

Temporal Key Release Infrastructure (TKRI)

Ricardo Felipe Custódio

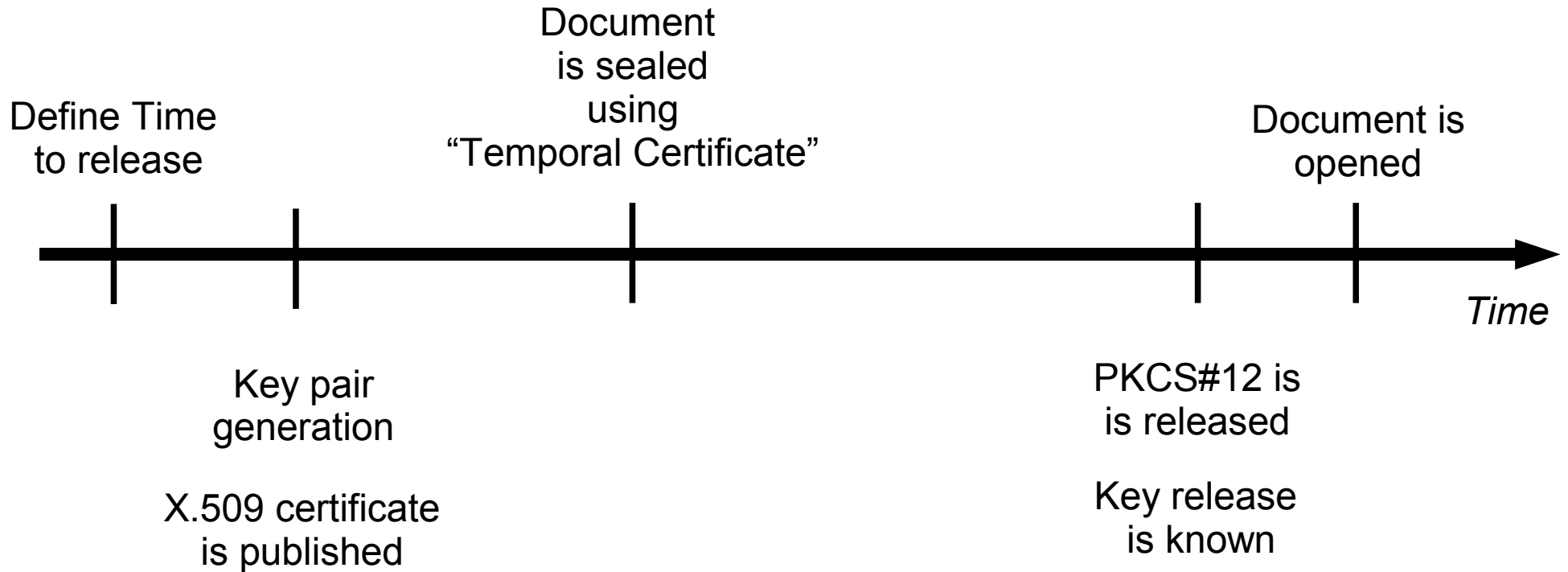
Júlio da Silva Dias,
Fernando Carlos Pereira, Adriana Elissa Notoya

Federal University of Santa Catarina
Brazil

Summary

- General Idea
- Requirements
- Timed Released Cryptography Bibliography
- Encipherment Module (EM)
- Temporal Key Release Infrastructure (TKRI)
- Prototype
- Example of Application
- Final Considerations

General Idea



General requirements for electronic or paper documents

- After the document has been sealed, it must not be possible to determine its content before the specified time of release
 - The decryption key that allows access to the document content cannot be known before the specified time of release
 - It must be possible to control access to the document content
 - The decryption key must be given only to the authorized entities
 - A mechanism is necessary to show the public part of the electronic document

General requirements for electronic or paper documents

- Once the document is released, the entity having the document cannot deny knowledge of the document's contents
- It must be possible to prove, after the decryption key has been published, that the document content has been revealed
- It must be possible to destroy the document without accessing its contents
- It must be possible to determine the group of users that witnessed the opening of the document

General requirements for electronic or paper documents

- It must be possible to verify in a irrefutable way the authenticity and integrity of the document. After being revealed, the document must be authentic and its content must be the same as that provided by the author
- It must be possible to audit the activities performed by the entities involved as well as to audit the resources used

Time Release Cryptography Bibliography

- Timothy May (1993)
 - “Timed-release cryptography”
 - trusted third parties (TTP) to store and release the document (or Key) at a specified time
- Ronald Rivest (1996)
 - proposed to model the problem as a time-lock puzzle (time capsule **LCS35**)
- Wenbo Mao (2001)
 - technique to control execution times of the puzzle
- Marco Mont, Keith Harrison and Martin Sadler (2003)
 - use of Identity-based Encryption (IBE)

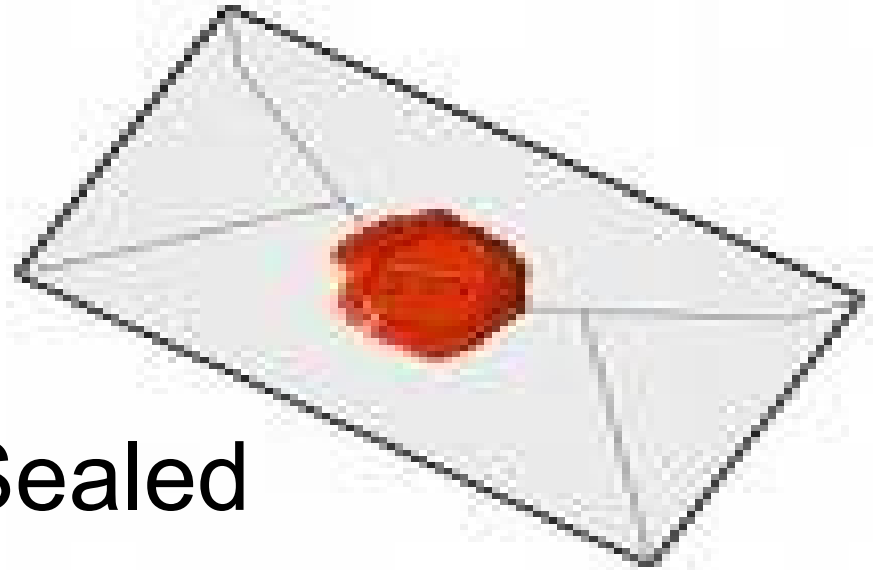
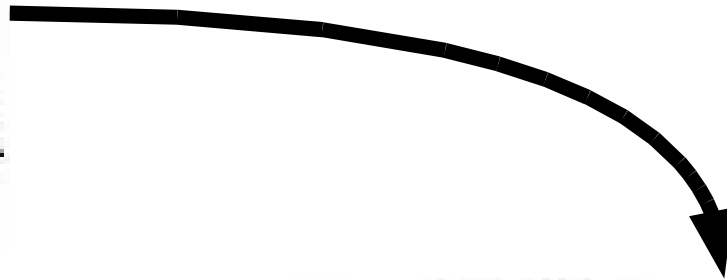
General Considerations

