Smart Cards & Remote Entrusting

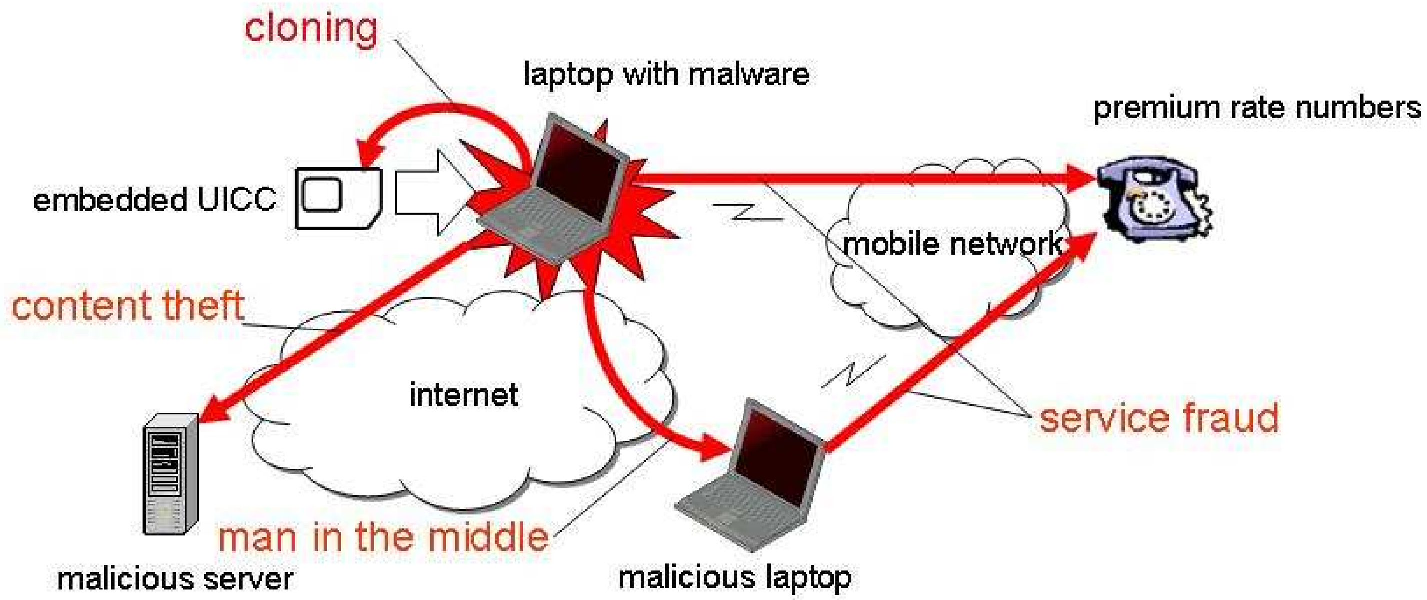
Jean-Daniel Aussel & Jerome d’Annoville

RE-TRUST workshop, Trento

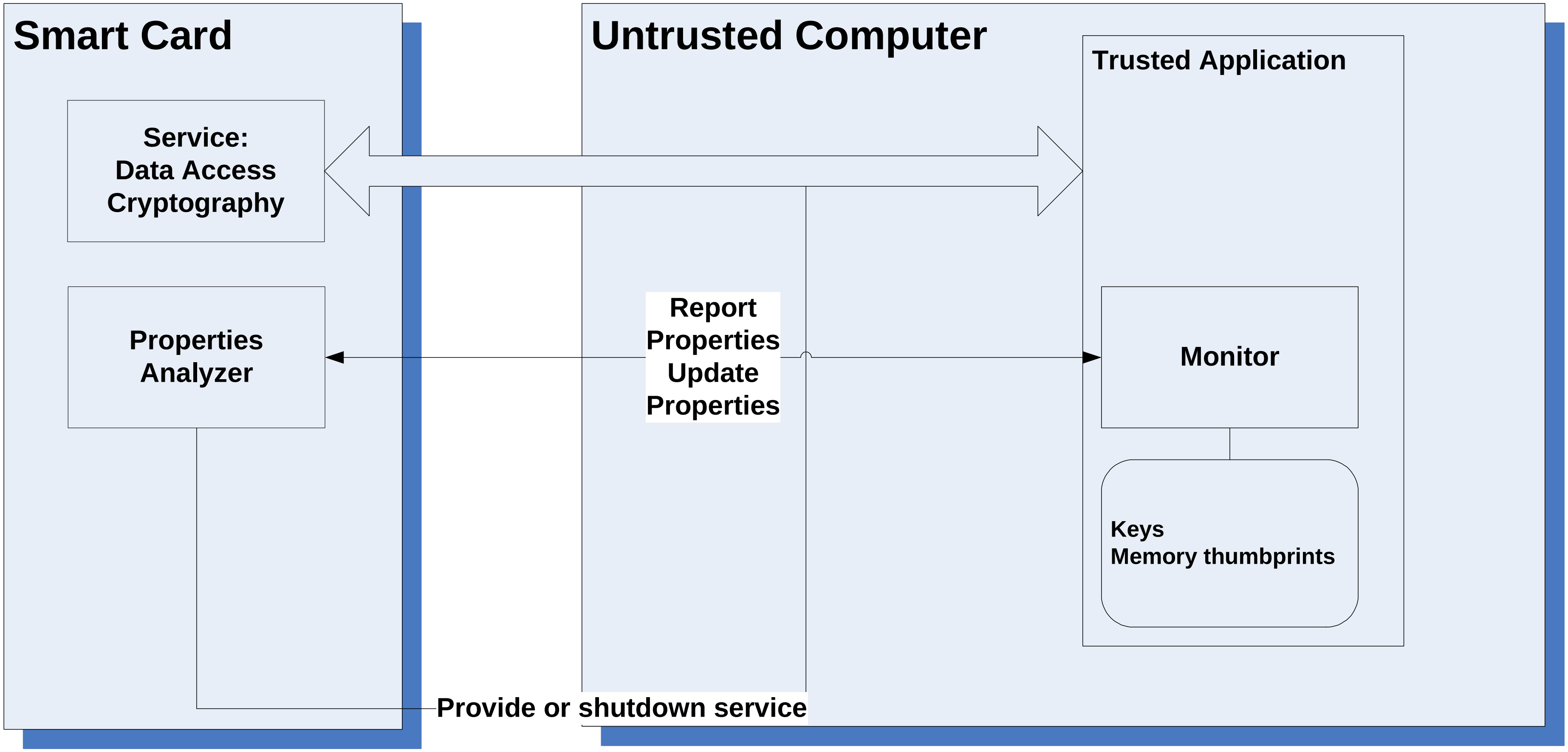
October 15, 2008

Voice Over IP Softphone

- The softphone needs access to the card (UICC) for retrieving phonebook entries or authenticate to the network
- The card must be sure that it is used by the genuine softphone, and that the softphone has not been tampered with before releasing data or performing authentication



