

BANKID: PRIVACY AND NON-REPUDIATION

KJELL JØRGEN HOLE
UNIVERSITY OF BERGEN
DEPARTMENT OF INFORMATICS

LAST UPDATED NOVEMBER 4, 2009

OVERVIEW

1. Privacy in BankID
2. Definitions and legal view of non-repudiation
3. Non-repudiation in BankID
4. Case study: e-voting system utilizing BankID
5. Conclusions

PRIVACY IN BANKID

PRIVACY DEFINED

- ❖ **Privacy.** The right of an individual to decide when and how sensitive personal information should be revealed

ATTACKER CAN COLLECT INFORMATION

Identifisering **BankID**

Fødselsnummer (11 siffer):

OK Avbryt

Identifisering **BankID**

Fokus Bank
PersonBankID

Bank:

- ✓ ----Velg----
- Fokus Bank
- SpareBank 1
- Terra-Gruppen AS

OK Avbryt

- ❖ Enter NBN (Norwegian Birth Number) of any BankID customer
- ❖ Get information

5

BANKID COLLECTS INFORMATION

- ❖ When a user accesses a web site, the certificates and the two-factor authentication cause the user and the site to be **uniquely identified** by the central infrastructure
- ❖ Possible for the central infrastructure to record where users e.g. shop and which government agencies they have dealings with

6

DETAILED PROFILES

- ❖ Since users enter their NBNs during the authentication process, it is possible to link information from BankID with information in other commercial and governmental systems
- ❖ Possible to build increasingly **detailed profiles** of users over time

7

PRIVACY HYPOTHESIS

The Norwegian banking community controls an ID system with the potential to build detailed profiles of half the Norwegian population

8

SUGGESTED NEW REQUIREMENTS

❖ Any end-user should be able to determine:

1. what personal information is stored
2. how information is made available to others
3. how the information is updated
4. how disclosure of information is prevented

NON-REPUDIATION DEFINED

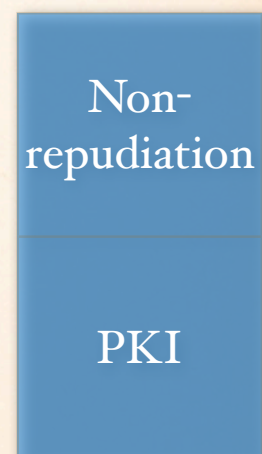
STANDARD DEFINITIONS

- ❖ **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



NON-REPUDIATION SERVICE

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



LEGAL VIEW (1)

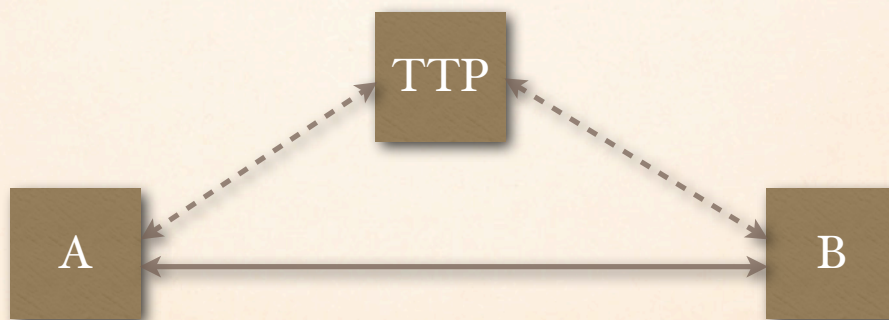
- ❖ Non-repudiation consists of the ability to convince a **third party** that a specific message or document originated with, or was delivered to a certain person
- ❖ **Credible evidence** is needed to persuade a
 - ❖ judge,
 - ❖ jury, or
 - ❖ arbitrator

LEGAL VIEW (2)

- ❖ Both the quality and the presentation of the evidence determine the **degree** of non-repudiation
- ❖ Note that the burden of proof is on the party wanting to rely on a digital signature
 - ❖ Non-repudiation doesn't take away a person's legal right to refute a signature

TRUSTED THIRD PARTY

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



15

TTP REQUIREMENTS

- ❖ During a conflict between the two parties the TTP must be able to
 1. withstand “pressure” from the parties, and
 2. present the non-repudiation evidence in an unbiased manner

16

CONSEQUENCE OF MISSING TTP IN BANKID

17

NO TTP

- ❖ BankID doesn't employ a TTP despite the fact that this is required by most (practical) non-repudiation protocols described in the research literature
- ❖ The following scenario illustrates why the missing TTP creates problems for BankID customers during conflicts involving repudiation of digital signatures

