Title Of Panel: Encryption Key Recovery: Off the Launch Pad

Panel Chair: Elaine Barker, National Institute of Standards and Technology

Panelists: Robert Frith, Motorola (Key Recovery Alliance)
Richard Guida, (Key Recovery Demonstration Project)
Dr. Stephen T. Kent, Chief Scientist, Information Security, BBN Technologies; Chief Technical Officer, CyberTrust Solutions (TACDFIPSFKMI)

Session Abstract:

Key recovery must be considered as another element of key management, which also includes the generation, distribution, control, storage, use and destruction of keying material. A method of acquiring decryption keys when normal key access mechanisms fail is required when an individual is unable to decrypt its own data, the organization employing that individual is unable to access the data to which it is entitled when the individual is not available, or any other legally authorized entity needs to access the encrypted data. The encrypted data could be part or all of an interactive communication session, a store-and-forward communication such as email, or stored on an electronic medium. Recovery could be needed by the entity that originally encrypted the data or by an entity to whom the data was sent. Key recovery information could be created by the encrypting entity or the decrypting entity. Communicating parties could use the same key recovery technique, different key recovery techniques or even communicate when one of them has no key recovery capability. This session presents three efforts in progress which are addressing various key recovery issues and are attempting to identify other issues which need to be addressed.

Position Statements or Summaries:

Key Recovery Demonstration Project (Richard Guida):

The Key Recovery Demonstration Project focused on the ability to recover stored, encrypted data to meet the business needs of the Federal Government. The KRDP pilot efforts included 13 projects performed by 11 agencies. Funding for these efforts, which were aggregated under the title "Phase I," was made available in late 1996, and work on the pilots began in mid 1997 with completion by late 1997. A variety of commercial off-the-shelf products was employed, including those from Entrust Technologies, AT&T, Netscape, and Trusted Information Systems. The results of Phase I demonstrated the value of key recovery and explored the different mechanisms used by contractors to achieve this capability. This work is being documented in a report which will be published on the Federal Public Key Infrastructure Steering Committee web page (http://gits-sec.treas.gov) once it is completed. A second phase of the KRDP effort is currently under consideration.

Summary for the Key Recovery Alliance:

The Key Recovery Alliance is a major international industry organization moving key recovery from the theoretical to the practical. The primary objective of the KRA members is to provide interoperable key recovery solutions that meet the needs of the commercial marketplace. The KRA has identified critical business requirements, created technical specifications and identified issues to deployment of key recovery products. More importantly, the KRA members are delivering products to the marketplace based on the specifications. The KRA will present the results of it's technical specification development, it's members' implementation plans and future activities of the Alliance.

TACDFIPSFKMI:

The Technical Advisory Committee to Develop a FIPS for the Federal Key Management Infrastructure (TACDFIPSFKMI) has developed a draft standard for the security of products incorporating key recovery functions. This standard focuses on security functionality and assurance aspects of such products, rather than attempting to establish specifications for key recovery technology per se. The TAC developed an abstract model that encompasses a broad range of key recovery approaches, to avoid excluding either existing products or new, innovative approaches to this problem that may arise in the future. Assurance requirements are derived from the Common Criteria, tailored for this environment, and from FIPS 140-1. The draft FIPS also imposes requirements on communication products embodying key recovery features, requiring that the introduction of key recovery not adversely affect interoperability of existing system making use of standard encryption protocols.

