CHAPTER 9

Vacation Planner Application

"The patterns are simple, but followed together, they make for a whole that is wiser than the sum of its parts, Where Good Ideas Come From: The Natural History of Innovation

—Steven Johnson

This chapter presents a vacation planner application that utilizes a privacy component that has already been developed, tested, and implemented. A large hospitality company requires a system to help its customers plan a vacation at one of their hospitality sites. The system will support both a telephone call center and a web site. The privacy component will be invoked by this new system to ensure that privacy policies are enforced. Additionally, this example will explain the privacy requirements and fair information privacy principles as they operate as functional specifications and quality control measures. The privacy engineering methodology steps are followed and the process of development is shown in more detail. This example scenario is based on a major project at a well-known hospitality company.

Requirements Definition

As a result of a scoping workshop, the first step would be to draw up a context diagram (Figure 9-1). Although the focus would be on the order entry portion of the system, the context diagram shows the major actors of the system as a whole.

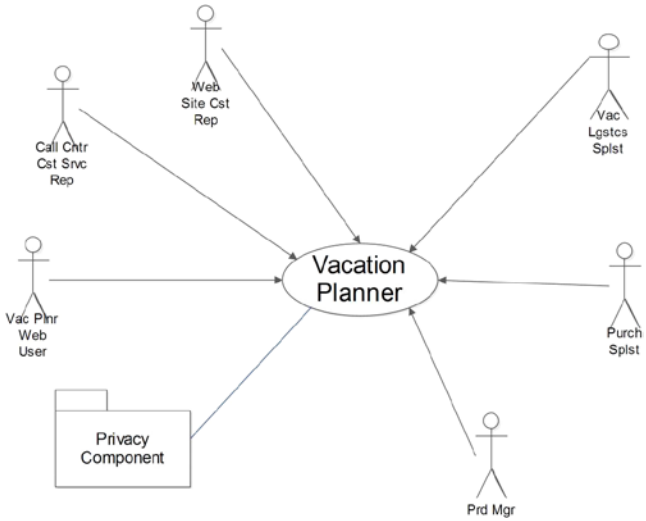

Figure 9-1. *Vacation planner context diagram*

Use Case Metadata for Hospitality Vacation Planner Enterprise Application

The privacy engineering methodology steps, as described in Chapter 6, are followed to start production on the vacation planner app.

- *Why:* Motivation—Vacationer wishes to order a planned vacation package.
- *Who:* Actors:
    - Vacation planner web user
    - Call center customer service representative (vacation planner)
    - Web site customer service representative
    - Vacation logistics specialist
    - Purchasing specialist
    - Customer credit specialist
    - Product manager
- *When:* Events:
    - Customer interface related:
        - Customer call
        - Customer selects vacation package

        - Customer enters order on web site
        - Customer receives credit approval
    - System related:
        - Customer service enters credit information
        - Credit check system invokes privacy component
        - Customer order system invokes privacy component
        - Order provisioned
- *How:* Processing or behavior:
    - Update customer credit data
    - Privacy component processing (see Privacy Component Use Case in Chapter 7)
    - Update customer order database
    - Process order
- *What:* Data:
    - See Customer Order data modeling, including Big Data Data Block (Figure 9-5)
    - Privacy component data model (Figure 9-4)
- *Where:* Location:
    - Call center
    - Hospitality locations

Additionally, in this example the enterprise business rules, including the privacy rules, are required for consistent integration with the enterprise:

- Customer call center business rules
- Web site business rules
- Credit check business rules
- Customer order business rules
- Customer credit check privacy rules
- Customer order privacy rules
- Customer order provisioning rules

Develop Business Activity Diagrams

Business Activity Diagram for Scenario 3: Vacation Planning

The business activity diagram in Figure 9-2 shows the events, processes, and decision making for the various business processes involved in supporting a vacation planning app. The diagram shows the call center's functionality, but the web site would also have that same functionality.