18

SCENARIO

- ❖ **Setting:** a bank and a customer have both digitally signed a document
- ❖ **Claim:** at some later point the bank claims it didn't sign the document
- ❖ **Challenge:** the customer must show that the bank did in fact sign

AVAILABLE INFORMATION

- ❖ **Bank's situation:** it has access to
 - ❖ detailed information about the technical and legal non-repudiation procedures
 - ❖ experts with extensive BankID knowledge
- ❖ **Customer's situation:** the customer and his lawyers have no access to a TTP that can provide the same information and knowledge

POSSIBLE OUTCOME

(SPECULATIVE)

- ❖ During a dispute between a customer and his bank, BankID* is, for all practical purposes, acting as a TTP
- ❖ The bank—part-owner of BankID—cannot afford to lose the dispute because this will damage the reputation of the whole BankID system and, potentially, reduce the revenue stream for many banks
- ❖ Because the bank must protect important business interests, it is likely to act “aggressively” to win the dispute

*BankID is operated by BBS, which is owned by the Norwegian banks

21

TTP HYPOTHESIS

The non-repudiation service in BankID gives a bank an advantage over its customers during conflicts involving repudiation of signatures because the customers cannot rely on help from a TTP

22

SUGGESTION

- ❖ The government should run a TTP

CONSEQUENCE OF UNUSUAL USER AUTHENTICATION

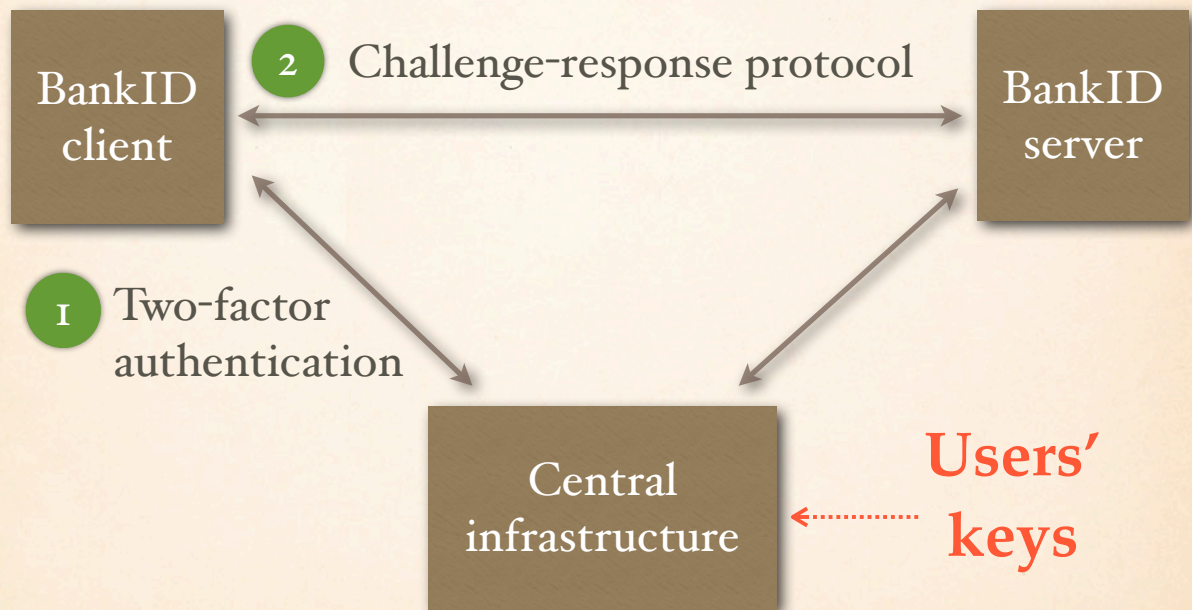
AUTHENTICATION LIMITS NON-REPUDIATION

1. In general, if the end-user authentication in a PKI is too weak, then it is possible for an attacker to steal a session
2. The attacker can then digitally sign a document on behalf of the user
3. It is difficult for the user to show that he didn't sign
4. If the PKI offers a non-repudiation service, this will increase the problem for the user because the other signee has access to "credible evidence"

WE HAVE

Strong authentication of users is needed to achieve a high degree of non-repudiation

