Tutorial description to be published in the Conference Proceedings

a. Title of tutorial : **Key Recovery**

b. Instructor : **Dr. Sarbari Gupta**
CygnaCom Solutions, Inc.
7927 Jones Branch Drive Suite 100W
McLean, VA 22102
(703)848-0883 ext 217 (VOICE)
(703)848-0960 (FAX)
Email: sgupta@cygnacom.com

c. Other speakers : **None**

d. Summary of topics to be addressed in your session

This tutorial provides in-depth coverage of all technical aspects of key recovery. It consists of three parts. The first part, entitled “Background and Definitions,” describes the fundamental issues that create the need for key recovery, defines relevant terms, describes a functional model for key recovery, and discusses key recovery policy. The second part, entitled “Current Status,” takes a quick tour of the various key recovery techniques that are currently available, describes the current work being pursued in vendor alliances and standards organizations, and provides an overview of key recovery trial projects being undertaken. Finally, part three, entitled “Deployment,” discusses interoperability issues, the steps involved in obtaining US export approval for key recovery products, and global deployment issues for key recovery systems. This tutorial does not address the political debates surrounding key recovery, or the privacy rights issues related to the use of key recovery.

A Tutorial on Key Recovery

Dr. Sarbari Gupta

CygnaCom Solutions

sgupta@cygnacom.com

(703)848-0883 ext 217

Outline

- **Background and Definitions**
- Current status
- Interoperability and Deployment

Background and Definitions

- The Need for Key Recovery
- Key Recovery Definitions
- Key Recovery Model
- Key Recovery Policy

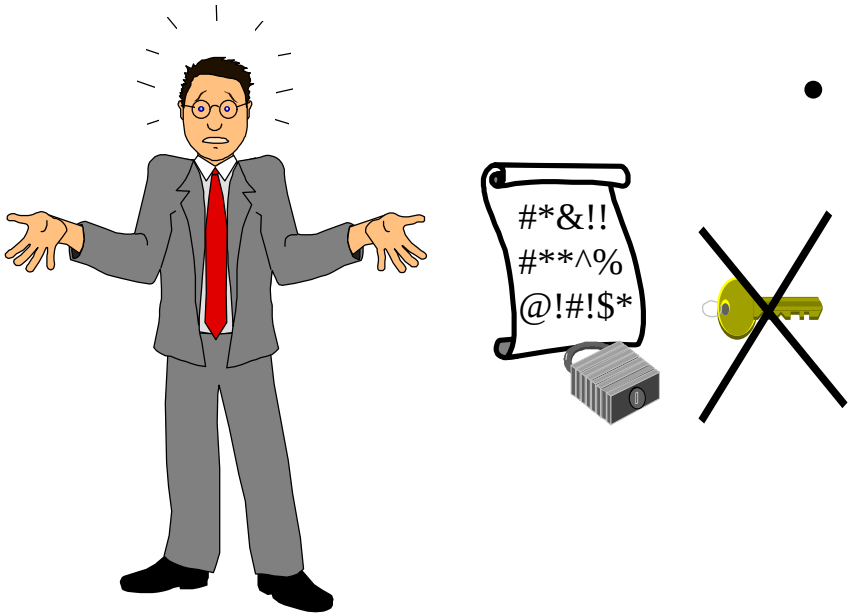
Need for Key Recovery

- Use of encryption for data confidentiality
- Problem for individuals
- Problem for enterprises
- Problem for law enforcement
- current US export regulations

Use of encryption for data confidentiality

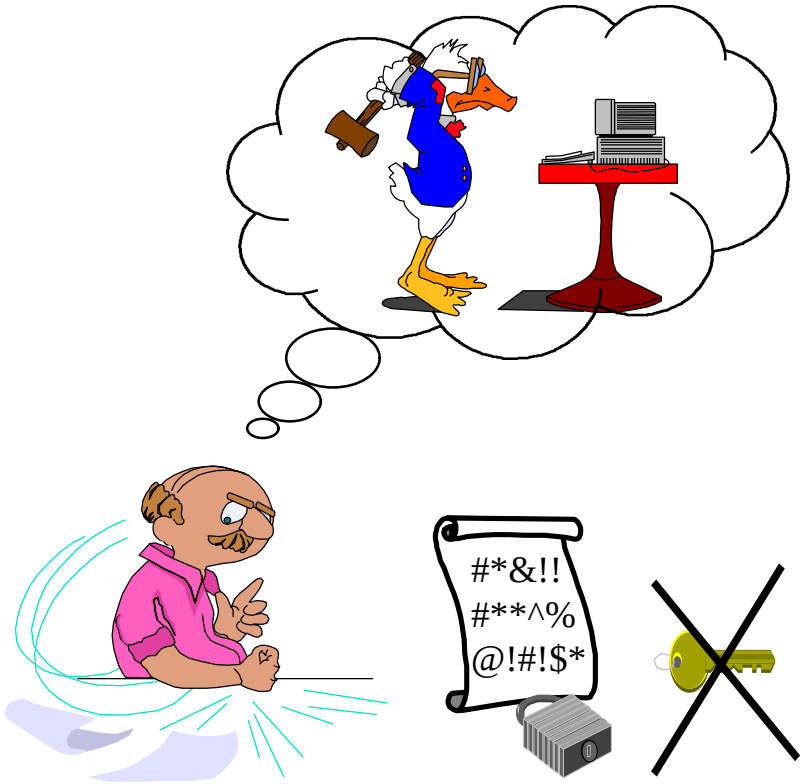
- Secure storage/transfer of electronic documents
- Secure E-mail
- Securing data on the Web
- Secure electronic commerce
- Secure network connections

