11.5 Non-Repudiation Requirements

A non-repudiation service must satisfy a set of requirements for both the service and the quality of service. The function of non-repudiation is to capture and maintain evidence so that the participants of a transaction or interaction cannot deny having participated in that activity. While each situation that calls for non-repudiation is unique, there are common generic requirements that apply to all non-repudiation situations. This pattern provides a common generic set of non-repudiation requirements. The pattern also helps you to apply the general requirements to your specific situation, and helps you to determine the relative importance of conflicting requirements.

Example

The museum seeks to increase the publicity of its new wing for gemstones. To do this, the museum seeks to have many exotic gems on display for the grand opening. The Crown Jewels of England are scheduled to be a part of the display. Manuela the museum manager would like to have a high degree of confidence that the receipt of the jewels by the museum and the release of the jewels after the opening are protected. Samuel the museum system engineer needs to specify the requirements for non-repudiation and the relative importance of those requirements, as a means of driving and evaluating a non-repudiation service that will support events such as this grand opening. How can Samuel define such a set of requirements?

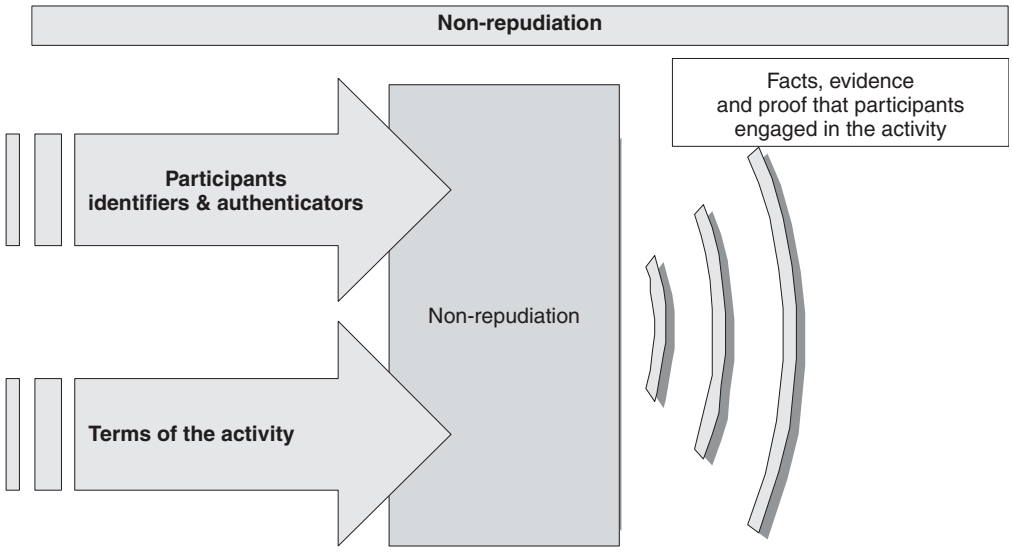
Context

Accounting requirements and their relative importance are understood, for example, from applying SECURITY ACCOUNTING REQUIREMENTS (360). The planned uses of non-repudiation are understood. A common transaction type is the sending and receiving of materials such as merchandise or contracts. Non-repudiation is used to prevent the receiver from denying that they received the materials when in fact they did receive them. Sometimes non-repudiation is used to prevent the sender from claiming that they sent the materials when in fact they did not send them.

Problem

Non-repudiation is a security service that captures and maintains evidence so that the participants of a transaction or interaction cannot deny having participated in that activity. The need is to identify the common requirements that drive the design of this service. The model in the figure places non-repudiation in the context of the

identity of the participants, in terms of the activity that it collects, and the facts and evidence that it provides. This ensures that the participants cannot deny having engaged in the activity. Non-repudiation needs information about the event that will disallow the participants from denying their participation. If the participants are allowed to deny their involvement in the activity, then the integrity of the activity will be jeopardized and other participants may suffer negative consequences. For example, if a purchaser receives a book that they ordered from Amazon.com, and then denies receiving it, Amazon may need to send another copy of the book, which is a financial loss to them.



Common model for non-repudiation

How can specific requirements for a non-repudiation service, and their relative importance, be determined?