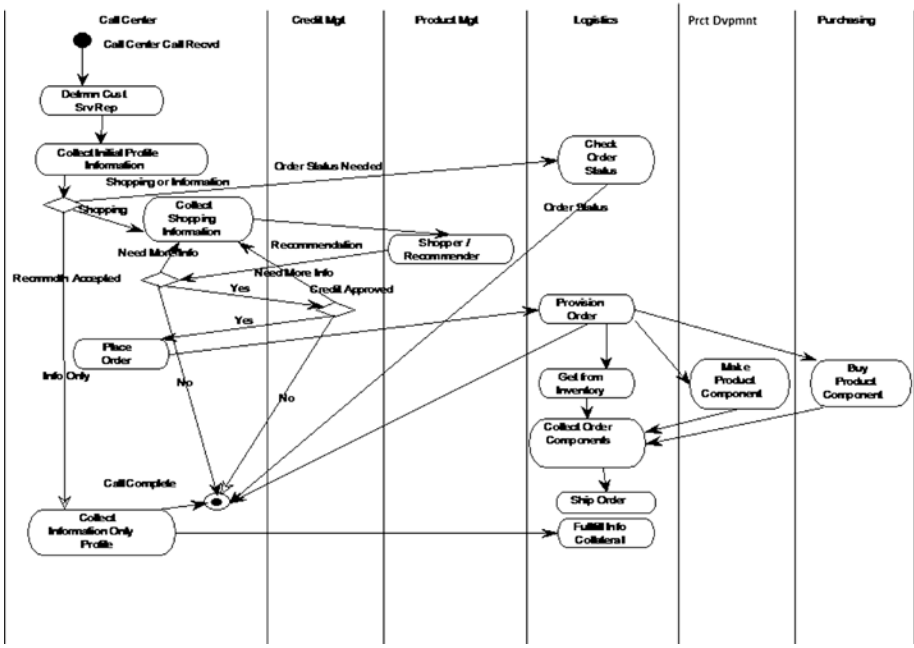

Figure 9-2. *Business activity diagram for the vacation planning app*

Activity Diagram Used as a Part of Privacy Assessment

The privacy team works with business stakeholders, including data stewards, to identify key data attributes, especially identifiers, within the business processes represented on the business activity diagram (Figure 9-3). Privacy rules will be developed for these and other attributes as found and entered in the metadata.

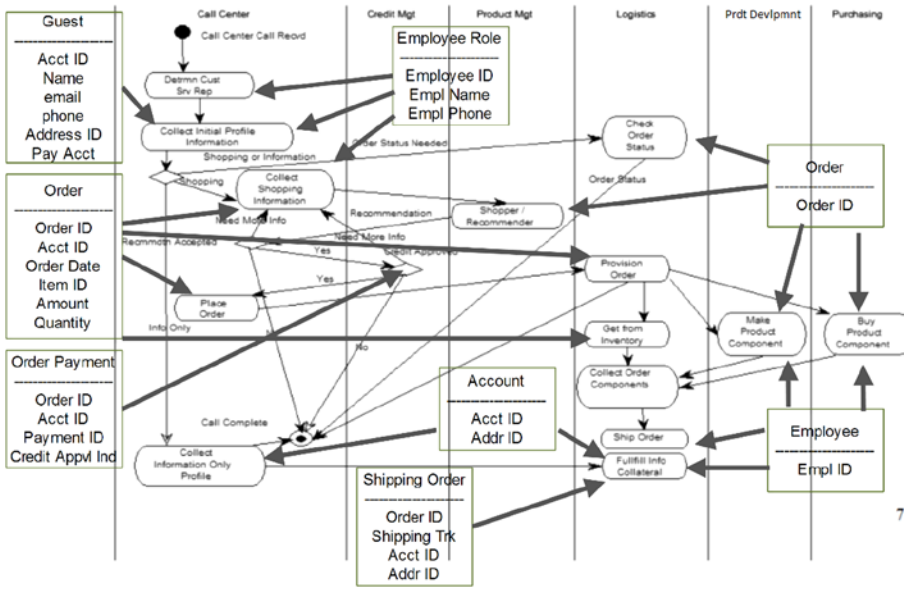

Figure 9-3. *Business activity diagram with key data attributes*

Privacy Component Class and Data Model

The privacy component class and data model (Figure 9-4) contains the overall data requirements for the vacation planner application. For illustration purposes, an additional, simplified portion of the vacation planner data model focusing on customer order entry is shown in Figure 9-5.