Problem for Individuals



- Lost Keys
- Corrupted Keys

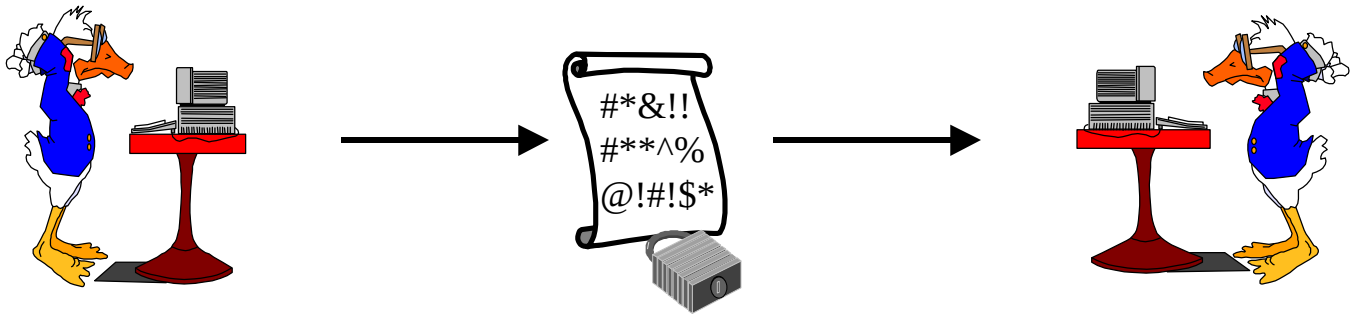
Problem for Enterprises



- Careless Employee
- Absent Employee
- Disgruntled Employee
- Employee under surveillance

Problem for Law Enforcement

- National Security
- Surveillance



US Crypto Export Policy
(Supp. 4 Part 742 Criteria)

- product must make decryption key available
  - under legal authority
  - w/o cooperation or knowledge of user
- crypto functions must be inoperable until key is made available
- output of product must contain recovery information
  - in accessible format
  - with reasonable frequency
- allow recovery whether product generates/receives ciphertext

Key Recovery Operational Scenarios

Law Enforcement Key Recovery (LE scenario)

- recovery for law enforcement needs
- mandatory key recovery
- based on key recovery policy set by jurisdictions of manufacture/use

Enterprise Key Recovery (ENT scenario)

- recovery for enterprise monitoring and audit needs
- mandatory key recovery
- based on key recovery policy set by enterprise of use

Individual Key Recovery (INDIV scenario)

- recovery for owner of data when keys are lost/destroyed
- discretionary key recovery
- triggered by owner of data

Background and Definitions

- The Need for Key Recovery
- **Key Recovery Definitions**
- Key Recovery Model
- Key Recovery Policy

Key Recovery

- Key Recovery encompasses mechanisms that provide a secondary means of access to the cryptographic keys used for data confidentiality.

  [NOTE: It is assumed that all cryptographic systems provide a primary means of obtaining the confidentiality key.]

Types of Key Recovery Mechanisms

Key Escrow

Keys or key parts escrowed with Escrow Agent(s)

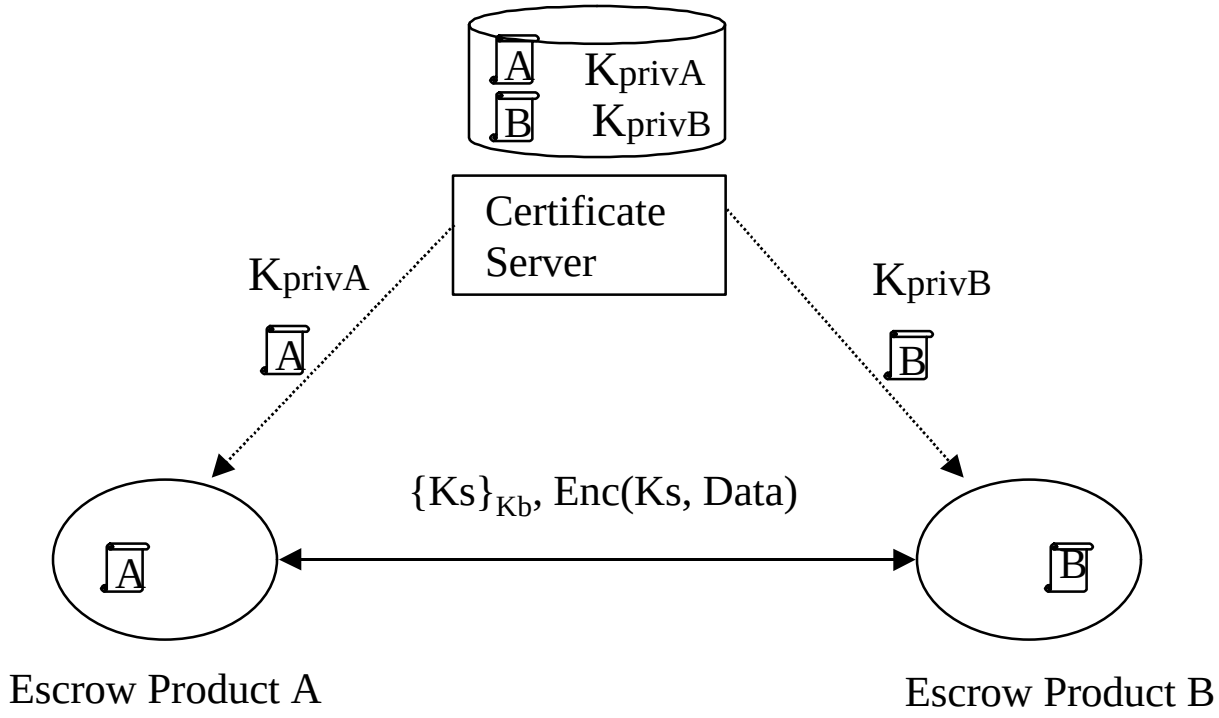
Key Encapsulation

Keys or key parts encapsulated into key recovery block and associated with ciphertext. The de-encapsulation may be done by Recovery Agent(s).

