Audit trail model for intermediated business document exchange

Mikael Ylijoki
Master's thesis
2003

Supervisor: Prof. Jormakka

Contents

- Background
- Research objectives
- Outline of the solution
- Central problems
- The thesis
- Model 1
- Model 2
- Final structure
- Conclusions
- Future research

Background 1

- Growth in the exchange of B2B electronic documents
  - electronic invoicing
  - marketplaces
  - contract negotiation and conclusion

- Various XML standards for business

Background 2

- A need to fulfill the requirements of contract law electronically

- EU legislation on
  - electronic commerce
  - digital signatures
  - electronic invoicing

Background 3

- Assumed environment includes an intermediary, i.e. a third party service provider
- XML is predominantly used in the service
  - mappings and transformations must be performed between different XML standards
- Business processes are unambiguously defined and their instances are identifiable

Research objectives

- Create an audit trail model that reliably records all the relevant documents exchanged
- The audit trail must guarantee
  - data integrity
  - non-repudiation
  - authentication
- Documents must be able to act as a proof of legal commitment in case of dispute

Outline of the solution

- Cryptographic methods are used to accomplish the security objectives
- In addition to the business documents some control messages must be exchanged, e.g.
  - to guarantee non-repudiation of receipt
  - to be able to monitor the intermediary as well

The central problem

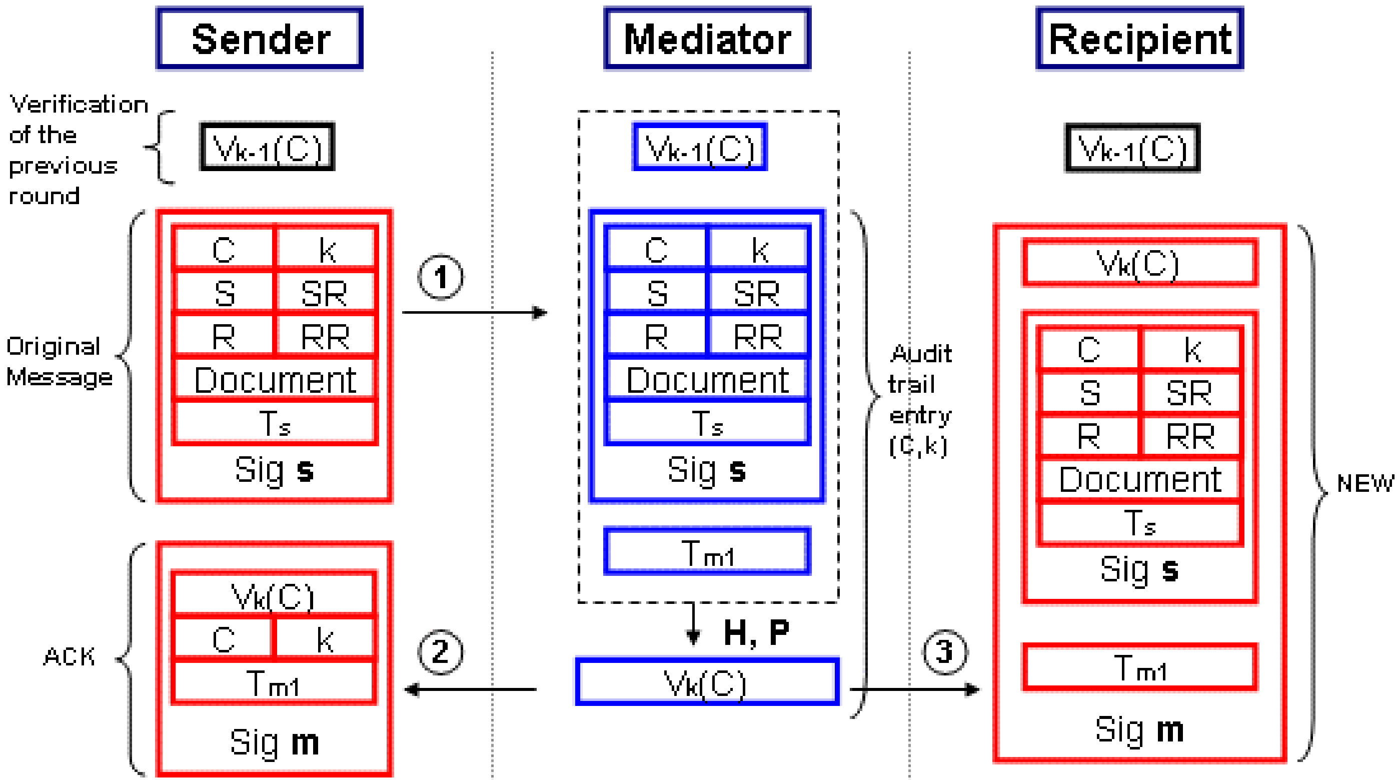
- What happens when a legally binding document with an electronic signature must go through an XML transformation?
  - the original signature will break in any case

