Chapter 3
The Architecture of VisiOn Privacy Platform

Amir Shayan Ahmadian, Sven Peldszus, Jan Jürjens, Mattia Salnitri, Paolo Giorgini, Haralambos Mouratidis, Jose Fran. Ruiz

3.1 VisiOn Privacy Components

The VisiOn Privacy Platform consists of a set of components and tools, which will work and collaborate in a single platform. The overview of the VisiOn architecture is provided in Figure 3.1.

Privacy Assessment Component

The two main groups of users of the VisiOn Privacy Platform are employees of public administrations (Public Administration (PA) users) and citizens. Both groups of users have different use cases of the VisiOn Privacy Platform. The Privacy Assessment Component (PAC) addresses use cases of both groups of users. PA users want to create questionnaires and citizens want to fill questionnaires.

Amir Shayan Ahmadian - corresponding author
University of Koblenz-Landau, Germany, e-mail: ahmadian@uni-koblenz.de

Sven Peldszus
University of Koblenz-Landau, Germany, e-mail: speldszus@uni-koblenz.de

Jan Jürjens
University of Koblenz-Landau, Germany, e-mail: juerjens@uni-koblenz.de

Mattia Salnitri
Politecnico di Milano, Milano, Italy e-mail: mattia.salnitri@polimi.it

Paolo Giorgini
University of Trento,Trento, Italy e-mail: paolo.giorgini@unitn.it

Haralambos Mouratidis
University of Brighton, Brighton, UK e-mail: H.Mouratidis@brighton.ac.uk

Jose Fran. Ruiz
ATOS, Madrid, Spain e-mail: jose.ruizr@atos.net

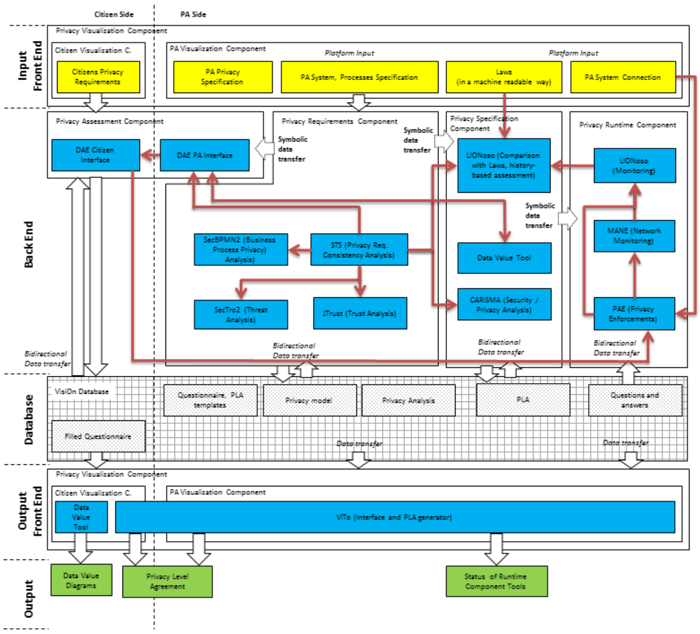
Citizen Side
PA Side
Input Front End
Privacy Visualization Component
Citizen Visualization C.
Citizens Privacy Requirements
PA Visualization Component
Platform Input
Platform Input
PA Privacy Specification
PA System, Processes Specification
Laws (in a machine readable way)
PA System Connection
Back End
Privacy Assessment Component
DAE Citizen Interface
DAE PA Interface
Symbolic data transfer
Privacy Requirements Component
Symbolic data transfer
Privacy Specification Component
LIONoso (Comparison with Laws, history-based assessment)
Privacy Runtime Component
LIONoso (Monitoring)
Symbolic data transfer
SecBPMN2 (Business Process Privacy) Analysis)
STS (Privacy Req. Consistency Analysis)
Data Value Tool
MANE (Network Monitoring)
SecTro2 (Threat Analysis)
JTrust (Trust Analysis)
CARiSMA (Security / Privacy Analysis)
PAE (Privacy Enforcements)
Bidirectional Data transfer
Bidirectional Data transfer
Bidirectional Data transfer
Bidirectional Data transfer
Database
VisiOn Database
Questionnaire, PLA templates
Privacy model
Privacy Analysis
PLA
Questions and answers
Filled Questionnaire
Data transfer
Data transfer
Output Front End
Privacy Visualization Component
Citizen Visualization C.
PA Visualization Component
Data Value Tool
ViTo (Interface and PLA generator)
Output
Data Value Diagrams
Privacy Level Agreement
Status of Runtime Component Tools

Fig. 3.1 The Vision Privacy Platform architecture.

Therefore, the inputs of the component are questions that are bundled into questionnaires. The outputs of the component are filled questionnaires, i.e., the questions and corresponding answers. Questions can be enriched with metadata that enables other components of the VisiOn Privacy Platform to relate the questions and corresponding answers to data items, systems and groups of persons involved in information processing tasks. For example, if a service offered by a PA system requires a citizen to agree on the processing of his/her personal data, a question may read “Do you allow the PA system to store your personal data?”. The question itself is hard to interpret by software, so additional information like “dataitem=personal data; operation=store” can be attached to the question to enable other components of the VisiOn Privacy Platform to automatically and precisely interpret citizen’s privacy requirement.

It is envisaged to have one questionnaire per PA (to support all services provided by this PA) and that a citizen will have to fill one questionnaire per PA. A citizen can update his or her privacy requirements by resubmitting a filled questionnaire where the answers reflect the updated privacy requirements. Furthermore, it is considered that the VisiOn Privacy Platform (VPP) derives certain parts of the questionnaire by using analysis results of the other components.

To explain the context of the PAC we refer to the VisiOn Privacy Platform Architecture (Figure 3.1). One can see that the Dynamic Audit Engine (DAE) was planned to be the only tool of the component. The inputs of the component are the Citizens Privacy Requirements (yellow box) that have to be recorded by the PAC. Data is exchanged with the Central Privacy Database. Questionnaires filled by citizens are called Citizen Questionnaire in the figure. These filled questionnaires are used by other components as illustrated by the dashed arrow “symbolic data transfer”.

The components of the VPP are grouped into a web framework and a desktop framework. The PAC is part of the web framework.

The goal of the component is the elicitation of citizens’ privacy requirements. To do that, privacy requirements are formulated as questions and bundled into questionnaires by the PA. Questions are enriched with metadata that support the automatic processing of questions and their answers. Citizens are asked to answer these questionnaires in order to state their privacy requirements. The answers are exported along the questions and their metadata to the VisiOn DataBase (VDB) in two different formats. One format contains questions, answers and metadata in a machine readable document, the other format is a typeset textual representation of the filled questionnaire excluding the metadata and intended to be displayed in the Privacy Level Agreement (PLA) document.

