



RecoverKey™

Emergency Secret-Key Recovery

**Trusted Information Systems
3060 Washington Road (Rt. 97)
Glenwood, MD 21738**

World Wide Web: <http://www.tis.com>

Internet E-Mail: tis@tis.com

Tel.: (301)854-6889

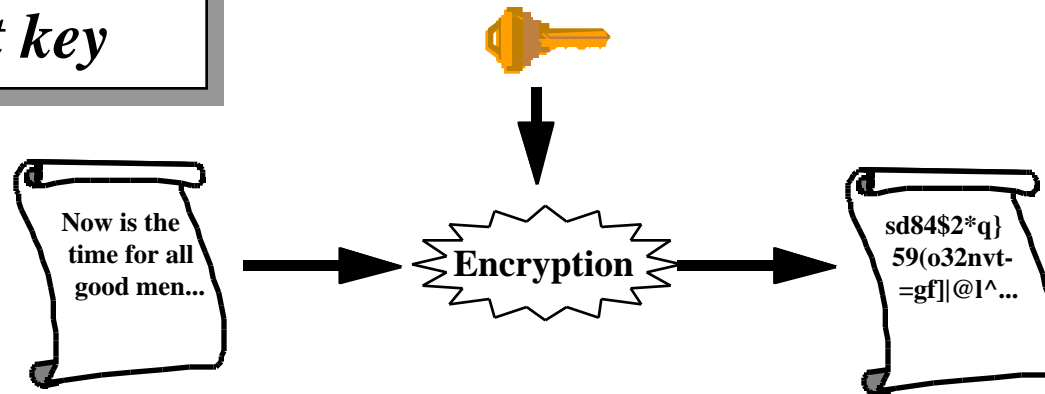
Overview

- Background
 - Problems
 - U.S. Export Restriction Evolution
 - Recent Events
- The RecoverKey Solution
- RecoverKey Products
- RecoverKey Benefits Summary
- Who to Contact

Problem

Recovering Lost Keys

*User encrypts file
with secret key*

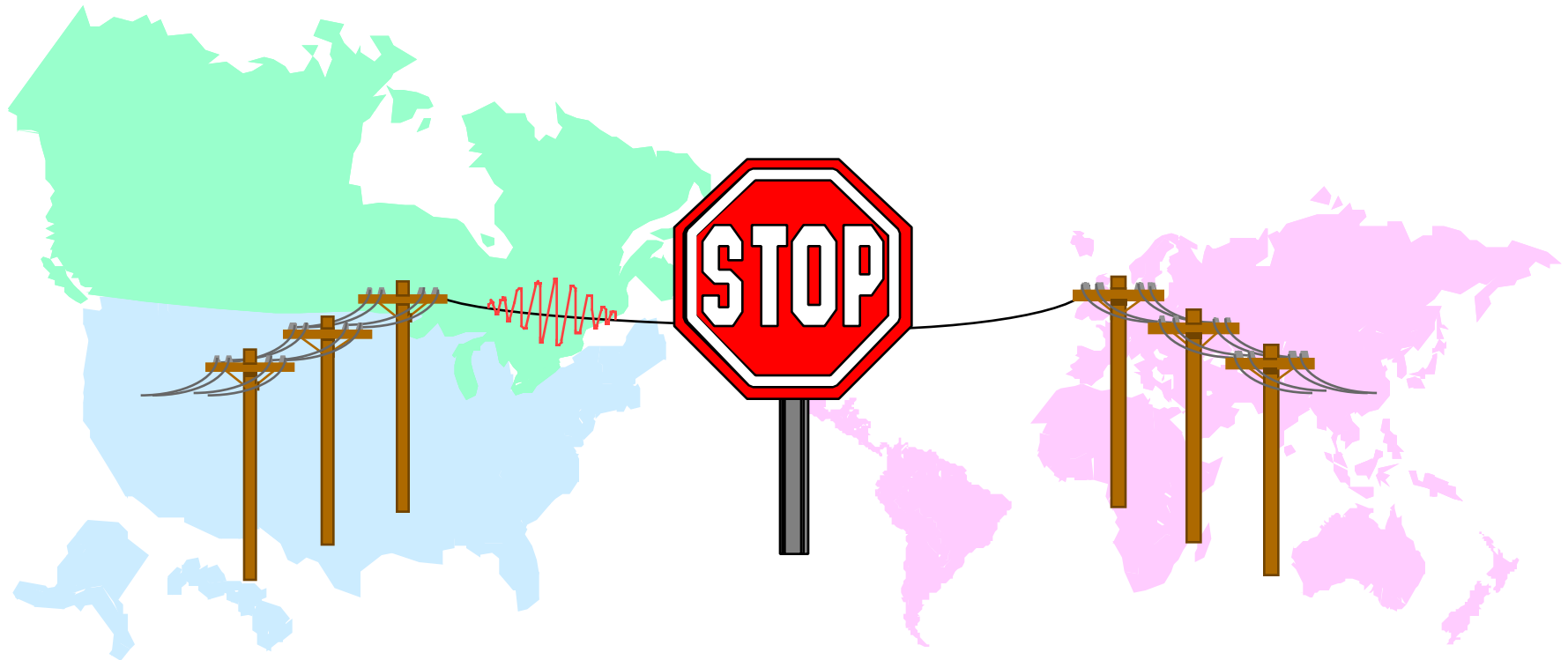


*If secret key is lost -
file cannot be decrypted*



Problem

Restrictions on Cryptography



U.S. Government restricts cryptography to protect law enforcement and national security interests

Last Year's Export Perspective

Recent Evolution...