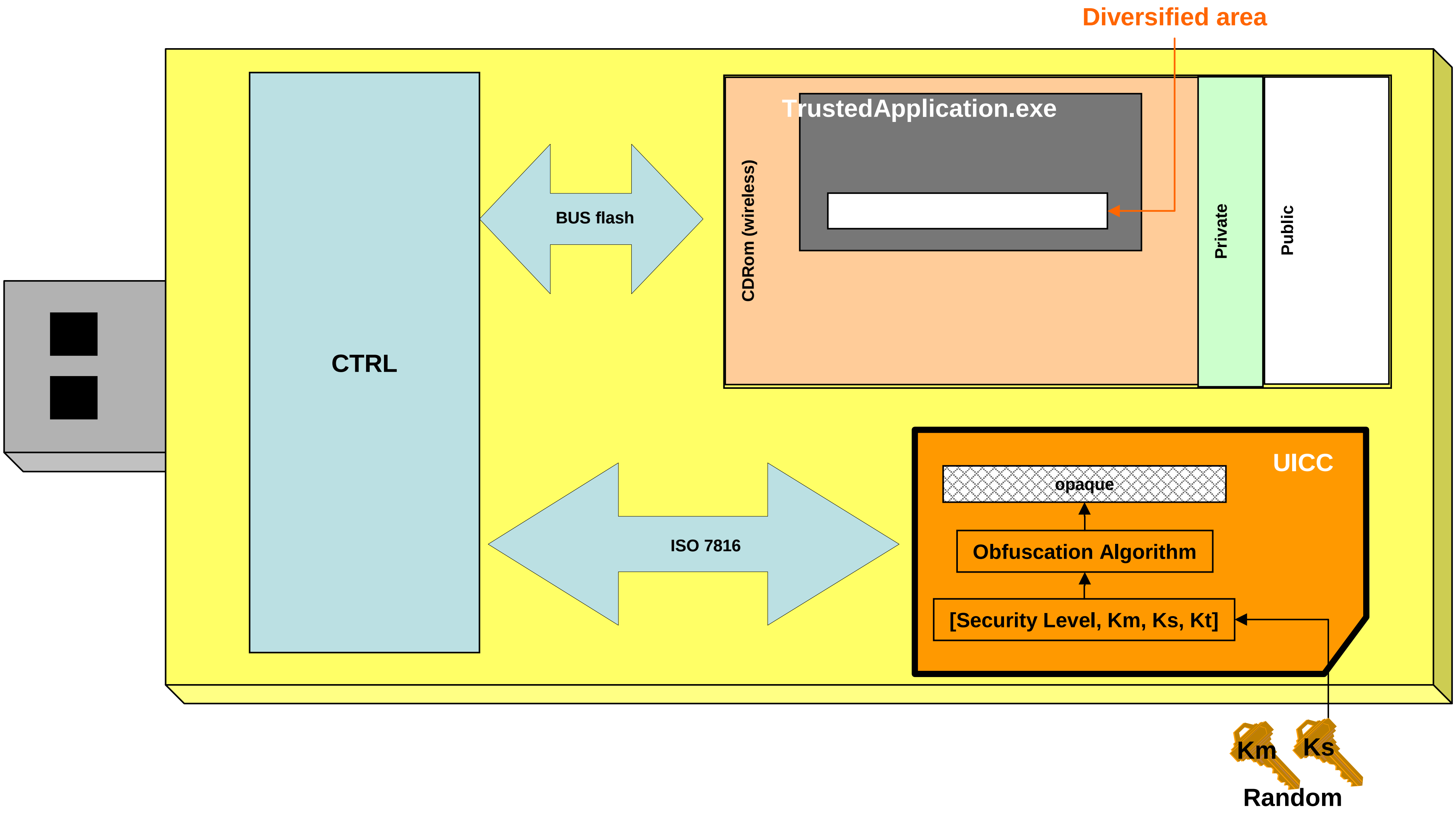
Overview of Remote Entrusting with Smart Cards



