The Tookan device API analyser

Graham Steel

LSV, INRIA & CNRS & ENS-Cachan

(joint work with Riccardo Focardi, Matteo Bortolozzo
& Matteo Centenaro, Università Ca' Foscari, Venezia)

RSA Public Key Cryptography Standard (PKCS) 11

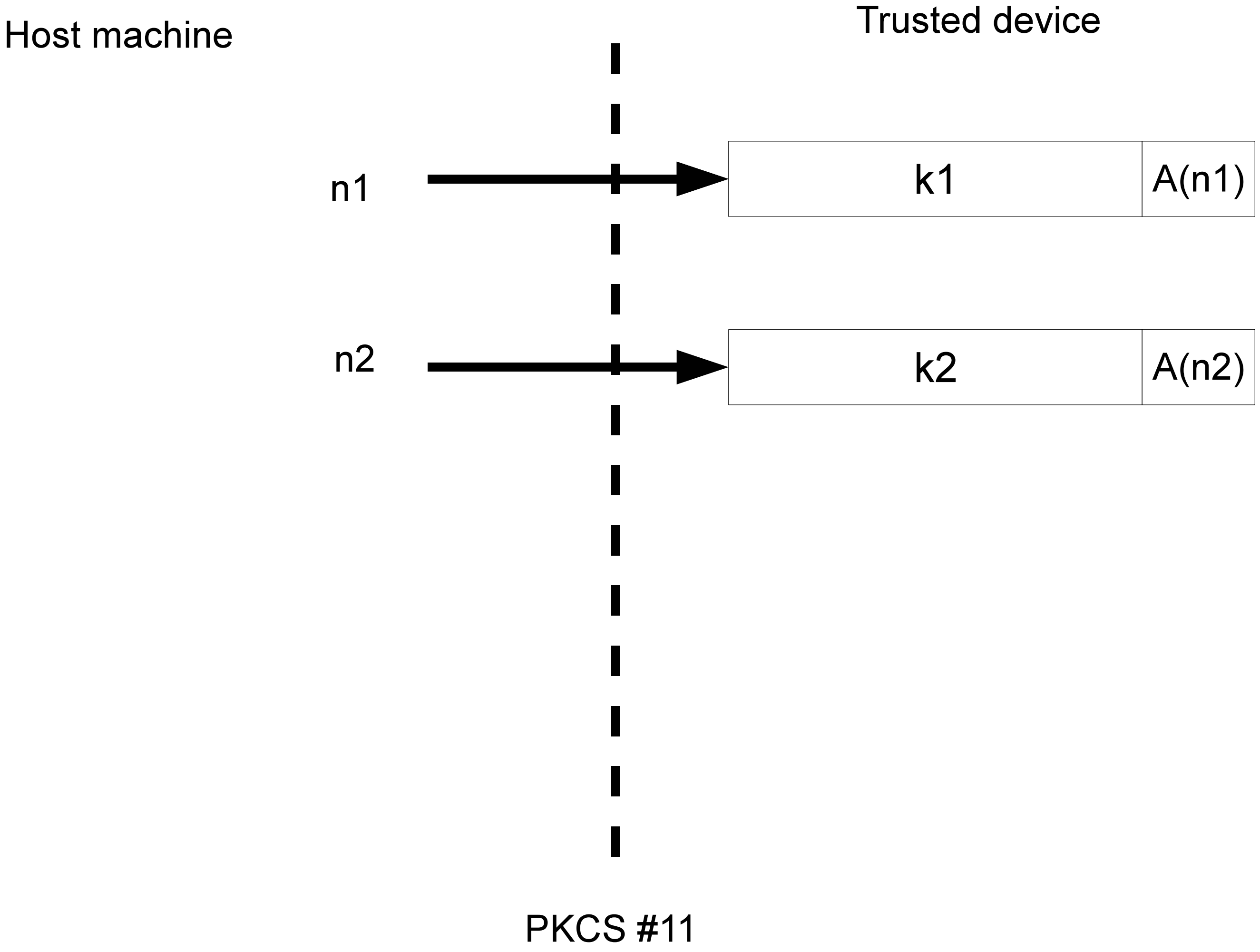
PKCS #1 describes the RSA encryption algorithm, padding etc.