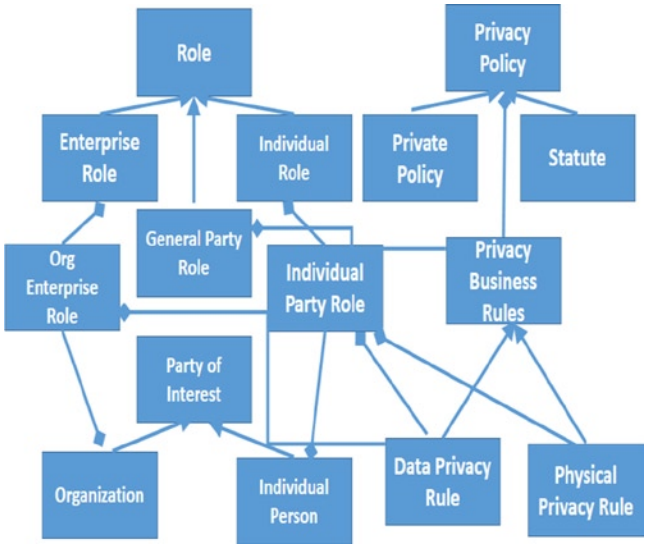

Figure 9-4. *Privacy component class and data model*

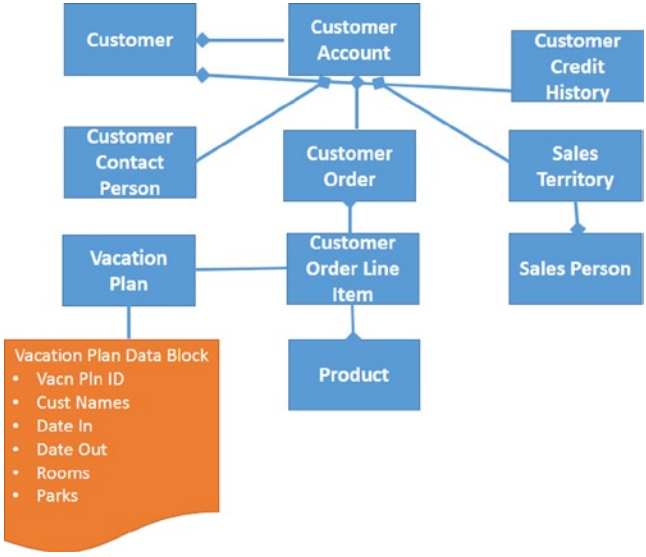

Figure 9-5. *Simplified customer order data model for the vacation planner app*

As discussed in Chapter 7, the privacy component class data model is used to design the database for both the privacy component (scenario 1) and as a part of the database in the vacation planner (scenario 3). The model shows the various roles played by parties of interest, whether that is an organization entity or an individual person. The privacy

rules are based on privacy policies that are related to the various role types. The vacation planner application invokes the privacy component as it deals with roles such as a customer or perhaps a contact person, sales person, or employee.

The data model presented in Figure 9-5 will be used to design the system database. The *Customer Person* is an *individual person* playing the *Individual Party Role* of *Customer* (or in the hospitality company, *Guest*). The *Customer Order* will contain a combination of *products* within a *Vacation Plan* developed from unstructured vacation planning data organized into a big data data block contained in one or more *Customer Order Line*. The *Sales Person* is another *individual person* who serves as a customer service representative. As a part of the order processing, a *credit history* check is performed.