1992 → 40 bits

1993 → Clipper X

1994 → Cantwell Initiative X

1995 → Key Escrow Initiative

At last year's RSA conference...

**Export relief for
64 bit crypto with
key recovery**

The Gore Initiative

- Announced October 1, 1996
- “...the **export of 56-bit key length encryption products will be permitted**...contingent upon industry commitments to build and market future products that support key recovery.”
- “**No key length limits** or algorithm restrictions will apply to exported key recovery products.”
- “**Domestic use** of key recovery will be **voluntary**...”

Industry Key Recovery Alliance

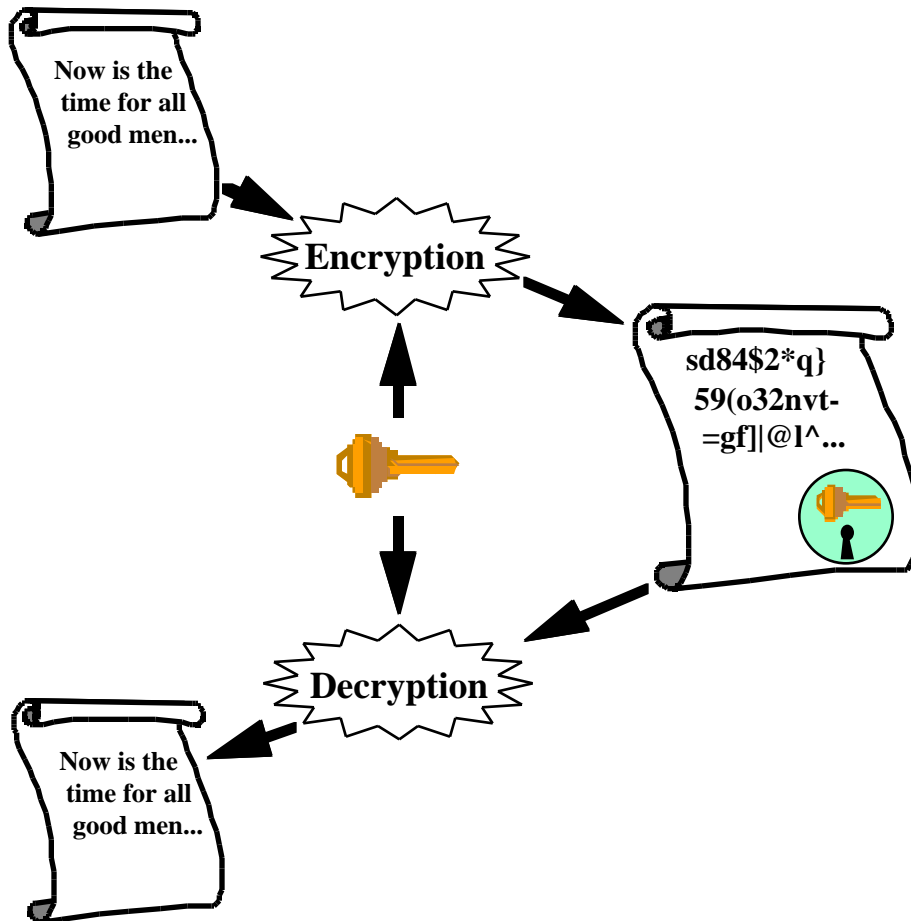
- **Goal: enable authorized recovery of encrypted information**
- The companies forming the alliance will achieve this goal by examining interoperability issues and technologies that meet the requirements of business and could allow easing of restrictions of cryptographic import/export around the world.

Founding Members

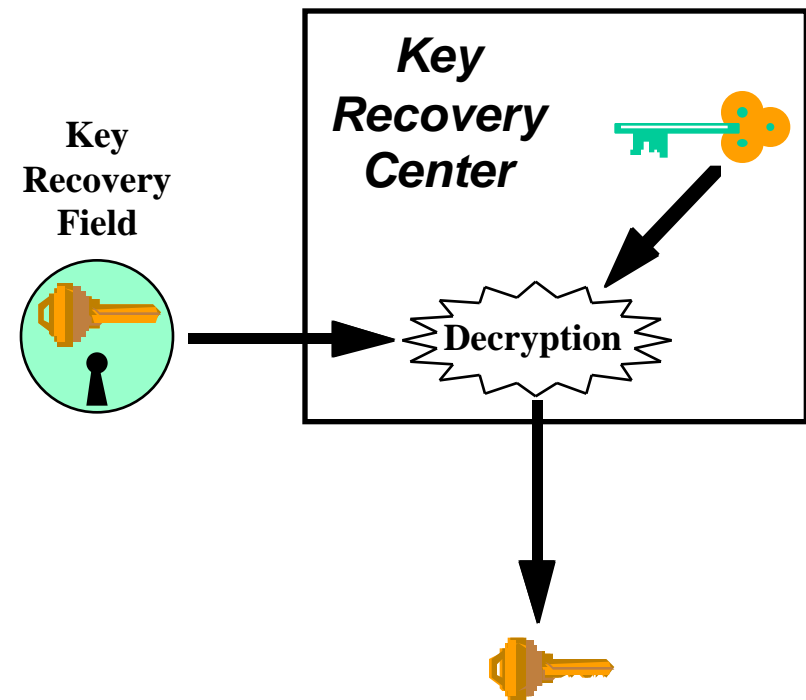
- | | |
|---------------------------------|-------------------------------|
| • Apple Computer, Inc. | • NCR Corp. |
| • Atalla | • RSA |
| • Digital Equipment Corporation | • Sun Microsystems, Inc. |
| • Groupe Bull | • Trusted Information Systems |
| • Hewlett-Packard Company | • UPS |
| • IBM | |