Biographies:

Elaine Barker has been involved in cryptographic activities for almost 30 years, the last 15 at NIST. While at NIST, she has been involved with the development of a number of Federal Information Processing Standards (FIPS) and American National Standards Institute (ANSI) standards, including FIPS 112 (Password Usage), FIPS 113 (Computer Data Authentication), FIPS 140-1 (Cryptographic Modules), FIPS 171 (Key Management Using ANSI X9.17), ANSI X9.9 (Message Authentication Codes), ANSI X9.17 (Key Management), ANSI X9.23 (Encryption), ANSI X9.28 (Multiple Center key Management), ANSI X9.41 (Security Services Management), ANSI X9.30 – Part 1 (Digital Signature Algorithm) and Part 2 (Secure Hash Algorithm), ANSI X9.57 (Certificate Management), and a number of ANSI standards currently under development or awaiting final approval. Ms. Barker has been associated with the area of key recovery since it became an issue in 1993. For the past two and a half years she has been a participant in both the Key Recovery Demonstration Project (KRDP) and the Technical Advisory Committee to Develop a FIPS for the Federal Key Management Infrastructure (TACDFIPSFKMI).

Robert Frith: To Be Provided

Richard A. Guida is a member of the Government Information Technology Services (GITS) Board, and Chair of the Federal Public Key Infrastructure Steering Committee comprising representatives from over 50 Federal agencies using or considering the use of public key technology. Richard has two degrees from the Massachusetts Institute of Technology, an S.B. in Electrical Engineering (Computer Science) and an S.M. in Nuclear Engineering (both 1973), and is a registered Professional Engineer in the Commonwealth of Virginia. He also has an MBA from the George Washington University (1981). He has been a member of the Senior Executive Service since 1989, and prior to his current appointment, he served as Associate Director of the Navy's nuclear propulsion program, where he was responsible for overseeing the management of spent nuclear fuel, environmental protection associated with nuclear powered warships, and related matters.

Dr. Stephen Kent has been engaged in network security research and development activities at for over 20 years. He was a member of the Internet Architecture Board, (1983-1994), and chaired the Privacy and Security Research Group (1985-1998). In the IETF, he chaired the Privacy Enhanced Mail (PEM) working group (1990-1995) and currently co-chairs the Public Key Infrastructure (PKIX) working group. In 1996, the Secretary of Commerce appointed Dr. Kent chair of the Technical Advisory Committee to develop a FIPS for the Federal Key Management Infrastructure. He served on several computer and network security study committees for the National Research Council, the Office of Technology Assessment, and other government agencies. He was a charter member of the board of directors of the International Association for Cryptologic Research, served on the Presidential SKIPJACK review panel for the Escrowed Encryption System, and chaired the ACM Special Panel on Cryptography and Public Policy. His work includes the design and development of user authentication and access control systems, network and transport layer and electronic messaging security protocols, and a multi-level secure directory system. Current activities focus on public-key certification systems for use in commercial and government environments, and design of denial of service countermeasures for routing systems.

Key Recovery Alliance

Enable Secure Global Business

http://www.kra.org

email: info@kra.org

About the Key Recovery Alliance

- **The Key Recovery Alliance (KRA) is a world-wide organization dedicated to the promotion of Global Electronic Commerce (GEC)**

- **Founded in October, 1996, the KRA serves as the focal point in the industry-led initiative to develop commercially acceptable solutions for recovery of encrypted information**

KRA
Key Recovery Alliance

The Commercial Impact of Cryptography

- Estimates predict that the Global Electronic Commerce market (GEC) could total $1trillion by 2000
- GEC can only be realized if organizations have confidence that information will remain secure from unauthorized or illegitimate access
- Cryptography has emerged as the most effective means of securing information transmitted or stored
- Encrypted information must be readily accessible in plain-text to ensure the continuity of business processes

KRA
Key Recovery Alliance

Why Commercial Key Recovery?

- **Sensitive information will be encrypted**
  - **Internal to a Company**
    - **Information on hard drives**
    - **Electronic distribution of Company information**
    - **Email**
  - **Company to Company to Customer**
    - **Electronic transfer of information**
    - **Email**

Without commercially acceptable key recovery solutions and the ability to recover encrypted information, an organization is vulnerable to situations where the in-ability to continue doing business can cause irreparable damage.

KRA
Key Recovery Alliance

Key Recovery Alliance Goals

- Stimulate global electronic commerce
- Promote the world-wide implementation, deployment and use of market-driven, interoperable key recovery solutions
- Define the business and technical requirements of a commercial infrastructure for key recovery technology
- Sponsor the development of a global infrastructure that supports the recovery of encrypted information

KRA
Key Recovery Alliance

What is Key Recovery?