Vacation Planner User Interface Requirements

The *customer*, also called *guest* at some hospitality companies, would either call into a call center or sign on to a web site. The *customer* can then decide whether he or she wishes to review the Privacy Notice. The *customer* would indicate what *vacation plans* he or she wishes to have. The *customer* would then enter information about him- or herself and the other members of his or her party. In this case, *privacy* rules may apply and the privacy component would be invoked. Once the *vacation plan* is fully defined, the *customer* will be asked to pay for the package. The *customer's credit history* will be checked and *privacy* rules may apply. If the customer passes the credit check, the *vacation plan order* will be entered. The *vacation plan* will go through a provisioning process. When the plan is provisioned, the *customer* will get a notice of approval and the *vacation plan* is made available for saving or printing.

HOSPITALITY GAMES

By Tom Finneran

Let's say that a hospitality enterprise develops a game based on their attractions, rides, shows, and movies. If the game appeals to children who are under 13 years of age, the Children's Online Privacy Protection Act (COPPA) applies in the United States. (There may be similar laws in other jurisdictions.) COPPA provisions regulate web sites upon which personal information of children under 13 years of age is likely to be collected. Therefore, if our hospitality enterprise wants to offer games to potential young *guests,* a set of privacy rules will need to be entered into the privacy metadata model so that our privacy component can enforce rules required by COPPA. The rules would require that:

- The clearly written privacy policy must be included in the Privacy Notice. Access to the Privacy Notice must be on the web site's home page and at each area where the site or online service collects personal information from children. The Federal Trade Commission (FTC) encourages that a privacy policy for a mobile app be posted by the Internet store at the point of the app download.

- There must be a description of the kinds of information collected from children, for example, name, address, e-mail address, hobbies, and age. This requirement applies to all information, not just personal information.
- There must be an explanation of how the data are collected, whether directly from the child or behind the scenes through "cookies."
- There must be an explanation how the web site operator uses the personal information, such as marketing to the child or notifying contest winners, and whether personal information is disclosed to third parties.
- Parents are given the web site operator's address, phone number, and e-mail address, including anyone who would be collecting or maintaining the children's personal information.
- There must be the capability for the parent to give consent before collecting, using, or disclosing personal information about a child.
- If parents don't consent to their child's personal information being processed, there must be the capability to search and delete the child's information from all systems under the enterprise's control.
- There must be the capability for parents to review and delete information about their children collected by such services.
- There must be reasonable procedures "to protect the confidentiality, security, and integrity of personal information collected from children."

COPPA is a very complicated law. This summary is insufficient for developing a complete set of privacy rules. The FTC maintains updated guides to COPPA on their web site.[1]

Other privacy rules over and above COPPA would be needed to complete the privacy engineering of these game applications.

[1]Available at www.business.ftc.gov/privacy-and-security/childrens-privacy.

Design the Vacation Planner Solution

The Vacation Planner Solution Architecture

The vacation planner use case along with the data identified in the overall vacation planner data model and the vacation planner user interface requirements should be used to develop the user interface architecture. The complete vacation planner class and data model, including the information outlined in Figures 9-4 and 9-5, constitutes the information architecture. We'll discuss the development of the application architecture in the next sections, but Figure 9-6 provides an overview.

