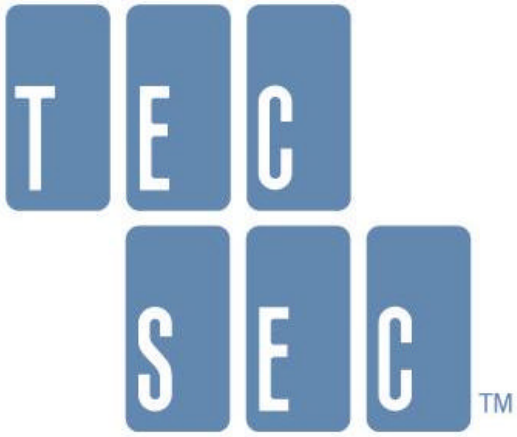


CKM® Enabling PKI

RSA Conference

© 2003-2008 TecSec Incorporated

Agenda

- What is CKM®?
- How does CKM work?
- How CKM can help fulfill the promise of PKI?
- Example applications of CKM technology
- Questions?

©TecSec®, Incorporated 2003-2008. All rights reserved.

What is CKM®?

- CKM, short for Constructive Key Management, is a technology that provides Role Based Access Control that is enforced via cryptography.

- Properties of CKM:
  - Key material not specific to individuals
  - Addresses the one-to-many distribution problem of key management
  - Access privileges bound to data via cryptography
  - Built-in key recovery performed by system owner

- What is CKM good for?
  - Modeling Role-Based Access Control (RBAC)
  - Content-based security
  - Complementing PKI

©TecSec®, Incorporated 2003-2008. All rights reserved.

Roles and Credentials

- Roles are established by function and responsibility
- A Role is defined by a set of Credentials
  - Each Credential represents an attribute of the data described in the underlying information classification model (e.g. Project X, Software Engineer, Company Employee)
  - Credentials may be further refined by access mode:
    - Read
    - Write
- Individuals may perform multiple roles
- Those performing the same role, and thus having the same Credential(s), share the same ability to access information

©TecSec®, Incorporated 2003-2008. All rights reserved.

Anatomy of a Credential

Credential

Label: <descriptive name>
Credential ID: <unique number>
Issue Date: <date>
Expiration Date: <date>

Public Key (Write Access)

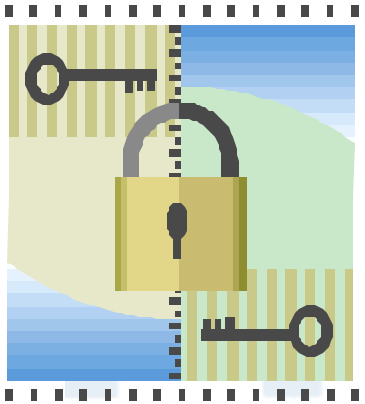
Private Key (Read Access)

Unlike PKI certificates, a Credential's public and private key must both be kept secret.

©TecSec®, Incorporated 2003-2008. All rights reserved.

CKM® System Architecture

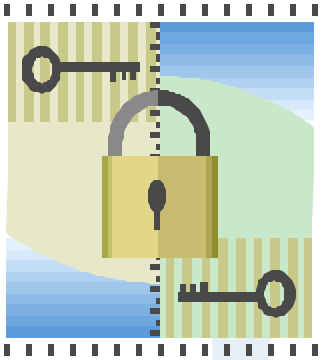
- System owner creates a CKM Domain
  - Domains contain:
    - Domain Value (shared symmetric key)
    - Maintenance Value (shared symmetric key)
    - Credentials
  - Roles are mapped to Credentials
- Members are enrolled into the system and assigned a Domain
  - Members can belong to multiple Domains
  - Members are assigned Roles
  - Token created for each Member



©TecSec®, Incorporated 2003-2008. All rights reserved.

How does CKM® work?

- CKM produces a unique Working Key that is used to encrypt data.
- After the data is encrypted, the Working Key is **destroyed!**
- What remains are the components used to create the Working Key.
- Credentials are used to encrypt the sensitive components, so that only authorized users will be able to recreate the Working Key.