PKCS#11 Describes ‘cryptoki’: cryptographic token interface

Ubiquitous in industry for authentication tokens, smartcards
(and HSMs, other devices, . . .)

Authentication token market alone estimated at 5 billion USD annually
(InfoSecurity Magazine Feb 2010)

RSA
SecurID
acs
ePass2000
IRONKEY
SafeNet



Host machine

Trusted device

n1

k1

A(n1)

n2

k2

A(n2)

PKCS #11

Generating keys

A *key template* is a partial specification of key attributes

Templates are used for creating, manipulating, and searching for objects

$$\mathsf{C\_GenerateKey}: \quad \mathcal{T} \xrightarrow{\text{new n,k}} \mathsf{h}(\mathsf{n},\mathsf{k}); \mathsf{T}$$

Setting Key Attributes

$$\mathsf{C\_SetAttributeValue:}$$

$$\mathcal{T}, \mathsf{h}(\mathsf{n}, \mathsf{k}) \quad \rightarrow \quad \mathsf{h}(\mathsf{n}, \mathsf{k}); \mathsf{T}$$

$\mathcal{T}$ can specify new values for any attributes, but may cause `CKR_TEMPLATE_INCONSISTENT`, `CKR_ATTRIBUTE_READ_ONLY`

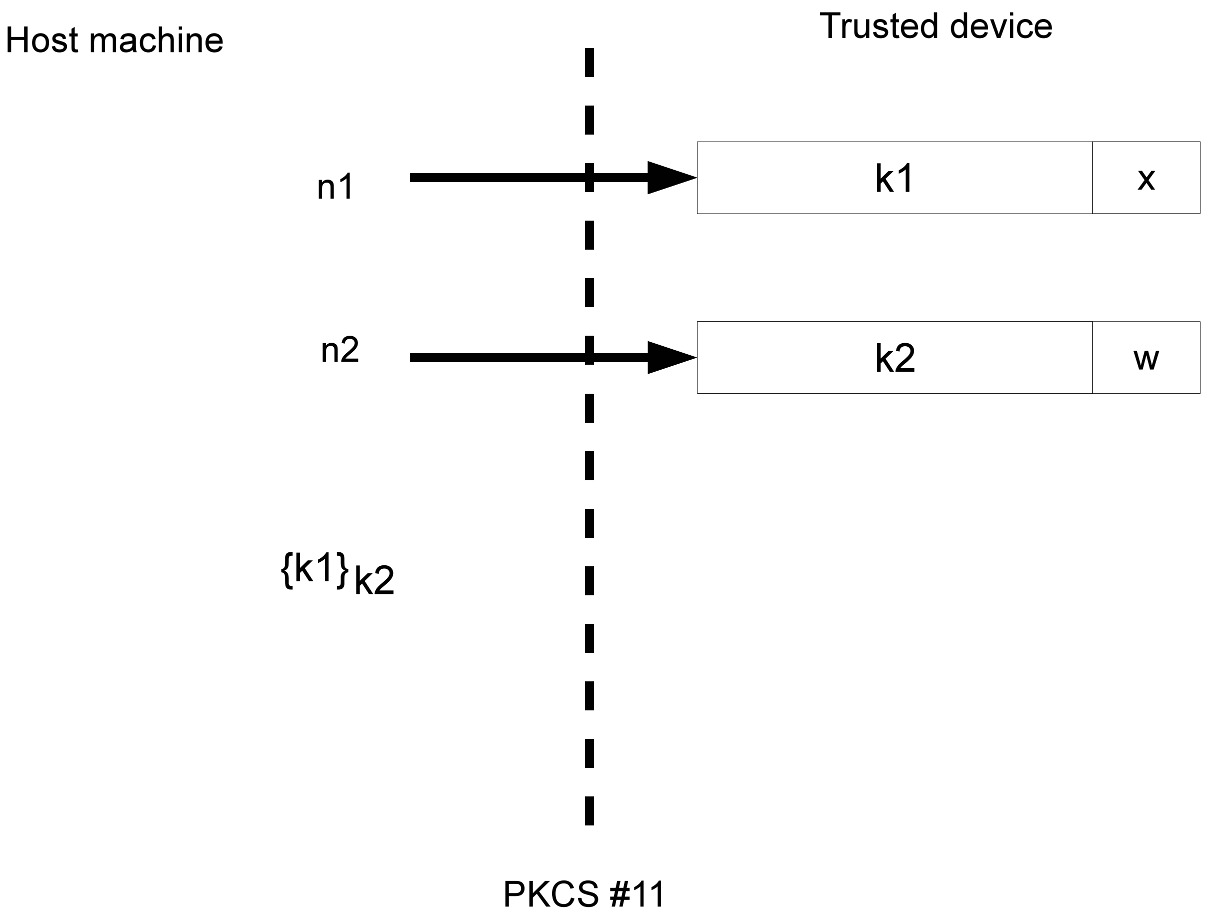