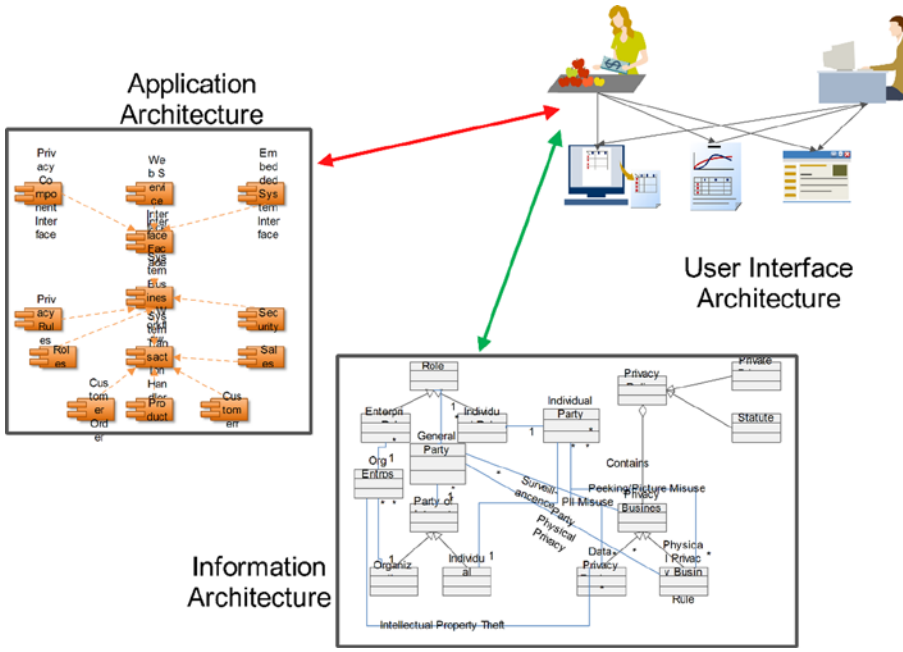

Figure 9-6. *Solution architecture example*

The Vacation Planner Component Architecture Structure

The vacation planner app can be developed using the component architecture approach discussed in Chapter 6. The component interface utilizes a database designed from the information architecture discussed previously. The component interface will also have a user interface that is used either by a call center representative or by the customer accessing the web site. The vacation planner use case shows several events and behavior processes that the event handler and the behavior processing will execute.

Develop System Activity Diagrams

The UML activity diagram is a workflow diagram used to model sequential aspects of a business process or system and the parallel and sequential interactions between use case actors. The activity diagram shows the interaction of the various role actors with system actors within each use case.

Figure 9-7 shows that the development team, including the privacy team, begins the process by developing the Privacy Notice and privacy rules that are entered into the privacy component. They also determine and implement the encryption mechanism. The system user invokes the privacy component to make a Privacy Notice decision and to manage security. The call center representative or the web site user enters, maintains, and corrects personal information according to privacy rules managed within the privacy component. The user will then review the vacation plan alternatives, choose a plan, and buy it with a credit checked card. The provisioned plan will then be submitted. The privacy component will periodically run the archiving rules. The diagram in Figure 9-7 is also used to ensure that all privacy principles are covered by the vacation planner system.

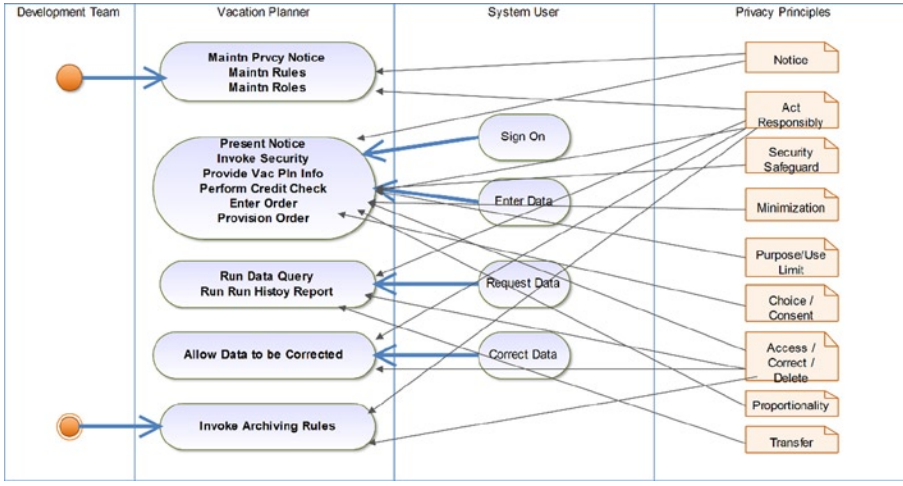

Figure 9-7. *System activity diagram of vacation planner app with tie to privacy principles*

Dynamic Modeling

Figure 9-8 is a simplified UML sequence diagram showing the entry of an order for the vacation planner using the privacy component.