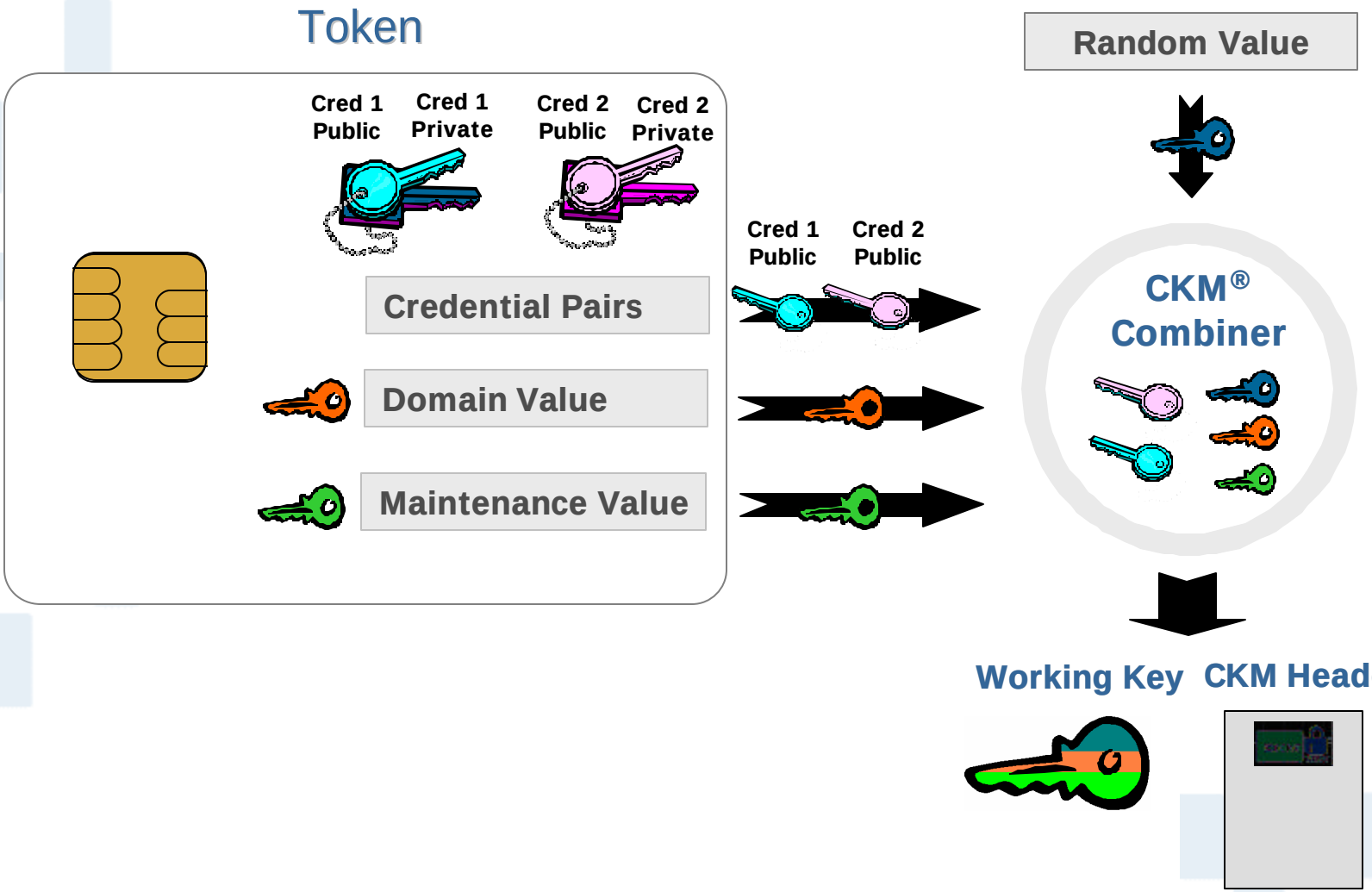


©TecSec®, Incorporated 2003-2008. All rights reserved.