Wrap and Unwrap

$$\mathsf{Wrap}:$$

$$\begin{array}{rcl} \mathsf{h}(\mathsf{x}_1,\mathsf{y}_1),\mathsf{h}(\mathsf{x}_2,\mathsf{y}_2);\ \mathsf{wrap}(\mathsf{x}_1), & \rightarrow & \{\mathsf{y}_2\}_{\mathsf{y}_1} \\ \mathsf{extract}(\mathsf{x}_2) & & \end{array}$$

$$\mathsf{Unwrap}:$$

$$\mathsf{h}(\mathsf{x}_2,\mathsf{y}_2),\{\mathsf{y}_1\}_{\mathsf{y}_2},\mathcal{T};\ \mathsf{unwrap}(\mathsf{x}_2) \quad \xrightarrow{\mathsf{new}\ \mathsf{n}_1} \quad \mathsf{h}(\mathsf{n}_1,\mathsf{y}_1);\ \mathsf{extract}(\mathsf{n}_1),\ \mathsf{T}$$



Host machine

Trusted device

n1

k1

x

n2

k2

w

$\{k1\}_{k2}$

PKCS #11

Key Usage

$$\mathsf{Encrypt:}$$

$$\mathsf{h}(\mathsf{x}_1, \mathsf{y}_1), \mathsf{y}_2;\ \mathsf{encrypt}(\mathsf{x}_1) \quad \longrightarrow \quad \{\mathsf{y}_2\}_{\mathsf{y}_1}$$

$$\mathsf{Decrypt:}$$

$$\mathsf{h}(\mathsf{x}_1, \mathsf{y}_1), \{\mathsf{y}_2\}_{\mathsf{y}_1};\ \mathsf{decrypt}(\mathsf{x}_1) \quad \longrightarrow \quad \mathsf{y}_2$$