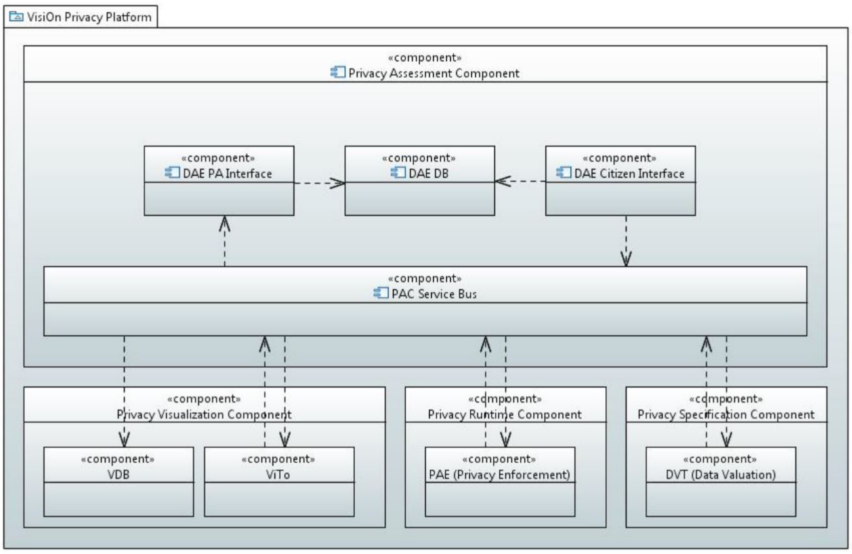

Fig. 3.2 The structure of PAC.

The constituent parts of the PAC are illustrated in Figure 3.2. The component consists of two web based applications provided by DAE (DAE PA interface and DAE citizen interface) and the PAC Service Bus. The two web applications of DAE require another component for internal storage, the DAE DB (e.g. a MySQL database). The PAC Service Bus is responsible for the communication with other tools and components of the VisiOn Privacy Platform and contains a message bus enabling asynchronous message passing. Only those parts of the Privacy Visualization Component, Privacy Runtime Component and Privacy Specification Component are illustrated in Figure 3.2 that directly communicate (using the VDB) with the PAC are shown.

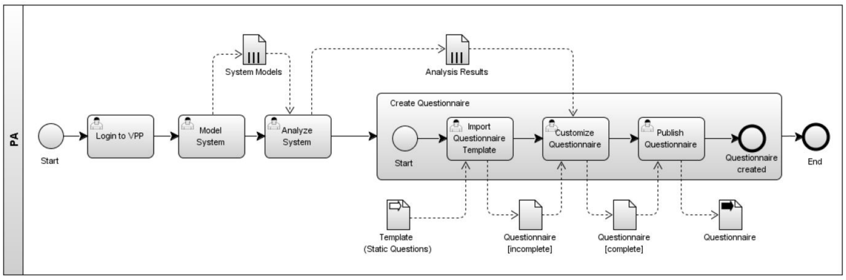

Fig. 3.3 The process of creating a questionnaire.

During PA user interaction, the PA manually creates a questionnaire based on the privacy analysis results provided by the Privacy Requirements Component using the web based interface provided by the PAC, more specifically by using the DAE PA Interface. The process diagram in Figure 3.3 illustrates the process of the PA with focus on the creation of a questionnaire. The sequence diagram in Figure 3.4 shows the communication between PA, components of the VPP and their subcomponents during the creation of a questionnaire, while details of the actual creation of a questionnaire are abstracted.

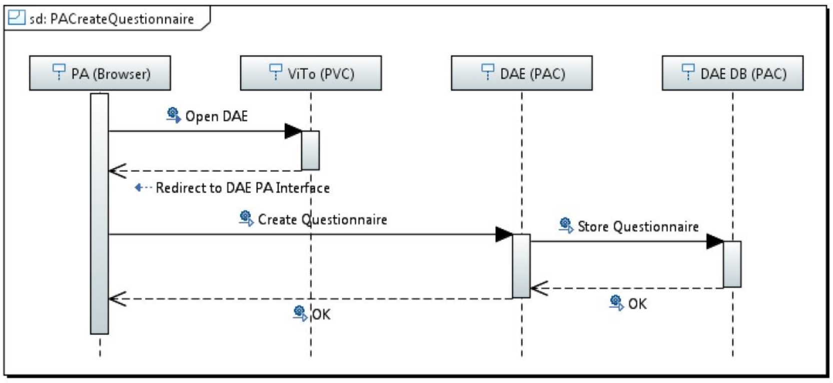

Fig. 3.4 User interaction of Public Administration with Privacy Assessment Component.

The citizen user interaction includes the steps of a citizen to state his or her privacy requirements by filling a questionnaire. The process of filling a questionnaire is illustrated in Figure 3.5. To update the privacy requirements, a citizen has to refill the questionnaire; the process is the same as for the initial filling of a questionnaire. The sequence diagram in Figure 3.6 shows the communication between citizen, components of the VPP and their subcomponents, while details of how a citizen fills a questionnaire are abstracted.

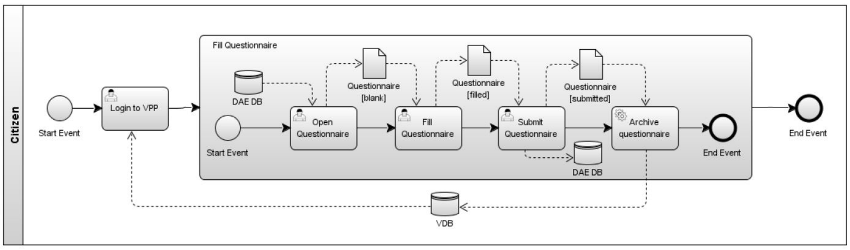

Fig. 3.5 The process of filling a questionnaire.

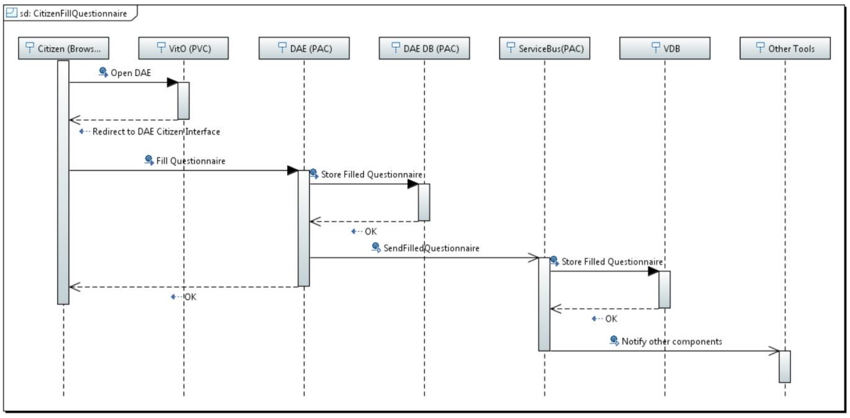

Fig. 3.6 User Interaction of citizens with Privacy Assessment Component.

Privacy Requirement Component

Privacy Requirements Component (PRC) is responsible for the modelling and consistency analysis of citizens' privacy requirements that will be retrieved by the functionality of the PAC and for the modelling of business processes, related to Public Administrations, and verification of their compliance against organizational privacy requirements. Moreover, threat and trust analysis is conducted to the PA privacy needs and requirements.