TIS Solution: RecoverKey

Application

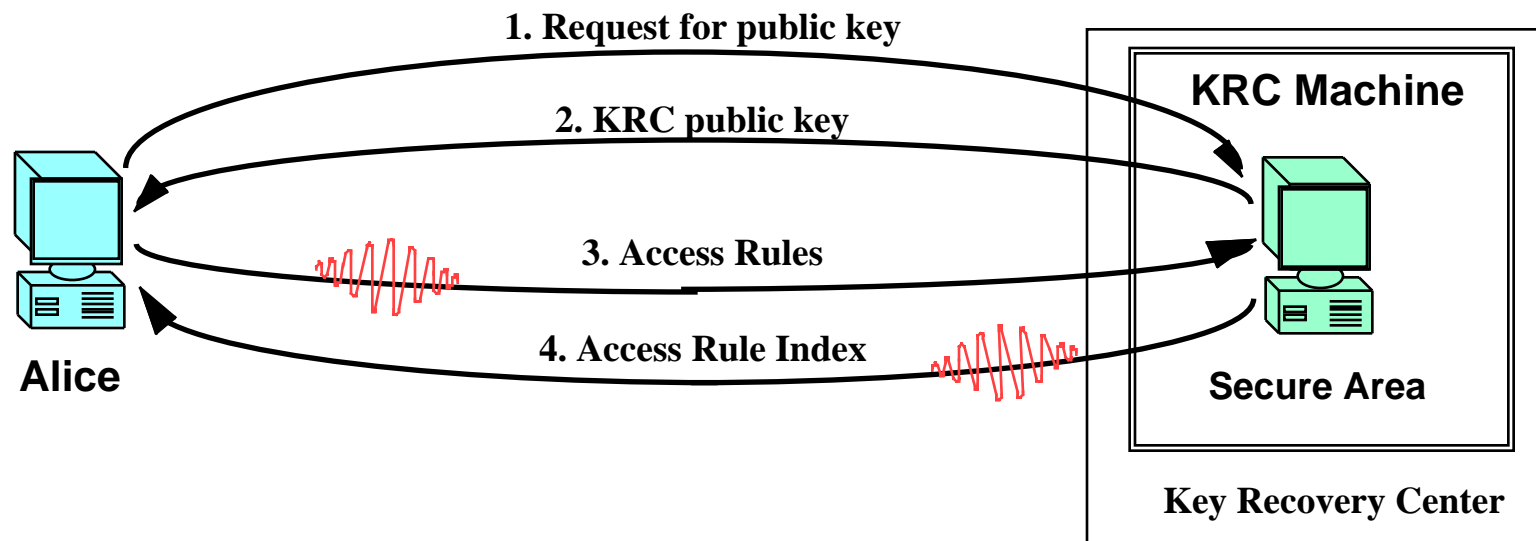


Key Recovery



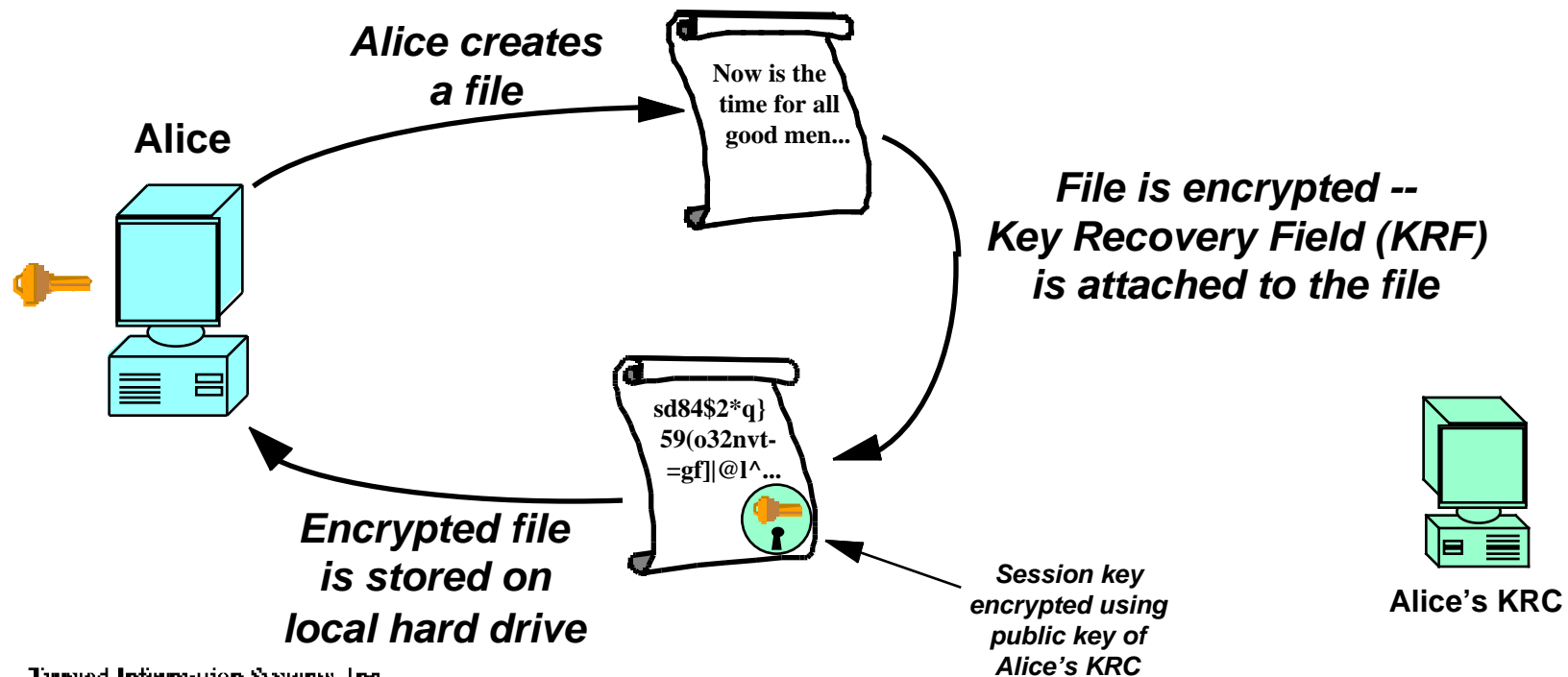
Client Registration

- Client retrieves a public key from the Key Recovery Center
- Client provides access rules and obtains access rule index (ARI)