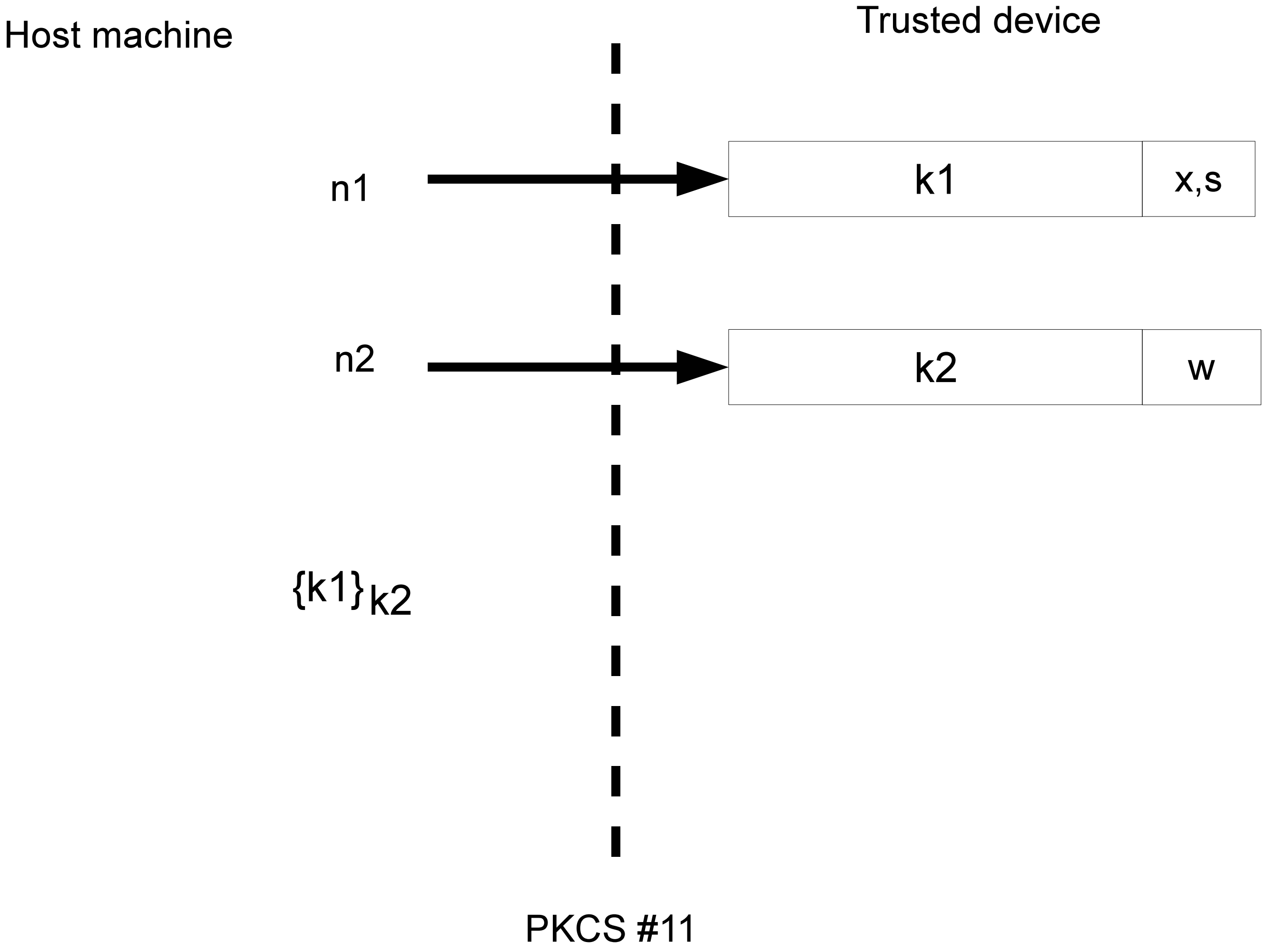
PKCS#11 Security

Section 7 of standard:

“1. Access to private objects on the token, and possibly to cryptographic functions and/or certificates on the token as well, requires a PIN.

2. Additional protection can be given to private keys and secret keys by marking them as “sensitive” or “unextractable”. Sensitive keys cannot be revealed in plaintext off the token, and unextractable keys cannot be revealed off the token even when encrypted”

“Rogue applications and devices may also change the commands sent to the cryptographic device to obtain services other than what the application requested [but cannot] compromise keys marked “sensitive,” since a key that is sensitive will always remain sensitive. Similarly, a key that is unextractable cannot be modified to be extractable.”