- Key recovery allows access to plaintext from encrypted information if the encryption key is lost, mismanaged or unavailable
- An authorized representative can retrieve, restore or reconstruct a cryptographic key with the intent to access data previously encrypted with that key

KRA
Key Recovery Alliance

1997 KRA Contributions to Industry

- **Incorporated KRA**
  - **Created by-laws, membership agreement, operational policies**
  - **Established 5 strategic committees**
  - **Established web site**
  - **Published 4 white papers**
  - **Grew from 11 to 70 companies world-wide**
- **Provided an open forum for suppliers and users of key recovery products and services to exchange information**
  - **Safe use of encryption**
  - **Deployment issues**
  - **World-wide changes in government policies**
  - **Changing market demands**

KRA
Key Recovery Alliance

1997 KRA Contributions to Industry

- **Strategic Committees**
  - **Business Scenarios** - identify global business scenarios that require key recovery
  - **Technology** - identify the requirements, needs and issues surrounding the interoperability with recovery and non-recovery technology
  - **Deployment** - identify requirements and barriers in the deployment of KR technology
  - **Public Issues** - identify global public policy issues regarding Key Recovery
  - **Outreach** - provide information about key recovery to the general public, businesses, educational institutions, governments and others

KRA
Key Recovery Alliance

Business Scenarios Committee

- **Charter - identify global business scenarios that require key recovery capabilities**
- **1997 accomplishments**
  - **Published the "Business Requirements for Key Recovery" white paper**
- **1998**
  - **Synchronize documented business scenarios with other committees**
  - **Develop new scenarios**

KRA
Key Recovery Alliance

Technology Committee

- **Charter - identify the requirements, needs and issues surrounding the interoperability with recovery and non-recovery technology on diverse hardware and software platforms**
- **1997 accomplishments**
  - **Published the "Cryptographic Information Recovery Using Key Recovery" white paper**
  - **Created internal drafts of key recovery system model & common key recovery block for interoperability**
  - **Created internal draft of Prepared key recovery extensions for internet specifications (e.g. ISAKMP and IPSEC)**
- **1998**
  - **Deliver white papers - Key Recovery System Model, Common Key Recovery Block for Interoperability, Key Recovery FACTs**
  - **Complete work on key recovery specifications of ISAKMP and IPSEC**
  - **Gain agreement on common key recovery block**

KRA
Key Recovery Alliance

Deployment Committee

- **Charter - identify requirements for deployment of KR technology and recommend actions to remove or reduce barriers to deployment**
- **1997 accomplishments**
  - **Created internal draft of deployment requirements**
- **1998**
  - **Publish deployment requirements paper**
  - **Direct the KRA's actions to facilitate deployment**

KRA
Key Recovery Alliance

Public Issues Committee

- **Charter - identify global public policy issues regarding Key Recovery**
- **1997 accomplishments**
  - **Published the "Public Policy Requirements for a Global Key Recovery Infrastructure" and the "Key Recovery and Electronic Commerce: Industry's Efforts to Develop New Tools to Support Strong Encryption" white papers**
  - **Developed outline for education module**
- **1998**
  - **External education**
  - **Monitor and respond to public policy changes**

KRA
Key Recovery Alliance

Outreach Committee

- **Charter - provide clear, concise information about key recovery to the general public, businesses, educational institutions, governments and other communities of interest**
- **1997 accomplishments**
  - **Published KRA FAQs**
  - **Responded to industry KRA press concerning KR**
- **1998**
  - **Publish 1997 KRA Year in Review Report**
  - **Enable KRA to be more proactive in communicating its goals and objectives world-wide**