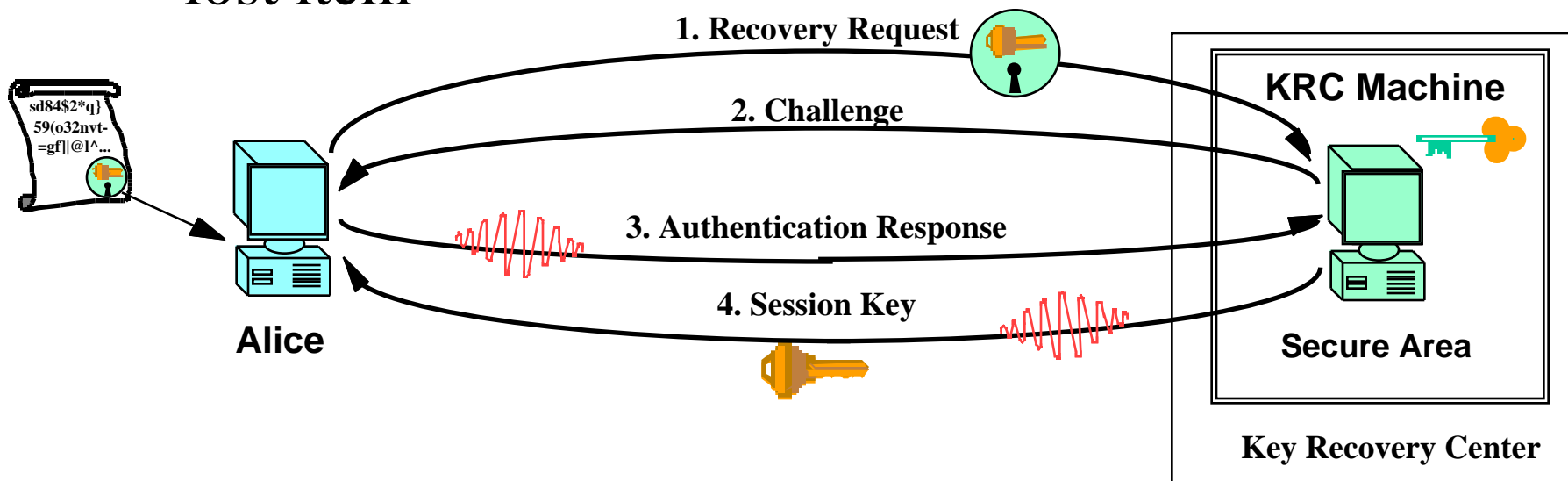
Example Client Application

- Client uses RecoverKey-enabled cryptography
 - Client product generates key recovery field, associates it with data
 - No communication with Key Recovery Center necessary unless emergency access is needed