The process of selecting and prioritizing non-repudiation requirements needs to balance the following forces:

- You can use non-repudiation to help achieve the desired security properties, especially integrity and accountability.
- Obtaining evidence that a person or organization participated in a transaction can have significant benefits in cases in which they deny participation, including favorable resolution of both economic and legal disputes.
- Applying non-repudiation has associated costs, including the time and resources required for continuously capturing identifiers and authenticators and

explicitly defining the terms of an event. This is counter to the organization goal of minimizing total costs.

- High need for non-repudiation often involves intrusive or inconvenient constraints on participants.
- There may be legal constraints that mandate that participants have access to the facts and evidence of their activities.
- The elements of the non-repudiation service need protection if the service is to perform its function.

Solution

Specify a set of non-repudiation requirements for a specific domain such as a system or organization, and determine the relative importance of each requirement. The solution has two aspects: a requirements process and a common set of generic requirements.

Requirements Specification and Prioritization Process

A system requirements engineer, in conjunction with an enterprise architect, typically perform the requirements process. An important first step is explicitly to define the domain for which non-repudiation requirements are being specified, such as a specific system or facility. You also define factors such as organization constraints that affect specialization and importance of requirements. You then specify non-repudiation requirements for the target domain, using the generic requirements provided below. The final activity is to define the relative importance of the specified requirements.

Generic Non-repudiation Requirements

The following is a general set of requirements appropriate to non-repudiation services. An engineer will need to consider each of these and determine its priority based on criteria specific to the target domain, as well as on broader organization constraints. Additional requirements may be added to this list to address system-unique characteristics. Some of the general requirements represent non-repudiation functional requirements. The remaining requirements represent non-repudiation non-functional requirements, including requirements for security of the non-repudiation service.

- Provide information that an actor took specified actions in an activity or event.

  Non-repudiation needs to have the ability to form strong links between the participants who engage in an activity and the activity itself. The evidence and facts that are derived from capturing information about the event need to be

explicit and detailed enough to help assign accountability. This requirement has increased priority when the events are of high importance. 'High' importance may mean critical to business functions or operations, providing legal or financial evidence, or otherwise significant.

- Provide identifiers, authenticators and the terms of an event when requested.

  Non-repudiation should examine any legal or external considerations regarding the gathering of information about participants of an event. There may be consequences for the organization if laws are not followed regarding the collection of identifiers and authenticators.

- Minimize the time it takes participants to provide their identifiers and authenticators.

  You need to consider that if events require non-repudiation and the events must happen for other business reasons, participants in these events should not be discouraged from joining due to complexities associated with identifiers and authenticators.

- Protect all non-repudiation information associated with an event.

  The confidentiality, integrity, and availability of facts and evidence need to be maintained. Due to the need to help to assign accountability, it is imperative that the information gathered by the non-repudiation service be uncorrupted. The better the non-repudiation service can maintain and provide a degree of confidence about the protection of the information, the more the service user can rely on the information that it provides. Non-repudiation also needs to verify that the information that it collects is not forged or misrepresented.

An additional set of requirements applies to all service requirements patterns. Instead of duplicating the discussion of the same set in each requirements pattern, they are simply listed here, because they do need to be considered in each requirements pattern. The requirements are: minimize mismatch with user characteristics, risks to user safety, costs of per-user set-up, costs of maintenance, management, and overhead, and changes needed to existing system infrastructure. Further discussion of each of these cross-cutting requirements, including implementation factors, is given in I&A REQUIREMENTS (192).

Implementation

This section provides more detail about the process that was summarized in the Solution section. The requirements process typically includes these steps:

1. Establish the domain for which the non-repudiation service is needed.

   Ensure that the domain has been identified and scoped: typical non-repudiation domains include categories of transactions or interactions. For example,

transactions at a company's public Web portal may be a different domain from transactions involving contracts with suppliers. Other constraints or distinctions may bound the domain as well, such as separating transactions that occur outside the organization from internal transactions.

2. Specify a set of factors that affect the specialization and importance of requirements.

   Factors can include uses of non-repudiation, non-repudiation needs, organization constraints, and priorities.

3. Specify non-repudiation requirements for the target domain.

   Specialize the set of generic requirements given above.