BANKID AUTHENTICATION



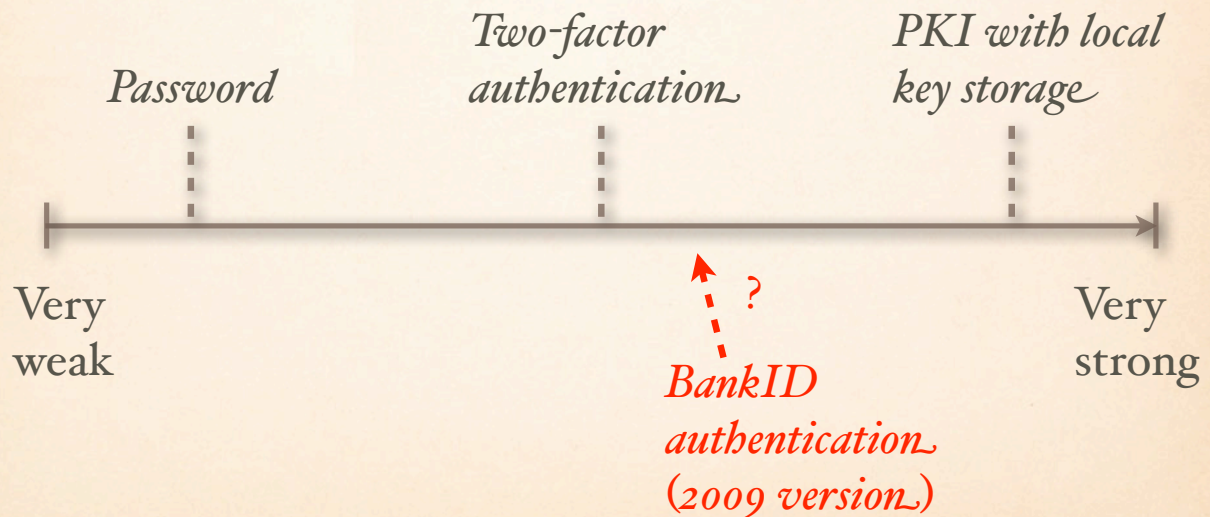
27

ANALYSIS

- ❖ **Unusual authentication:** The user must authenticate to the central infrastructure to give the BankID client access to cryptographic functionality utilizing the user's keys
- ❖ **Observsation:** If step 1 in the authentication procedure can be "circumvented," then the BankID client runs step 2 automatically
- ❖ **Consequence:** The authentication in BankID is about as strong as "traditional" two-factor authentication

28

AUTHENTICATION STRENGTH



29

AUTHENTICATION HYPOTHESIS

The end-user authentication in BankID is too weak to support the degree of non-repudiation needed to support legally binding contracts

30

SUGGESTION

- ❖ The BankID-member banks should publish information about the technical and judicial non-repudiation protocols

BANKID CASE STUDY: E-VOTING AND PRIVACY

E-VOTING IN NORWAY

- ◆ The *Ministry of Local Government and Regional Development* is developing a national e-voting system
- ◆ Trials with e-voting at municipal elections in 2011
- ◆ E-voting for selected groups in 2013
- ◆ Full roll out of solution in 2017

E-VOTE 2011 PROJECT

- ◆ The *E-vote 2011 project* plans to
 - ◆ choose an e-voting solution in 2009
 - ◆ complete system for elections in selected municipalities in 2011
- ◆ Full disclosure: author assists the E-vote 2011 project

E-VOTING SYSTEM NEEDS NATIONWIDE PKI

- ❖ The Norwegian Government is also developing a PKI to
 - ❖ authenticate voters
 - ❖ digitally sign votes
- ❖ The PKI may not be available for the trials in 2011
 - ❖ BankID may be used instead

BANKID DESIGN REVISITED

- ❖ In a standard PKI, a user's key pair is stored locally, preferably on a smart card
- ❖ In BankID, the key pair is stored on the central infrastructure
- ❖ It is likely that the central infrastructure will sign a hash of each vote during an election
- ❖ The central infrastructure must know identity of voter to use the correct private key

E-VOTING HYPOTHESIS

BankID can build a list of all individuals casting votes during an election

SUGGESTION

- ❖ BankID should not be used to sign votes during an election

SUMMARY OF HYPOTHESES

39

HYPOTHESES

- ❖ The non-repudiation service in BankID gives a bank an advantage over its customers during conflicts involving repudiation of digital signatures
- ❖ The degree of non-repudiation in BankID is too weak to allow digitally signing of contracts involving large sums of money
- ❖ If BankID is used to digitally sign all votes during an election, then the central infrastructure will be able to create list over all individuals casting votes

40

BANKID RISK ASSESSMENT

❖ K. J. Hole, A. N. Klingsheim, L.-H. Netland, Y. Espelid, T. Tjøstheim, and V. Moen, **Risk Assessment of a National Security Infrastructure**, *Security & Privacy*, January/February 2009, pp. 34-41.

❖ www.nowires.org/Papers-PDF/RiskEvaluation.pdf

Thank you!