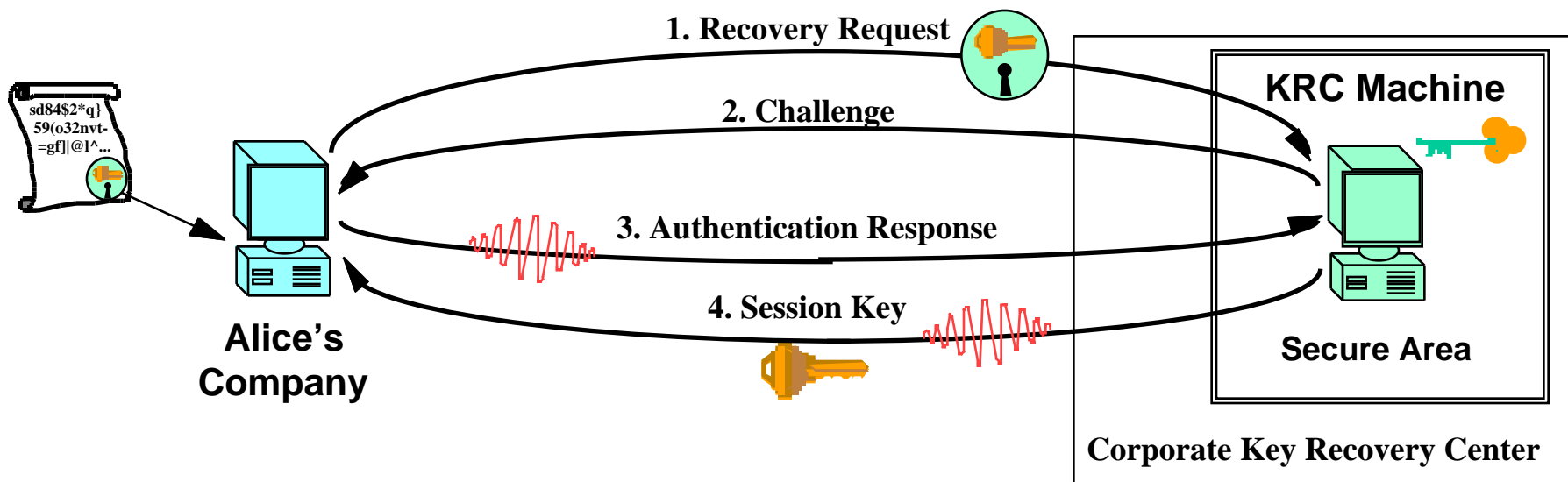
Client Key Recovery

- If the client loses their data key, the KRF and corresponding authentication information are sent to the KRC
- The KRC validates the information and returns the lost item



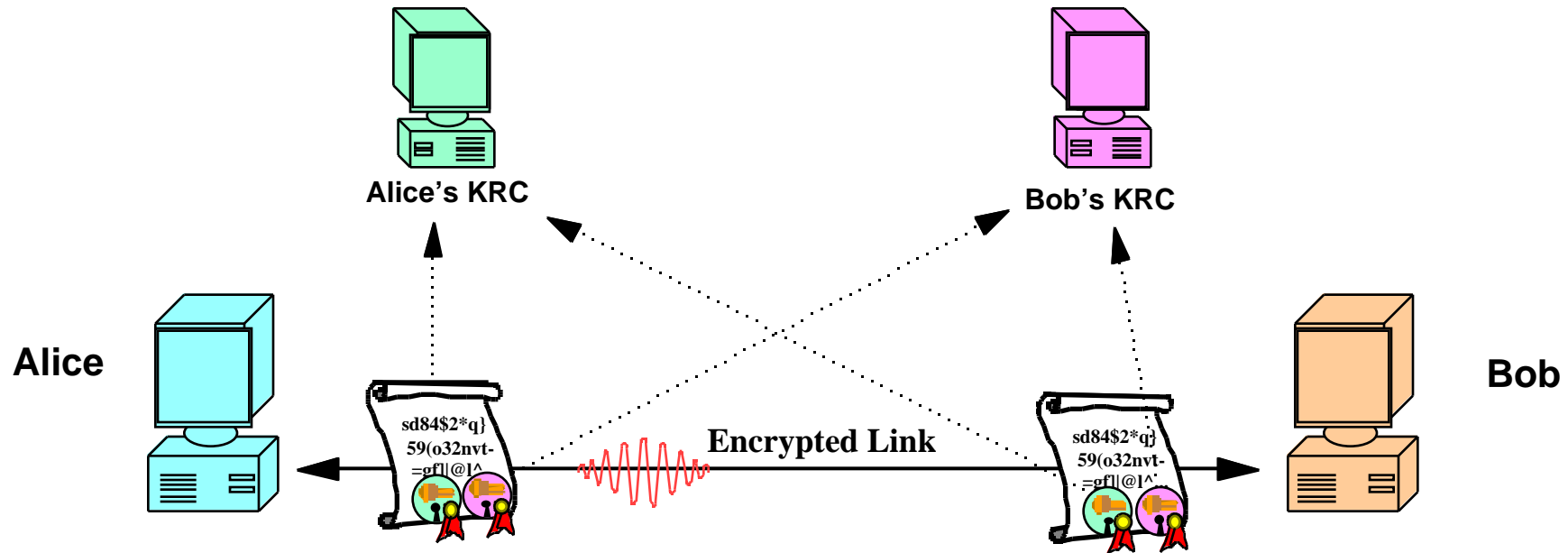
Corporate Key Recovery

- If a corporation owns their own KRC, the corporation may recover the key on the user's behalf...or on the corporation's behalf
- A corporation may also own their own KRC for export purposes