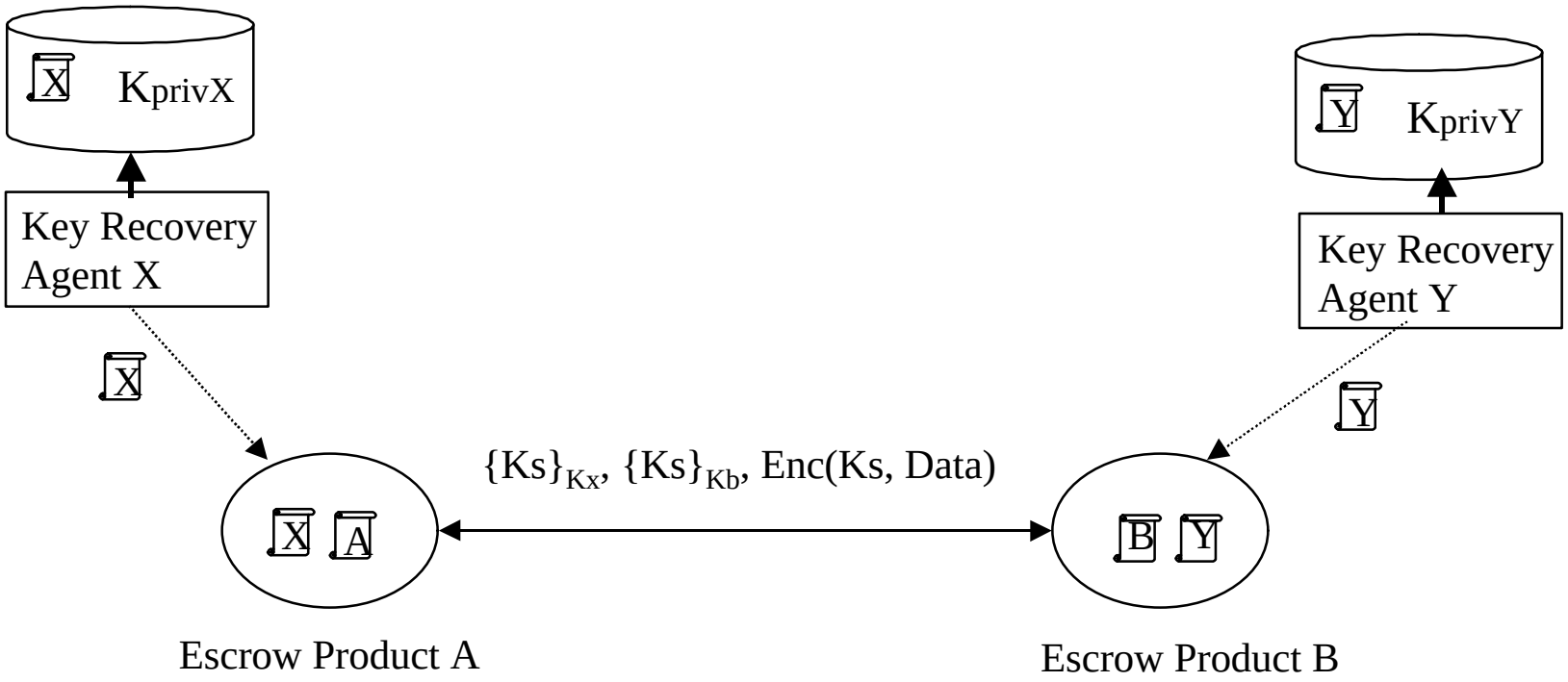
Hybrid

Combination of escrow and encapsulation mechanisms

Key Escrow Example

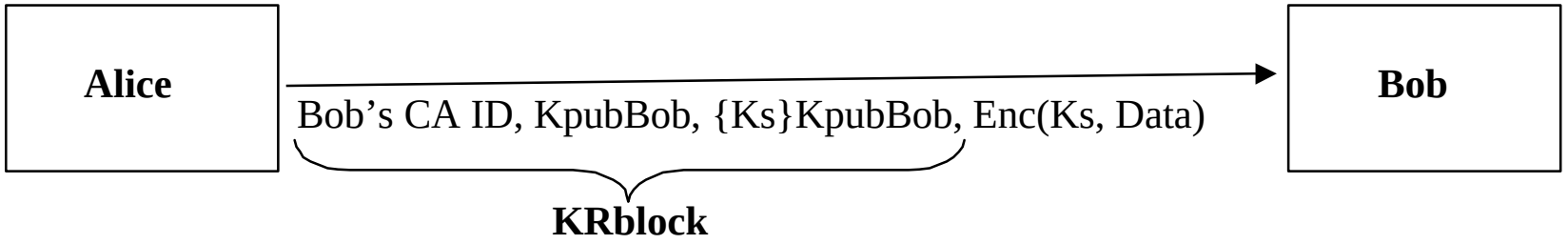


Key Encapsulation Example