The thesis

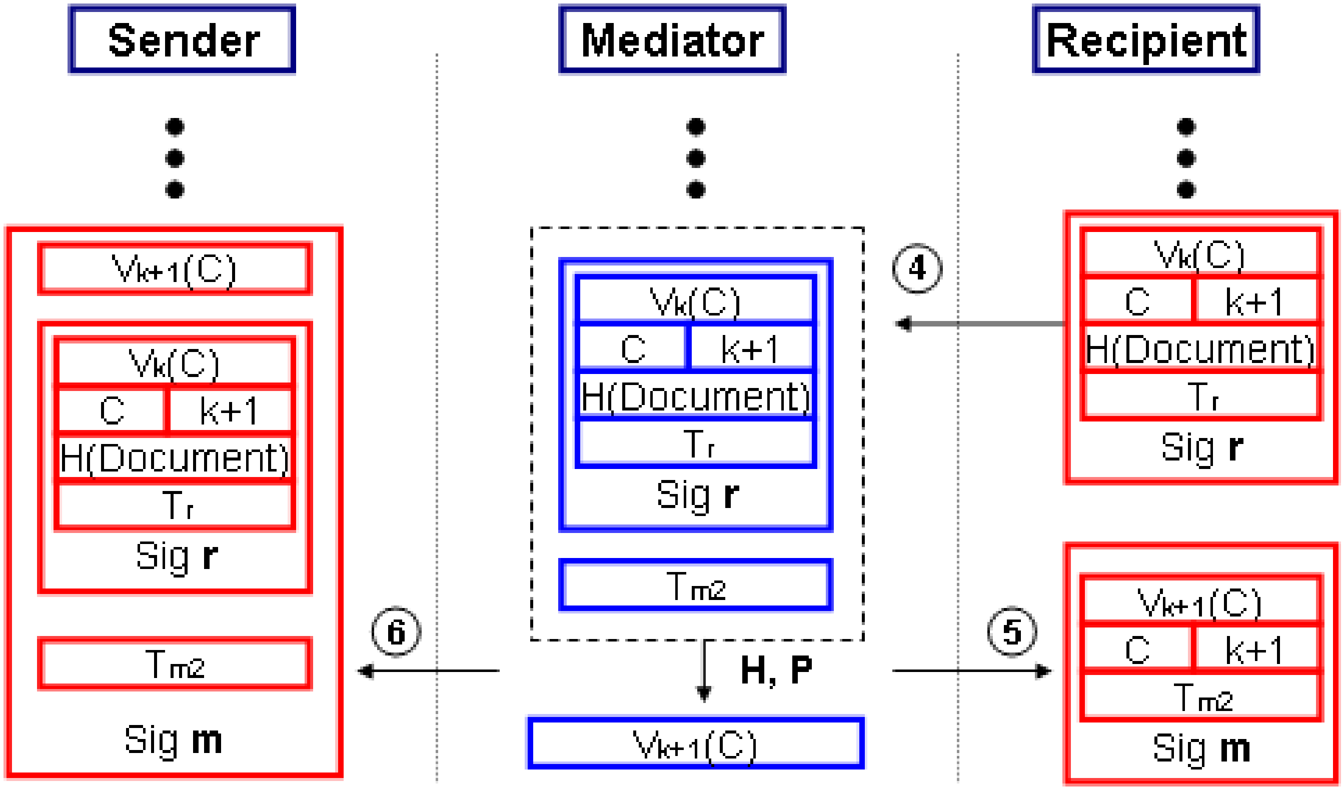
- Background (literature) research
  - business models
  - XML – basics and several business related standards
  - cryptographic methods
  - evolving EU legislation
- Proposed audit trail model