After the Privacy Requirements analysis, the PA can use those results in order to design, or redesign (either the system is a new one or already exists, respectively) their system. Thereafter, through Privacy Specification Component (PSC) , the PA can develop the UMLsec diagrams, can check the compliance of the requirements with the legal regulations and finally, can assess the value of citizens' personal data.

With the results of the different analyses, the PA can use the PAC to define the questionnaire and provide it to the citizens. A citizen fills in the questionnaire in the PAC and their answers are used by the VisiOn Privacy Platform to create the Privacy Level Agreement (PLA). The PLA is sent to the Privacy Run-Time Component (PRTC), which creates a privacy policy. The privacy policy is used to observe, verify and enforce the privacy needs of the citizen against the PA system. The status and the results of the PRTC can be seen in the PA interface of the Privacy Visualization Component (PVC). Additionally, from the PAC the results are given to the Citizen interface of the PVC.

Through the PVC, PA has an overview of the available analysis activities of the PRC and can launch the corresponding tools (see Figure 3.7).

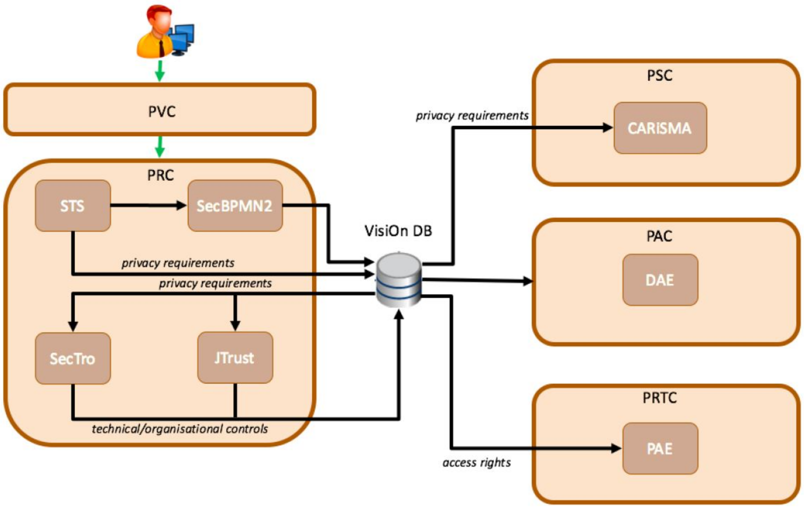

Fig. 3.7 Interaction of PRC tools with the VPP elements.

At first, PA uses the STS-tool to perform a privacy analysis of their system. STS-tool is able to graphically represent the purpose for which an entity has access to citizen's data. PA will use the STS-tool to graphically model the source entity and destination entity in a transmission of citizen's information. PA will also use the STS-tool to create a graphical model that visualizes privacy requirements and social and organizational aspects of the system.

PA is able to check whether its existing business processes are compliant with procedural privacy policies by using the Secure Business Process Modelling Notation 2.0 (SecBPMN2) tool. After the completion of this analysis, the produced models are stored to VisiOn Database.

Then, PA carries out, using the SecTro tool, a privacy threat analysis and identifies vulnerabilities and appropriate privacy related organizational actions and technical controls to satisfy privacy requirements and mitigate threats.

PA also identifies and justifies privacy related trust relationships, using the JTrust tool. In particular, through JTrust, PA can perform a trust/distrust analysis in order to build confidence that authorized users will not misuse their granted authorizations. JTrust tool will also support the PA in modelling trust relationships between entities and reasoning about the behaviour of those entities. Alternative solutions, such as control measures, could be identified in case that entities are not trusted.

Both SecTro and JTrust tools will use as basis STS models in order to proceed with their analysis. The produced models will be stored in the VisiOn Database. This information will be relevant to PA and the services it is offering.

Figure 3.8 depicts the sequence of interactions between PA and the PRC tools.

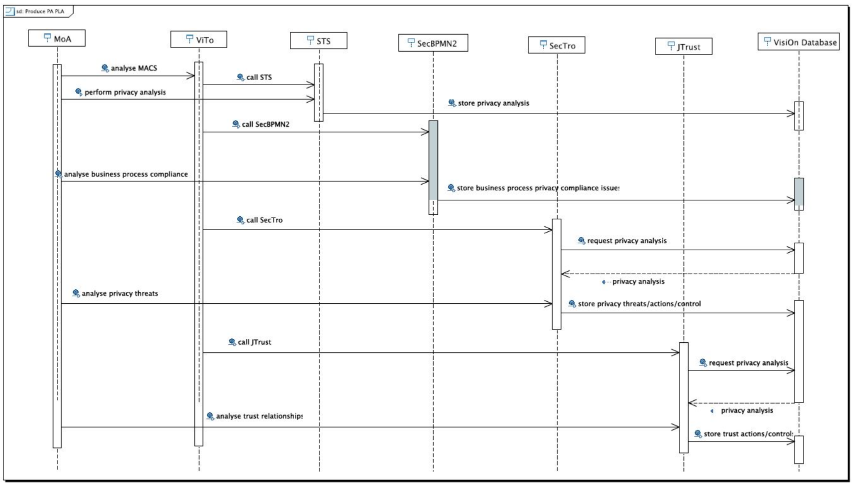

Fig. 3.8 PRC sequence diagram.

Privacy Specification Component

The VisiOn project aims to provide a platform to improve transparency and accountability of PA authorities. To this end, the VisiOn Privacy Platform provides citizens with the means to create and monitor a personal PLA and enables them to visualize their privacy preferences, relevant threats and trust issues. As mentioned before, the VisiOn platform consists of five core components. The PSC is responsible for specifying the PLA and indicating the citizen's data value.

The PSC is used to specify the PLA, i.e. populates the PLA with security and privacy reports, shows the compliance level with European Union (EU) privacy laws and increases awareness on data valuation. The PSC is composed of three tools, each is responsible for one of the component's functionalities.

The CompliAnce, Risk, and Security Model Analyzer (CARiSMA) tool performs security and privacy checks on PA systems by developing Unified Modelling Language (UML) models that at the end will be used to check whether these models satisfy the privacy requirements. Through CARiSMA, the PA user is able to perform information flow analysis that is able to identify potential security/privacy breaches and also to support the design of the system of the PA for assuring that citizen's information is transferred through secure channels/means. The generated security and privacy report as well as the identified risk level of citizens' critical information are transferred as part of the information included in the Privacy Level Agreement.

Moreover, PSC includes the LIONoso tool which is responsible for checking the compliance of the PA system with EU privacy laws and to estimate a score for the citizen using history-based assessment of citizen requirements and monitoring results from PRTC. The PA can use LIONoso to check the compliance of the PLA with the relevant laws and legislation. In case the PSC identifies non-compliance with law, the PA has to go back and reanalyze and redesign aspects of the system, taking into account this new information.

Last but not least, the Data Value Tool (DVT) is a tool of the component to assess the value of citizen's data. The DVT is an awareness tool that through information gathered from citizens (questionnaire), compares different perceptions on personal data valuation (e.g. data footprint, economic value, data conflicts, etc.) assisting them in the understanding of the risks and the importance when sharing data.

