Key Management - From Cryptoprocessors to OASIS

Christian Cachin

IBM Zurich Research Laboratory

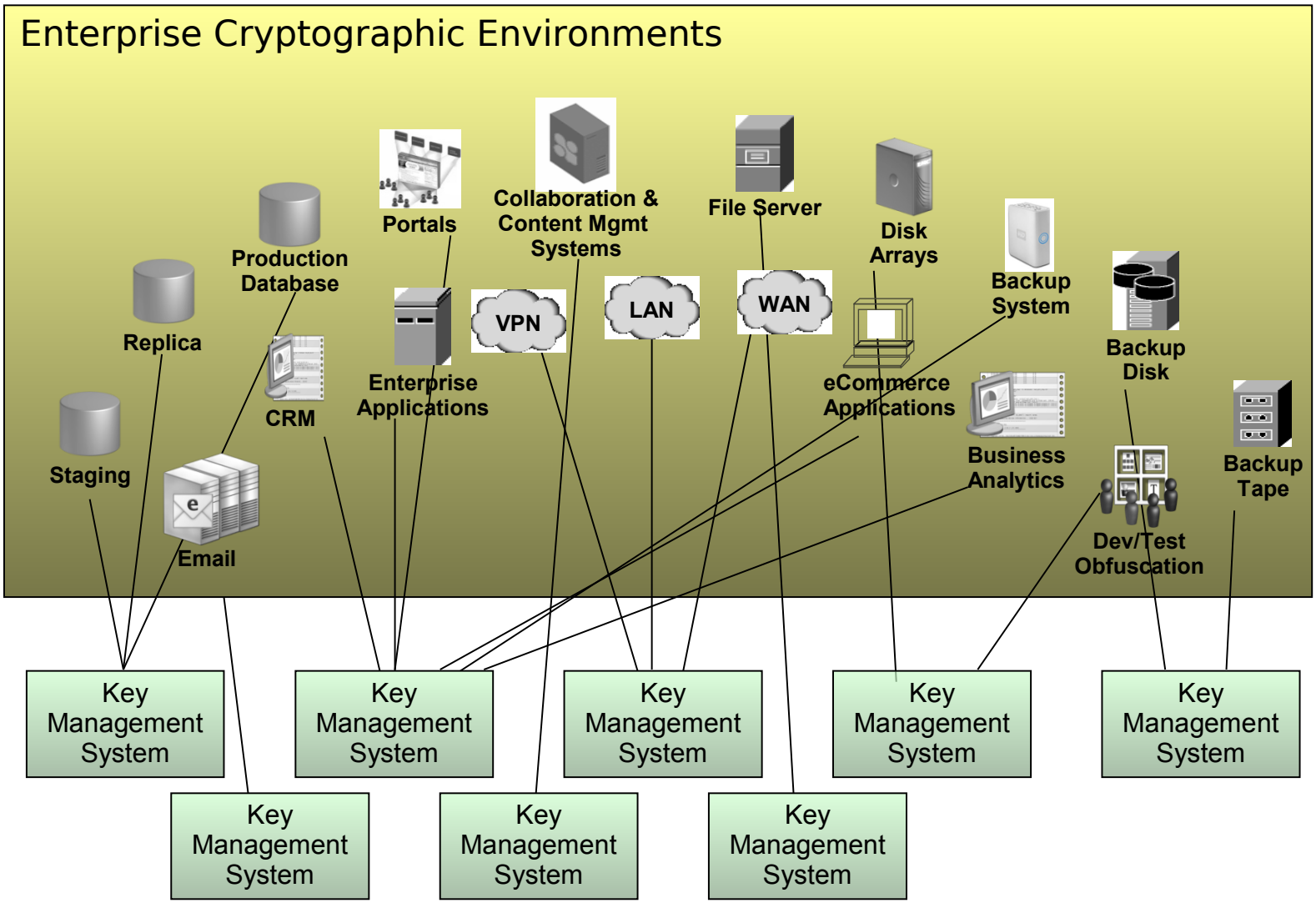
28 April 2009

Warning

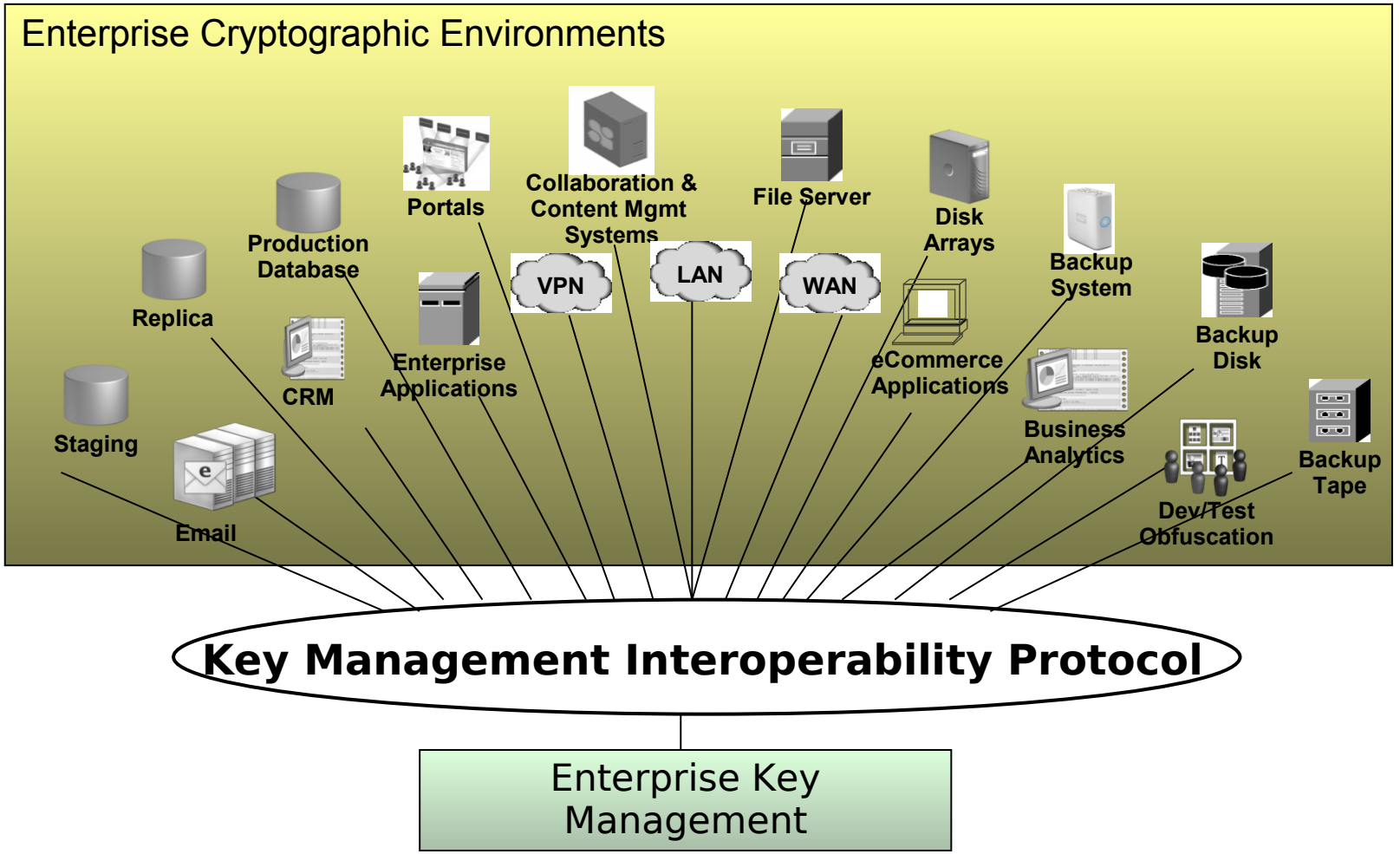
This presentation contains explicit exposure to applications, standards, and the commercial world.

Key management?

Today: Proprietary key mgmt.



Future: Standardized key mgmt. across enterprise



OASIS Key Management Inter-operability Protocol (KMIP)

- OASIS...? XML
- Client-server protocol
- Defines objects with attributes, plus operations
  - Objects: symmetric keys, public/private keys, certificates, threshold key-shares ...
  - Attributes: identifiers, type, length, lifecycle-state, lifecycle dates, links to other objects ...
  - Operations: create, register, attribute handling ...