Encryption Process

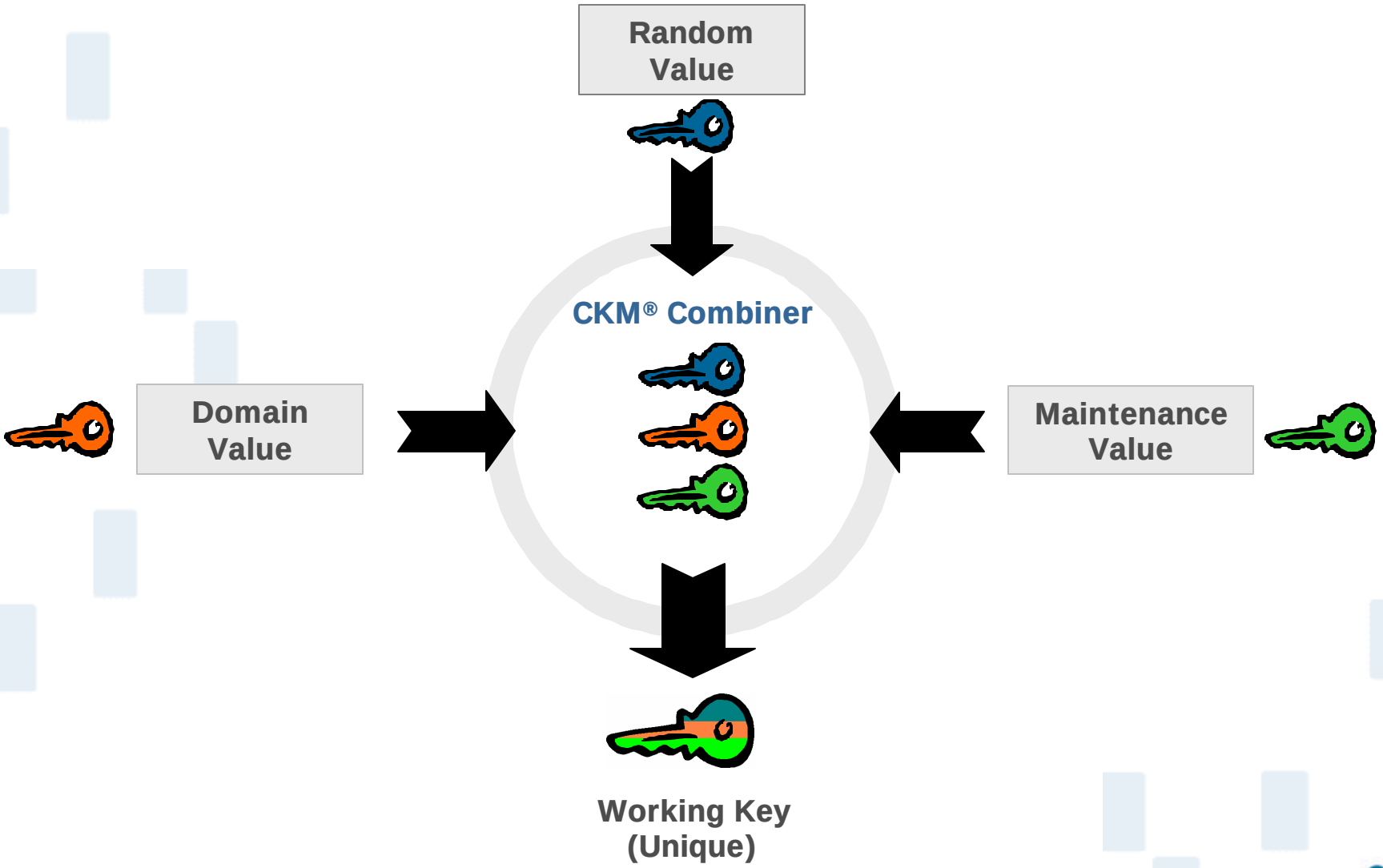
©TecSec®, Incorporated 2003-2008. All rights reserved.

Encryption – Logical View



©TecSec®, Incorporated 2003-2008. All rights reserved.

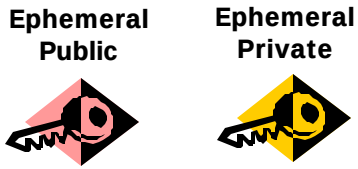
Encryption Functional View
Phase I - Working Key Generation



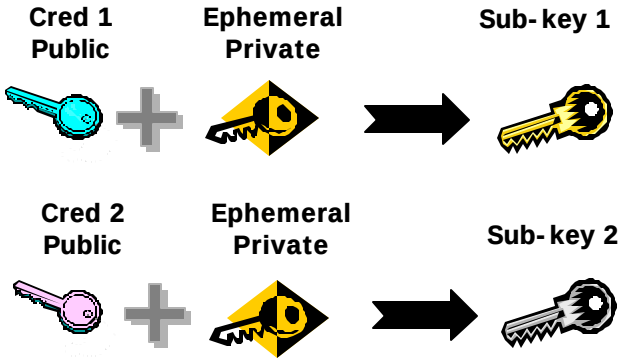
©TecSec®, Incorporated 2003-2008. All rights reserved.