The tools are combined together as the Privacy Specification Component of the VisiOn platform. All the information used by the PSC is fed by the Privacy Assessment Component and in turn PSC provides input to both Privacy Requirement and Runtime Components. End-users visualization information related with the PSC (as for example the outcome of the DVT) is passed on to the Privacy Visualization Component.

In Figure 3.9 the structure of the PSC component and its interactions with the other components are demonstrated, in this figure the focus is on the process of security analysis.

Furthermore the interactions of the PSC with other tools and components are presented in Figure 3.10.

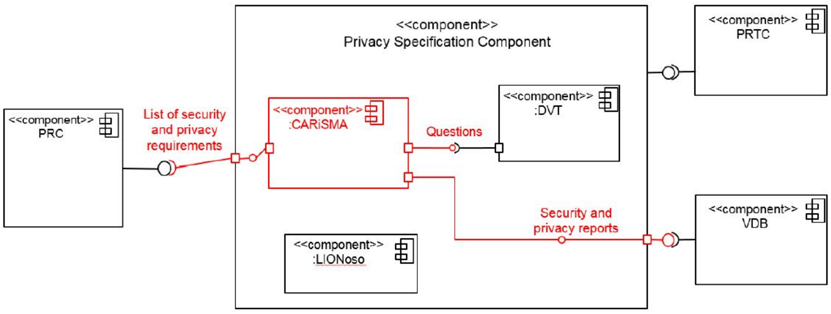

Fig. 3.9 Privacy Specification Component.

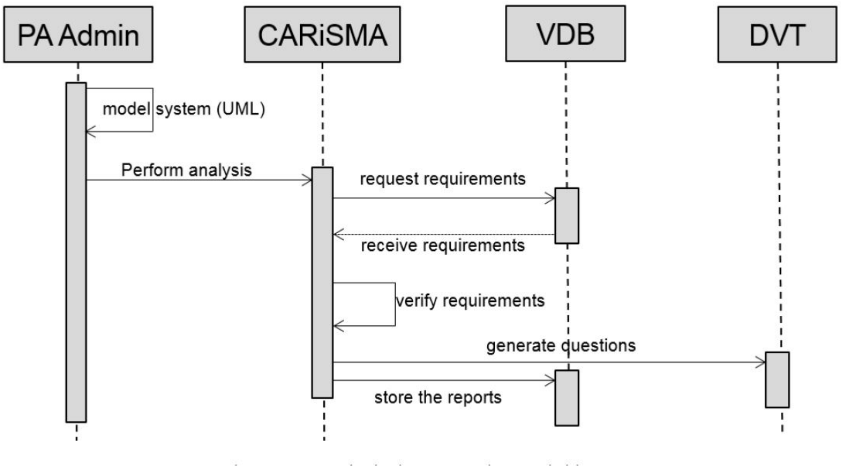

Fig. 3.10 Communications between PSC and the data base (VDB).

Privacy Runtime Component

The Privacy Run-Time Component (PRTC) is a component that will be active during runtime. It provides different functionalities: monitoring of events in the component, monitoring data exchanged between the different pilot users provided by the Media Network Aware Element (MANE) tool and enforcing the PLA by using privacy policies provided by the Privacy Agreement Enforcer (PAE) tool.

As we have explained in the previous sections, the PRTC is in charge of real-time functionalities in the VPP. These functionalities are provided by different tools and include the generation and management of privacy policies, the enforcement of the generated privacy policies, and the process of monitoring data packet transmissions and the generation of usage and access logs. These functionalities are, in fact, the final step of the VPP, and they run continuously within the system of a PA.

As we can see in the diagram of the architecture of the VPP, the PRTC exchanges information with the other components by means of the PLA Database. These interactions are done by only two tools in the PRTC: PAE and LIONoso. The PAE reads the VDB and extracts information of the questionnaires done by the citizens in the PAC. Using this information, the PAE creates the privacy policies and stores them in a local database. Using them, the PAE can control the accesses to the data. The LIONoso tool, on the other hand, exchanges information of the logs of the PAE and the MANE in order to show it to the citizens or public administration.

Regarding internal interaction in the PRTC, the tools work very closely. The PAE, by controlling accesses to the data generates logs about the rules and accesses that are used by both the LIONoso and the MANE. On the one hand, the MANE uses the information of the rules for controlling data packet exchange in the PA system and also generates logs about them. On the other hand, the LIONoso uses the logs generated both by the PAE and the MANE for statistics and information for the citizens and the PA. It requests the information to both tools depending on the time constraint defined for it (the polling can be hourly, daily, etc.). In the following sections we describe more in depth each tool of the PRTC, its functionality and interaction with the other tools.

The Privacy Run-time Component works at run-time, its main goals are:

- Monitoring the events and traffic: this will provide citizens and PAs a way of controlling who is requesting the data, also helping ensure that the privacy preferences set by the citizen are being fulfilled.
- Evaluating the requests concerning citizens' privacy preferences: the main goal is to ensure that the privacy preferences of the citizens control the accesses to data. Therefore, these preferences are considered by the VPP to evaluate received data.

The PRTC is formed by three different tools, which are: PAE, MANE and LIONoso. Each described in more detail in their own section (Integrated Tools).

Figure 3.11 shows the interaction between the tools in the component and how the component reacts to an external request from the PA system. The figure helps explaining the functionalities of the component, which focus on fulfilling the goals, which are the following:

- PAE: enforcement of the privacy preferences. Privacy policies are generated for each citizen according to the privacy preferences provided and all requests to access the protected data are evaluated against the policies. This fulfills the goal of "Evaluation of requests based on citizens' privacy preferences", since these preferences are first transformed into privacy policies and then any received request is evaluated against them.
- MANE: Monitoring and filtering the network traffic. Acts as an extra layer of data protection by applying access rules according to the data received from PAE. This fulfills the goal of "Monitoring of events and traffic", specifically monitoring the network traffic through the platform.
- LIONoso: Monitoring of events by reading and parsing logs of PAE and MANE tools. It extracts features from logs to use as the training data for the history-based

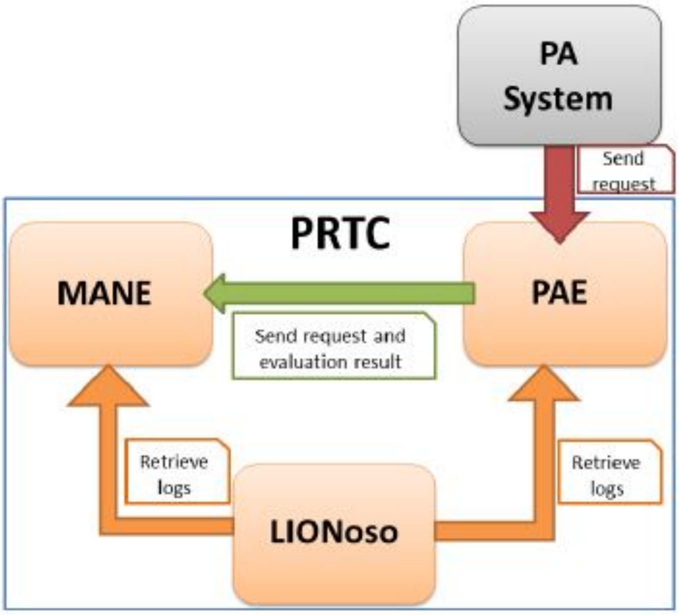

Fig. 3.11 PRTC abstract diagram and interactions.

assessment in the PSC and to display them as notifications in the PVC. This fulfills the goal of "Monitoring of events and traffic", since it will be reading this information from the logs of MANE and PAE.