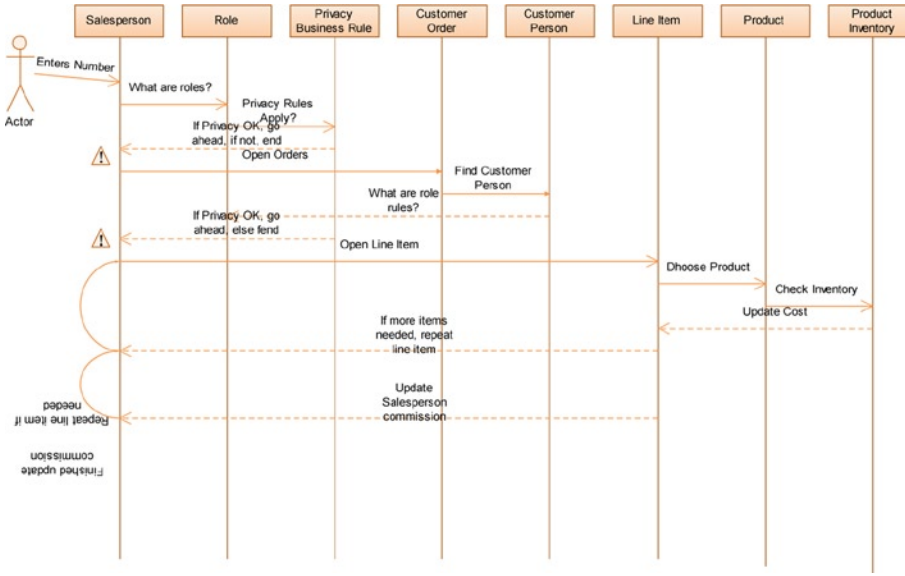

Figure 9-8. *Customer order sequence diagram*

Figure 9-9 is a zoomed-in version of part of Figure 9-8, drawn larger to improve readability. The actor, who is either a call center customer service representative or the web site application component, enters an order number identifying the order. The role of the actor is determined and verified. Next, it must be determined whether privacy rules apply. The privacy component is invoked using the privacy component data model. If privacy rules are satisfied, the flow goes forward. Otherwise, an error is flagged. If the flow goes forward, the order is opened. Next, the customer contact person and his or her role is determined. Privacy rules' analysis is invoked to ensure that privacy rules for the customer are protected. If so, the process moves forward and the transaction sequence is completed. Otherwise, an error is flagged.

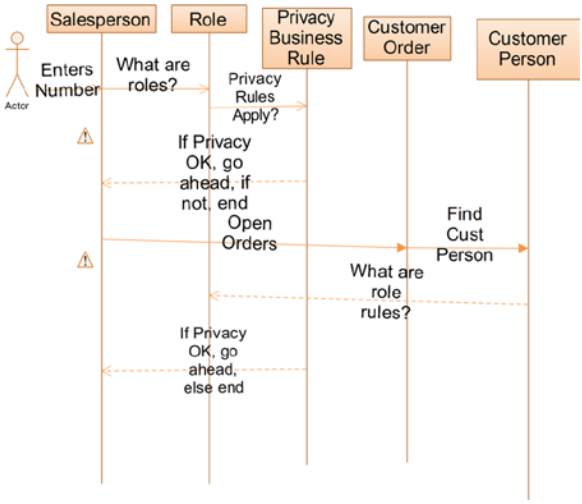

Figure 9-9. *Entering customer orders and related privacy rules in a vacation planner transaction*

Before the privacy component can be used, privacy rules for each role type need to be entered by privacy team members working with data stewards from the various business units and information technology system administrators. As stated before, these privacy rules are based on privacy policies and policy processes, procedures, guidelines, or standards.

Farther along in the vacation planner transaction, the actor will need to enter the names of persons who will play the role of guests. The guest role will have one or more privacy rules included as metadata including creation rules. When entering an order, it must first be determined whether any of the named persons who will be guests at the hotel(s) or park(s) already appear in the enterprise database. If a customer is a returning customer, the system would display the data currently held about the person and give the user the chance to make any corrections. FIPPS/GAPP suggests that a person should have the ability to make such changes. "Maintain Guest" business and privacy rules (examples of customer order business and privacy rules) should govern. They are rules that cover changes to Guest information.