Exportable Product Use

- Client uses RecoverKey-International™-enabled product
 - sender client's product always generates KRFs and Recovery Verification Fields (RVFs) and associates them with the data
 - sender client's product generates KRF/RVF pairs for both sender and recipient KRCs
 - recipient client's product must always both verify KRF/RVF pairs



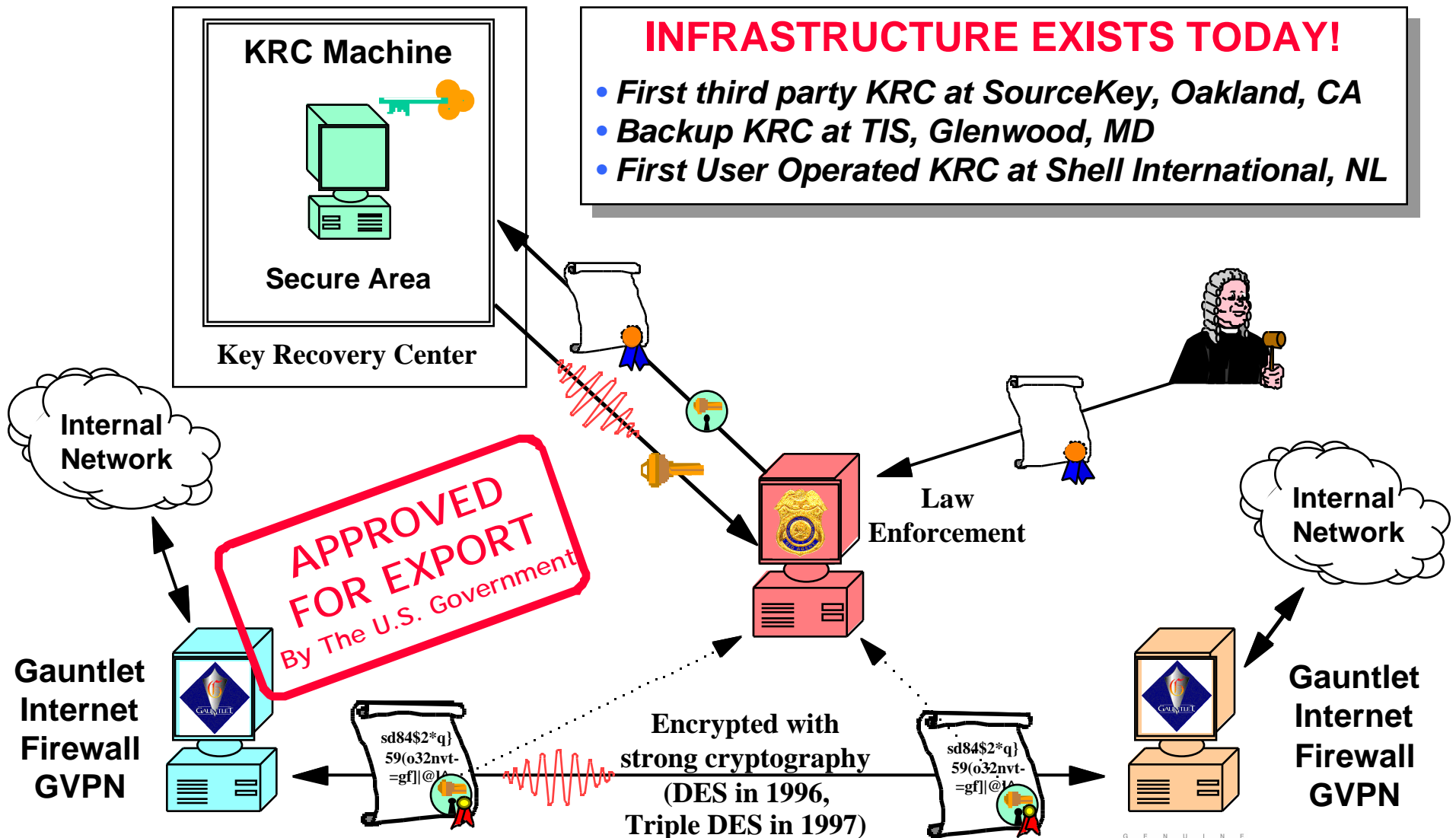
Session Key vs. Private Key Access

- Session key access constrains the scope of a third party access to only the authorized time period--private key access allows a third party access to the entire period that a private key was in use.
- Session key access allows a user to change their his/her keys without re-escrowing to a third party.
- A domestic user may allow session key access in order to communicate overseas--but not allow session key access for domestic communications. Private key access doesn't permit this distinction.
- *RecoverKey uses session key access to ensure the minimal amount of third party access permitted by law.*