The PRTC works in the background as part of the VisiOn Privacy Platform. The PA can configure some options of the component, but besides that, it will work by being directly contacted by the PA system to evaluate requests to access citizens' data.

Figure 3.12 displays the component diagram, showing the interfaces exposed by each tool to interact among them and also the interfaces that the component will expose either to other components or to the PA system. As can be seen, there are three interfaces that the component exposes to interact with other components:

- MANE Graphical User Interface (GUI): is the Graphical User Interface that MANE offers. It can be used by the PA administrator to configure MANE or to check information about MANE.
- Evaluate Request: this interface is meant to be used by the PA system to send requests to access citizen's data. The requests are sent to the PAE tool to be evaluated against the privacy policies which were created according to the privacy preferences provided by the citizen.
- Get monitoring results: this interface is provided by LIONoso and it provides all the information it has retrieved and parsed from both MANE and PAE logs. This

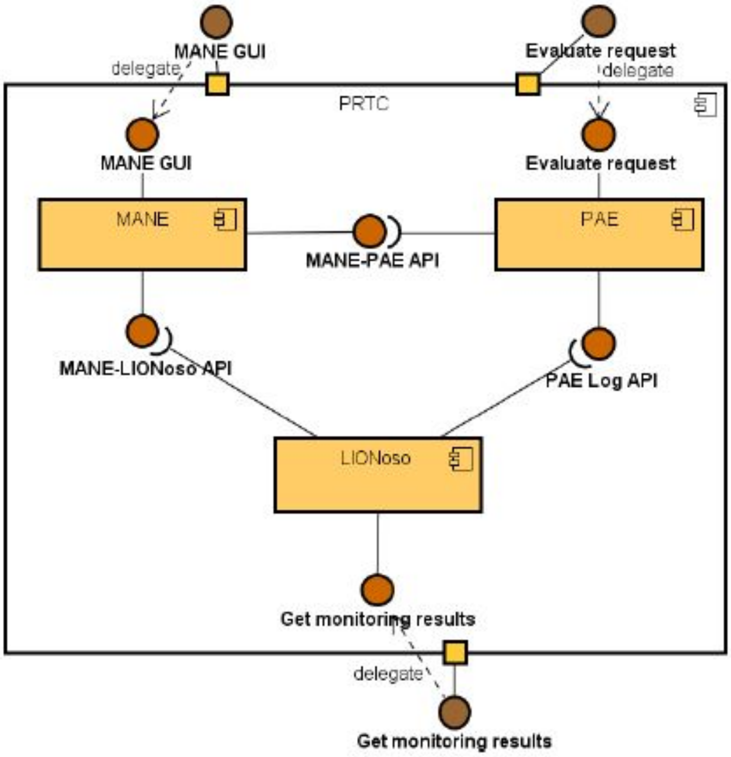

Fig. 3.12 The component diagram of PRTC.

information describes the requests that both tools have received as well as the responses to these requests.

As the figure shows, there are also some internal interfaces which were developed in order to integrate the different tools inside the component:

- MANE-PAE API: this interface is provided by MANE and used by PAE to send the requests and the results of evaluating these requests. This information is then used by MANE to generate network rules.
- MANE-LIONoso API: this interface is provided by MANE and used by LIONoso to retrieve the logs that the MANE tool has generated from monitoring the network access.
- PAE log API: this interface is provided by PAE as an API so that LIONoso can obtain the logs where the information about the requests and the results of their evaluation are stored.

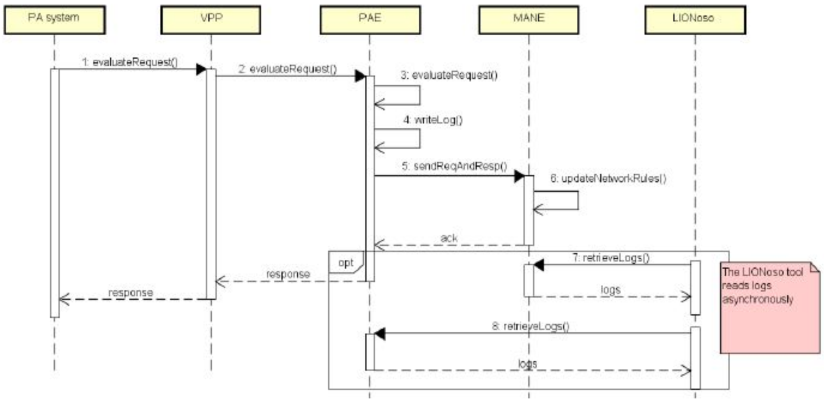

Fig. 3.13 Request Evaluation sequence diagram.

Figure 3.13 demonstrates a sequence diagram to specify how the interfaces displayed in Figure 3.12 are used. There are eight interactions in this sequence diagram that can be explained individually:

1. The process starts when the PA sends a request to be evaluated to the VPP.
2. The VPP, where the PRTC is integrated, redirects the request to the PAE.
3. The PAE takes the request and evaluates it against the correspondent privacy policies.
4. After the evaluation, the PAE tool writes a log including the request and the response (result of the evaluation). This log is made available through the log manager API so that LIONoso can retrieve it.
5. The PAE tool sends the request and the response to the MANE tool through the interface exposed by MANE.
6. The MANE tool receives the request and the response in XACML format, updating its network rules accordingly to the information received.
7. Here starts a process which is asynchronous. This process is started by LIONoso and on this step it uses the interface exposed by MANE to retrieve its logs.
8. To finish the process, the LIONoso tool retrieves the logs of the PAE tool through the log manager API.

As explained in the sequence diagram, there are two different processes: one synchronous and one asynchronous. The synchronous process goes from the first step to the sixth. Part of the process is also the response. This response includes the result of the evaluation of the request against the privacy policies protecting the requested resource. The response is therefore generated by the PAE tool and is sent to the PA system.

Privacy Visualization Component

The VPP has two conceptual subcomponents, which provides user interfaces to citizens and PA administrators. These subcomponents allow the user to select the functionalities of the platform and to enter the data. These are (Figure 3.1):

- The Citizen Visualisation Component (CVC): Guides the citizens to submit or change their privacy requirements using the questionnaire provided by the DAE tool of PAC. Next, it allows the citizen to view the Privacy Level Agreement (PLA) created by the privacy requirements provided by the citizen and the PA. Finally, it displays data value diagrams generated by the Data Value Tool (DVT) of the Privacy Specification Component (PSC) .
- The PA Visualisation Component: Allows PA administrators to monitor the status of the runtime component tools by displaying notifications of Privacy Run-Time Component (PRTC) and to define the questionnaire for the citizen using the DAE tool. This component also includes STS, SecBPMN2, JTrust, SecTro, CARiSMA to manually pre-analyze the system which are part of PRC and Privacy Specification Component (PSC) . These tools have their own interface and they are installed and launched independently.

