CKM is a More Flexible Solution

1

Information Created

2

Active Attributes chart

Audience Selected

*By Content Rule/Description

*From Organization's Taxonomy/Permission Board

e.g.
Raytheon/Engineering/Chain/Software Development

3

Digital Signature Applied

4

CKM Seals the Object

Working Key Generated

5

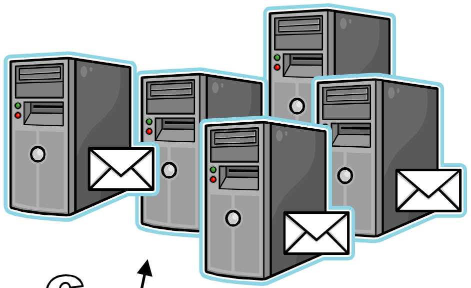
CKM Creates Unique (per object)

Confidentiality Wrapper

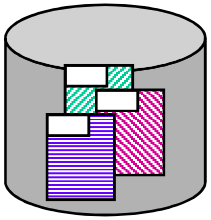
Protects any digital data, text, graphics, audio, video in any

transmission format

6



Data Protected not the network



Encrypted Objects

Any server/servers

7

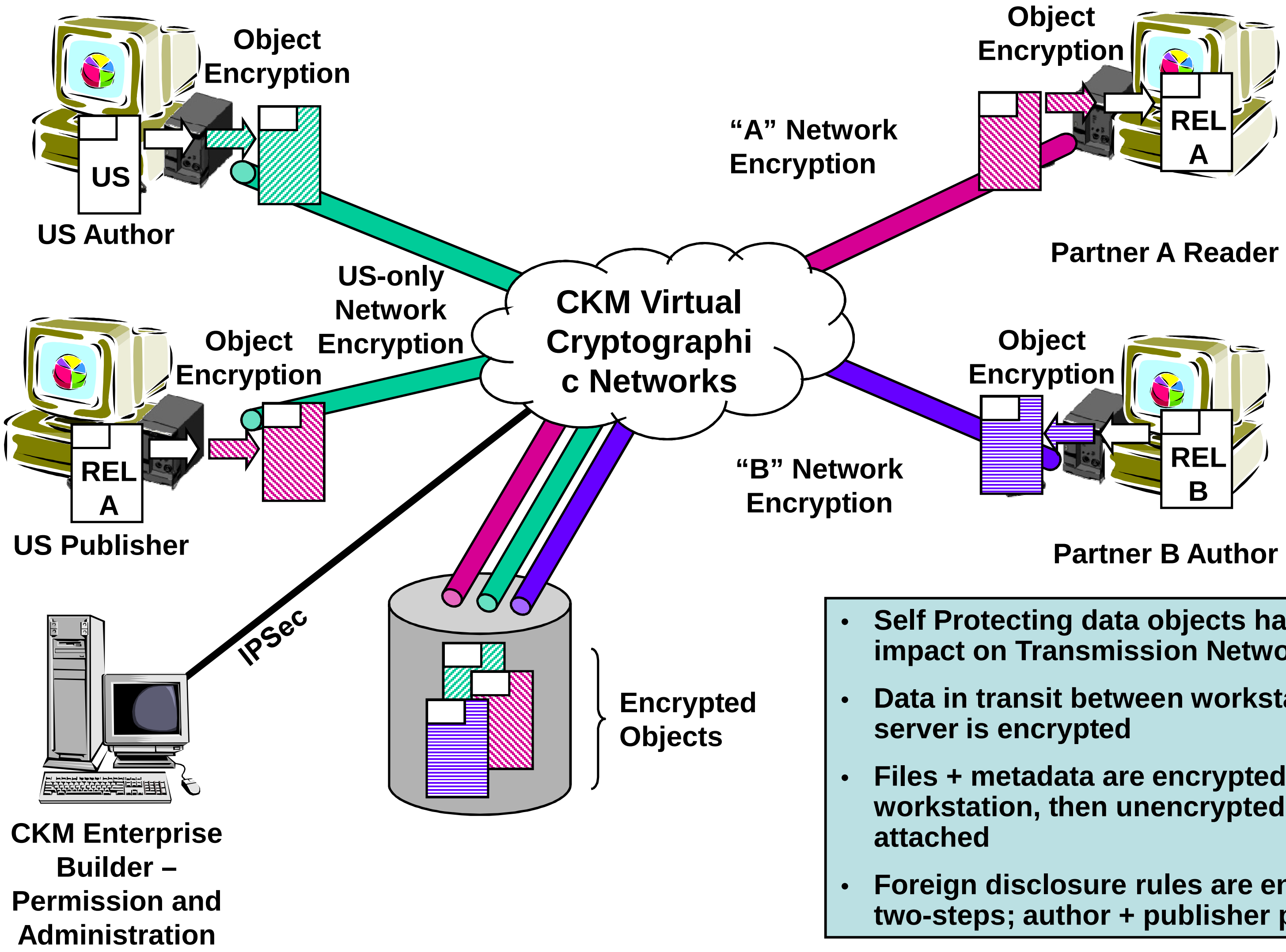
Employees with the correct credentials/ Permissions can read the information and reply in a similar fashion as the original Author.
Credentials/Permissions Revocations are controlled by the employees' organization such as Raytheon/US Navy/NAVAIR etc**.**
Data remains in an encrypted state indefinitely and always available with the proper permissions.

Meets Published Standards

ANSI X9.69 Framework For Key Mgmt Extensions
X9.73 Cryptographic Message Syntax
X9.96 Secure XML
X9.112 Secure Wireless

ISO 22895

CKM System Overview



- Self Protecting data objects have no impact on Transmission Networks
- Data in transit between workstations and server is encrypted
- Files + metadata are encrypted on the workstation, then unencrypted metadata is attached
- Foreign disclosure rules are enforced via two-steps; author + publisher processes

PKI Issues Improved by CKM	
1. PKI is a Static Key System a. Every controlled item needs a pair of keys e.g: If there are 1million controlled items per day then 2 million keys are required b. Cannot re-key system, must replace old keys 2. Information is attached to a person not their position/function 3. PKI system cannot prevent Users from generating their own keys. 4. PKI is a ComSec solution – Person to Person (when known) 5. PKI allows Digital Signature and Creates a Chain of Trust	1. CKM is a Dynamic Key System a. Keys are created at time of need e.g: 100 million objects can be managed with less that 100 control words b. Designed for re-keying without changing the pool of control words 2. Information belongs to Originating Organization 3. Users have no capacity to create key fragments or control words 4. CKM is an InfoSec solution – providing role based access to any digital object 5. CKM takes PKI and leverages it into Role Based Access to Content. CKM brings Scalability that PKI lacks on its own