OASIS KMIP

- Draft for KMIP V1 prepared by
  - Brocade, HP, IBM, LSI, NetApp, RSA-EMC, Seagate, nCipher/Thales
- OASIS KMIP TC formed in Apr. 2009
- http://www.oasis-open.org/committees/kmip/

KMIP Operations

- Mostly standard attribute handling, except:
  - Key wrapping: encrypt a key with another key
  - Key derivation: create a symmetric key from an existing one using a PRF
- Access control on keys depends on their cryptographic dependencies:
  - Wrapping key leaks wrapped keys
  - Parent key leaks derived keys

Cryptographic problems

- Key wrapping = circular encryption

  → PK-encryption secure against key-dependent CCA
  [Camenisch, Chandran, Shoup; Eurocrypt 2009]

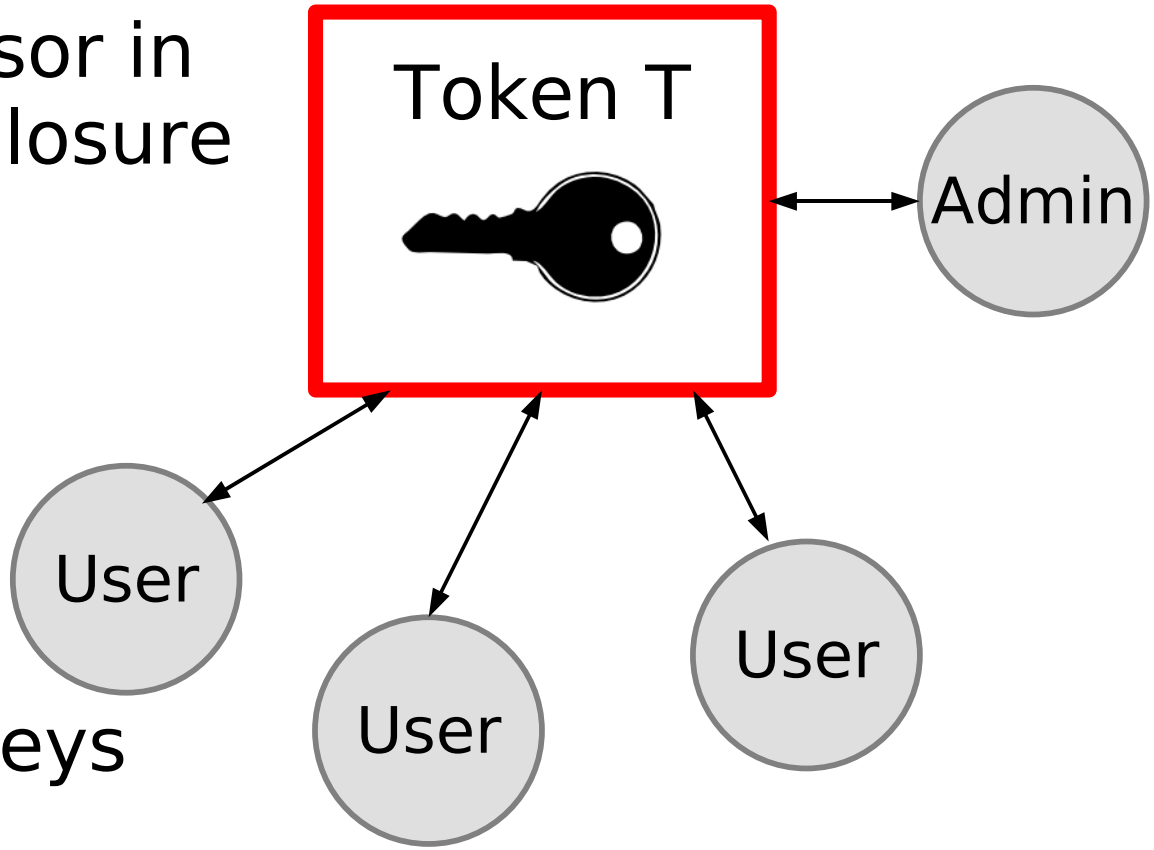
- Access control to keys without "API attacks"
  - Same problem exists in cryptoprocessors APIs (IBM 4758, PKCS #11 ...)
  - Attacks by Andreson, Bond, Clulow ...

  → Secure cryptographic token interface
  [Cachin & Chandran; CSF-22, 2009]

Cryptoprocessors

Cryptographic tokens
Hardware security modules (HSM)

- Crypto co-processor in tamper-proof enclosure
- Keys never leave token in clear
- Executes all cryptographic operations with keys



Commercial cryptoprocessors

HP Atalla Ax150

IBM 4764

nCipher/Thales netHSM

Infineon TPM

Tamper-resistant and -responsive according to FIPS 140-2, up to Level 4

Follow up

- A Public-Key Encryption Scheme Secure against Key-Dependent Chosen-Plaintext and Adaptive Chosen-Ciphertext Attacks
  - Jan Camenisch, Nishanth Chandran, Victor Shoup
    Eurocrypt 2009 (**tomorrow, 10h05**)

- A Secure Cryptographic Token Interface
  - Christian Cachin & Nishanth Chandran
    Computer Security Foundations Symposium 2009
    (July 8-10)