- Use of Digital Certificates
 - X.509
 - PKCS#12
- FIPS 140-2
 - Encipherment Modules
- Infrastructure
 - TSA
 - TCA
 - EM

Envelope

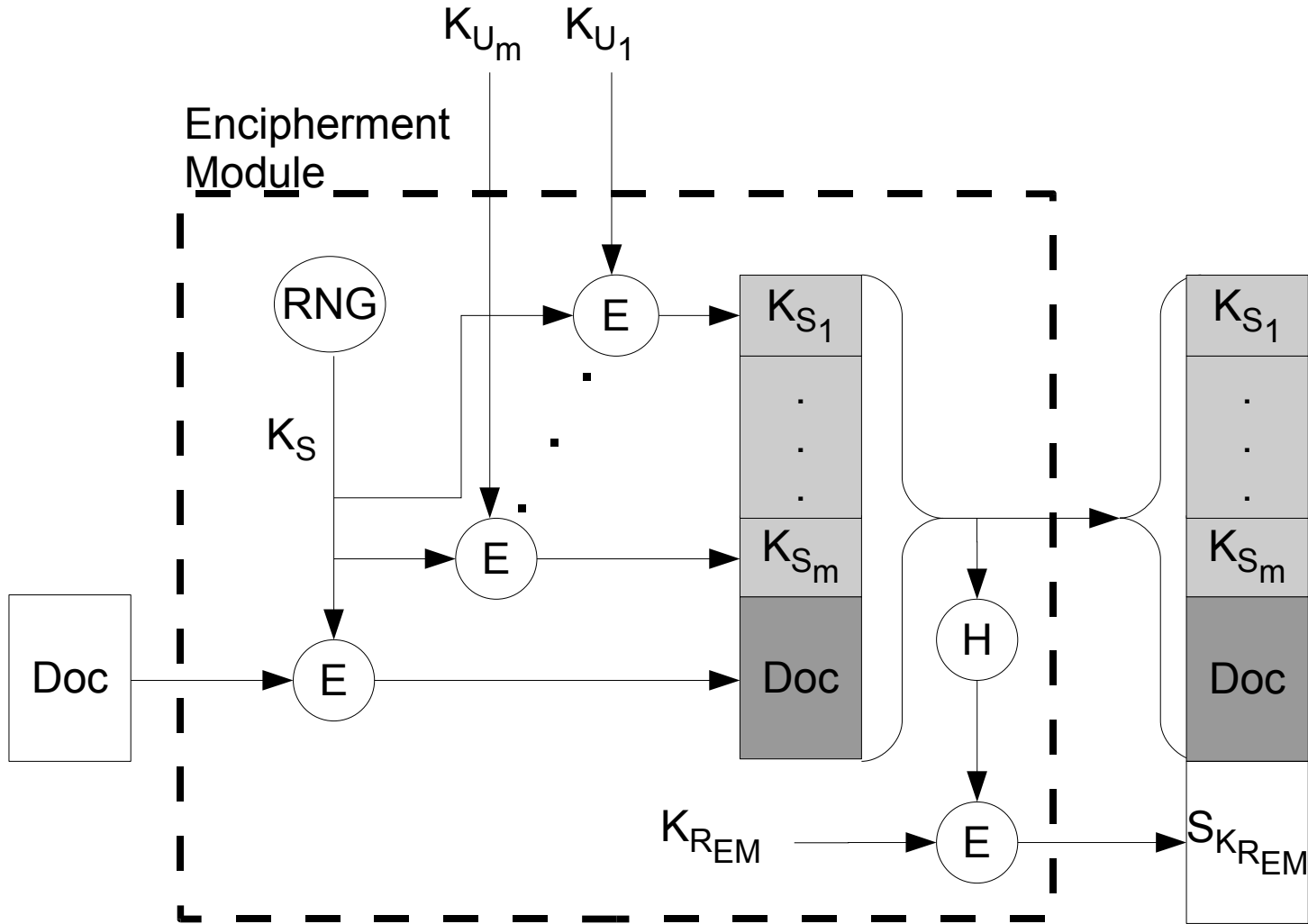