KRA
Key Recovery Alliance

1997 KRA Participants

America OnLine,Inc.
American Express Corp.
Apple Computer, Inc.
Atalla
Baltimore Technologies
Boeing
Candle Corporation
CertCo
Certicom
Compaq Computer Corp.
Compatible systems Corp.
Cryptomathic
CygnaCom Solutions, Inc.
Cylink Corp.
DASCOM, Inc.
Data Securities, Int'l, Inc.
Deere & Company
Digital Equipment Corp.
Digital Signature trust Co.
Entrust Technologies
First Data Corp.
Fort Knox Escrow Services
Fortress Technologies Corp.
Frontier Technologies Corp.
Fujitsu Ltd.
GemPlus
Gradient technologies
Groupe Bull
Hewlett-Packard
Hitachi
IBM
ICL
Intel
IRE, Inc.
Mitsubishi Corp. of Japan
Mitsubishi Electric America
Motorola
Mykotronx
Mytec Technologies, Inc.
NCC Escrow
nCipher
NCR
NEC
Network Systems Group of StorageTek
Novell, Inc.
NTT Software Corp.
Open Horizon, Inc.
Portland Software
Price Waterhouse
Racal Data Group
Rainbow Technologies
RedCreek Communications
RPK
RSA
SafeNet Trusted Services Corp.
Santa Cruz Operation, Inc.
Secant Network Technologies
Secure Computing Corporation
Siemens AG
Silicon Graphics, Inc.
SourceFile
Spyrus
Sterling Commerce
Sun Microsystems, Inc.
Tandem
Technical Communications Corp.
Toshiba
Trusted Information Systems, Inc.
Unisys
UPS
Utimaco Safeware AG
VeriSign
VPNet Technologies

KRA
Key Recovery Alliance

Board of Directors and Officers

- **KRA Officers**
  - President — Bob Frith (Motorola)
  - Vice-President — Peter Bolton (Cylink)
  - Treasurer — Tucker Cox (SourceFile)
  - Secretary — Gayle Meyer (IBM)
- **KRA Directors at Large**
  - Roger French (Digital Equipment Corp.)
  - Bob Jueneman (Novell)
  - Fran Rooney (Baltimore Technologies)
  - Jim Schlinder (Hewlett Packard)
  - Bill Thompson (Trusted Information Systems)
  - Haruki Tabuchi (Fujitsu)
  - Paul Van Oorschot (Entrust Technologies)

KRA
Key Recovery Alliance

KRA1998 Vision

To be the leading provider of information on market driven, interoperable, and secure key recovery technology for use with strong encryption in global business

KRA
Key Recovery Alliance

KRA 1998 Goals

- Increase world-wide participation in KRA
- Submit technical requirements and extensions to appropriate standards organizations for adoption
- Leverage pilots to provide interoperability “proof of concepts”
- Increase awareness and educate the market on key recovery concepts and objectives through published articles and speaking engagements

KRA
Key Recovery Alliance

Key Recovery Membership

- **Membership in the KRA is open to commercial entities**
  - **using encryption products in the course of its business**
  - **manufacturing, licensing, selling, or servicing encryption products**
- **For more information on membership benefits and dues**
  - **Tel: +1 415 750 8353**
  - **Fax: +1 415 751 4829**
  - **e-mail: Info@kra.org**
  - **http: www.KRA.org**

KRA
Key Recovery Alliance

Key Recovery Demonstration Project

Richard A. Guida, P.E.
Chair, Federal Public Key Infrastructure Steering Committee
Member, GITS Board (Champion for Security)

Purpose

- **Information briefing on KRDP**
- **Discussion of status & future activities**

Phase I Demonstration Objective

- **Demonstrate viability of key recovery for federal business applications**
- **9-15 month duration**
- **Chartered in August 1996**
- **Funding available December 1996**
- **Began work April 1997**

Federal Business Rationale

- **Need for security and privacy requires encryption of information**
- **If keys are not available, encrypted information cannot be retrieved**
- **Thus, ability to recover keys is required in the event of loss, theft, compromise**