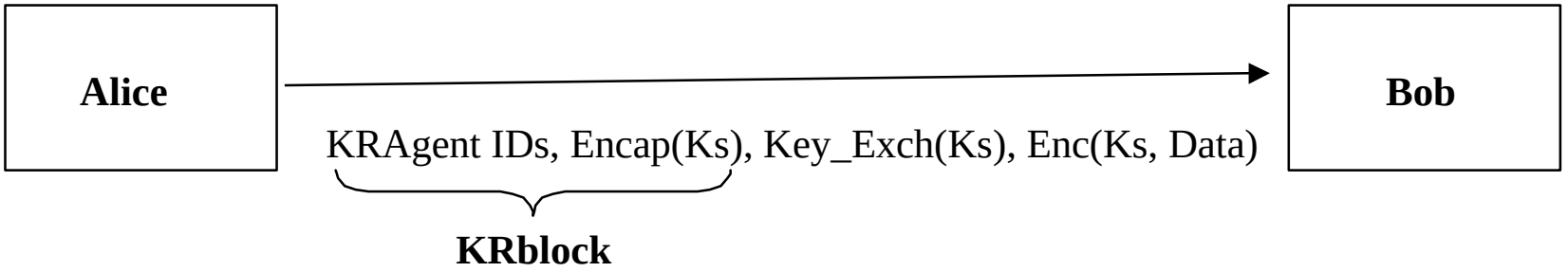


Key Recovery Block Examples

Private Key Escrow



Ephemeral Key Encapsulation

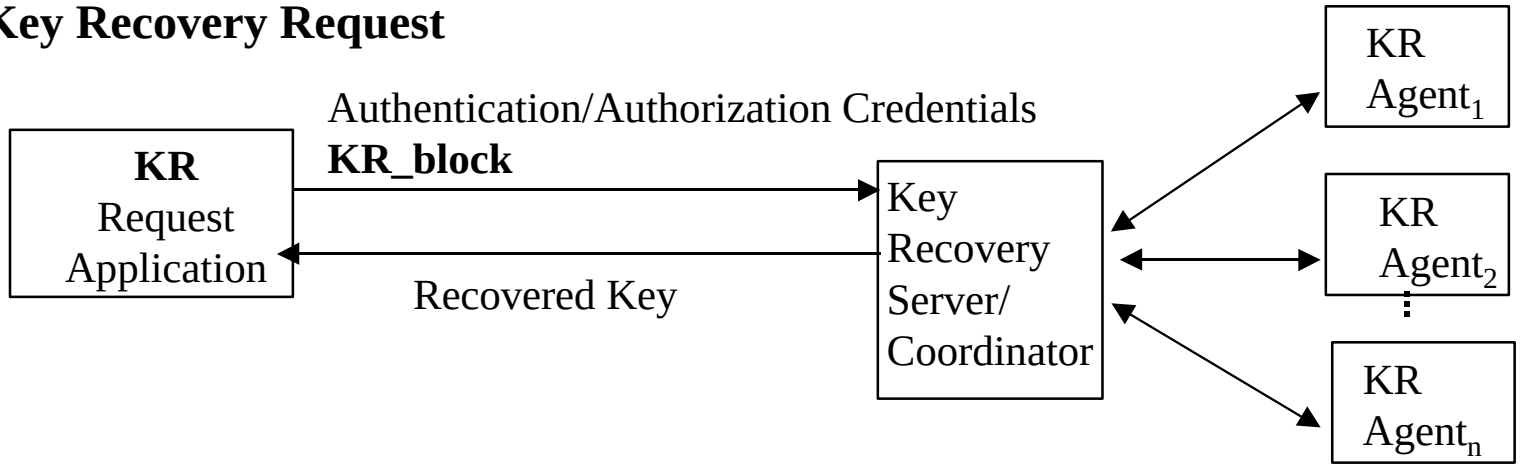


Phases of Key Recovery

Key Recovery Registration/Setup (optional)