4. Define the relative importance of specific requirements.

   Priority is increased when the transactions or their consequences are of high importance. 'High' importance may mean critical to business functions or operations, providing legal or financial evidence, or otherwise significant.

Example Resolved

Samuel the museum system engineer defines the domain for non-repudiation to be transactions in which the museum lends or borrows gems of high value. Borrowing the Crown Jewels for an exhibit is an example of a transaction in this domain. To ensure protection of the reception and dispatch of the Crown Jewels, the museum defines specific non-repudiation requirements. Table 11.9 shows the specific requirements and relates them to the general requirements defined in the Solution section.

Although many aspects of this exchange will be time-consuming, it will also provide a very high degree of confidence that the parties exchanged the Crown Jewels and that the Crown Jewels were returned in the same condition as that in which they were received.

Known Uses

The general non-repudiation requirements and the process of specifying non-repudiation requirements described in this pattern are widely known, but are generally used informally, as opposed to being codified or published. The requirements as stated in this pattern represent a consolidation of MITRE Corporation's experience in working with multiple customers over several decades. However, some publications on non-repudiation requirements exist.

- [ISO13335-4] discusses non-repudiation as one of the primary safeguards, in the context of integrity.
- [ISO15408] is an international standard that defines evaluation criteria for information technology security. It includes non-repudiation requirements in the context of communication.

Table 11.9 Museum specific requirements for non-repudiation

GENERAL REQUIREMENT	SPECIFIC REQUIREMENT FOR THIS TRANSACTION
Provide information that an actor took specified actions in an activity or event	Capture, store, and record the receipt and return of the Crown Jewels by video taping the event or having it done with witnesses from both the sender and the receiver.
Provide identifiers, authenticators and the terms of an event when requested	• Identify and authenticate the individual(s) from whom the Crown Jewels should be received and to whom they should be given after the opening. • Explicitly outline the terms of the exchange and have all participants provide an authenticated signature. • Provide copies of this agreement to the sender and the receiver.
Minimize the time it takes participants to provide their identifiers and authenticators	Prepare everything, including video taping preparations and writing down the agreement, to make it as efficient and unobtrusive as possible. Document the process and have standard forms available for use in similar transactions.
Protect all non-repudiation information associated with an event	Store this agreement, the signatures, and the videotape in a secure location.

- [ISO13888] is an international standard on non-repudiation.
- [Louridas00] discusses non-repudiation protocol guidelines and stresses the need to match protocols with requirements.
- [IETF99] discusses requirements for non-repudiation in the context of the Internet.
- [Gindin01] discusses technical requirements for non-repudiation, in contrast with legal requirements.

Consequences

The following benefits may be expected from applying this pattern:

- It facilitates conscious selection of non-repudiation requirements, so that decisions about selecting non-repudiation mechanisms have a clear basis, rather than occurring in a vacuum.

- It promotes explicit analysis of trade-offs that encourages balancing and prioritizing of conflicting requirements. This helps to avoid stronger than necessary non-repudiation which places increased burden on the parties to a transaction, and at the same time it helps to avoid weaker than necessary non-repudiation, which would make it easy to deny participation.
- It results in documentation of non-repudiation requirements which communicates to all interested parties and also provides information for security audits.
- The pattern fosters a clear connection of non-repudiation requirements to security accounting policies. This also encourages organizations to make their policies more explicit.

The following potential liabilities may arise from applying this pattern:

- It requires an investment of resources to apply the pattern, including time to analyze domains and non-repudiation needs. In some cases the cost of applying the pattern may exceed its benefits.
- It poses a danger of over-engineering and complexity creep if stakeholders are offered too many options. You can mitigate this by using the requirements only as guidelines for analysis, or by selecting those parts of the pattern that give the most help.
- The formal selection process may be too long and costly and produce too much overhead. You can mitigate this in the same ways as noted above.
- Specific circumstances might not be covered by generic non-repudiation requirements. You can mitigate this by adding specific requirements and including them in the trade-offs.
- Documentation of requirements implies that they must be maintained as they change over time. You can mitigate this by keeping the requirements in a form that is easy to update, integrated with other system documentation.