

PKI

Part 5: Non-repudiation

Kjell Jørgen Hole
NoWires Research Group
Department of Informatics
University of Bergen

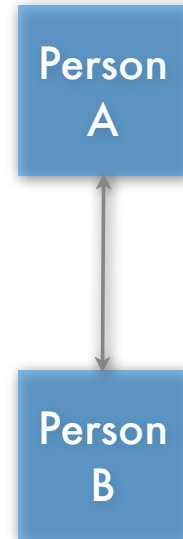
last changed October 21, 2011

Outline

- Introduction to non-repudiation
 - types of non-repudiation
 - technical model
- Non-repudiation service based on PKI
 - mechanisms for non-repudiation
- Dispute resolution?

Standard definitions

- **Non-repudiation.** Offers a person protection against a false claim by another person that a communication never took place
- **Non-repudiation of origin.** A person cannot falsely deny having originated a message or document
- **Non-repudiation of delivery.** A person cannot falsely deny having received a message or document



3

Legal view (1)

- Non-repudiation consists of the ability to convince a **third party** that a specific message or document originated with, or was delivered to a certain person
- **Credible evidence** is needed to persuade a
 - judge,
 - jury, or
 - arbitrator

4

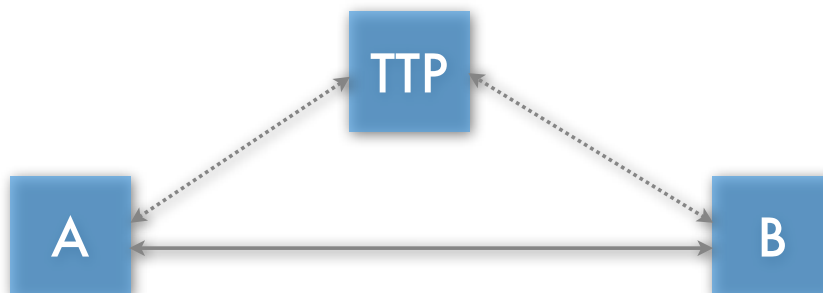
Legal view (2)

- Both the quality and the presentation of the evidence determine the **degree** of non-repudiation

5

Trusted third party needed

- To obtain a high degree of non-repudiation, it is essential that at least one **Trusted Third Party (TTP)** collects, validates, time stamps, signs, and stores relevant non-repudiation evidence



6

Non-repudiation in practice

- Non-repudiation consists of the ability to prove to a third party and **after the fact** that a specific communication originated with or was delivered to a certain person
- credible evidence is needed to persuade the judge, jury, or arbitrator that there is enough non-repudiation

7

Example: signed message via traditional mail

- Supports a moderate degree of non-repudiation
- Difficult to forge signature
- **Physical binding** of signer's identity to message
- Can use witnesses to increase degree of non-repudiation

8

Example: digitally signed message

- Can provide strong non-repudiation when used together with the **correct technical and legal protocols**
- Signature is **logically bound** to message
- Can also provide strong authentication and data integrity

9

Non-repudiation of origin

- **Non-repudiation of origin** *protects a recipient* from disputes where he claims to have received a message
- but the party identified as sender claims not to have originated the message
- different from that which the sender claims to have originated
- originated on a specific time and date, but the party identified as sender claims not to have originated the message at that specific time and date

What is the real problem?

1. The originator is lying
2. The recipient is lying
3. A computer or communications error has occurred
4. An intervening third party has deceived the two parties

11

Needed evidence

- The identity of the originator
- Content of message
- Date and time when origination occurred
- Identity of the intended recipient
- Identity of any TTPs involved in generating or retaining records

12

Non-repudiation of delivery

- **Non-repudiation of delivery** *protects an originator* in a dispute where he claims to have sent a message
 - but the party identified as recipient claims not to have received the message
 - different from that which the recipient claims to have received
 - on a specific date and time, but the recipient claims not to have received the message at a time and date consistent with the originator's claim

What is the real problem?