Encryption Functional View
Phase II – Protecting the Random

Ephemeral Key Pair is generated



Each supplied Credential's Public Key & the Ephemeral Private Key are used to produce a Sub-key.



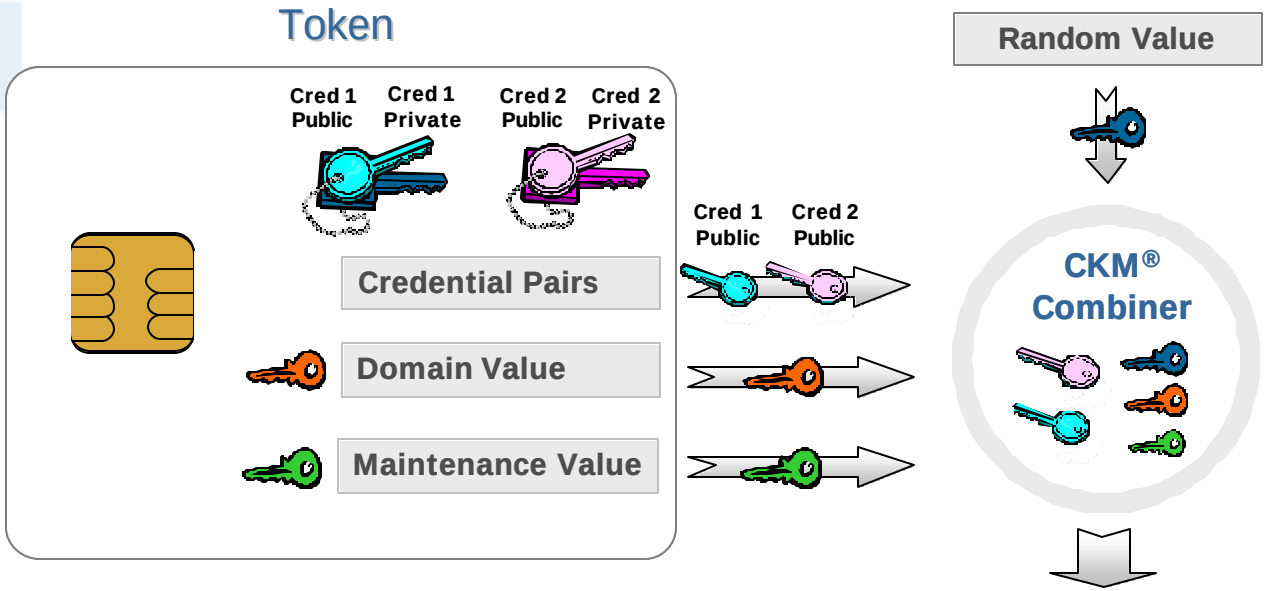
Sub-keys are combined to produce a key to encrypt the Random

Random destroyed

Ephemeral Private destroyed

©TecSec®, Incorporated 2003-2008. All rights reserved.

Encryption Logical View – Completed



CKM Header

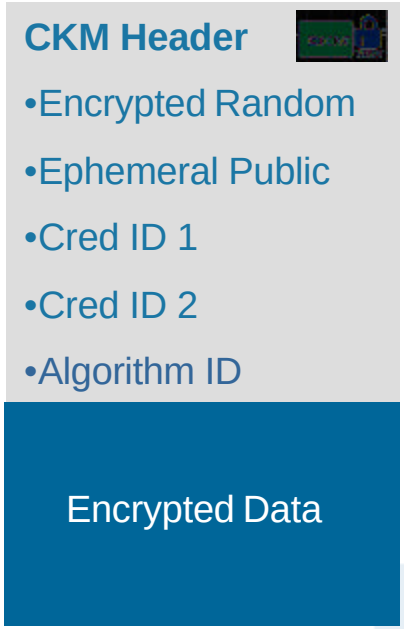
- Encrypted Random
- Ephemeral Public
- Cred ID 1
- Cred ID 2
- <more data>

©TecSec®, Incorporated 2003-2008. All rights reserved.

Encrypting the Data

- Once the Working Key and CKM Header have been created, the following steps occur:

1. The Working Key is truncated to the desired length based on the selected encryption algorithm
2. The CKM Header has the algorithm ID included in it
3. The data is encrypted with the Working Key and the Header is attached to the encrypted data.
4. The Working Key is destroyed.