Team Members

- **Core Task Group:**
  - Treasury - Chair FPKI Steering Committee
  - 1 NSA (full-time), 1 NIST (part-time)
  - Contractor - program management & integration support
  - NIST - technical testing/evaluation
- **Advisory**:
  - NIST, NSA, FBI

Demonstration Approach

- **KRDP's implementation evaluation criteria**
- **Pilot implementation plans**
- **Testing and evaluation**
- **Final report**

Evaluation Criteria

- **Source Documents and Material**
  - Draft Key Escrow Agent Criteria (12/95)
  - Draft Standard for Cryptographic Escrow Systems (6/96)
  - Discussions with Business Software Alliance (7/96)
  - Draft Software Key Escrow Encryption Export Criteria (11/95)
- **Harmonized with Administration Export Criteria**
- **Copy of criteria available on website**

Pilot Applications

- **DOE - EDI/Internet Security**
- **DOT - Electronic Grants Program**
- **LLNL - Public Key Infrastructure Pilot**
- **NIST - Root Certification Authority**
- **U.S. Customs - North American Trade Automation Prototype**

Pilot Applications (continued)

- **NTIS - FedWorld Secure Web/CA Project**
- **SSA - Annual Wage Reporting System**
- **Patent and Trade Office (PTO) - International Priority Document Exchange**
- **SBA - Electronic Lending Program**
- **Treasury - Secure Electronic Messaging Services**

Pilot Applications (continued)

- **PTO - Electronic Patent Application Filing System**
- **FBI - Secure E-Mail**
- **FBI - Computer Investigations and Infrastructure Threat Assessment Center (CITAC)**

Pilot Selection Criteria

- **Serve large number of diverse constituents**
- **Support diverse applications and missions**
- **Use different technologies and emergency access techniques**

Industry Partners

- **TIS**
- **VeriSign**
- **Pitney-Bowes**
- **SourceFile**
- **Entrust**
- **ISC**
- **RAMS-FIE**
- **ActiveSW**
- **DataKey**
- **QueriSoft**
- **CNIDR**
- **Netscape**
- **Cygnacom Solutions**
- **Xcert Software**

Industry Selection Criteria

- **Have existing customer base within Federal government**
- **Represent diverse products and services**
- **Able to provide future products and services to support emergency access**

We did **NOT**

- **Recover digital signature keys**
- **Create a key management infrastructure**
- **Limit technology used or method of emergency access**
- **Mandate which cryptography was used**

Key Recovery Approaches

- **DOE - third Party; TIS/SourceFile**
- **SBA - self-recovery; product level - AT&T Secret Agent™**
- **LLNL - self-recovery; at own Entrust CA**
- **NTIS - CA and KR service provider, Entrust/Netscape**
- **NIST - root Certification Authority, Entrust**
- **Treasury - self-recovery, split key, Xcert**

Key Recovery Approaches (cont'd.)

- **DOT - third party; NTIS**
- **PTO - self-recovery; TIS RecoverKey**
- **NATAP - self-recovery; BSAFE toolkit with custom KR capability**
- **FBI - self-recovery; AT&T Secret Agent ™**
- **FBI - third party; AT&T Secret Agent™**
- **SSA - third party; Entrust/Pitney-Bowes**

Pilot Applications (cont'd.)

- **All pilots are domestic applications with exceptions of:**
  - NATAP
  - Patent and Trade Office (PTO)

Status

- **Final Report describes technical validation, areas for further work, legal and policy issues**
- **Draft completed and in coordination for public release**
- **Once coordination completed, Final Report - including documentation on each pilot and test reports - will be placed on website**

Future

- **Phase II of KRDP under consideration**
- **Details will be provided upon programmatic approval**

For More Information

- Website: http://gits-sec.treas.gov
- Richard A. Guida
  - richard.guida@cio.treas.gov
- Denise Silverberg
  - denise.silverberg@cio.treas.gov

Developing a Key Recovery Federal Information Processing Standard

Dr. Stephen Kent
Chief Scientist- Information Security
BBN Technologies
Chief Technology Officer
CyberTrust Solutions

INTERNETWORKING
POWERED BY BBN

Outline

- Committee history & composition
- Scope
- FIPS outline
- FIPS parts

What's in a Name?