Model 1 (1/2)

Sender and recipient share a common XML standard
⇨ signature does not break



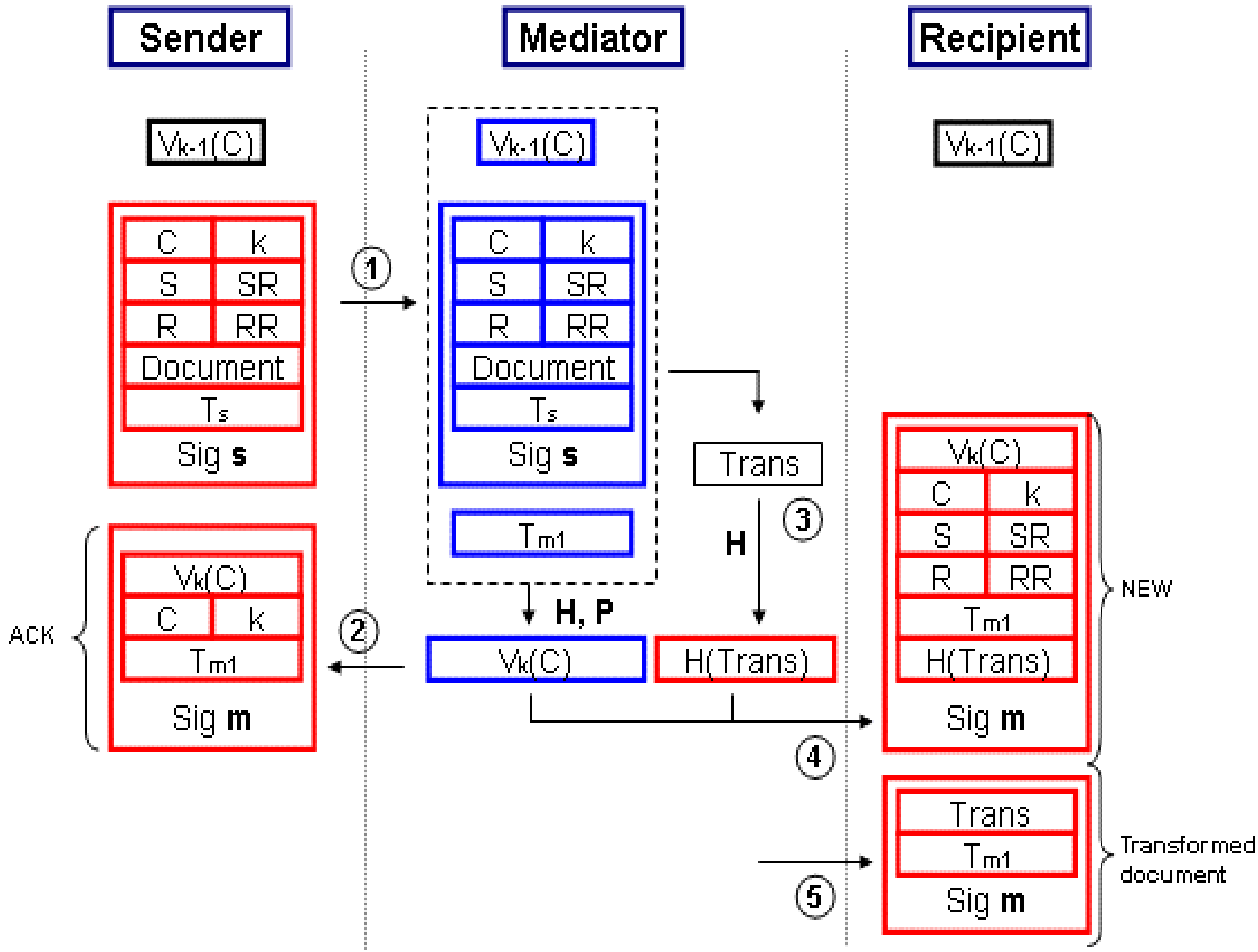
Model 1 (2/2)