- Same problems as before:
 1. the originator is lying
 2. the recipient is lying
 3. a computer or communications error has occurred
 4. an intervening third party has deceived the two parties

Needed evidence

- The identity of the recipient
- Content of message
- Date and time at which delivery of the message occurred
- Identity of originator
- Identity of any TTPs involved in generating supporting records

15

Architecture: a technical model

- The non-repudiation process can be divided into five phases:
 1. non-repudiation request
 2. record generation
 3. record distribution
 4. record verification
 5. record retention

16

1. Non-repudiation request

- At least one of the participants to a communication must request the service of non-repudiation
- a standing agreement may also establish that the non-repudiation service should always be applied to certain events

17

Non-repudiation request ...

- The recipient requests the non-repudiation service to obtain non-repudiation of origin
- The originator requests the non-repudiation service to achieve non-repudiation of delivery

18

2. Record generation

- A non-repudiation record captures data that can be used to resolve disputes
- The record contains a copy of part of the communication
- A TTP may participate in the record generation process

19

3. Record distribution

- The record must be made available to the party (or parties) who may need to use it during a dispute
- A TTP may be used to receive, verify, and store the record

20

4. Record verification

- A party receiving a non-repudiation record must verify that the content is correct and sufficient to provide support for non-repudiation
- The verification should be a part of the normal communication process, and not a consequence of a dispute

21

5. Record retention

- A communication party, or a TTP, must archive the the record

22

Non-repudiation service

- A non-repudiation service utilizing digital signatures can be built on top of a standard PKI
- Basic PKI services must be combined with the correct combination of **legal** and **technical** non-repudiation protocols

Non-repudiation

PKI

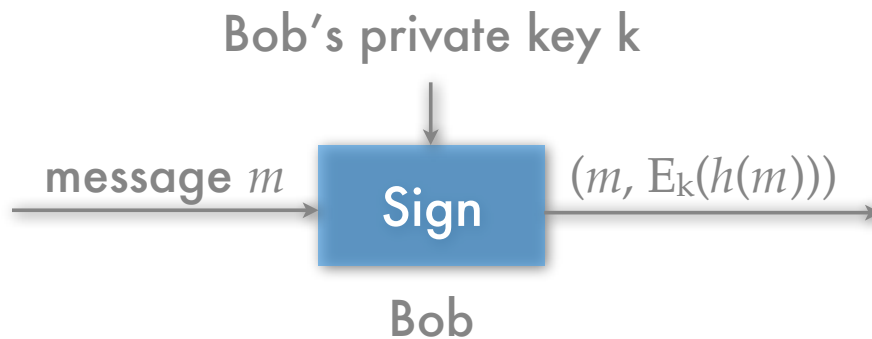
23

Digital signature (1)

- Non-repudiation service utilizes digital signatures based on private keys
- **Digital signature**—an authentication mechanism that enables the originator of a message to attach a code that acts as a signature
- the signature guarantees the source and integrity of the message

24

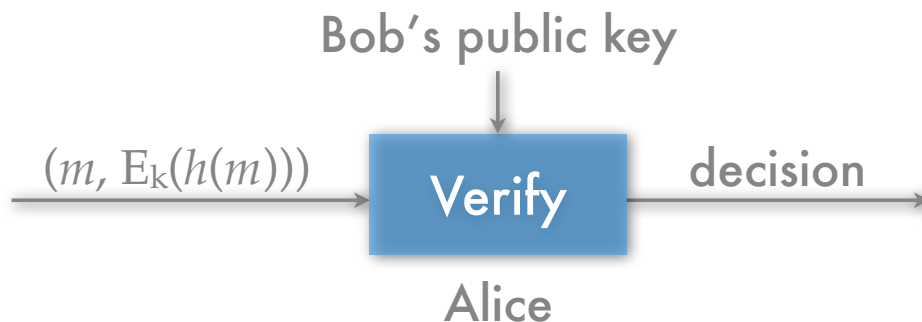
Digital signature (2)