If the person is new to the system, he or she is assigned the role of "Guest" with this order. This event will trigger decisions using the "Create Guest" privacy rules. According to FIPPS/GAPP, the privacy component should offer the ability to review the Privacy Notice. Once the Review Privacy Notice processing is completed, the Enter Guest Information processing begins. If the input is through the user interface, the call center guest representative, whose authorization has been verified, enters the guest data. When the data have been entered through the hospitality enterprise's web site, it will be entered by the guest or the guest's representative.

Both enterprise and statutory influenced policies govern the gathering of the data being entered. Under FIPPS/GAPP, the hospitality enterprise must:

- Ensure that there is a reason for every attribute of data being collected.
- Ensure that the guest or the guest's representative can consent to the personal information being collected. If the guest or guest representative does not consent, the guest has made an implied choice to not place the order.
- Be accountable for the process and procedures that may process the data.
- Collect only the minimum amount of data necessary to achieve the legitimate purpose of the hospitality enterprise. This includes the use of these data for ongoing marketing purposes. The use of data for these purposes should be explained in the Privacy Notice.
- Limit data collection wherever possible proportionate to the need, purpose, and sensitivity of the data being collected.
- Retain the data only as long as it is useful. This implies there is a reasonable archiving strategy.
- Adequately protect any data transferred to third parties for uses explained in the Privacy Notice to create an implied consent for such transfers. Encryption may be used as part of this process. Authentication and authorization are other parts of the process.

In the case of the hospitality enterprise mentioned, there was an enterprise business privacy rule that data would be encrypted when stored and whenever transferred to third parties. Therefore, when the guest data were entered, an encryption indicator would be set. If the guest being entered is a child, additional rules, both private and statutory, must be taken into account.

Once all of the guest's data have been entered, the guest representative or the web site will ask if there is another guest to be covered under this order. If this is the last guest to be entered for this order, the remaining data needed to complete the order will be entered. If, however, there is an additional guest, the Create Guest process will be repeated.

Define Service Components and Supporting Metadata

The privacy component can be seen as a component containing several subcomponents. For instance, although Figure 9-10 would reflect a simplified component design for the vacation planner app, that scenario does contain the embedded privacy component. The privacy component interface, the privacy rules, the roles, and the security components on the diagram are actually subcomponents of the privacy component.

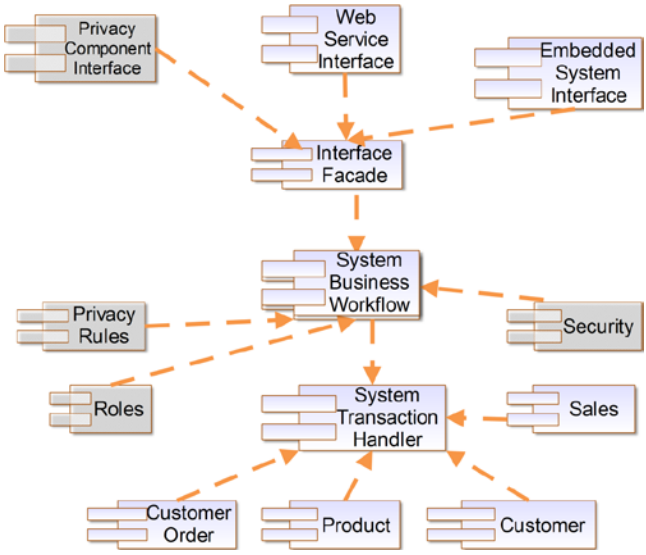

Figure 9-10. *Sample component diagram*

Using the System Development Methodology

It is recommended that the steps described in Chapter 6 should be followed completely. This methodology with an Agile overlay was used with great success on a similar project.

Conclusion

This chapter discussed the vacation planner application as an example of the complete use of the privacy engineering methodology for an enterprise system that invokes the privacy component. When the privacy component is used, enterprise system modifications for privacy rule alterations, whether due to statute, regulation, or enterprise policy changes, will be made in a single component and available to the entire embedding system. Chapter 10 discusses Privacy Engineering quality assurance.