Host machine

Trusted device

n1

k1

x,s

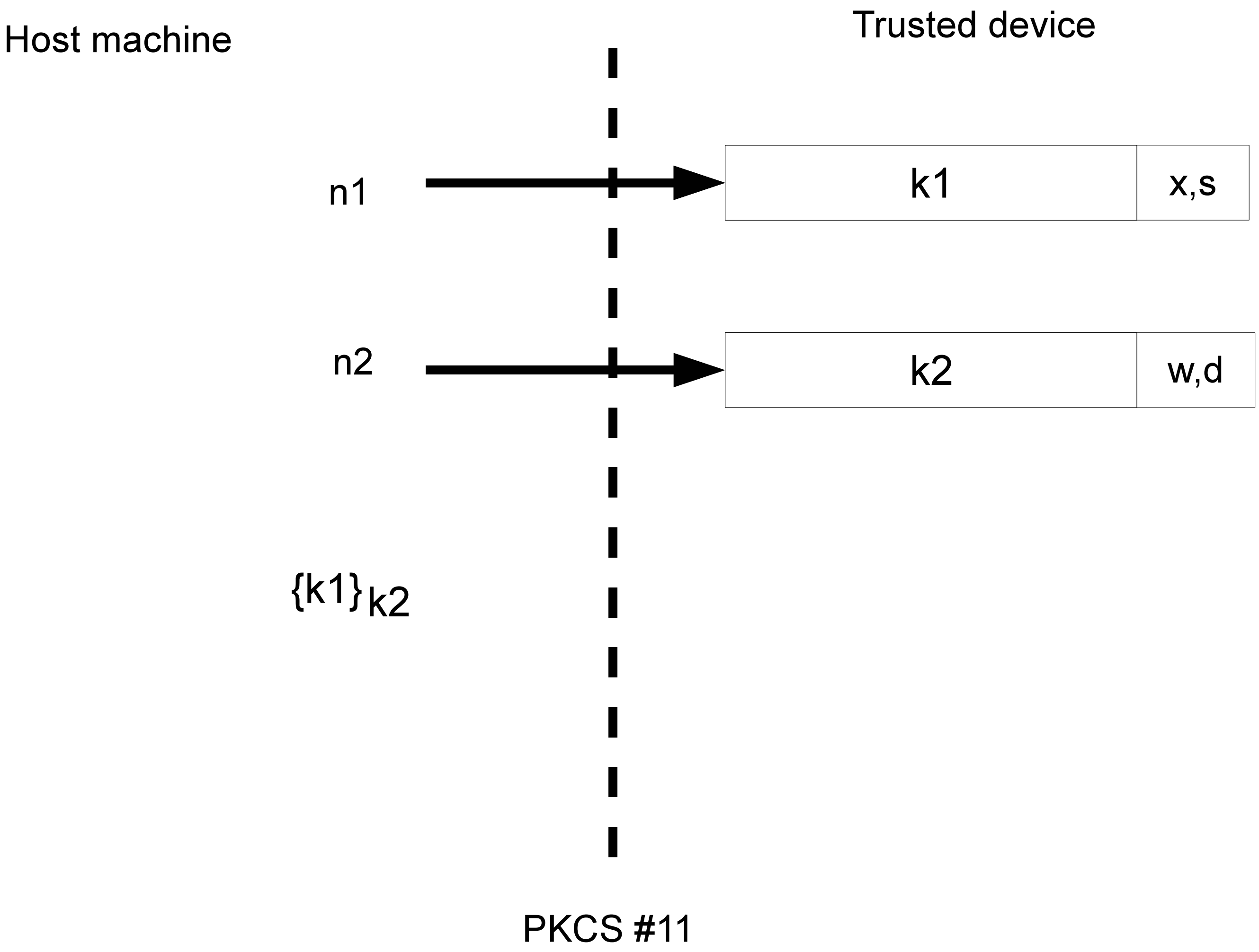
n2

k2

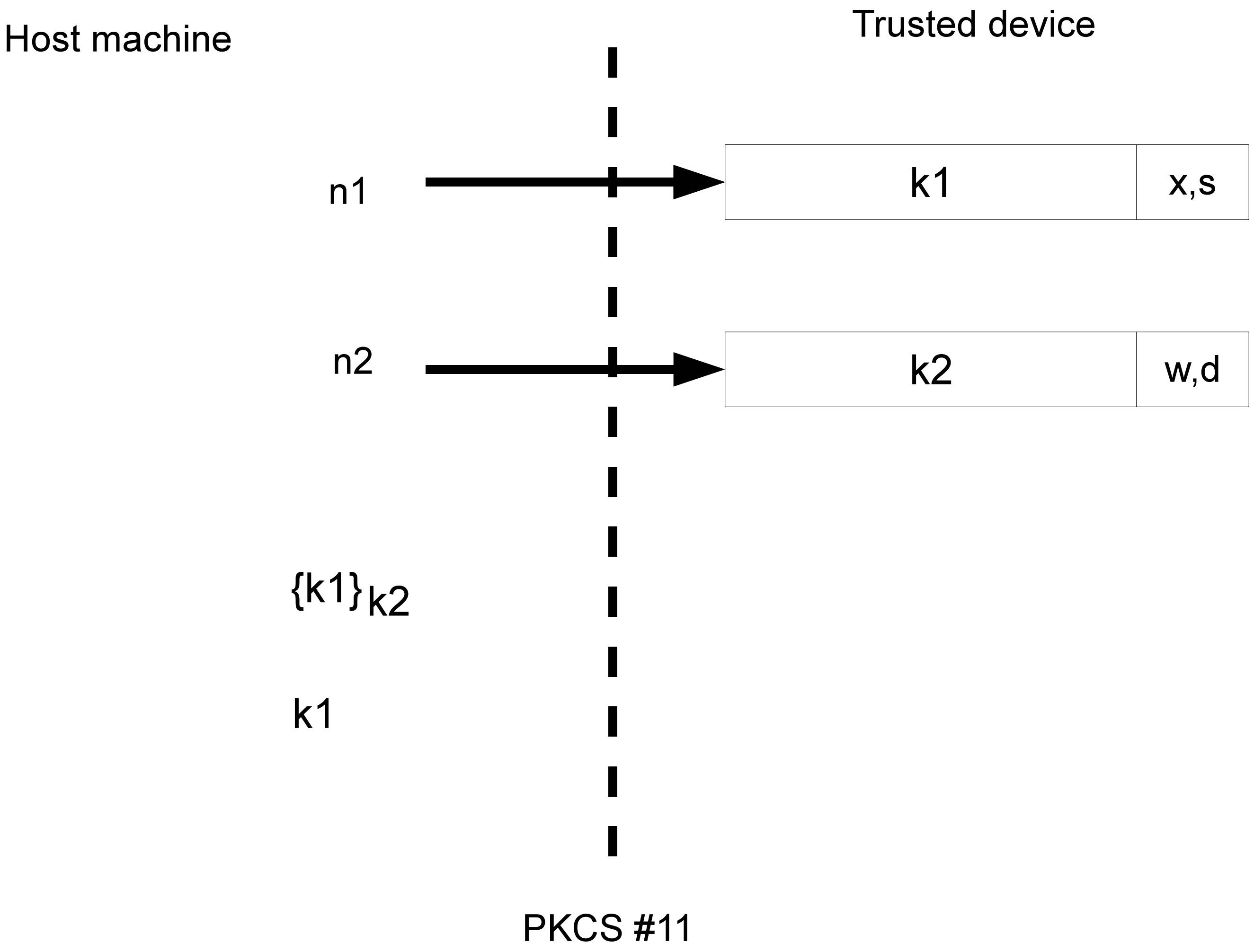
w

$\{k1\}_{k2}$

PKCS #11


Host machine
Trusted device
n1
k1
x,s
n2
k2
w,d
{k1}k2
PKCS #11

Clulow, CHES 2003



Host machine

Trusted device

n1

k1

x,s

n2

k2

w,d

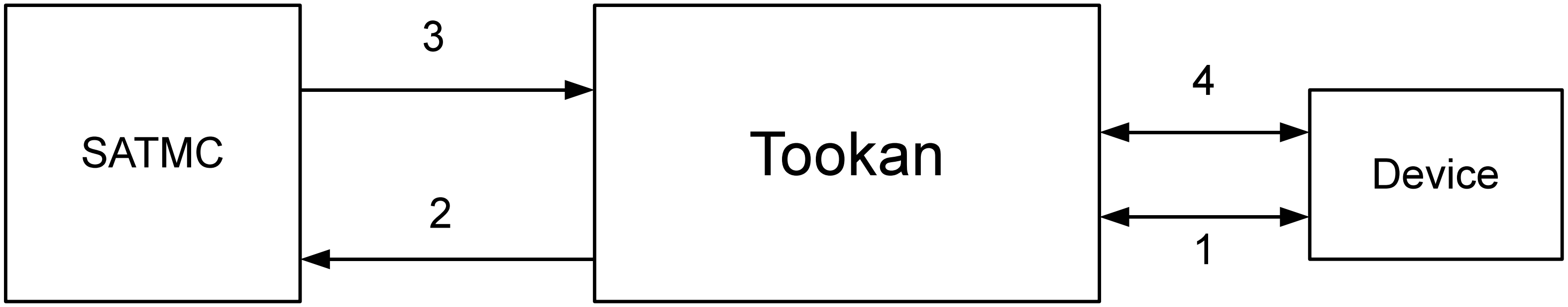
$\{k1\}_{k2}$

k1

PKCS #11

TOOKAN

‘Tool for cryptoKi Analysis’



TOOKAN

Device		Supported Functionality						Attacks found				
Brand	Model	s	as	cobj	chan	w	ws	wd	rs	ru	su	Tookan
Aladdin	eToken PRO	✓	✓	✓	✓	✓	✓	✓				wd
Athena	ASEKey	✓	✓	✓								
Bull	Trustway RCI	✓	✓	✓	✓	✓	✓	✓				wd
Eutron	Crypto Id. ITSEC		✓	✓								
Feitian	StorePass2000	✓	✓	✓	✓	✓	✓	✓	✓	✓		rs