Opened

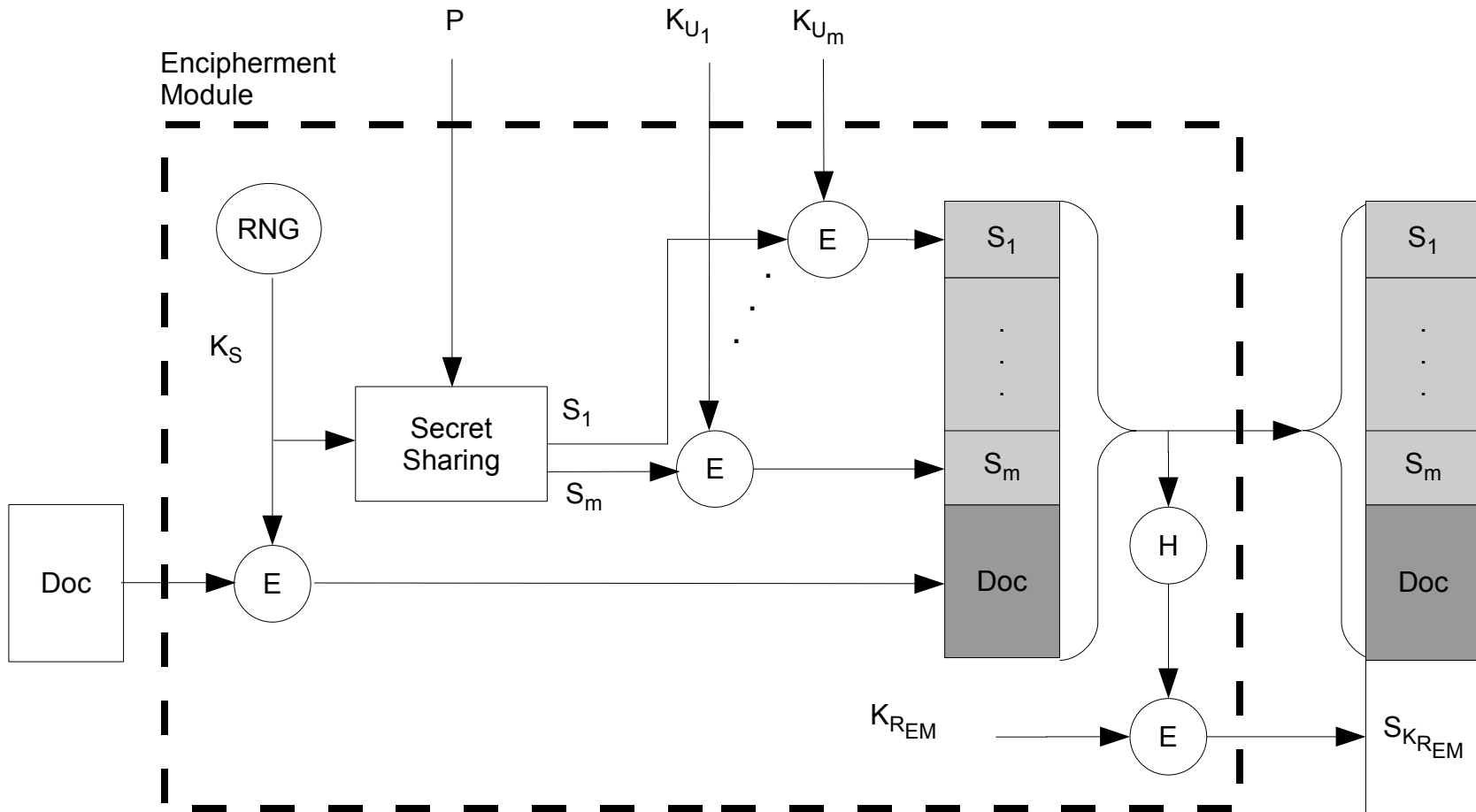


Sealed

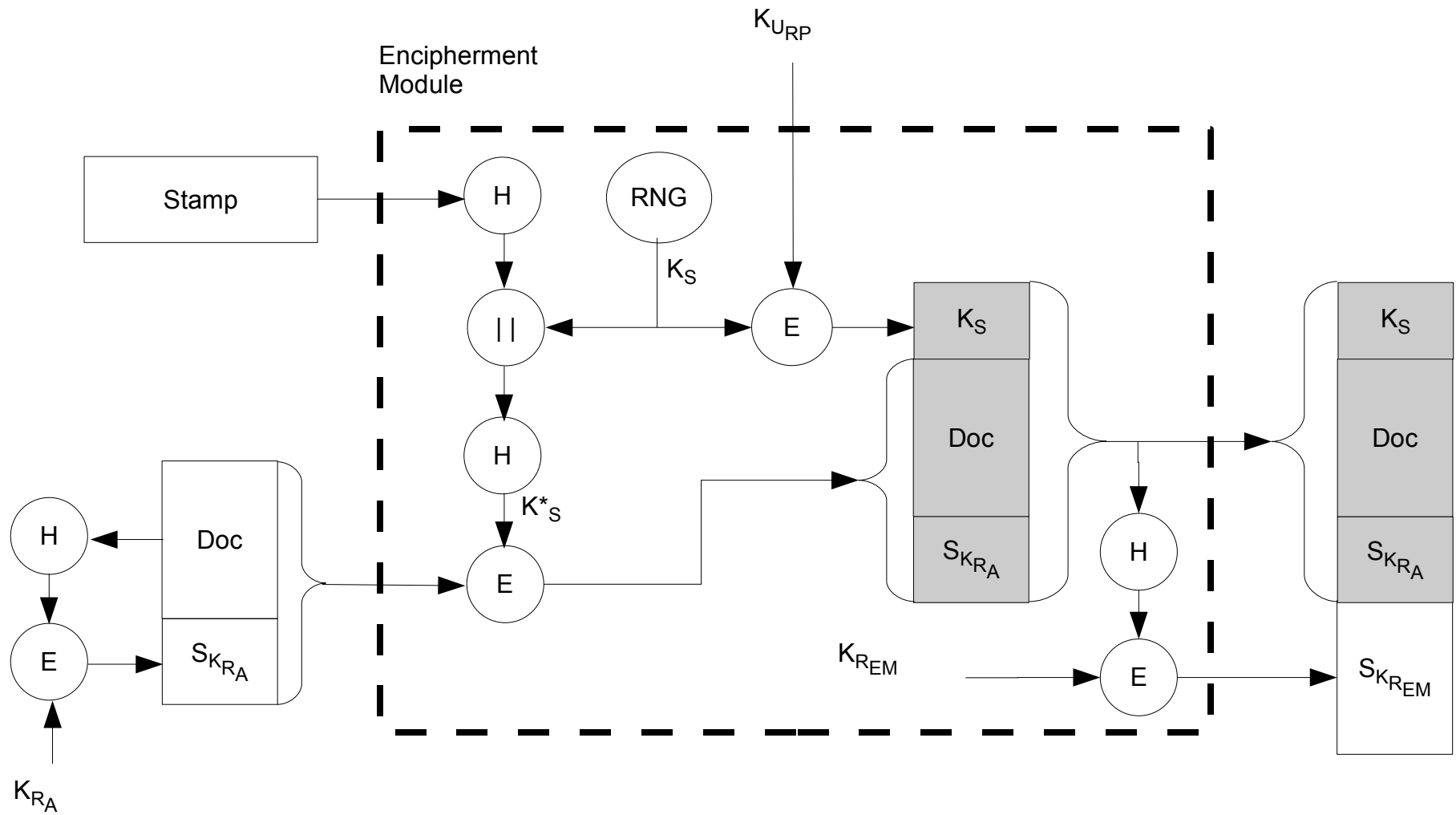
Basic Encryption Module



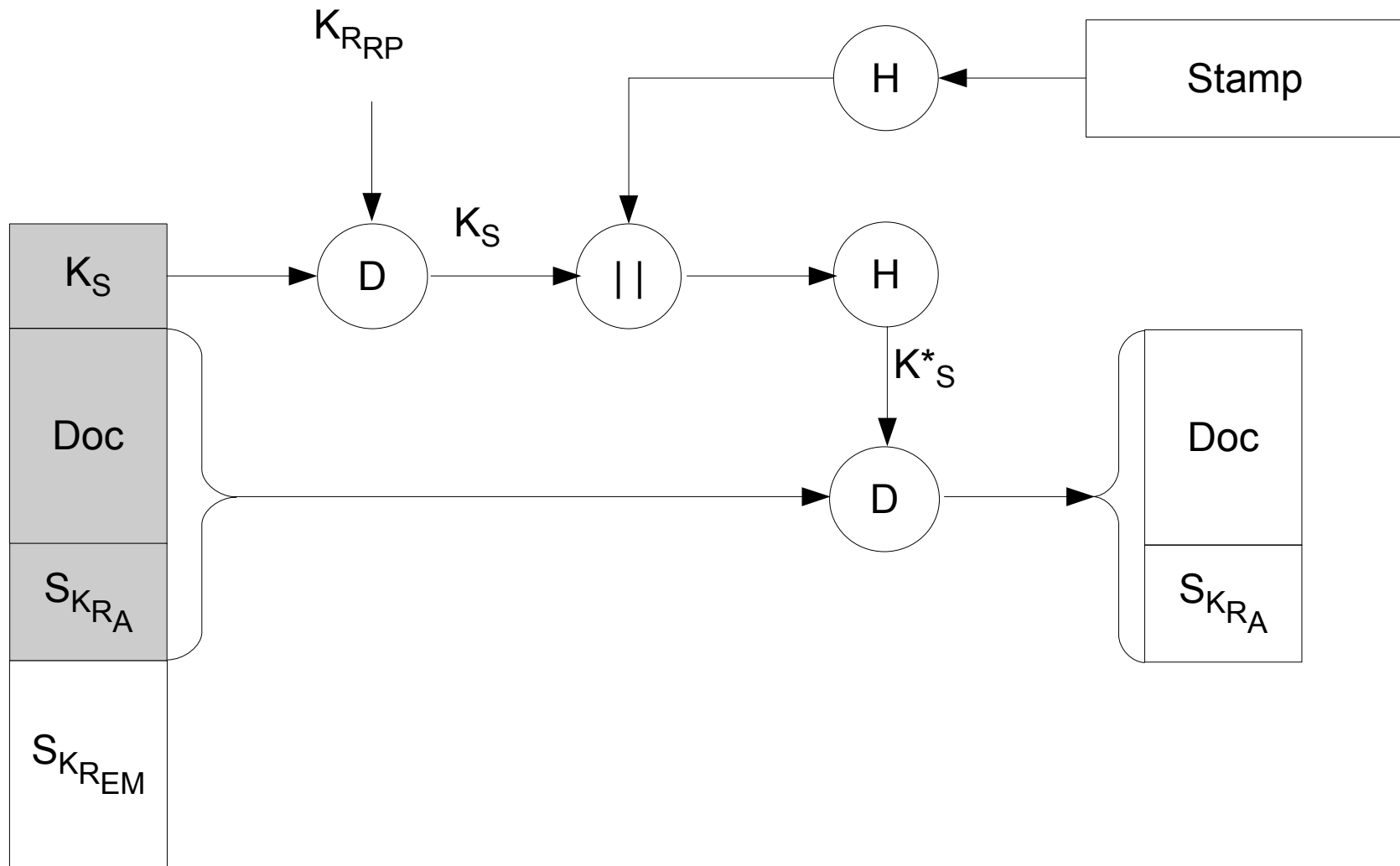