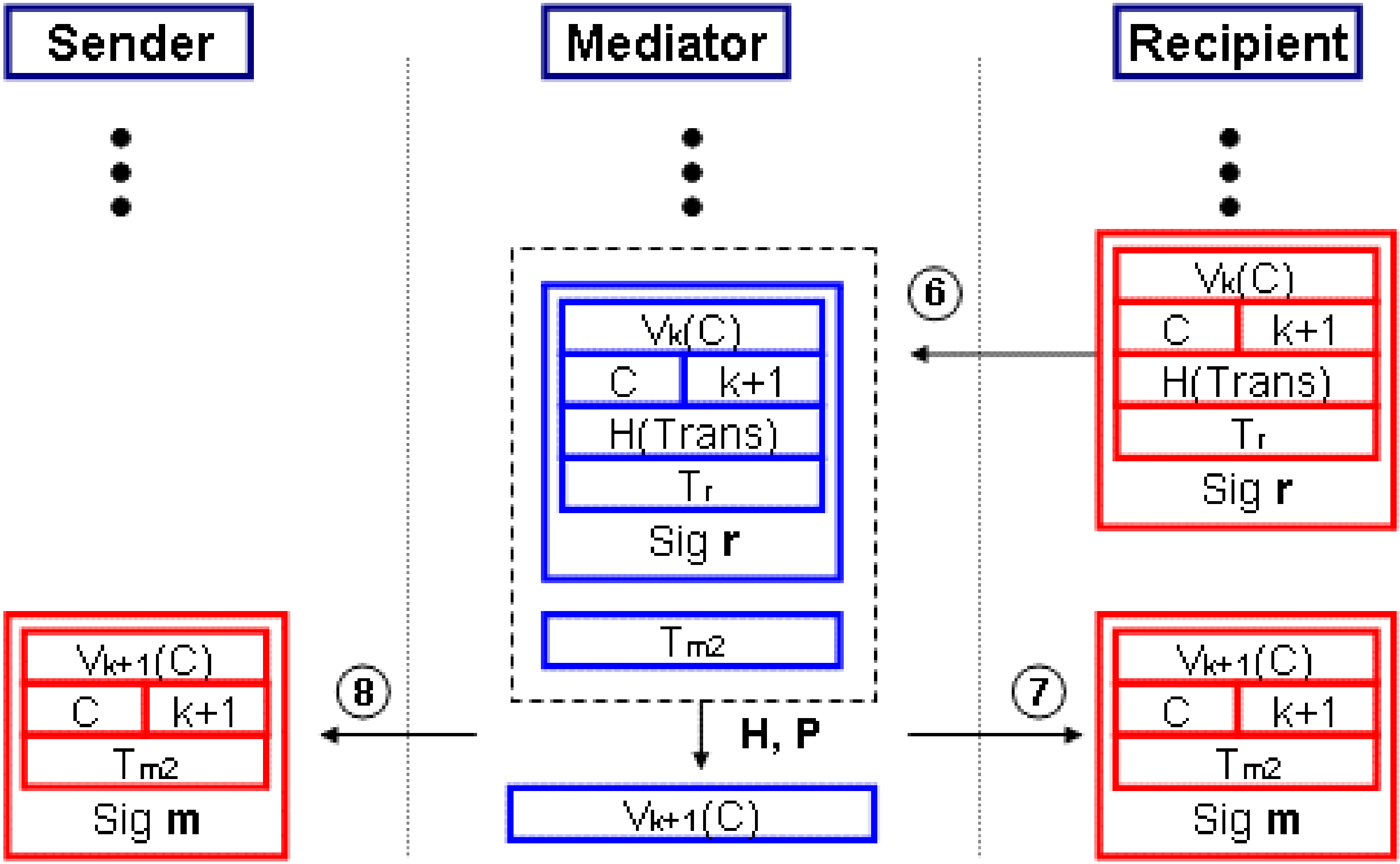
Sender
Mediator
Recipient
Vk+1(C)
Vk(C)
C
k+1
H(Document)
Tr
Sig r
Tm2
Sig m
4
5
6
H, P