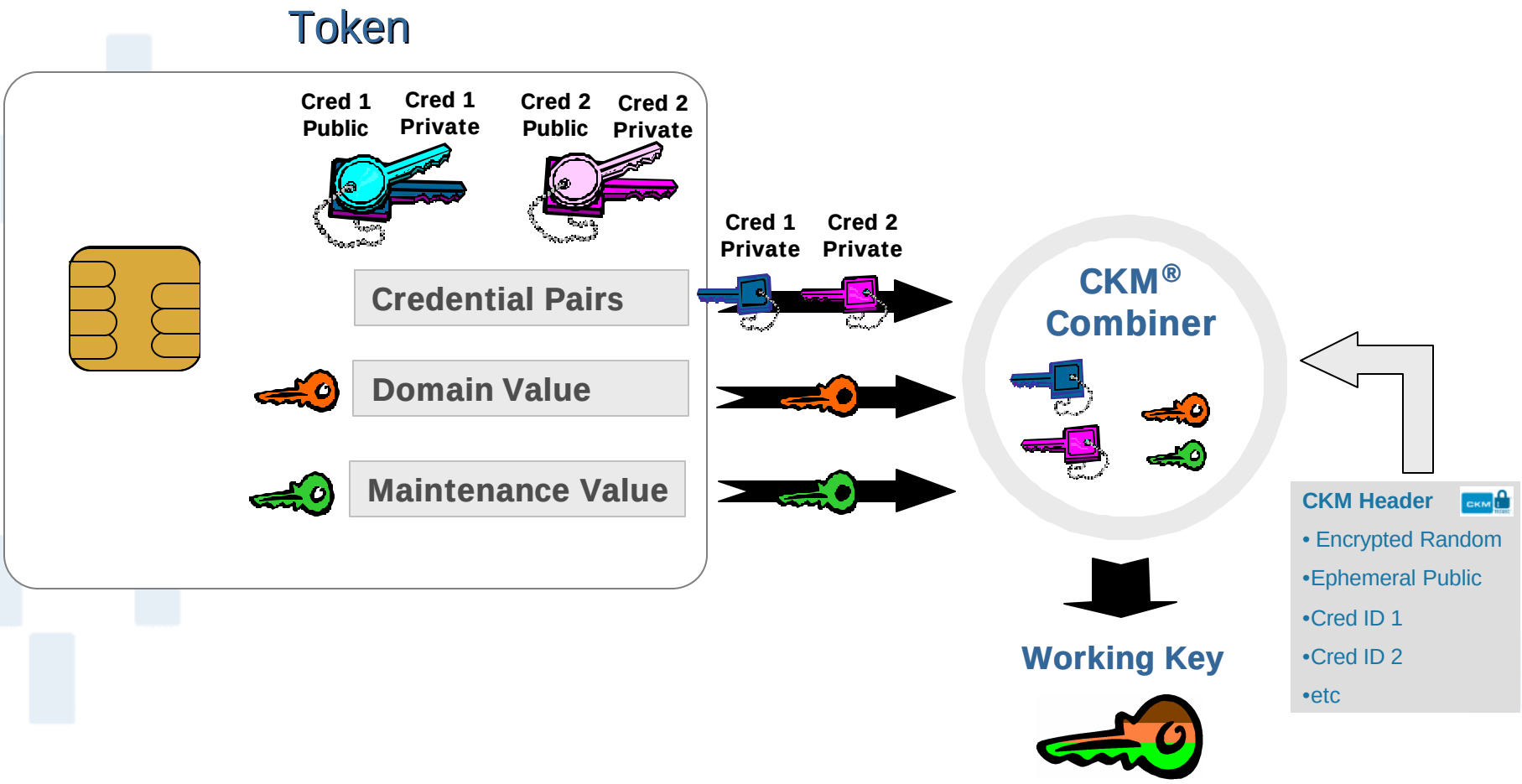


©TecSec®, Incorporated 2003-2008. All rights reserved.

Decryption Process

©TecSec®, Incorporated 2003-2008. All rights reserved.

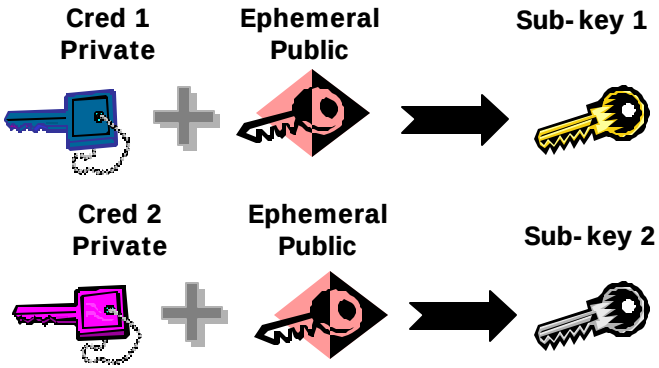
Decryption – Logical View



©TecSec®, Incorporated 2003-2008. All rights reserved.