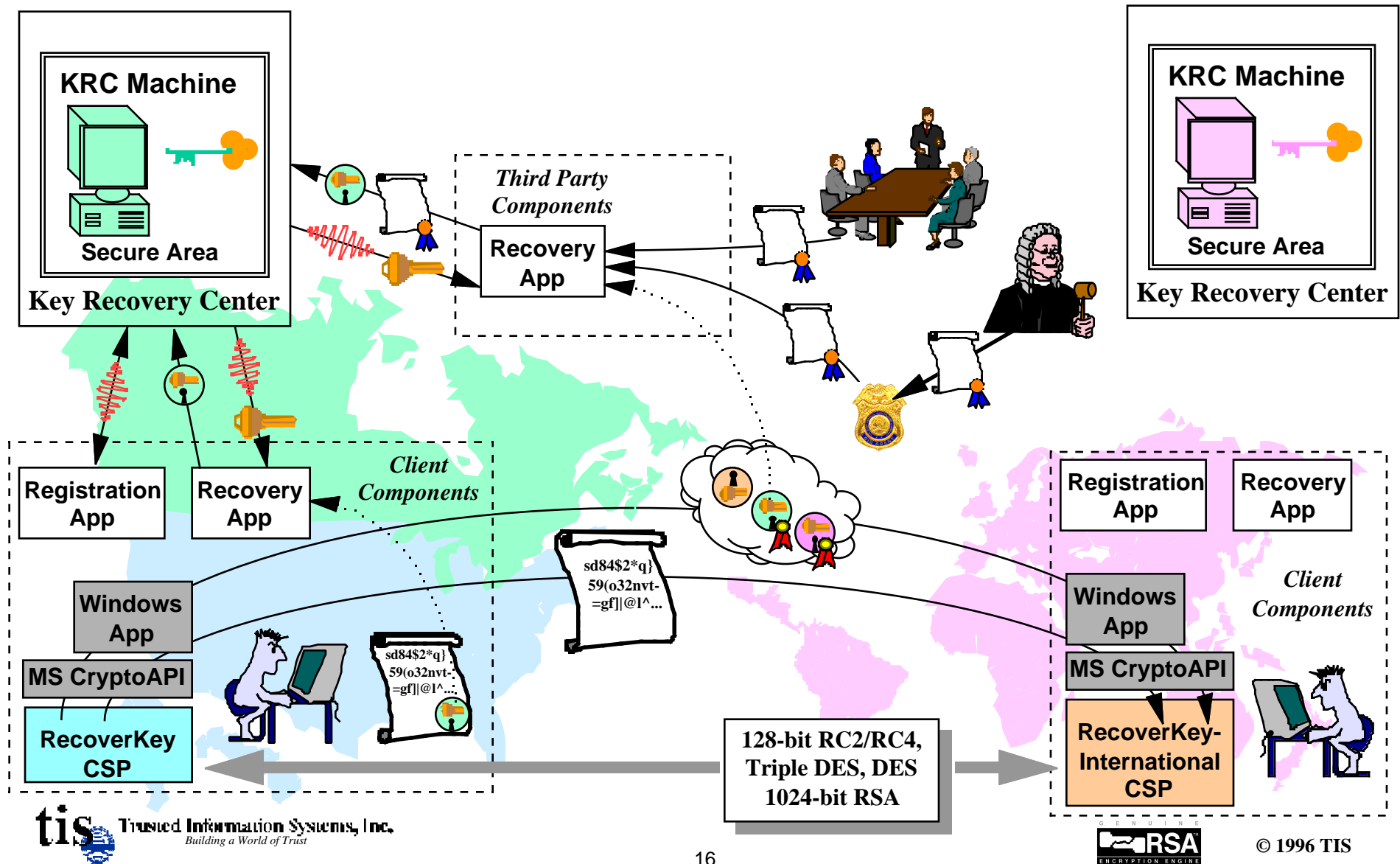
RecoverKey/Gauntlet System

INFRASTRUCTURE EXISTS TODAY!