Furthermore, citizens and PA administrators use Visualization Tool (ViTo) and Data Value Tool, which are directly a part of this component to perform additional visualization functionalities. These tools are implemented as web based tools in order to provide to the citizens and PA administrators online access using a wide range of devices. Therefore, it is not required for the citizens and PA administrators to install third party software and a recent browser will be adequate in order to access the VPP interface.

The Privacy Visualisation Component provides both an input front-end and output front-end for citizens and PA administrators.

- Citizens are able to:
  - submit their privacy preferences using the DAE tool of the PAC,
  - display and download their PLA using ViTo of the PVC,
  - display their data value diagrams using DVT of the PVC.
- PA administrators are able to:
  - create questionnaires using the DAE tool in PAC, pre-analyse system using STS, SecBPMN2, JTrust, SecTro of the PRC, LIONoso and CARiSMA of the PCS,
  - monitor, access and configure using PAE and MANE of the PRTC,
  - display PLAs, data value diagrams and runtime notifications using ViTo and DVT of the PVC.

STS, SecBPMN2, JTrust, SecTro, and CARiSMA are desktop-based tools and have their own user interface. They work independently and store their results directly to the VDB. DAE, MANE, PAE, and LIONoso provide web-based access for the PA administrators integrated as a web-based framework. PVC also provides web-based interfaces, both for input and output to the citizens and PA administrators, to interact with the platform.

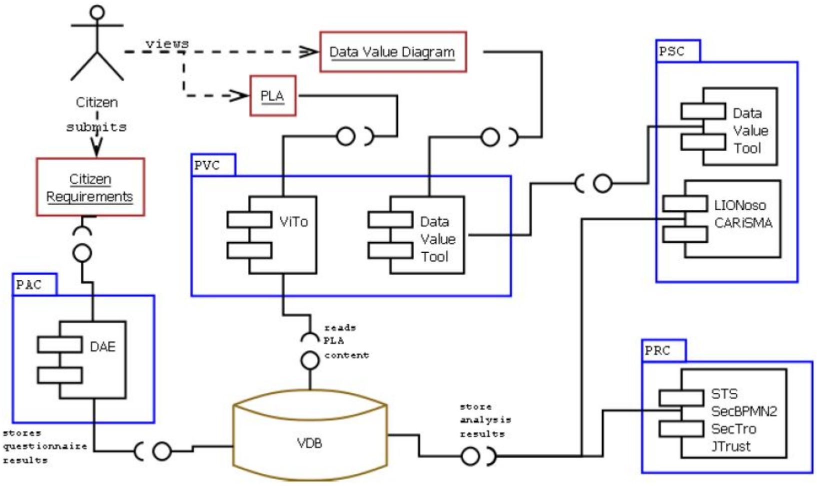

Fig. 3.14 Citizen’s interaction with PVC.

Concerning Figure 3.14, the CVC allows citizens to submit their requirements using DAE tool of PAC, to display PLA created using their requirements and PA system analysis results in ViTo and to display their data value diagrams created by DVT in PSC . As presented in Figure 3.14, PVC interacts with PSC directly and interacts with PAC and PRC via VDB. Citizens describe their privacy requirements using DAE tool in PAC. Their requirements are stored in VDB and later displayed them as a part of their PLA. DVT primarily operates in PSC and stores its results in VDB and displays data value diagrams to the citizens in PVC. PRC and PSC analysis tools store their results in VDB and PVC displays these results as a part of PLA of the citizen. PVC assists the citizen to interact with the VPP easily from one central interface.

Concerning Figure 3.15, the PA Visualization Component carries out the visualization tasks of the PA administration of the platform. It directly interacts with PA administrators and allows them to perform the following tasks:

- It provides a page to list PLAs of all the citizens who submitted their privacy requirements by filling the questionnaire.
- It provides a page to list all the notifications extracted by log monitoring of the tools in the PRTC.
- It allows to create and update questionnaires via DAE in PAC.
- Tools of the PRC and the PSC are accessible independently to perform the analysis.

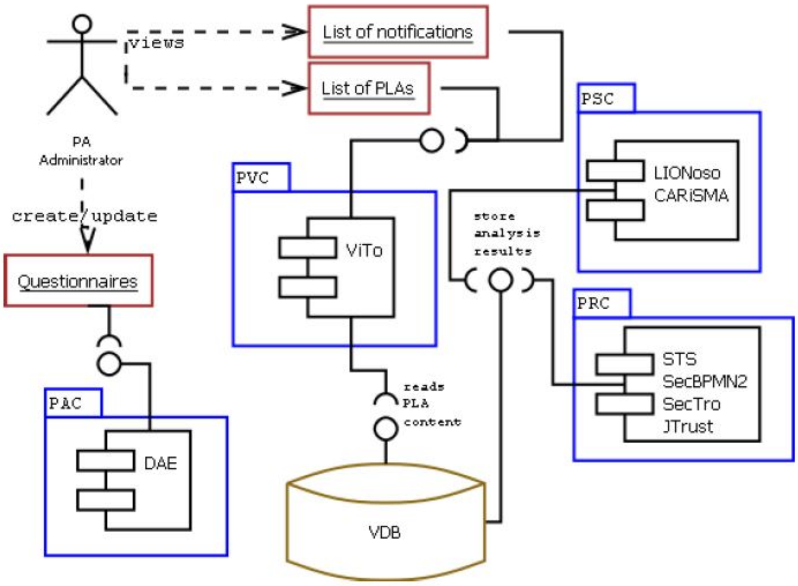

Fig. 3.15 PA's interaction with PVC.

3.2 Integrated Tools

DAE

In companies, many different questions have to be answered during the normal business or especially during audits. Mostly a single person cannot answer these upcoming questions. Therefore, Fraunhofer ISST has developed the DAE to lower the staff time and effort, which is needed to delegate questions and gathering the information. DAE tool of the Fraunhofer ISST will perform the elicitation of the user privacy needs using as basis for the information input the data provided from the public administrations.

STS-Tool and SecBPMN2

Socio Technical Security-Tool (STS-Tool) (developed by the University of Trento) [5, 4] is a software for enforcing social and organizational security requirements in business processes. It permits to (i) specify social and organizational security requirements using a goal based modelling language, (ii) specify business processes with security concepts using an extension of BPMN 2.0; (iii) verify the enforcement of the security requirements in the business processes; (iv) generate security documents that contain the information specified in the models and the results of the analysis. STS-Tool already integrates SecBPMN2 as a plugin. The STS-Tool can be used to address many issues related to privacy.