Decryption Functional View
Phase II – Recovering the Random

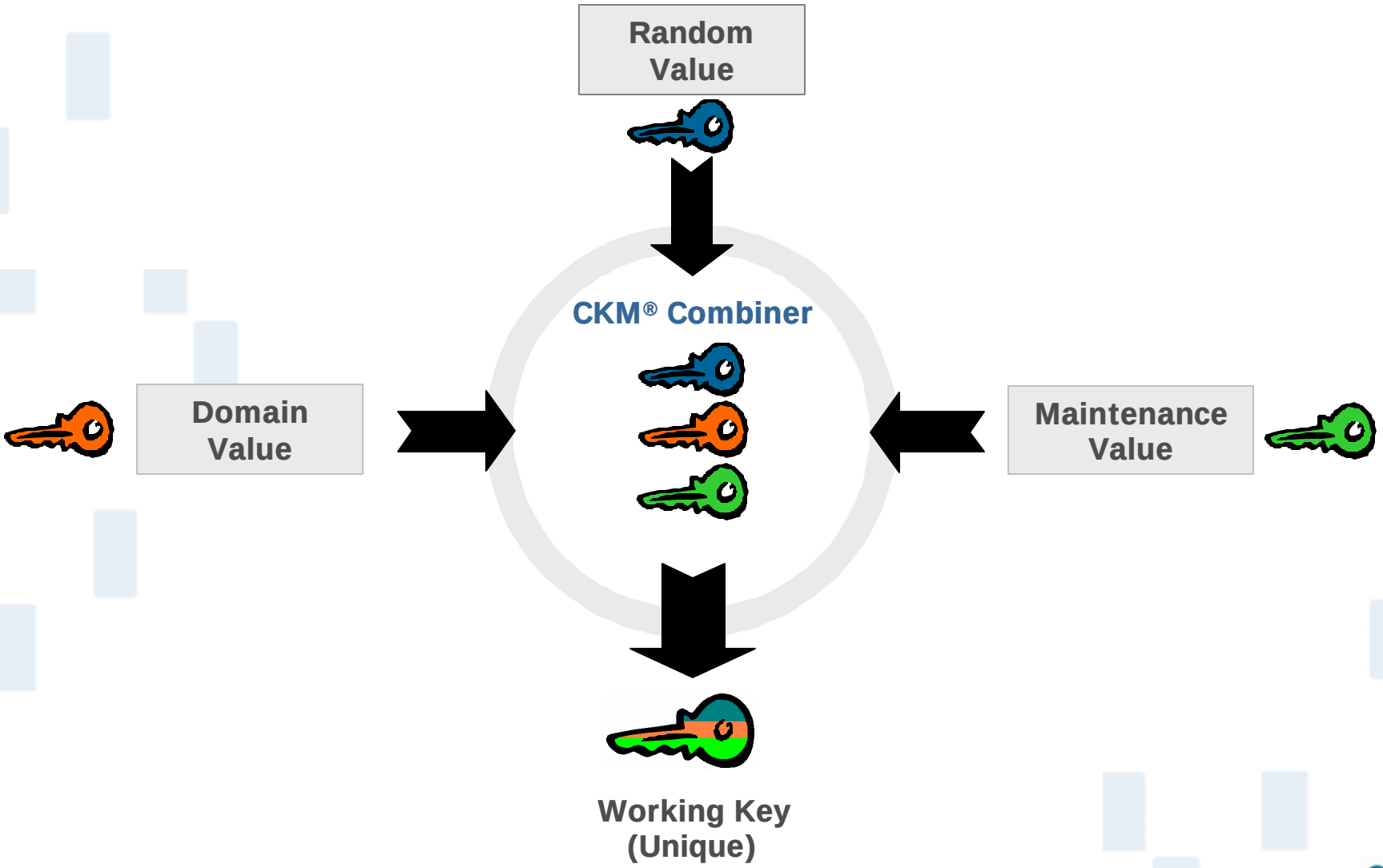
Each supplied Credential's Private Key & the Ephemeral Public Key are used to produce a Sub-key.