Key Recovery Enablement

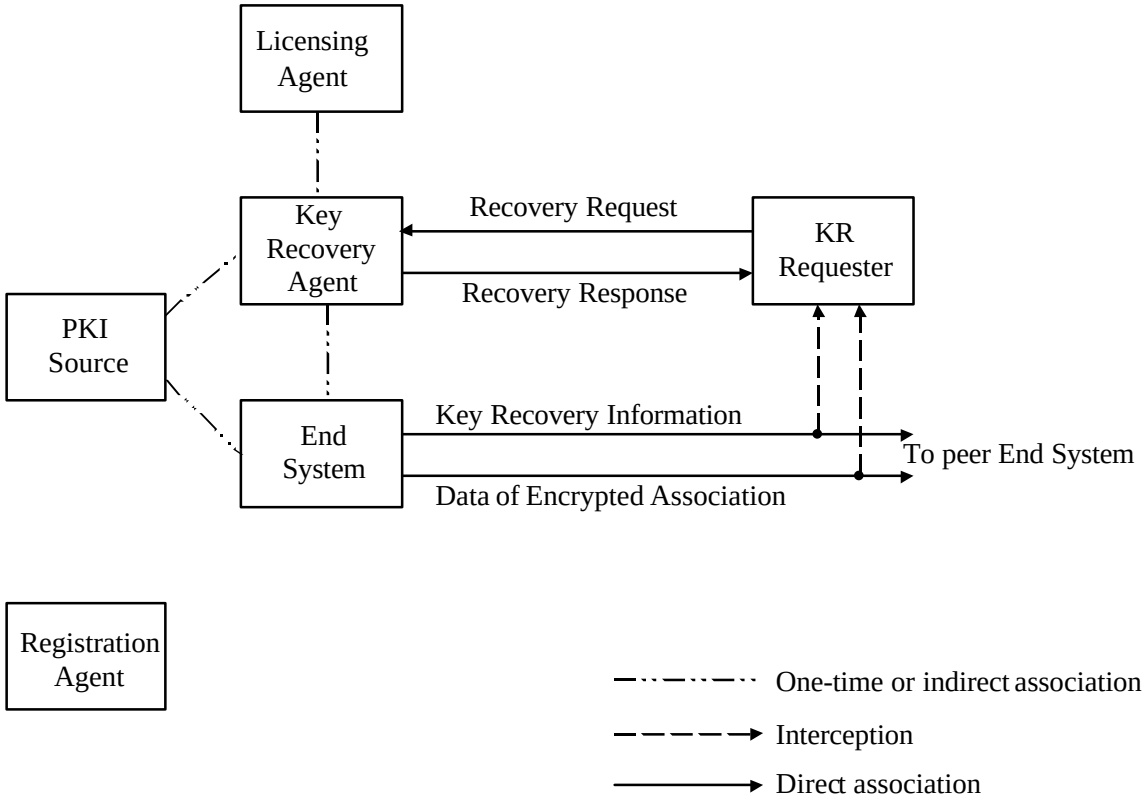
Key Recovery Request



Background and Definitions

- Key Recovery Definitions
- The Need for Key Recovery
- **Key Recovery Model**
- Key Recovery Policy

Key Recovery Model



Key Recovery Information

Aggregate of the information that is used to facilitate the (direct or indirect) recovery of the confidentiality key used by end systems to encrypt data.

- typically generated by the encryptor end system
- may be validated by the decryptor end system
- made available to the requestor entity
- used to recover the confidentiality key

End Systems

Parties or clients who generate confidentiality-protected data and wish to have their data made recoverable through key recovery techniques

Key Recovery Agents

The escrow agents or the recovery agents that possess the keying material required to recover the keys needed to decrypt confidentiality-protected data.

Key Recovery Requester

Entity that interacts with one or more KRAs to recover the key needed to decrypt the confidentiality-protected data generated by the end systems.

- responsible for the location and collection of the KRI
- needs to provide proof of authorization to KRA(s)
- May act on behalf of end user, enterprise or law enforcement

KR Public Key Sources

The Certification Authorities that provide public key certificates to the other entities (e.g. end systems, KRAs, requestors, etc.) in the key recovery system.

Licensing/Registration Agents

- *Licensing Agent* - An entity who maintains information on the various key recovery products, the schemes the products deploy, and the location of key recovery information
- *Registration Agent* - An entity which accredits KRAs in order to ensure the security, trustworthiness, and impartiality of the KRAs to be able to handle incoming key recovery requests, and maintain the keying material needed to perform key recovery.

Background and Definitions

- Key Recovery Definitions
- The Need for Key Recovery
- Key Recovery Model
- **Key Recovery Policy**

Key Recovery Policy

The Key Recovery Policy determines:

- when key recovery information is to be generated
- when key recovery information is to be received
- how key recovery information that is received is to be processed/validated
- what key recovery agents may be used by the product in the generation and processing of KRI

Key Recovery Policy Types

- Jurisdiction-controlled policy
- Organizational policy
- Individual policy

US Export based Key Recovery Policy

Policy for exported cryptographic products for non-US use

Encryption Algo	Maximum Allowed Encryption Key Length w/o Key Recovery
DES	56 bits
RC2	56 bits
RC4	56 bits
All	0 bit

Policy for US domestic use

Encryption Algo	Maximum Allowed Encryption Key Length w/o Key Recovery
All	infinity

Configurability

Key Recovery Products may allow limited configurability of the KR policies used by them:

- Enterprise KR Policy (system administrator configurable)
- Individual KR Policy (end user configurable)

Non-circumventability

The implementation of mandatory key recovery policies need to be non-circumventable or non-bypassable

- Law Enforcement KR policy
- Enterprise KR policy

Outline

- Background and Definitions
- **Current status**
- Interoperability and Deployment

Current Status

- Tour of available key recovery techniques
- Organizations working on KR Issues
- Key Recovery Trial Projects

Outline

- Background and Definitions
- Current status
- **Interoperability and Deployment**

Key Recovery Interoperability

Compatibility areas:

- Application Protocol
- Key Recovery Mechanism
- Key Recovery Policy
- Key Recovery Agent