Analysis of complex organizations: Many PAs are complex organizations composed by technical components and people. In such organizations the verification of the enforcement of privacy requirements is a complex and error-prone task. The STS-Tool can be used to automate this task, remarkably reducing its time of execution and eliminating the errors that a person may commit. Fast adaptation to external changes: The automated verification of privacy allows a fast adaptation of the PA organizations when security requirements change because of external factors. For example, when a law on privacy is modified, a modification of the security policies on privacy is enough to check if the PA organization is compliant or it shall be adapted. Moreover, the STS-Tool indicates where the security issues are, and therefore, it helps security analysts in identifying the problem and, therefore, in solving it.

Within the VisiOn Privacy Platform, STS-Tool can be used as part of requirements engineering, having its derived (social) security requirements translated/mapped to technical security/privacy specifications, to ease the transition from the requirements phase to the system design phase.

Sectro and JTrust

Secure Tropos (developed by the University of Brighton) [6] is a security-aware software systems development methodology, which combines requirements engineering concepts, such as actor, goal, plan together with security engineering concepts such as threat, security constraint and security mechanism, under a unified process to support the analysis and development of secure and trustworthy software systems.

The idea is, for Information Technology (IT) related users that work for public administration organizations, to use SecTro and identify privacy related threats and; vulnerabilities that exist in their systems. Moreover, the tool identifies the appropriate security and privacy mechanisms that are necessary in order to protect their systems against the identified threats. To this end, SecTro will support the PA IT employees with a library of privacy threat pat-terns and also a library of PET that mitigate privacy threat. Additionally, SecTro will feed the Privacy Visualization Component with information about privacy threats and then be presented to the citizen/patient in a user friendly and understandable way.

The JTrust tool (provided by the University of Brighton) is a graphical editor supporting the modelling of trust and control, and the automatic assessment of system's trustworthiness in the JTrust methodology. The tool supports modelling of system dependencies, resolutions, and entailments, and performs an automatic assessment of the system's trustworthiness based on the identified system dependency resolutions.

The idea is that IT related users that work for Public Administration organizations to use JTrust in order to model the privacy related trust relationships that affect the trustworthiness of their systems in terms of ensuring privacy. Then, to reason about these trust relationships in a structured way and to identify technical or organizational controls in cases where there are gaps of trust in order to ensure that data privacy is pre-served.

LIONoso

LIONoso (developed by the University of Trento) is a platform for data analytics that focuses on visualiza-tion, modelling (predictive analytics) and optimization (prescriptive analytics). In the setup phase, the user defines a workflow (by means of a visual tool) by combining various modules for data input and manipulation, model creation (factories), prediction and optimization, visualization. The workflow structure can then be hidden from the final user, who can use LIONoso as a black box that reads or receives data from a source and produces graphical and textual reports, predictions and recommendations.

Within the VisiOn Privacy Platform, LIONoso will be used to: (1) Verify the compliance of a PLA with a set of rules representing the relevant EU privacy laws, and (2) try to identify potential problems that a citizen could face during his interaction with the PA by examining past cases of citizens with similar privacy requirements. In the latter context, LIONoso will complement rule-based tools by providing an additional heuristic evaluation, which will prove useful in reducing potential grey areas and will help assess novel cases.

CompliAnce, Risk, and Security Model Analyzer (CARiSMA)

Modelling allows the design of high-quality critical systems and identification of security requirements/properties during the design time in order to provide a natural integration of security in the system. CARiSMA [3, 1, 2] provides an opportunity to perform compliance analysis, risk analysis and security analysis of software models. Generally, CARiSMA provides a platform to model system architectures using UMLsec diagrams. Moreover, it supports and implements UMLsec checks. Due to its EMF-based implementation, CARiSMA can also support domain-specific modelling languages such as BPMN. A flexible plugin architecture makes CARiSMA extensible for new languages and allows users to implement their own compliance, risk, or security checks. In the VisiOn platform, CARiSMA is used to perform a security and privacy analysis. The PA system architecture is modelled as a UML diagram, afterwards the UML diagrams are annotated with security and privacy requirements. The CARiSMA performs different security and privacy checks to verify

PA systems. At the end CARiSMA generates a report, informing about the security and privacy threads and vulnerabilities.

Media Network Aware Element (MANE)

MANE (developed by NCSRD, National Centre for Scientific Research "Demokritos") is capable of applying Deep Packet Inspection (DPI) for packet filtering at both the network and the application layer. The DPI approach indicates that network flows are inspected and information is extracted from higher layers of packet data (up to the application layer). By exploiting the rich high layer information that is provided through DPI, contents' aware network node control functions can provide various options in packet flow handling, for in-stance, information about the enforcement of privacy policies. NCSRD's DPI software called MANE can locate, identify, classify, reroute and block packets with specific payload, something that is not possible with conventional packet filtering techniques that assess only packet headers.

MANE is extended to accept and parse VisiOn privacy policies in the format that they will be submitted. Additionally, they will have to be translated from the privacy policy format into real time network traffic rules, and be applied accordingly.

Privacy Agreement Enforcer (PAE)

The PAE (developed by ATOS) provides two main functionalities. On the one hand, it provides functionalities for managing users' privacy policies, allowing them to create, remove and modify the level of privacy protection that they want to apply to their personal information. On the other hand, it has an engine in charge of ensuring that any given request trying to access a protected resource has to comply with h the policies that have been described by the owner of that information, granting access only when these policies are satisfied. PAE will be extended in VisiOn in order to allow users who do not have knowledge about XACML to also be able to manage their XACML privacy policies. In addition, PAE will protect private data by providing accesses only to authorized users and complying with the privacy policies defined by the data owners.

Data Value Tool (DVT)

Data valuation is the process to identify which information is most important and most valuable. In others words, it is a promise of value to be delivered and a belief of the receiver that the value will indeed be delivered and experienced. Personal data valuation is a complex and difficult task and while no commonly accepted methodology exists, two main approaches can be identified:

- market valuation of the data, i.e. market cap/revenues/net income per data record, market prices for data, cost of a data breach, data prices in illegal markets are some of the proposed methods to estimate the value of personal data.
- individual perceptions of the data value, i.e. surveys and economic experiments used to estimate the individual valuation of personal data and the individual valuation of privacy.

In VisiOn project the DVT aims to capture the perspective of citizens in regards to the data they are willing to share and the importance they have about these data and compare this with both the PA's expectations and average users' perspective. To achieve its goals, the DVT uses the VisiOn questionnaire to gather input from both the PA and the citizens, calculates metrics based on the answers and visualizes the results to the users.

3.3 VisiOn Database

The PLA is one of the central elements of the VPP, since it will contain, for each citizen, her privacy preferences and other useful information to be used by the PA when accessing her data. For this reason, it is required to have all the PLAs centralized in a database where all the different components of the VPP can access it, either for adding new data or for managing it.

With this in mind a database was created to contain all the information required to generate a PLA for each citizen, providing an API that all tools could use to access it easily. The database will store two different types of documents: specific for the PA and specific for each citizen. The documents specific for the PA will contain information about the system that the PA uses, such as models.

The VPP consists of different tools that generate outputs with variable types. Therefore, it is important to use a storage system that can handle large files, several formats, and multi-structured data types. One typical solution is using non-relational databases to meet these requirements. Although there are many different solutions, MongoDB distinguishes between these solutions by being easy to install, having support in many different languages and frameworks, having a permissive commercial license to use, and high popularity, which makes it have a big community. It is the fourth most popular database management system in overall, and most popular for document stores according to DB-Engines Ranking.