Model 2 (1/2)

Sender and recipient use different standards.
A transformation must be performed.



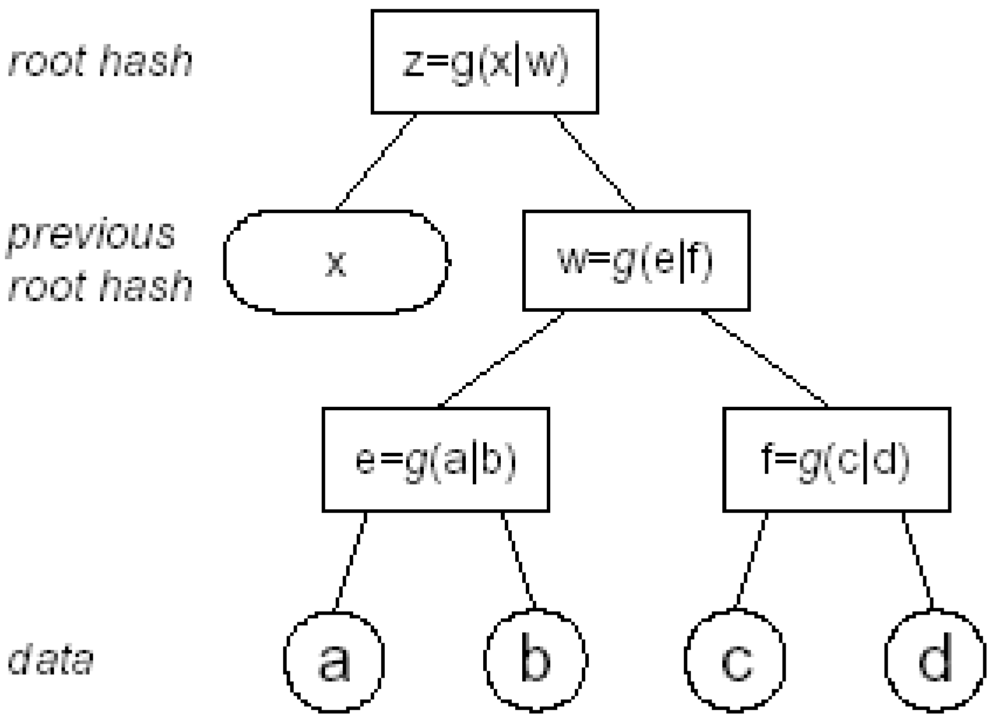
Model 2 (2/2)



Sender
Mediator
Recipient
Vk(C)
C
k+1
H(Trans)
Tr
Sig r
Tm2
6
7
8
H, P
Vk+1(C)
Sig m

Final structure

A Merkle hash tree



Conclusions

- Requires many public key operations
  - guarantees security objectives
  - heavy
- must consider more extensive use of symmetric encryption
  - if the intermediary is regarded as trustworthy, a simpler and lighter model is possible.

Future research

- Performance measurements
  - using different cryptographic methods
  - limitations on scalability