Protocol Interoperability

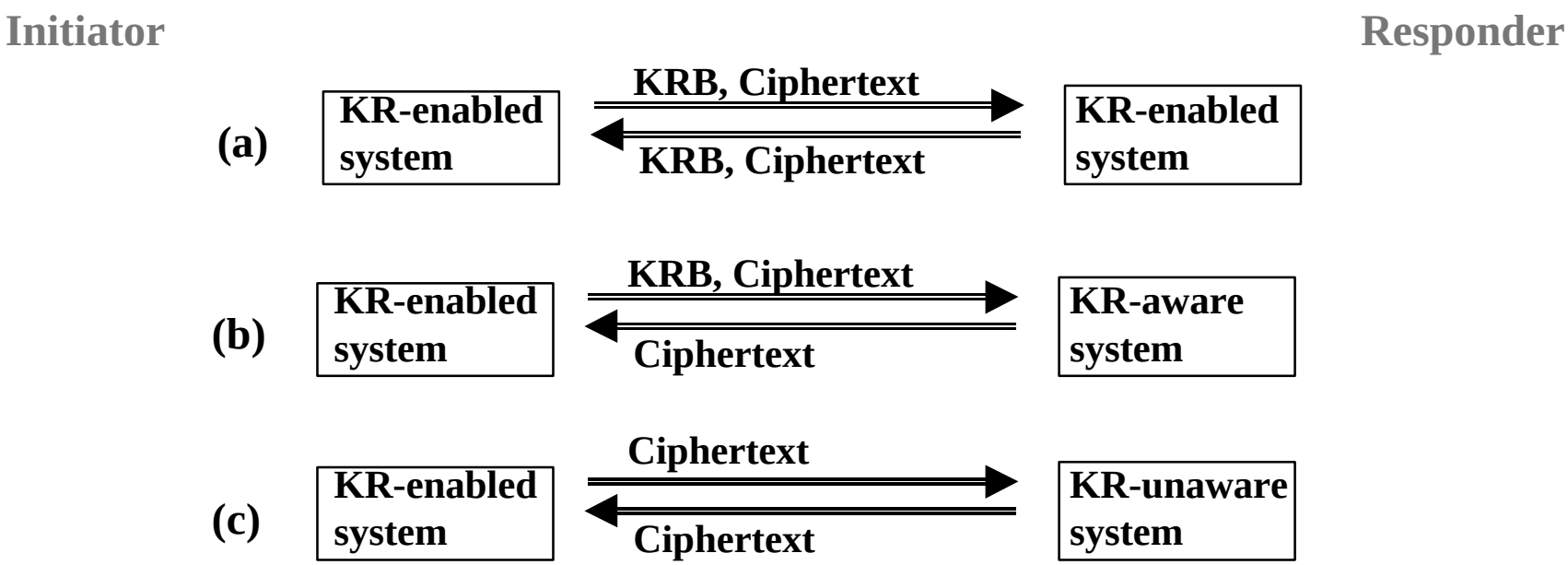
KR system has to make KRB available to interceptor. Choices:

- ***Primary Channel***: flow KRB within data security protocol (e.g. SSL, IPSEC, S/MIME)
  - – legacy protocols need to accommodate KRB
    - – use of existing hooks or reserved fields to carry KRB
    - – explicit extension of protocol to carry KRB
  - – new data security protocols designed to accommodate KRB

- ***Secondary Channel***: flow KRB along protocol separate from data security protocol
  - – no extensions required to data security protocol
  - – linking of the KRB and the data security protocol instantiation required

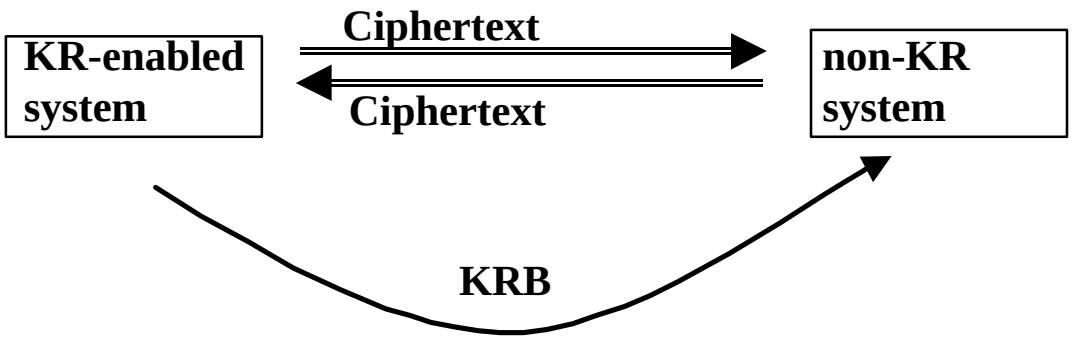
Interoperability Scenarios

(KRB carried in data security protocol)



Interoperability Scenarios

(KRB carried in separate protocol)



Key Recovery Mechanism Compatibility

- KRI generation
  - sender generates KRI for receiver (sender needs to support KR mechanism of receiver)
- KRI Validation
  - semantic validation of KRI (receiver needs to support KR mechanism of sender)
  - non-semantic validation of KRI (use of Common Key Recovery Block Format options)

Key Recovery Policy Compatibility

- Policy on KRI generation
  - if one party generates KRI, it must satisfy the KR policy of both sides of association
- Policy on KRI receipt and validation
  - if KRI validation is required by receiver, sender and receiver need to agree on validation technique

Key Recovery Agent Compatibility

- ***Use of common KRA(s) by both parties*** **-** the policies of the common KRA(s) must be agreeable to both sides

- ***Use of different KRA(s) by each party*** **-** the KRA(s) used by one party may have to be trusted (through certificate chaining / validation) by the other party

Global Deployment of Key Recovery

- National sovereignty issues
- Need for standardization
- Need for global public key infrastructures

National Sovereignty

Each country wants sovereignty over their :

- Crypto and Key Recovery policies
- KRA Policies and Procedures
- PKIs for the KRAs