Secret Sharing Encryption Module



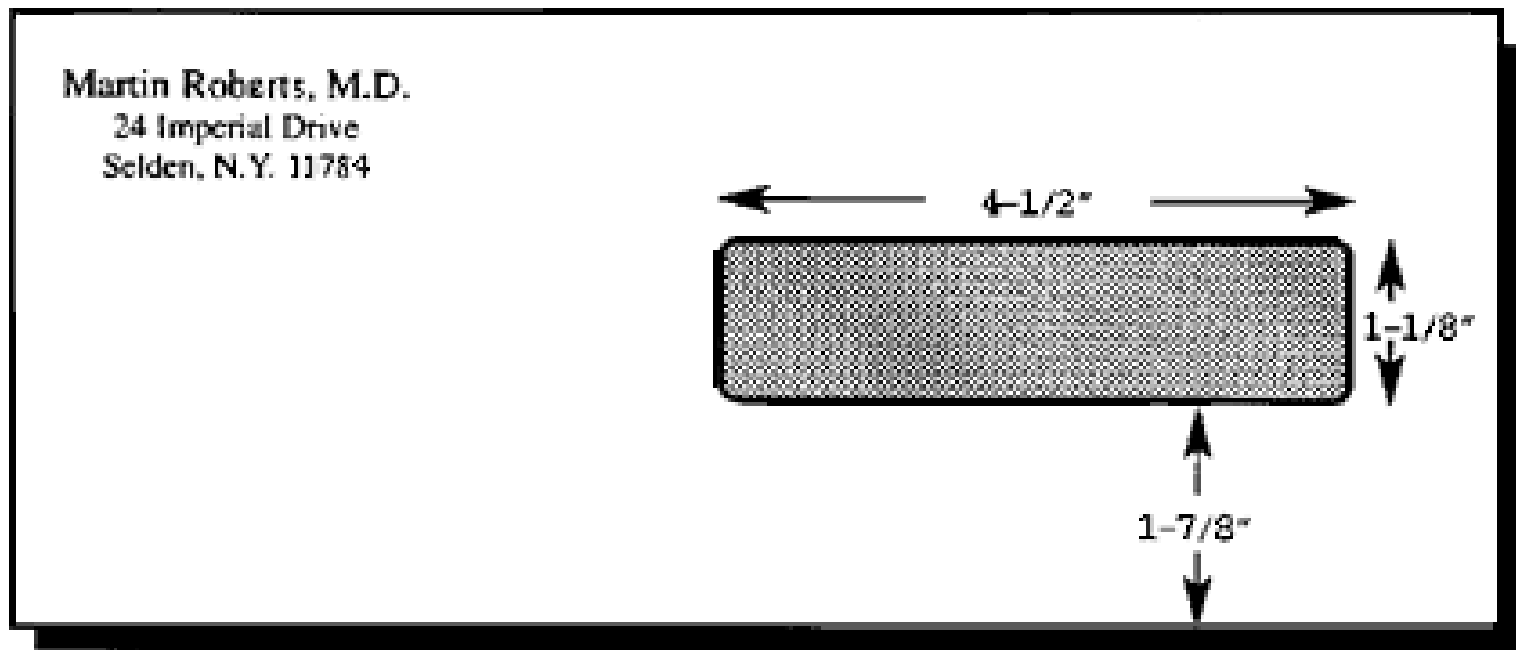
Stamp Insertion



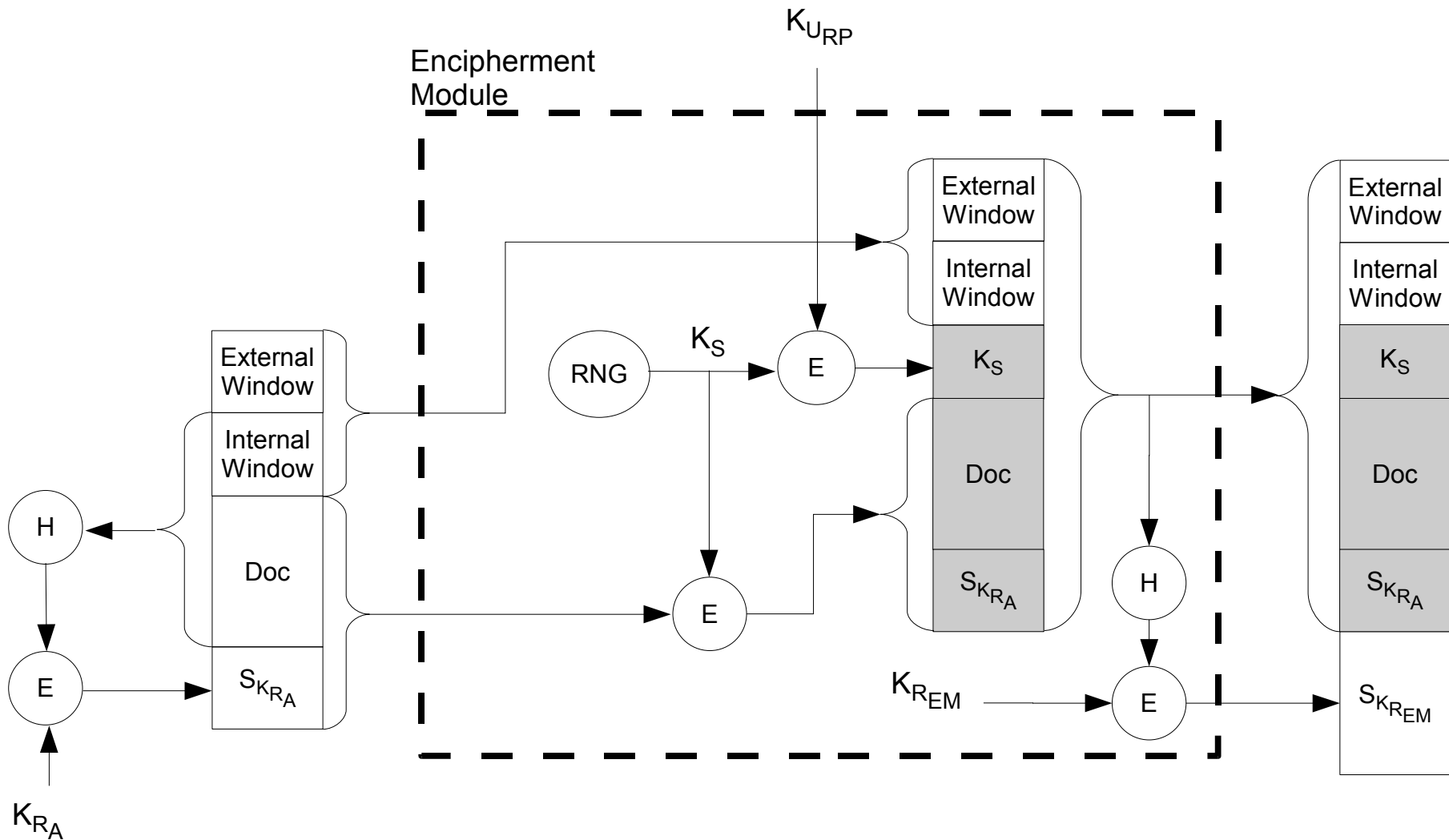
Electronic Document Disclosure When Using Stamp