Technical Advisory Committee to Develop a Federal Information Processing Standard for the Federal Key Management Infrastructure

(TACDFIPSFKMI)

History

- Establishment
  - Federal Advisory Committee Act, 5 U.S.C. App. 2, and
  - GSA rule on Federal Advisory Committee Mgmt., 41 CFR Part 101-6
- Purpose
  - Advisory body
  - Technical recommendations
- Output
  - Baseline for for key recovery FIPS

Committee Composition

- Members
  - 24members from industry & academia
  - Software & hardware vendors, system integrators, financial organizations, ...
- Government liaisons (non-voting)
  - NIST, NSA, DISA, DOE, Treasury, FBI, SBA, NASA, ...
- Public
  - Meetings open to the public, but not many showed up!

What is the FIPS?

- Establishes security and interoperability requirements for products embodying key recovery technology
- Not a design for a key recovery system
- Not a set of requirements for operation of a key recovery service
- FIPS is technology neutral
- Analogous to FIPS 140-1 (security requirements for cryptographic modules)

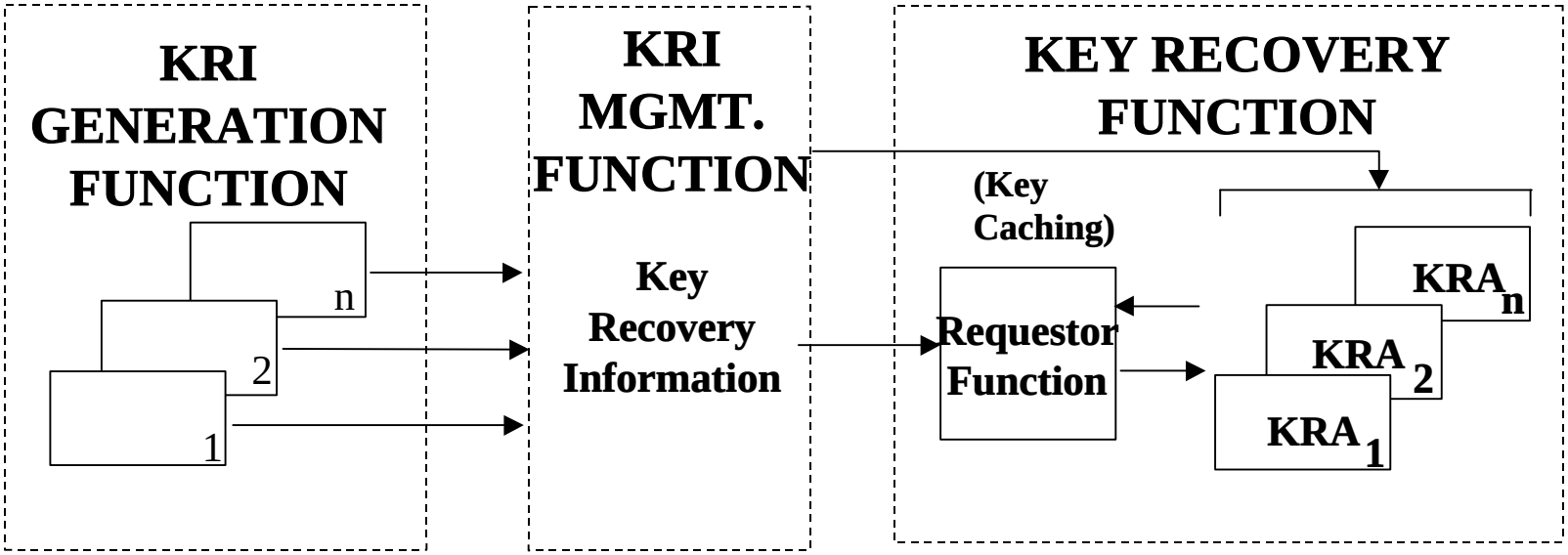
Not Our Job!