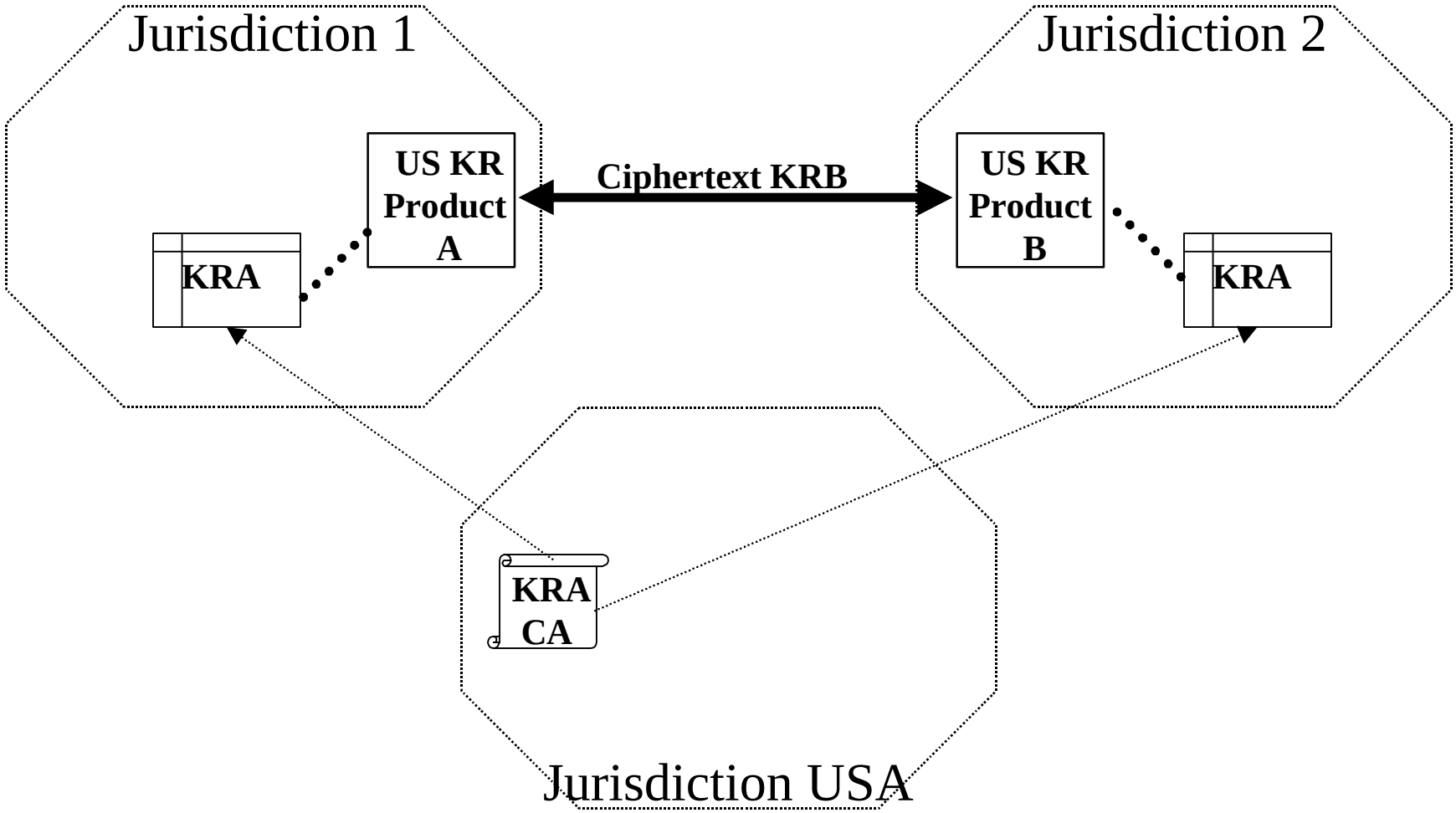
Need for Standardization

- Protocols to accommodate KRI
- KRI formats
- Crypto and Key Recovery policies
- KRA Policies and Procedures