Sub-keys are combined to produce a key to decrypt the Random

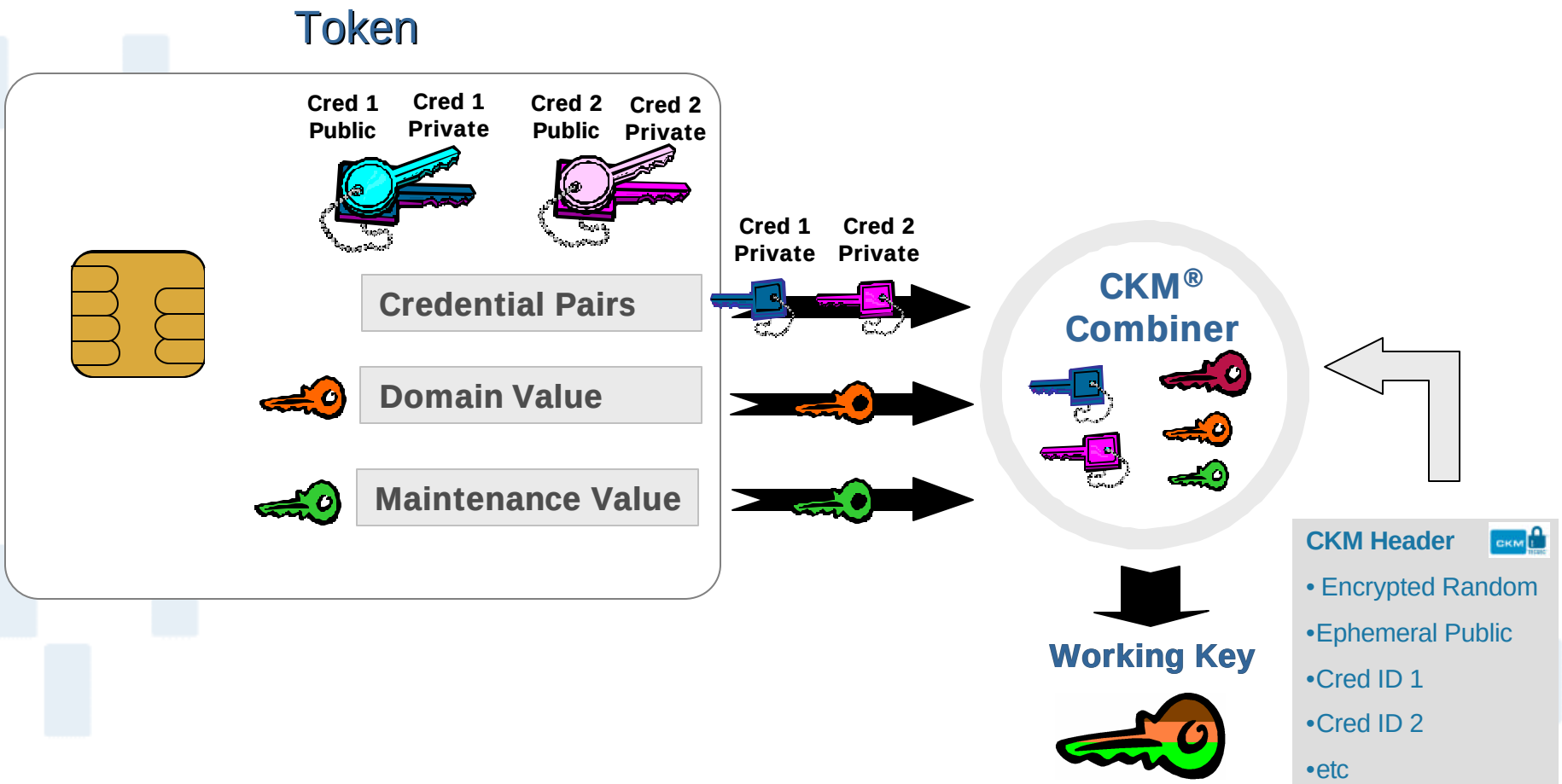
©TecSec®, Incorporated 2003-2008. All rights reserved.

Decryption Functional View
Phase I - Working Key Generation



©TecSec®, Incorporated 2003-2008. All rights reserved.