- When Bob wants to digitally sign a message m to Alice, he calculates a hash $h(m)$, signs the hash with his private key $E_k(h(m))$, and appends the result to the message $(m, E_k(h(m)))$

25

Digital signature (3)



- To verify the signature, Alice “decrypts” the signed hash $E_k(h(m))$ and compares $h(m)$ to a calculated hash of the received message m

26

Mechanism for non-repudiation of origin

- Originator of message **digitally signs** the message
- Recipient verifies the digital signature
- Digital signature, message, and originator's public-key certificate are retained by recipient in a non-repudiation record

27

Certificate revocation (1)

- If a public-key certificate is revoked, then it is important to communicate the precise time of revocation to all users of non-repudiation records
- a record generated before the revocation is considered valid, but a record generated after is not

28

Certificate revocation (2)

- Non-repudiation may require real-time revocation status notification
- The use of OCSP (Online Certificate Status Protocol) may be a good solution
- **Alternative:** it is also possible to employ the digital signature of a TTP

29

Mechanism for non-repudiation of delivery

- The recipient of a message digitally signs an acknowledgment containing
 - a copy or digest of the message content
 - time of message delivery
- The signed ack is sent back to the originator

30

More on the degree of non-repudiation

- Independent third parties increase the degree of non-repudiation
- The following TTP services may be used
 1. delivery agent/notarization service
 2. secure time stamping
 3. archival service

31

1. Trusted delivery agent

- A TTP acts as a **delivery agent**
 1. the originator transmits the message to the delivery agent
 2. agent delivers message to recipient
 3. agent acknowledges receiving the message using the signature-based mechanism

32

Trusted delivery agent ...

- Gives protection against recipient that does not acknowledge received message
- Delivery agent provides notarization services
 - notary certifies that the data is valid

33

2. Secure time stamping

- A **time stamp** is a notation that specifies the date and time that an activity occurred
 - associated with the identity of a person/entity
 - appended to, or logically associated with, a message
- Secure time stamping involves a **trusted** time authority associating a time stamp with a particular message

34

3. Archive

- TTP that archive non-repudiation records
- Records must often be retained for several years
- Archive must retain the ability to read the data formats

35

Dispute resolution?

- Dispute resolution involves
 1. retrieval of the non-repudiation records,
 2. presentation of the records to the parties,
 3. presentation of the matter before the arbiter, and
 4. the arbiter's decision.

36

Serious practical problems

- **Obtainable degree of non-repudiation:** expensive and complicated technical and legal framework needed to provide a high degree of non-repudiation
- **Lack of openness:** users must have access to independent evaluations of a service to build understood level of trust

37

Technical challenge

- Person A can claim to have lost control over his private key before signing the digital contract
- Person B must convince the arbitrator that A is lying
- A complicated technical framework is needed for B to be able to convince the arbitrator

38

Legal challenge

- What is the correct type and amount of non-repudiation information?
- How should information be collected and stored to convince a judge (with little or no technical understanding of PKI)?

39

Understood level of trust?

- Today users of non-repudiation services are told that the service is highly secure, but no information is provided to enable independent experts to evaluate the services
- Hence, it is not possible for users to obtain an understood level of trust in these services

40

Lack of understanding?

- Is there really a good way to explain PKI to non-technical people?
- Do computer scientists and lawyers have a common understanding of PKIs and non-repudiation?

41

Concluding remarks

- A high level of non-repudiation requires three TTP services
 - archive
 - secure time stamping
 - notarization
- This makes for a very expensive and complicated implementation

42

Sources

- C. Adams and S. Lloyd, [Understanding PKI](#), 2nd Edition, Addison Wesley, 2003
- W. Ford and M. S. Baum, [Secure Electronic Commerce](#), 2nd Edition, Prentice Hall, 2001
- R. Housley and T. Polk, [Planning for PKI](#), Wiley, 2001

43



44