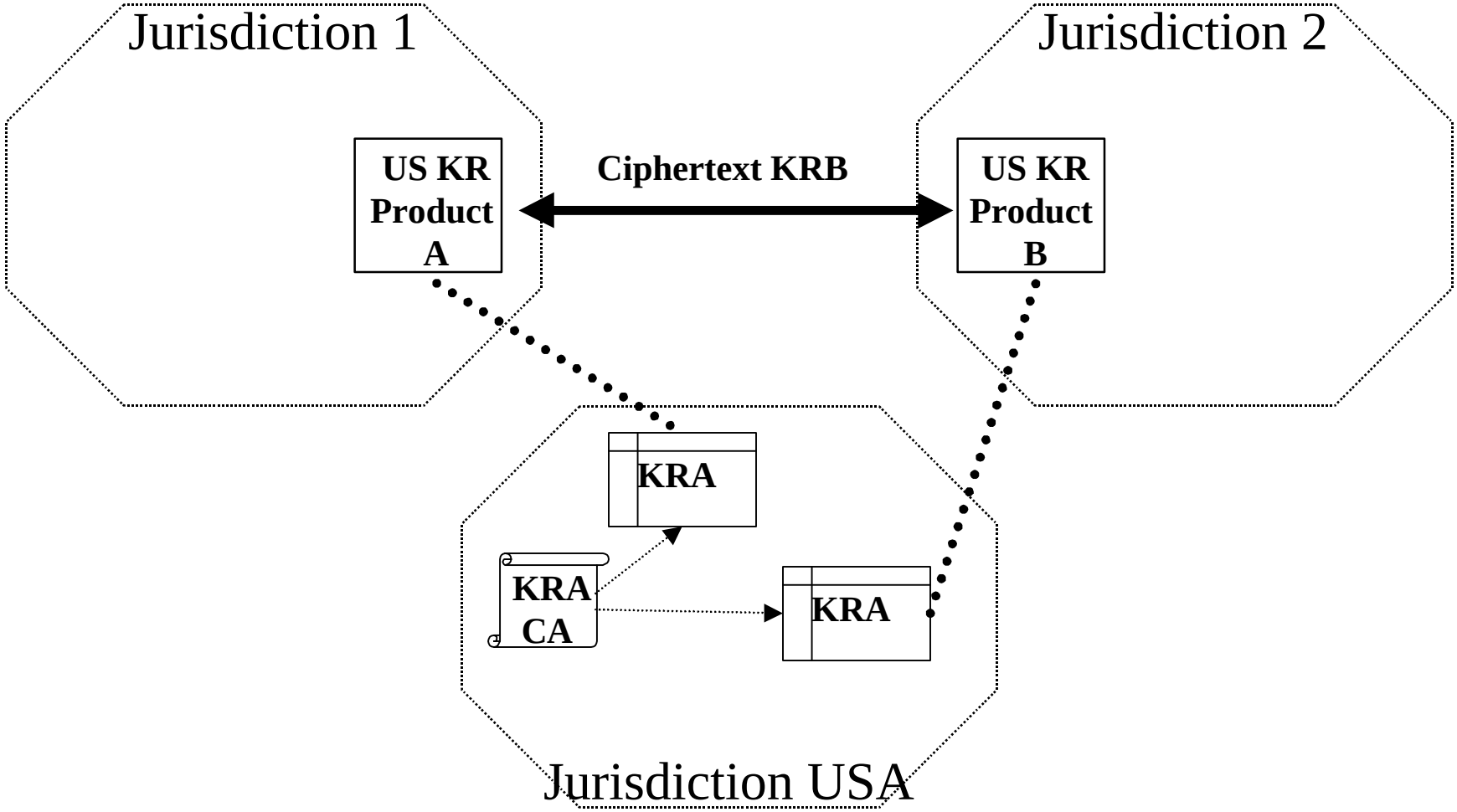
Need for Global PKIs

- Global hierarchy with single root
- Comparable certification policies for CAs
- Cross-certification of CAs

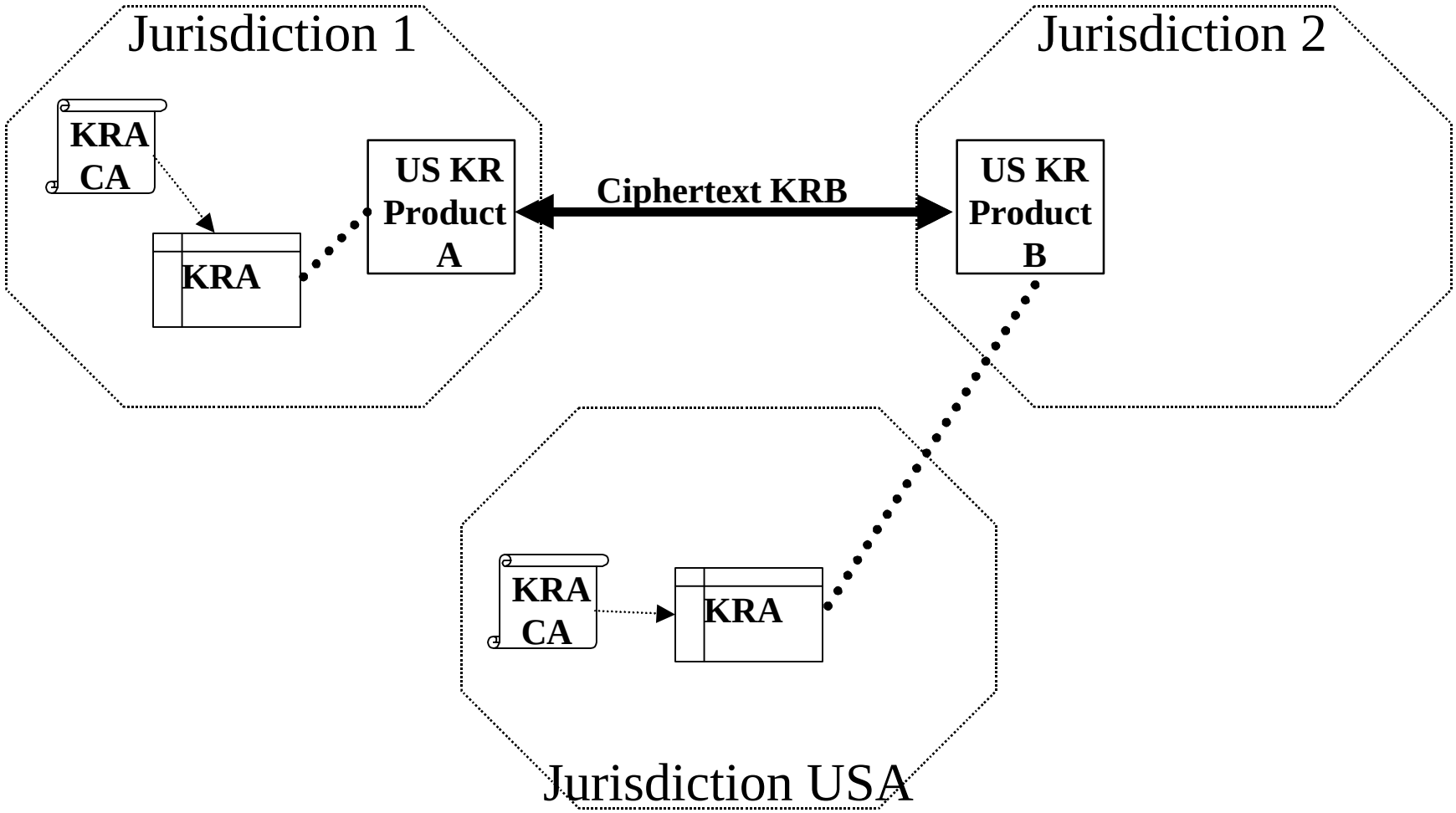
US KR Product Deployment Scenario I



US KR Product Deployment Scenario II



US KR Product Deployment Scenario III



US KR Product Deployment Scenario IV