What is nonrepudiation?

Nonrepudiation ensures that no party can deny that it sent or received a message via encryption and/or digital signatures or approved some information. It also cannot deny the authenticity of its signature on a document.

Although it originated as a legal concept, nonrepudiation is also widely used in computing, information security and communications.

Information assurance and nonrepudiation

Nonrepudiation is one of the five pillars of information assurance (IA), which is the practice of managing information-related risks and protecting information systems, like computers, servers and enterprise networks. The other four pillars are the following:

1. integrity
2. availability
3. authentication
4. confidentiality

Nonrepudiation provides proof of the origin, authenticity and integrity of data. It provides assurance to the sender that its message was delivered, as well as proof of the sender's identity to the recipient. This way, neither party can deny that a message was sent, received and processed.

Nonrepudiation is like authentication, particularly with respect to implementation. For instance, a public key signature can be a nonrepudiation device if only one party can produce signatures.

In general, nonrepudiation combines both authentication and integrity.

5 pillars of information assurance

Availability	Integrity	Authentication	Confidentiality	Nonrepudiation
Ensures information is ready for use and at the required performance level.	Guarantees data, associated systems only accessible or modifiable by authorized users.	Ensures users are who they say they are (i.e., user names/passwords, biometrics, digital certificates and security tokens).	Limits access or places restrictions on data like personally identifiable information/ classified corporate data.	Ensures individuals cannot deny an action because a system provides proof of the action.