GJM

Author(s): Juan A. Garay, Markus Jakobson, Philip MacKenzie 1999
Submitted by Alexandre Boisseau October 30, 2002

Summary: The goal of this protocol is to achieve distributed contract signing in an abuse-free way, that is no party ever can prove to a third party that he is able of determining the issue of the exchange (validate or invalidate the contract). To achieve this goal, a special construction called private contract signature is introduced. Such a private contract signature has the particular property that it is meaningful only for a given trusted third party. Moreover, this protocol is optimistic in the sense that the trusted third party is required only in case of problem.

Protocol specification (in common syntax)

```
A,B,T :            principal
C :                msg
PCS :              (principal,msg,principal,principal):msg
S-SIG :            (principal,msg):msg
TP-SIG :           (principal,msg):msg
resolved,aborted : bool
abort :            msg

Exchange-1.    A  ->  B  :  PCS(A,C,B,T)
Exchange-2.    B  ->  A  :  PCS(B,C,A,T)
Exchange-3.    A  ->  B  :  S-SIG(A,C)
Exchange-4.    B  ->  A  :  S-SIG(B,C)
Abort-1.       A  ->  T  :  S-SIG(A,[C,A,B,abort])
Abort-2.       T  ->  A  :  if (resolved) then S-SIG(B,C) else S-SIG(T,S-SIG(A,[C,A,B,abort]))
Resolve-A-1.   A  ->  T  :  [PCS(B,C,A,T),S-SIG(A,C)]
Resolve-A-2.   T  ->  A  :  if (aborted) then S-SIG(T,S-SIG(A,[C,A,B,abort])) else if (resolved) S-SIG(B,C) else TP-SIG(B,C)
Resolve-B-1.   B  ->  T  :  [PCS(A,C,B,T),S-SIG(B,C)]
Resolve-B-2.   T  ->  B  :  if (aborted) then S-SIG(T,S-SIG(A,[C,A,B,abort])) else if (resolved) S-SIG(A,C) else TP-SIG(A,C)
```

Description of the protocol rules

About cryptographic primitives involved :

- `S-SIG(X,M)` denotes standard signature of contractual text `M` by principal `A`,

- `PCS(A,M,B,T)` denotes private contract signature of contractual text `M` by `A` inside a session involving participant `B` and TTP `T`. It is assumed that such a construction has the following properties:
  - a "fake-version" of `PCS(A,M,B,T)` can be computed by `B`, identical to the true one from the point of view of an external observer `O` (distinct from `A`, `B` and `T`),
  - `PCS(A,M,B,T)` can be converted by `T` into a "TTP-signature", denoted `TTP-SIG(A,M)` and identical to `S-SIG(A,M)` from the point of view of an external observer.

About the execution of the protocol:

- when no problem appears between `A` and `B`, the `Exchange` subprotocol is able to complete contract distribution,
- after sending the first message, if `A` does not receive any response from `B`, she can run the `Abort` subprotocol,
- after sending the second message, if `B` does not receive any response from `A`, she can run the `Resolve-B` subprotocol,
- after sending the third message, if `A` does not receive any response from `B`, she can run the `Resolve-A` subprotocol.

Requirements

This protocol was designed in order to satisfy the following properties:

- *completeness*: an adversary (submitted to some restrictions) cannot prevent two honest participants from obtaining a valid signature on a contractual text,
- *fairness*: it is impossible for a corrupted participant to obtain a valid contract without allowing the remaining participant to do the same. Moreover, once an honest participant has obtained an abort confirmation from the TTP, it is impossible for any other participant to obtain a valid contract. Finally, every honest participant is able to complete the protocol.
- *abuse-freeness*: it is impossible for a (possible corrupted) participant, at any point of the protocol, to be able to prove to an external observer that he has the power to determine the outcome of the protocol (validate or invalidate the contract).

References

[GJM99]

Claimed proofs

[SM01] [KR02] [CKS01]

Claimed attacks

[SM01]

Citations

[CKS01] R. Chadha, M.I. Kanovich, and A. Scedrov. Inductive methods and contract-signing protocols. In P. Samarati, editor, *8-th ACM Conference on Computer and Communications Security*, pages 176–185. ACM Press, November 2001.

[GJM99] J. A. Garay, M. Jakobsson, and P. MacKenzie. Abuse-free optimistic contract signing. In *Advances in Cryptology: Proceedings of Crypto'99*, volume 1666 of *Lecture Notes in Computer Science*, pages 449–466. Springer-Verlag, 1999.

[KR02] Steve Kremer and Jean-François Raskin. Game analysis of abuse-free contract signing. In Steve Schneider, editor, *15th Computer Security Foundations Workshop*, pages 206–220, Cape Breton, Nova Scotia, Canada, June 2002. IEEE Computer Society.

[SM01] Vitaly Shmatikov and John Mitchell. Finite-state analysis of two contract signing protocols. *Special issue of Theoretical Computer Science on security*, 2001. Accepted for publication.