- Encryption export cont
- Federal policy
- Legislation
- LEA access controls
- Liability issues
- PKI structure
- Applicability of key recovery

FIPS Contents

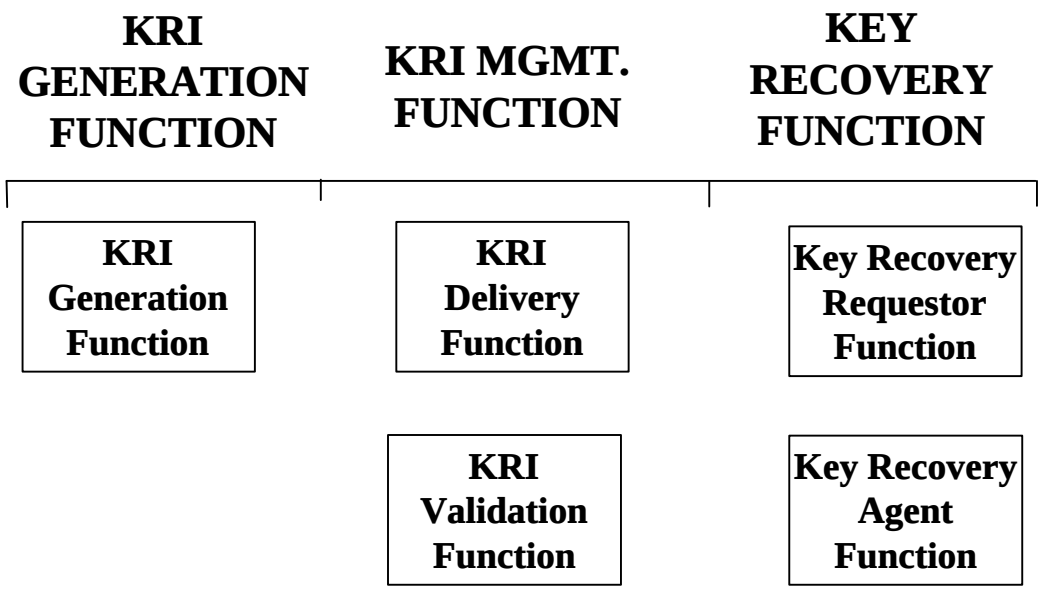
- Announcement
- Overview
- Model
- Security & interoperability requirements
- Assurance requirements
- Appendices (not normative)

The Key Recovery Model



KRI = Key Recovery Information
KRA = Key Recovery Agent

Another Model Perspective



Security Functional Requirements

- Requirements for each function in the model
  - KRI generation, delivery & validation
  - Key recovery agent & key recovery requestor
- Two levels of security
  - medium
  - high
- Each level, for each function, maps to one of three assurance levels (see the next slide)

Interoperability Requirements

- Requirements apply only to end system products used for communication (not storage)
- Does not apply to KRAs or KRRs
- Introduction of key recovery must not “break” existing, interoperable, standards-based encryption protocols
- Cognizant standards bodies are responsible for approving any changes needed to accommodate key recovery syntax & processing (re interoperability)

Assurance Requirements

- Designed to test the product security features
- Based on the Common Criteria
- Three assurance levels, but each security functional level maps to exactly one assurance level
- Seven assurance classes
- Actions for the developer & the evaluator

Appendices (not normative)

- Example
  - Functionality within a product
  - Multiple KRI functions
  - KRI generation scenarios
  - Key recovery scenarios
- Key Recovery Block
- Certificate extensions
- Interoperability examples

Summary

- TAC did not complete document review & approval, but substantial work was accomplished
- TAC may resume work, awaiting DoC approval
- Completed document will provide basis for development of a FIPS for security, interoperability and assurance
- Result will be technology neutral, analogous to 140-1
- Stay tuned!