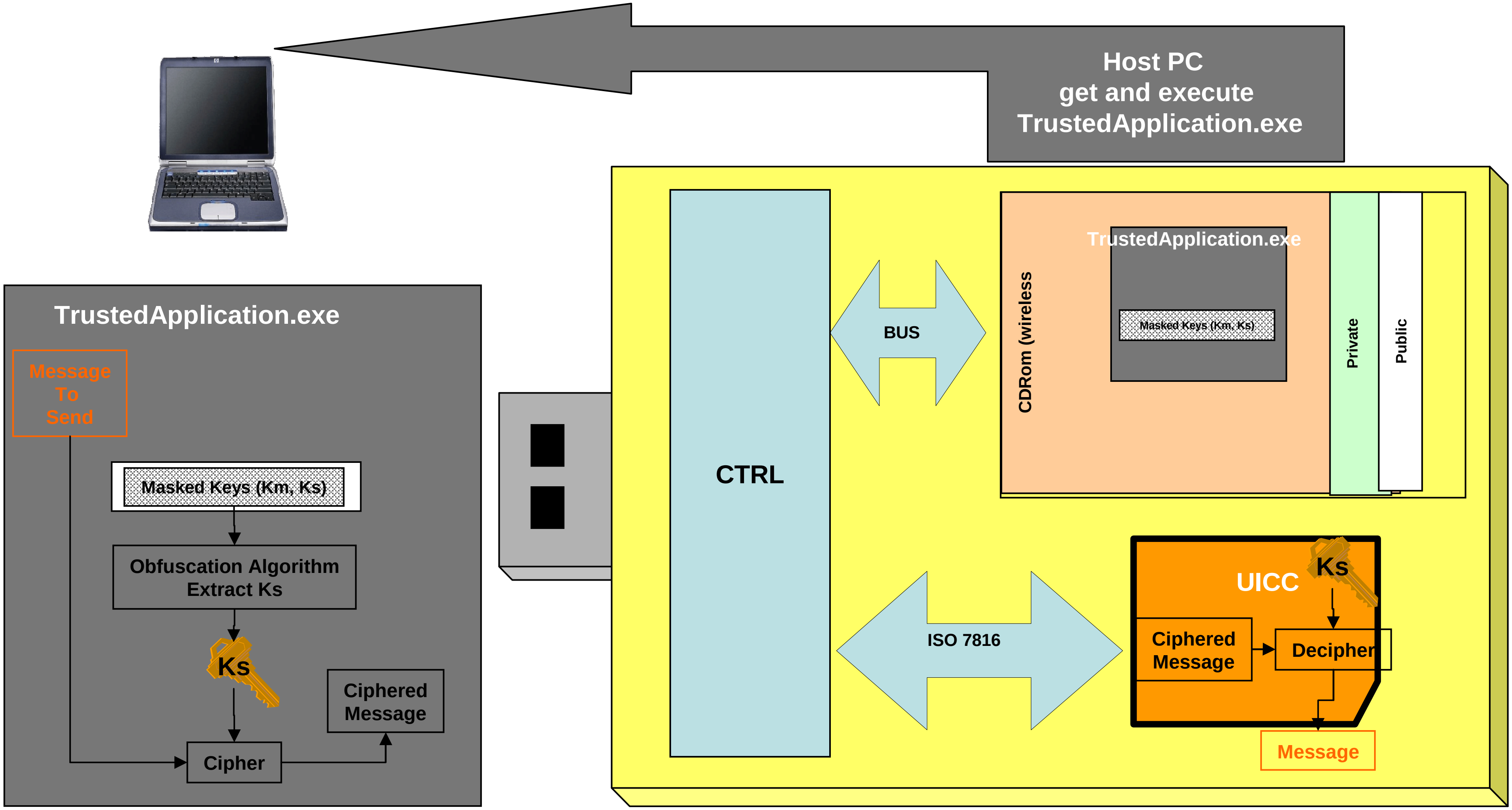
Smart Card for Remote Entrusting

- Dongle with USB 2.0 interface for high speed communication
- Flash memory to store trusted application that will be provisioned to the un-trusted terminal
- Monitor, keys and thumbprints are embedded in the trusted application
- Zero install: does not required any driver, and uses the mass-storage interface (USB memory stick and CDROM operating system drivers)
- Provide secure channel access to standard smart cards (e.g. SIM card)

Secure Channel Establishment: Card Insertion



Secure Channel: Messaging



Host PC
get and execute
TrustedApplication.exe

TrustedApplication.exe

Message
To
Send

Masked Keys (Km, Ks)

Obfuscation Algorithm
Extract Ks

Ks

Cipher

Ciphered
Message

CTRL

BUS

ISO 7816

CDRom (wireless

TrustedApplication.exe

Masked Keys (Km, Ks)

Private

Public

UICC

Ks

Ciphered
Message

Decipher

Message

Thumbprints

- A thumbprint is a section of code segment which is hashed
- A set of thumbprints is stored in the smart card at personnalization time (code segment hash, offset and length)
- Thumbprints are used for secure channel session key renewal regularly

Thank You

Questions?