Feitian	ePass2000	✓	✓	✓	✓	✓	✓	✓	✓	✓		rs
Feitian	ePass3003Auto	✓	✓	✓	✓	✓	✓	✓	✓	✓		rs
Gemalto	SEG		✓		✓							
MXI	Stealth MXP Bio	✓	✓		✓							
RSA	SecurID 800	✓	✓	✓	✓				✓	✓	✓	rs
SafeNet	iKey 2032	✓	✓	✓		✓						
Sata	DKey	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	rs
ACS	ACOS5	✓	✓	✓	✓							
Athena	ASE Smartcard	✓	✓	✓								
Gemalto	Cyberflex V2	✓	✓	✓		✓	✓	✓				wd
Gemalto	SafeSite V1		✓		✓							
Gemalto	SafeSite V2	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	rs
Siemens	CardOS V4.3 B	✓	✓	✓		✓				✓		ru

Manufacturer Reaction

All 7 received notification at least 5 months before publication.

We offered to publish responses on project website

RSA sent response, registered vulnerability with Mitre (CVE-2010-3321), issued security advisory 6 Oct 2010

Aladdin (now Safenet) sent a 2-page response for website

Minimal response from anyone else (e.g. requests to know who else is vulnerable)

Since the first presentation of Tookan (CCS Chicago Oct ’10),
Tookan licenced to Boeing and a major UK bank.

Summary and Conclusions

Tookan: an effective tool for formal analysis of PKCS#11 configurations

State of art of tokens not great (10/18 vulnerable, the rest very limited functionality)

Some manufacturers patching, no reaction from others

Recently: testing on HSMs. Interesting results.

Project webpage:

`http://tookan.gforge.inria.fr/`