy controls at the process level. Furthermore the adaptability of the proposed approach allows the derivation of several similar but slightly different process instances from the same midway hybrid reference model. This is achieved by capturing all the potential implementation solutions at the goal model level, linking that information to specific activities at the process level via the hybrid reference model and allowing the designers and privacy experts to decide which solution better fits their ad-hoc needs during the final process model instantiation. Therefore a multitude of process designs can be derived from the same model, with the variability sourcing from the different combinations of implemented privacy controls. Each of the produced instances is aligned with the high level goals of the system and its operationalisation is guided by predefined privacy patterns.

Future work will attempt to extend the identified patterns to cover even more complex combinations of privacy requirements which will allow our approach to better handle more demanding and privacy-intense systems. Additionally, we plan to provide further support to the decision making process taking place for the selection of specific privacy controls during the instantiation phase.

Acknowledgment

This research was partially supported by the Visual Privacy Management in User Centric Open Environments (VisiOn) project, supported by the EUs Horizon 2020 programme, Grant agreement No 653642.

References

[1] L. Rainie, S. Kiesler, R. Kang and M. Madden, Anonymity, *Privacy and Security Online*, Carnegie Mellon University, available at: http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/, accessed: 03 February 2016.

[2] TRUSTe, *US Consumer Confidence Privacy Report*, available at: http://www.truste.com/us-consumer-confidence-index-2014/, accessed: 03 February 2016.

[3] C. Kalloniatis, *Designing Privacy-Aware Systems in the Cloud*, In Trust, Privacy and Security in Digital Business, pp. 113-123, Springer, 2015.

[4] C. Kalloniatis, E. Kavakli and S. Gritzalis, *Addressing privacy requirements in system design: the PriS method*, Requirements Engineering, 13(3), 241–255, 2008.

[5] H. Mouratidis and P. Giorgini, *Secure tropos: a security-oriented extension of the tropos methodology*, International Journal of Software Engineering and Knowledge Engineering, 17(02), 285–309, 2007.

[6] N. Argyropoulos, H. Mouratidis and A. Fish, *Towards the Derivation of Secure Business Process Designs*, Advances in Conceptual Modelling, pp. 248–258, Springer, 2015.

[7] N. Argyropoulos, L. M. Alcañiz, H. Mouratidis, A. Fish, D. G. Rosado, I. G. R. de Guzmán and E. Fernández-Medina, *Eliciting Security Requirements for Business Processes of Legacy Systems*, The Practice of Enterprise Modelling, pp. 91–107, Springer, 2015.

[8] S. H. Houmb, S. Islam, E. Knauss, J. Jürjens and K. Schneider, *Eliciting Security Requirements and Tracing them to Design: An Integration of Common Criteria, Heuristics, and UMLsec*, Requirements Engineering Journal, 15, 63-93, 2010.

[9] G. Sindre and A. L. Opdahl, *Eliciting security requirements with misuse cases*, Requirements Engineering Journal, 10, 34-44, 2005.

[10] S. Romanosky, A. Acquisti, J. Hong, L. F. Cranor and Friedman B., *Privacy patterns for online interactions*, Proceedings of the 2006 conference on Pattern languages of programs (PloP 06), Portland, Oregon, pp. 12:1–12:9. ACM New York, NY, USA, 2006.

[11] M. Hafiz, *A Pattern Language for Developing Privacy Enhancing Technologies*, Software Practice and Experience. 43, 769–787, 2013.

[12] S. Islam, H. Mouratidis and S. Wagner, *Toward a framework to elicit and manage security and privacy requirements from laws and regulation*, Proceeding of Requirements Engineering: Foundation for Software Quality(REFSQ), Essen, Germany, pp. 255–261. Springer-Verlag, Berlin, Heidelberg, 2010.

[13] A. K. Massey, P. N. Otto, L. J. Hayward and A. I. Antón, *Evaluating existing security and privacy requirements for legal compliance*, Requirements Engineering Journal, 15, 119–137, 2010.

[14] M. Mulazzani, S. Schrittwieser, M. Leithner, M. Huber and E. Weippl, *Dark Clouds on the Horizon: Using Cloud Storage as Attack Vector and Online Slack Space*, Proceedings of the 20th USENIX conference on Security, San Fransisco, CA, pp. 5–5. USENIX Association Berkeley, CA, USA, 2011.

[15] C. Gong, J. Liu, Q. Zhang, H. Chen and Z. Gong, *The Characteristics of Cloud Computing*, Proceedings of the 2010 39th International Conference on Parallel Processing Workshop, San Diego, CA, pp. 275–279. IEEE Computer Society, Washington, DC, USA, 2010.

[16] S. Pearson and A. Benameur, *Privacy, Security and Trust Issues Arising from Cloud Computing*, Proceedings of the 2nd IEEE International Conference on Cloud Computing Technology and Science, Indianapolis, Indiana, USA, pp. 693–702, IEEE Computer Society, UK, 2010.

[17] S. Islam, H. Mouratidis and E. Weippl, *A Goal-driven Risk Management Approach to Support Security and Privacy Analysis of Cloud-based System*, Security Engineering for Cloud Computing: Approaches and Tools, IGI global publication, 2012.

[18] M. zur Muehlen and M. Indulska, *Modeling languages for business processes and business rules: A representational analysis*, Information Systems, 35(4), 379–390, 2010.

[19] Object Management Group, *Business Process Model and Notation (BPMN) Version 2.0*, Technical Report, 2011.

[20] M. Salnitri, F. Dalpiaz and P. Giorgini, *Modeling and verifying security policies in business processes*, Enterprise, Business-Process and Information Systems Modeling, pp. 200–214. Springer, 2014.

[21] A. Rodríguez, E. Fernández-Medina and M. Piattini, *A BPMN extension for the modeling of security requirements in business processes*, IEICE Transactions on Information and Systems, E90-D(4), 745–752, 2007.

[22] M. Salnitri, E. Paja and P. Giorgini, P., *From Socio-Technical Requirements to Technical Security Design: an STS-based Framework*, Technical Report, University of Trento, 2015.

[23] H. A. López, F. Massacci and N. Zannone, *Goal-equivalent secure business process re-engineering*, Service-Oriented Computing - ICSOC 2007 Workshops, pp. 212–223, Springer, 2009.

[24] G, Frankova, M. Séguran, F. Gilcher, S. Trabelsi, J. Dörflinger and M. Aiello, *Deriving business processes with service level agreements from early requirements*, Journal of Systems and Software, 84(8), 1351–1363, 2011.

[25] EU-Information Society DG, *E-VOTE: An Internet-Based Electronic Voting System*, IST Programme 2000#29518, Project Deliverable D 7.6, University of the Aegean, Greece, 2000.