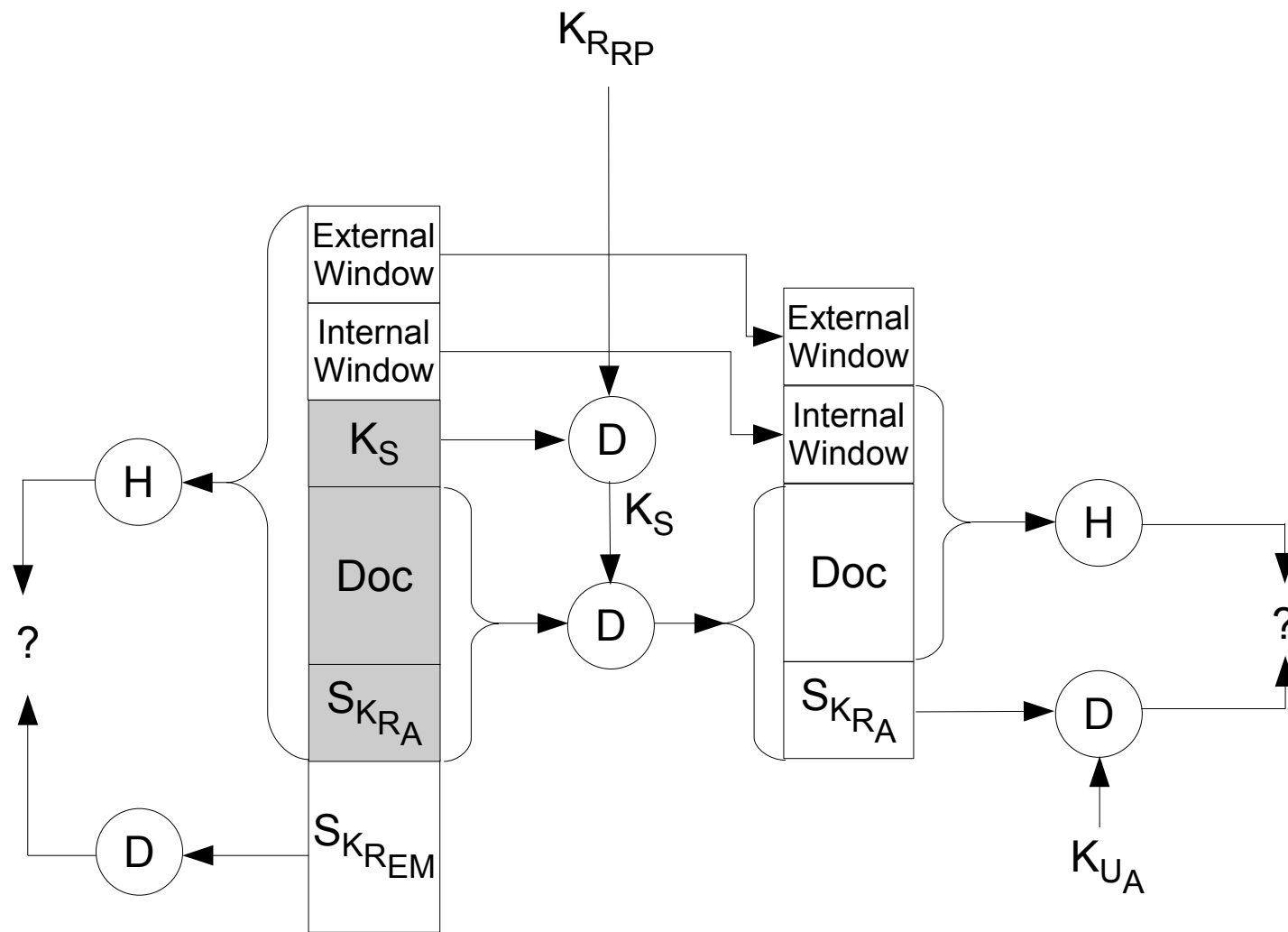
Window in a business envelope



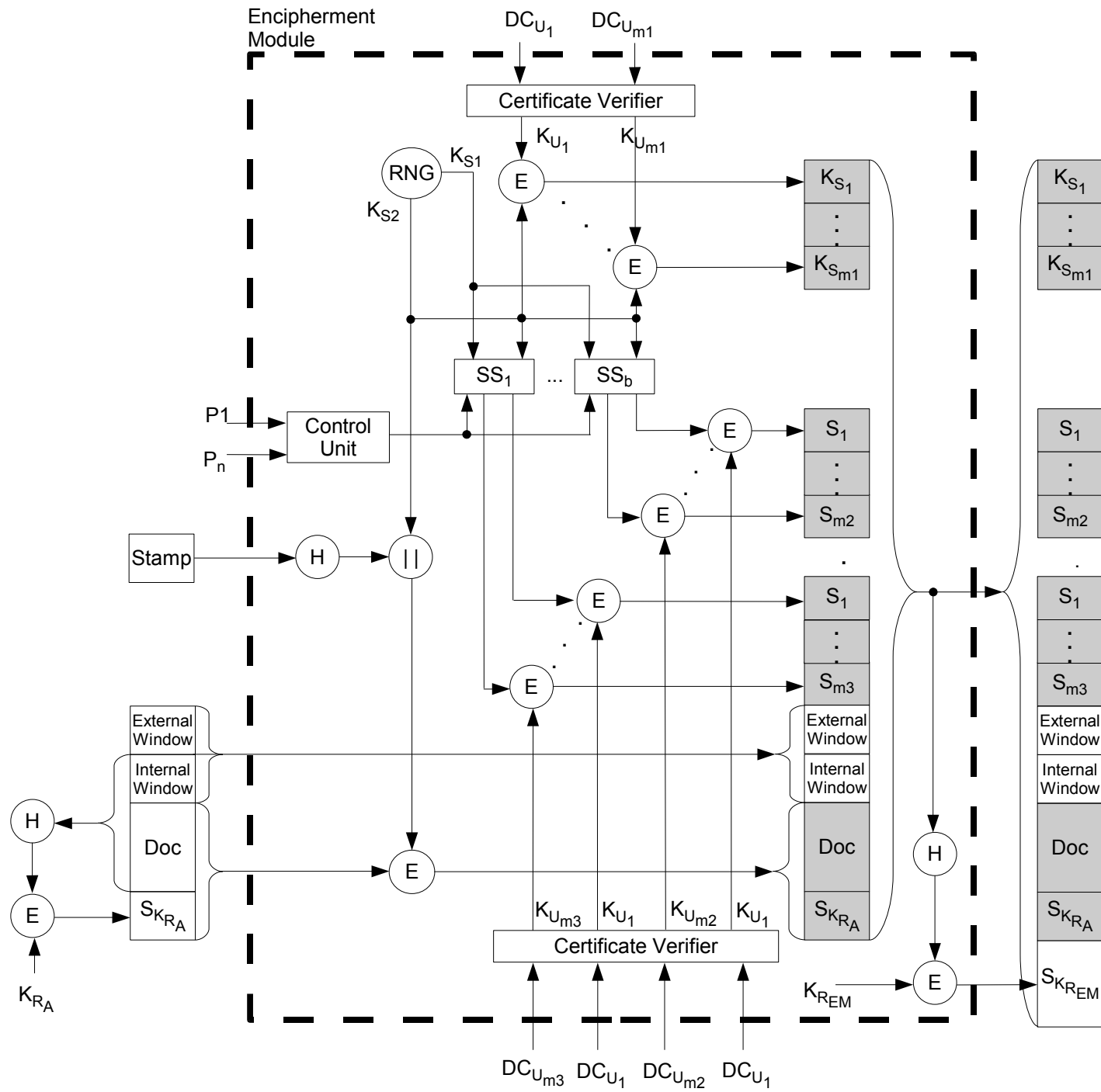
Electronic Document Information Window



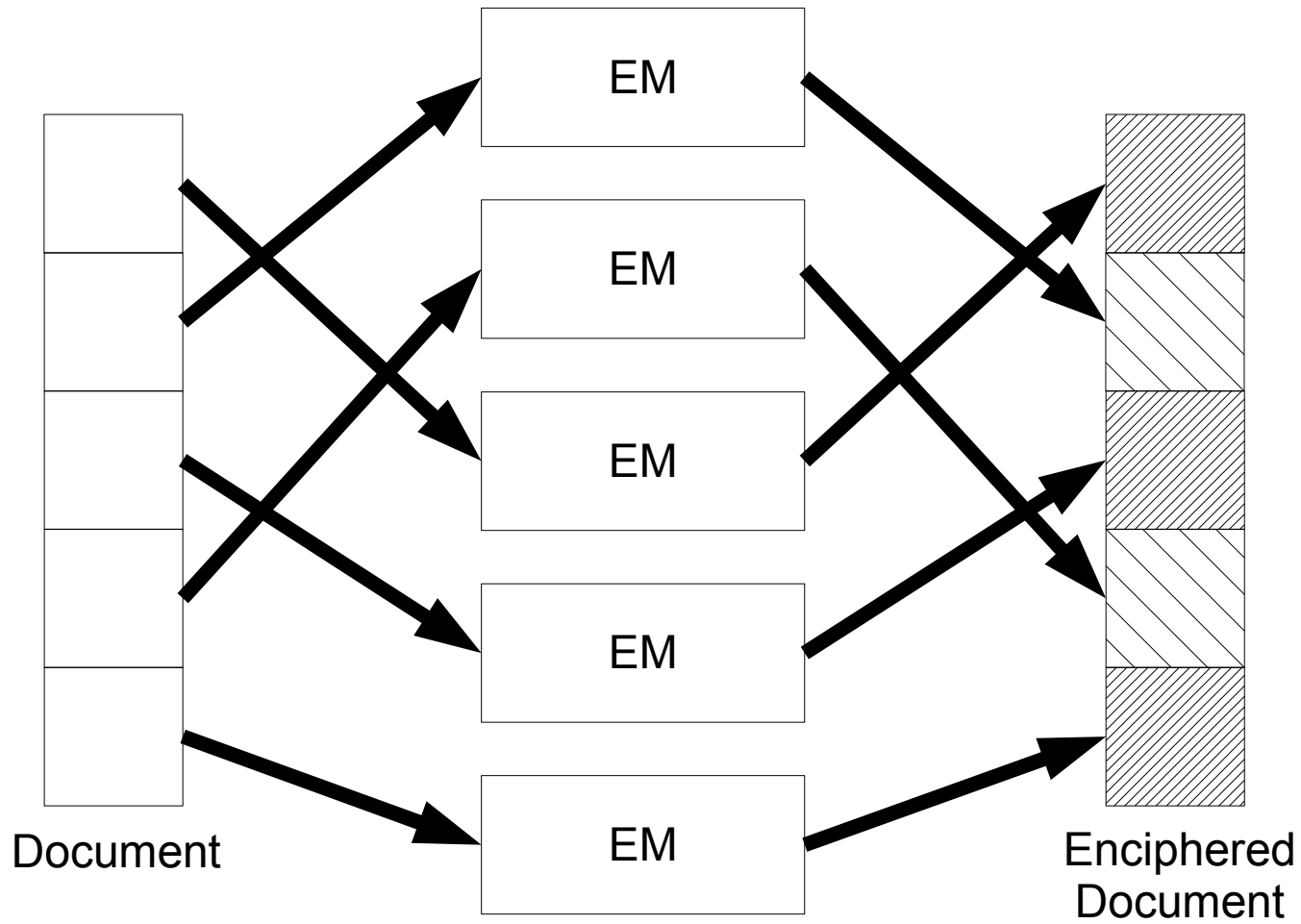
Window Verification



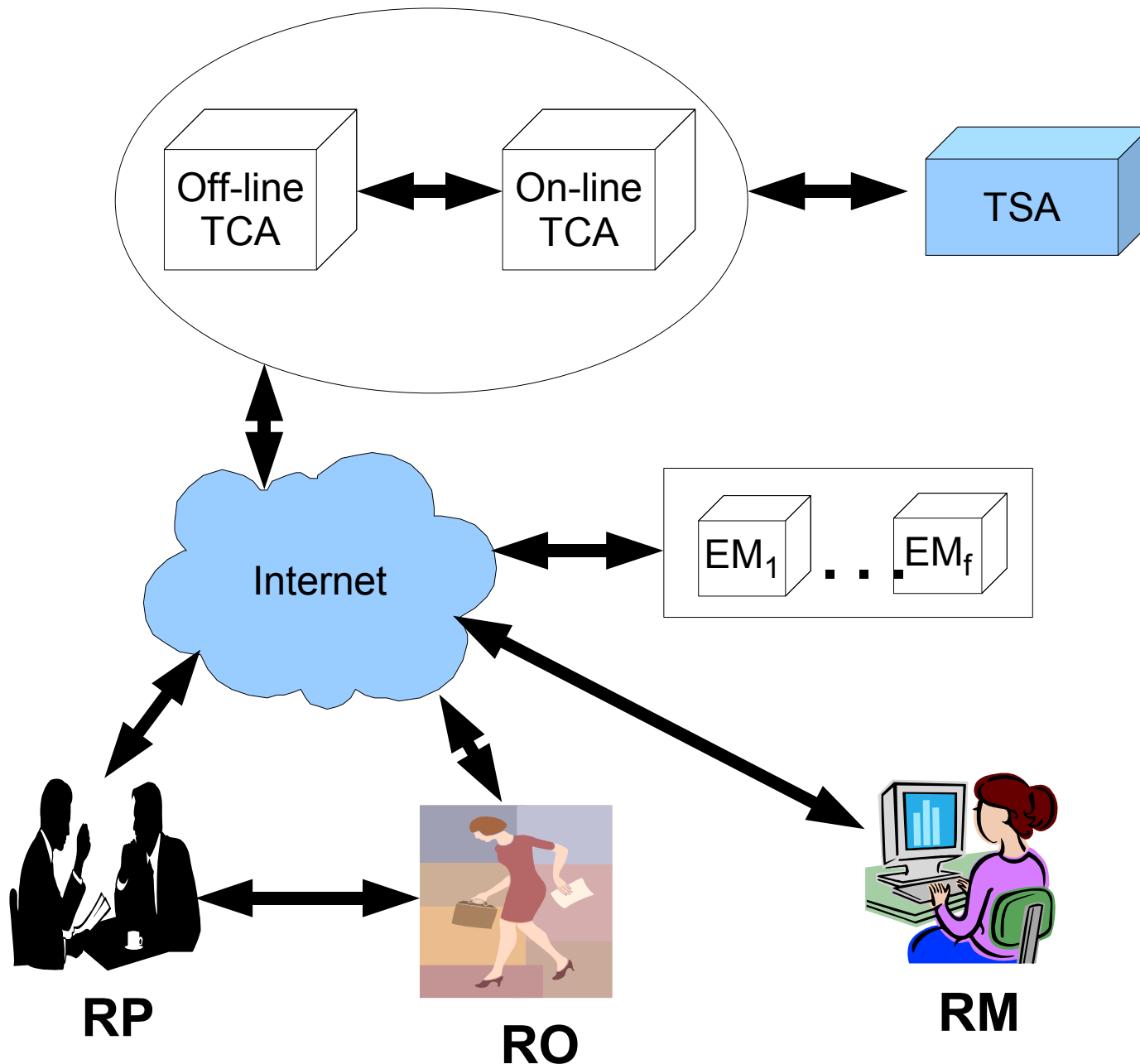
Complete Encryption Module



Use of Multiple EM



Temporal Key Release Infrastructure



Temporal Digital Certificate Request Interface

Form for Request of Temporal Digital Certificate

Information for the management of the private key:

Time release / / - :

Release method Automatic Manual (*against authentication*)

Allowed delay days