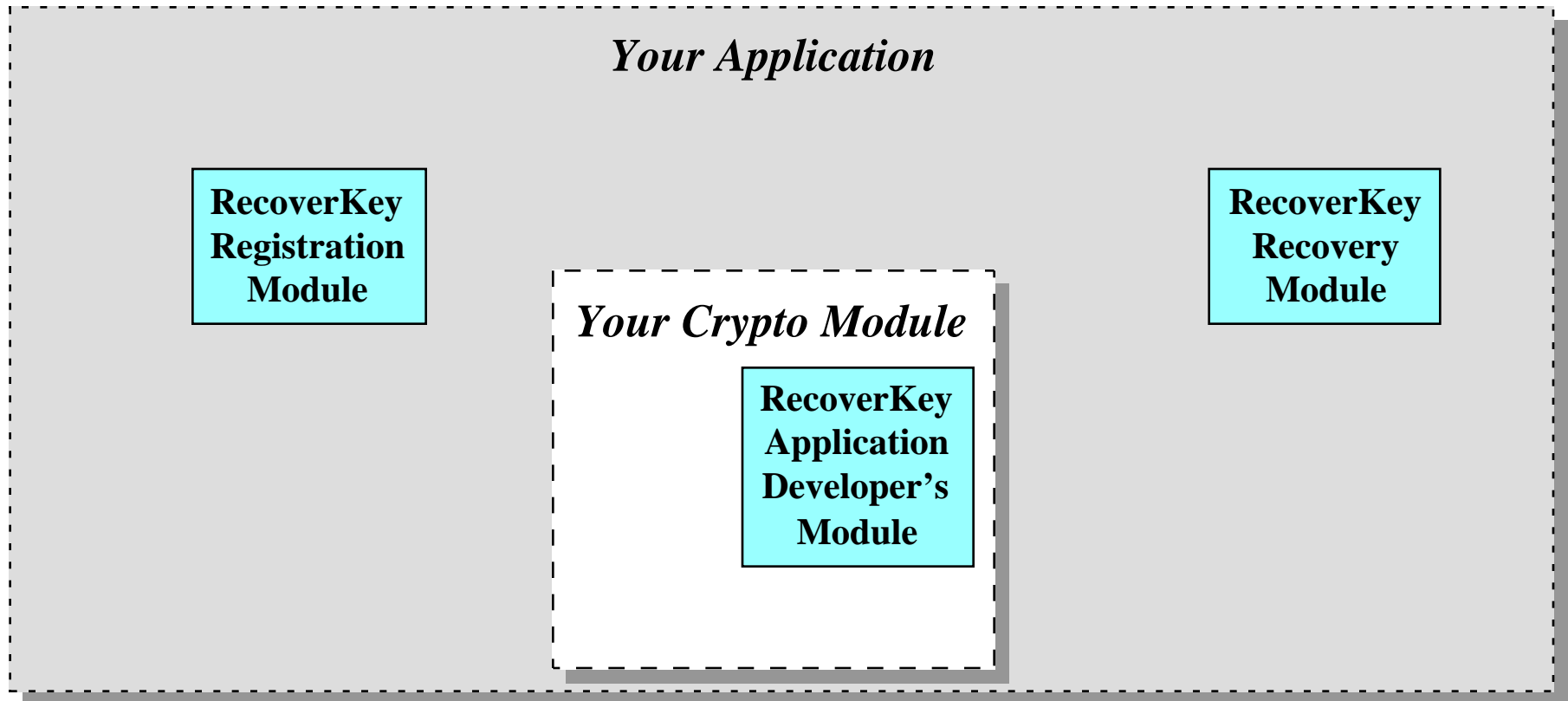
- First third party KRC at SourceKey, Oakland, CA
- Backup KRC at TIS, Glenwood, MD
- First User Operated KRC at Shell International, NL



RecoverKey/CryptoAPI System

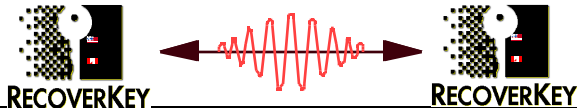

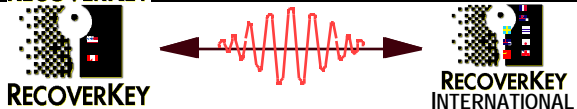
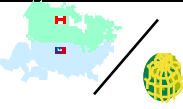
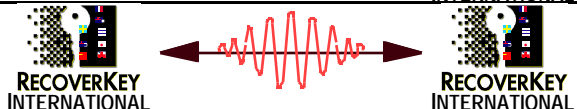

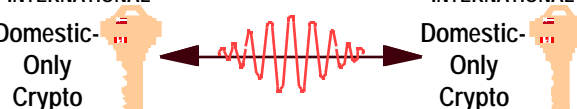

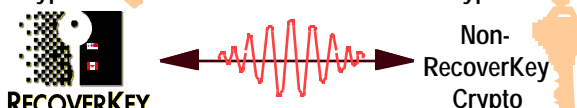





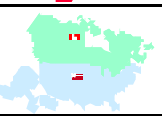




RecoverKey Toolkit



- **Algorithm Independent**
- **Key Size Independent**
- **KMI Independent**
- **Domestic or Exportable**

RecoverKey Interoperability

Application Type	Participants	Where Applicable	Recovery Field Generation
Communications			Optional
Communications			Mandatory
Communications			Mandatory
Communications			None
Communications			None
Communications			
Storage			Optional
Storage			Mandatory

RecoverKey Benefits



- **Global users and their corporations**
 - Provides back-up access to users if they lose their keys
 - Provides back-up access to corporations if they lose their employees
 - Allows corporations to operate their own recovery capability
 - Allows everyone to participate on an equal footing
 - Allows multinational firms to deploy secure global systems, and reach out to customers, partners and suppliers with complete security
- **Information owners**
 - Yields iron-clad information security
 - Allows senders to mandate both sender and receivers' recovery centers and the legal systems to protect them
 - Does not risk any private keys

Who to Contact

- I want to purchase a Key Recovery Center for my corporation
- I want to purchase a Recovery-Interational CSP
- I want to license RecoverKey for my crypto product
- I want to find out how RecoverKey can help make my crypto products exportable
- I want to purchase a RecoverKey toolkit

Bill Thompson
Vice President,
Business Development
E-mail: thompson@tis.com
Tel: (415)962-8885

- I want to purchase a RecoverKey-enabled Gauntlet Firewall

Gina Dubbé
Vice President, Sales
E-mail: gdubbe@tis.com
Tel: (301)947-7124

- I want to find out the technical details about...

Dave Carman
RecoverKey Development Mgr
E-mail: dwcarman@tis.com
Tel: (301)854-5374