Decryption – Logical View – Completed

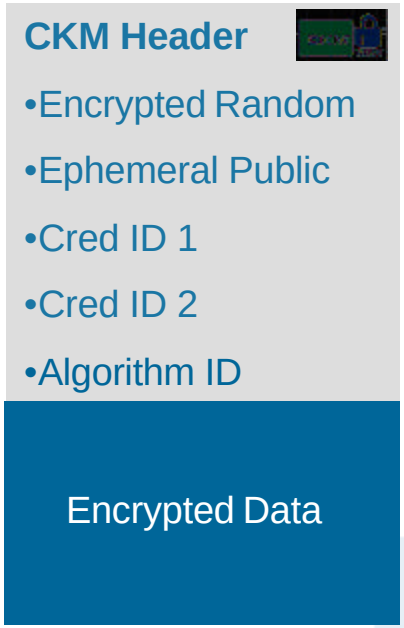


©TecSec®, Incorporated 2003-2008. All rights reserved.

Decrypting the Data

- Once the Working Key has been created, the following steps occur:

1. We look in the CKM Header to determine the correct algorithm to use based on the algorithm ID
2. The Working Key is then truncated to conform to the algorithm specified
3. The data is decrypted with the Working Key and the Header is discarded
4. The Working Key is destroyed



©TecSec®, Incorporated 2003-2008. All rights reserved.

Review of CKM®

- Working Key and Header are output from the CKM Combiner
- CKM Header describes how to regenerate the Working Key
- Credentials are used to protect components used in the Working Key generation process
- Without knowledge of all necessary key material the Working Key cannot be regenerated
- Cryptographically enforced Role Based Access Control is achieved

©TecSec®, Incorporated 2003-2008. All rights reserved.

Advanced CKM® Concepts

- Credentials can be supplied to the combiner to produce multiple encrypted random values - each protected with a different set of Credentials
  - Logical AND / Logical OR
- X.509 Certificates can be used to protect the Working Key
  - CKM Header can include entries which specify individuals using PKI and groups using CKM

©TecSec®, Incorporated 2003-2008. All rights reserved.

Comparison of CKM® and PKI

CKM

- One-to-Many Key Management
- Role Based Access Control
- Centralized Key Creation

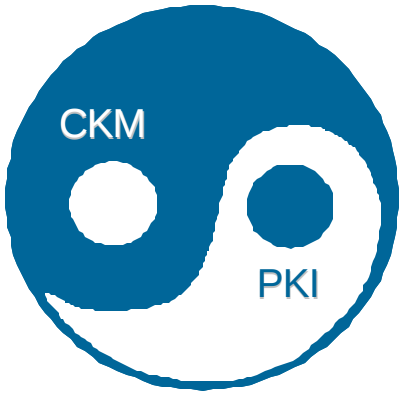
PKI

- One-to-One Key Management
- Identification & Authentication
- Distributed Key Creation

©TecSec®, Incorporated 2003-2008. All rights reserved.

Combining CKM® and PKI

- One-to-One Key Management
- One-to-Many Key Management
- Identification & Authentication
- Role Based Access Control



©TecSec®, Incorporated 2003-2008. All rights reserved.

Example Applications of CKM®

- Digital Rights Management
- Workflow
- Collaborative Development
- Broadcasting Encrypted Information

©TecSec®, Incorporated 2003-2008. All rights reserved.

Questions?

©TecSec®, Incorporated 2003-2008. All rights reserved.

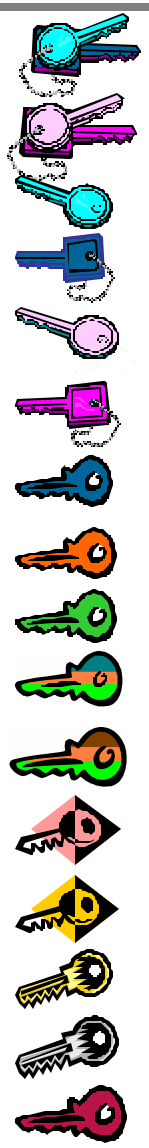
Contact Information

TECSEC, Incorporated
E-mail: info@tecsec.com

©TecSec®, Incorporated 2003-2008. All rights reserved.

Key Legend

- Credential 1 Key Pair
- Credential 2 Key Pair
- Credential 1 Public
- Credential 1 Private
- Credential 2 Public
- Credential 2 Private
- Random Value
- Domain Value
- Maintenance Value
- Working Key (Encryption)
- Working Key (Decryption)
- Ephemeral Public
- Ephemeral Private
- Sub-key 1
- Sub-key 2
- Encrypted Random



©TecSec®, Incorporated 2003-2008. All rights reserved.