Purpose of the temporal certificate

Password for release

Password confirmation

Distinguished Name:

Common Name

Organization

Organization Unity

Locality

E-mail

State

Country

Request Certificate

Cancel

Client TDC Management Interface

Temporal Certificate Authority

Client: Adriana Elissa Notoya

Temporal Digital Certificates

[Request a new temporal digital certificate](#)

Server Current Date and Time: 11/16/2005 10:21:31 am

Common Name	Issue Date	Release Date	Temporal Digital Certificate	Private Key	Report
Adriana Elissa Notoya	11/10/2005 09:42:07am	11/10/2005 10:00:00am	Download	Download	View
Adriana Elissa Notoya	11/10/2005 10:12:44am	11/10/2005 11:00:00am	Download	Download	View
Adriana Elissa Notoya	11/12/2005 05:10:55pm	11/14/2005 08:45:00am	Download	Download	View
Adriana Elissa Notoya	11/15/2005 02:30:22am	11/20/2005 08:00:00am	Download	Unavailable	--
Adriana Elissa Notoya	11/15/2005 02:40:09am	11/20/2005 09:30:00am	Donwload	Unavailable	--

TCA Administrator Interface

Policy

Additional validity days

Key length

Algorithm:

Key Usage: digitalSignature nonRepudiation keyEncipherment
 dataEncipherment cRLSign keyAgreement
 keyCertSign encipherOnly decipherOnly

CPS Pointer:

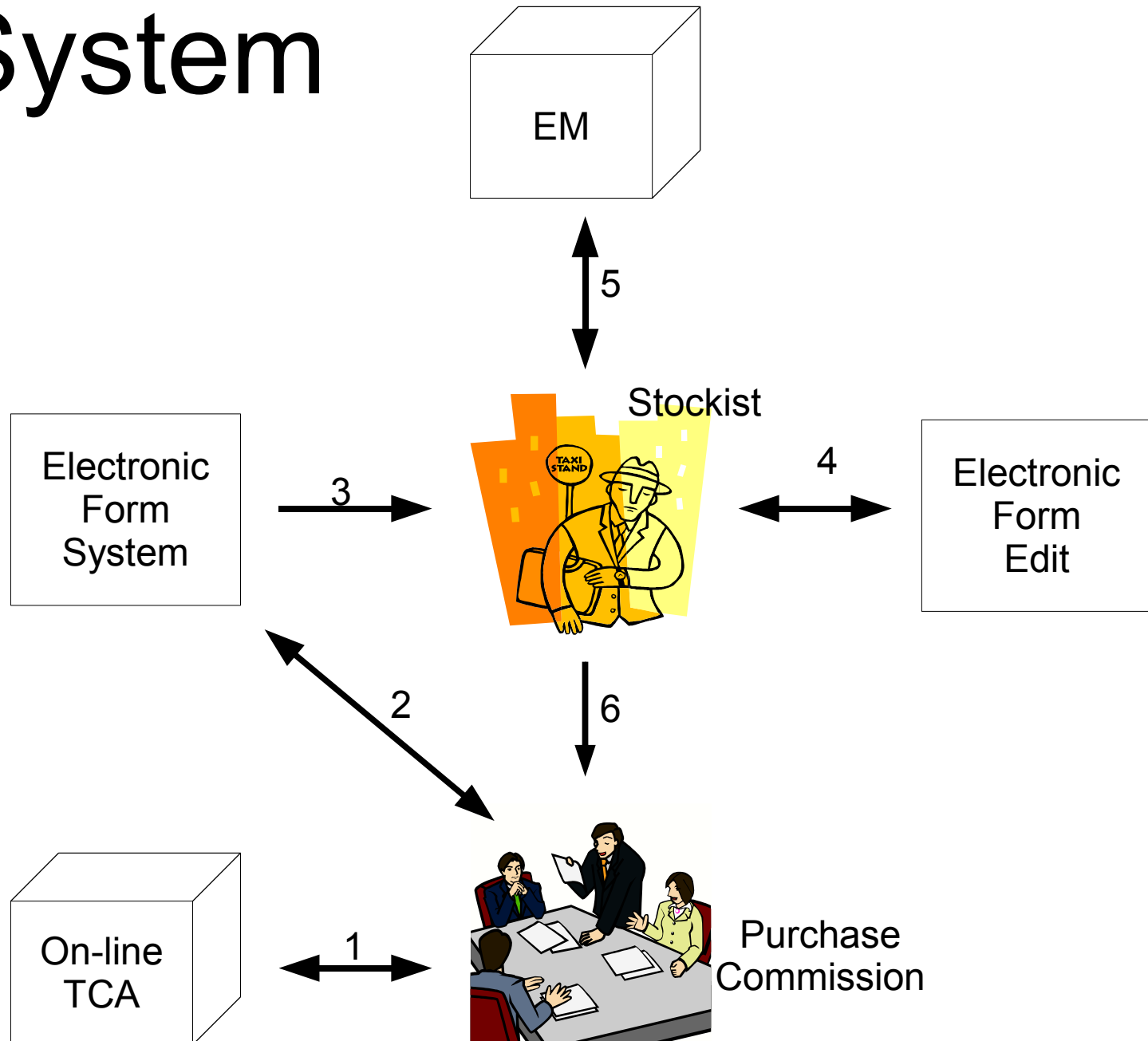
CPS text:

insert

cancel

Bid System

***Brazilian
Act 8666***



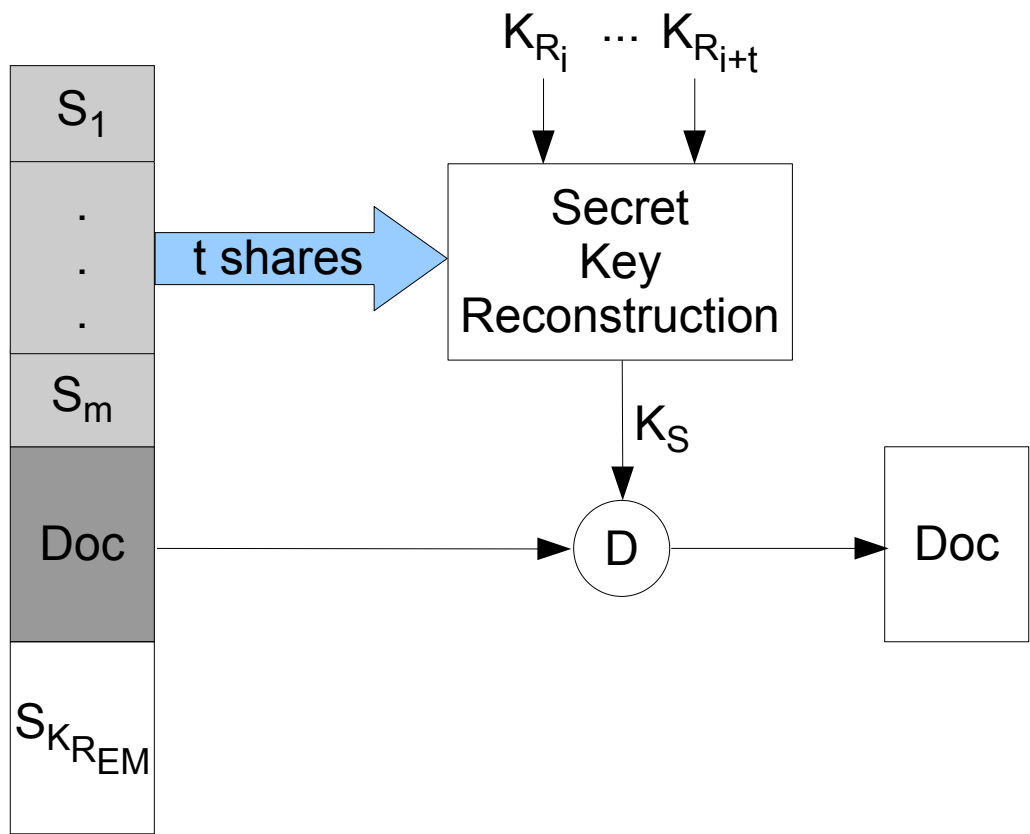
Final Considerations

- Real and practical solution
- Needs to be better codified in law
- Simulates a paper based envelope
- Testing a prototype
- Product already in use in Brazil
- Safe place created to install the infrastructure

Questions?
Suggestions?

Please, send
your questions/suggestions to
custodio@inf.ufsc.br

Electronic Document Disclosure When Using Secret Sharing EM



Electronic Document Disclosure When Using the Basic EM