MongoDB simplifies storage of various models created by the tools in the platform by being a document-oriented database. Document-oriented databases are general purpose, useful for a wide variety of applications due to the flexibility of the data model, the ability to query on any field and the natural mapping of the document data model to objects in modern programming languages.

MongoDB is also an agile database that uses a flexible document data model so schemas can change quickly as applications evolve. This flexibility allows us to write and read information in various formats to the database and adapt the document model to our needs easily.

For the integration process this flexibility that MongoDB provides is very useful, but at the same time the capability of storing large files is perfect for the VPP, since it will store different kinds of documents, such as models, which can get potentially very large. To be able to provide easy access for all the components of the VPP to the PLA database a REST API was created. This RESTful API provides different functions to create, read, update and delete data from the database.

Having an API instead of allowing direct access to the database is helpful for security reasons, making components database agnostic so that if any details about the database are modified the components will not require any further modification since the API will stay the same.

3.4 Vision Framework

When designing the VPP, we noticed we had very different tools with different objectives and that providing all of them in a single framework (e.g. same technology, usage, etc.) and, after several discussions, we decided it would be better to have different frameworks due to the nature, characteristics and goals of the different tools we have in VisiOn. This way, we have tools that were desktop base (heavy-processing) and other were web-based (accessible from any location at any time). Therefore, the web-based framework could cover all the tools for working with the generation and management of the privacy preferences, reports, data value, etc., which by being online would improve vastly the impact and usability of the platform. On the other hand, the desktop-based framework contains the tools for modelling and generation of privacy reports of the system, so they could fit better to be used in a desktop by expert users.

Together with these two frameworks we need a back-end that provided all the interfaces for communication between the component and tools and a database that was created for facilitating the exchange of data between them. This database provides an API that the tools and components use for storing and retrieving data, allowing an easier and faster communication between the two frameworks (web and desktop). The design of the two frameworks and the back-end followed the architecture defined in Figure 3.1, as it clearly identified the interactions between the tools and components, and the list of the VPP requirements. That way, these two frameworks cover all the necessities of the Public Administrations and citizens in an easy and simple way. Following we describe more in-depth each of the frameworks and the back-end.

VPP Back-End

The VPP back-end provides all the internal functionality, interactions and exchange of data in the VPP, more specifically for the two frameworks developed in the project: web and desktop frameworks. Therefore, it provides a database (VisiOn database) that is used for storing and retrieving data by the tools of the VPP components. This way tools can exchange data as they need and it is also used for generating the PLAof each citizen, as it contains all this data provided by the tools. The access and interaction with the database is done by means of an API, which aims to facilitate the work with the database and also makes easier to create new functionalities for the database or modify the existing ones. This component acts as a pivotal element for interconnecting the tools, components and framework as can be seen in the Figure 3.1 of the architecture of the VPP.

Web Framework

Web applications allow users to access universally from any computer with and Internet connection and a browser supporting latest web technologies without requiring any prior installation. For these reasons, tools that are part of assessment, runtime and visualization components are integrated as a web framework to allow citizens and PA administrators to access the platform easily. The web framework will be used by several users, both citizens as well as members of the PA. To control the access to the different functionalities of the platform it was deemed necessary to include an authentication and authorization mechanism.

Desktop Framework

The VisiOn Desktop Framework integrates the components and tools more heavy-processing that are used by the PAs for modelling. This framework runs in the computer of the Public Administration and allows it to design and specify privacy and security analysis of their system (either new or existing one) in order to a) obtain information about privacy issues that will be used in the creation of questions later in the VisiOn Web Framework and b) provide security and privacy reports of the system of the PAs. The VisiOn Desktop Framework is connected with the VisiOn database in order to exchange data and communicate with other tools and components of the VisiOn Web Framework.

The usual work with this framework done by the PA is as follows, although it is not mandatory to do it in this way or even go through all the tools. Each of them provides a report with specific characteristics and descriptions of the system under development or existing so it depends on the PA which tools they want to use. Through the tools that belong to the Privacy Requirements Component, the PA can use the STS tool to identify and collect privacy requirements and the SecBPMN2 tool to check the compliance of the business process with procedural privacy policies. Then, with the usage of the SecTro tool the PA can analyze privacy threats and identify system vulnerabilities. The use of SecTro also allows the PA user to define appropriate privacy related organizational actions and technical controls that satisfy privacy requirements and mitigate threats. Finally, the PA can use the JTrust tool for privacy related trust relationships, mitigation actions and organizational actions.

In addition, the desktop framework will support the Public Administration (PA) in the system design. In particular, through the Privacy Specification Component, the PA can use the CARiSMA tool to perform proper privacy and security checks in order to analyze the system design and architecture. To this end the PA requires the PA's system models and the SRS file generated by the STS tool, which contains the list of security and privacy requirements. The system models are expressed as UML diagrams that the PA can annotate with relevant security and privacy requirements and perform the checks. Finally, through the LIONoso tool, the PA can check the compliance of the requirements with the legal regulations, and through Data Value Tool the PA assesses the value of given citizens' personal data (e.g. data footprint, economic value, data conflicts, etc.)

References

[1] Amir Shayan Ahmadian et al. "Model-Based Privacy Analysis in Industrial Ecosystems". In: *Modelling Foundations and Applications - 13th European Conference, ECMFA 2017, Held as Part of STAF 2017, Marburg, Germany, July 19-20, 2017, Proceedings*. 2017, pp. 215–231. DOI: 10.1007/978-3-319-61482-3_13. URL: https://doi.org/10.1007/978-3-319-61482-3_13.

[2] Amir Shayan Ahmadian et al. "Model-based privacy and security analysis with CARiSMA". In: *Proceedings of the 2017 11th Joint Meeting on Foundations of Software Engineering, ESEC/FSE 2017, Paderborn, Germany, September 4-8, 2017*. 2017, pp. 989–993. DOI: 10.1145/3106237.3122823. URL: http://doi.acm.org/10.1145/3106237.3122823.

[3] Jan Jürjens. *Secure systems development with UML*. Springer, 2005. ISBN: 978-3-540-00701-2. DOI: 10.1007/b137706. URL: http://dx.doi.org/10.1007/b137706.

[4] Elda Paja, Fabiano Dalpiaz, and Paolo Giorgini. "{STS}-Tool: Security Requirements Engineering for Socio-Technical Systems". In: *Engineering Secure Future Internet Services and Systems*. Springer, 2014, pp. 65–96.

[5] Elda Paja et al. "Specifying and reasoning over socio-technical security requirements with sts-tool". In: *Conceptual Modeling*. Springer, 2013, pp. 504–507.

[6] Michalis Pavlidis and Shareeful Islam. "SecTro: A CASE Tool for Modelling Security in Requirements Engineering using Secure Tropos". In: *Proceedings*

of the Conference on Advanced Information Systems Engineering (CAiSE) Forum. 2011, pp. 89–96.