



The Security of Trusted Computing

Rick Wash

`rwash@citi.umich.edu`

CITI - University of Michigan



TCPA Functions

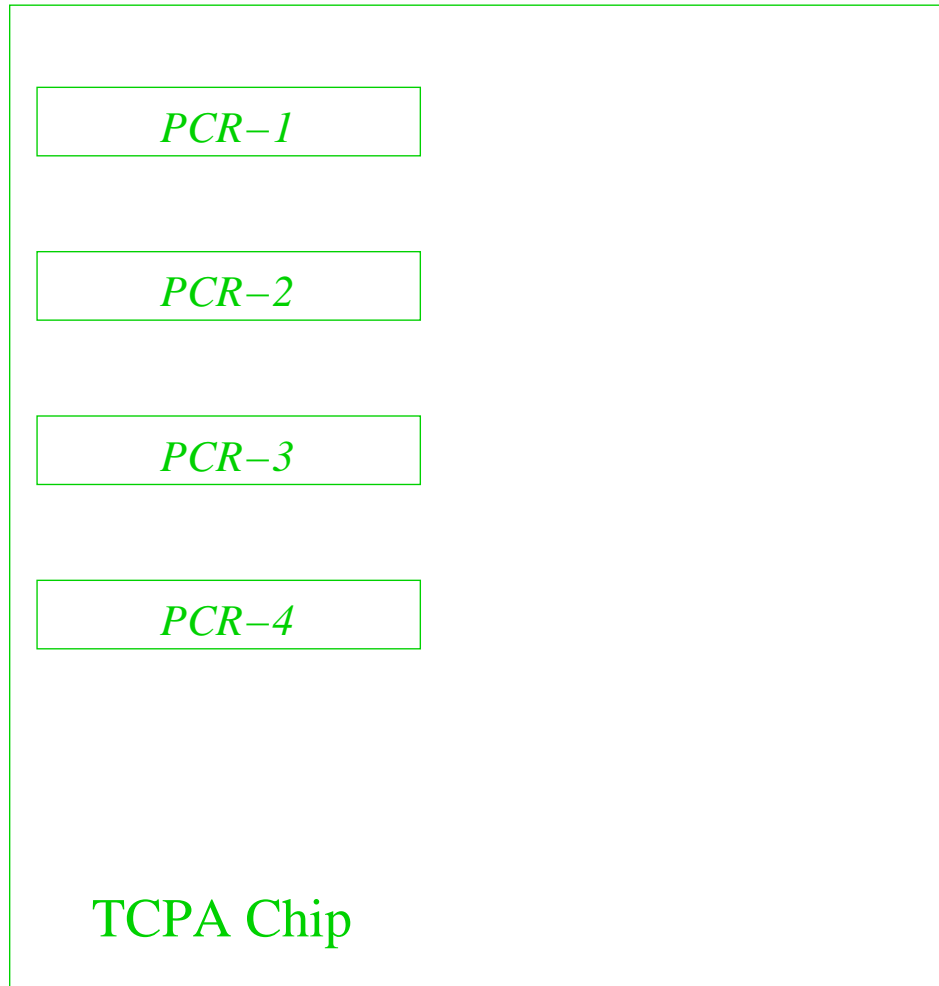
- ⑥ Public Key Functions
 - △ Key Generation
 - △ Signature
 - △ Encryption / Decryption
- ⑥ Trusted Boot
 - △ Hash Functions
 - △ Platform Configuration
- ⑥ Initialization and Management

TCPA Chip

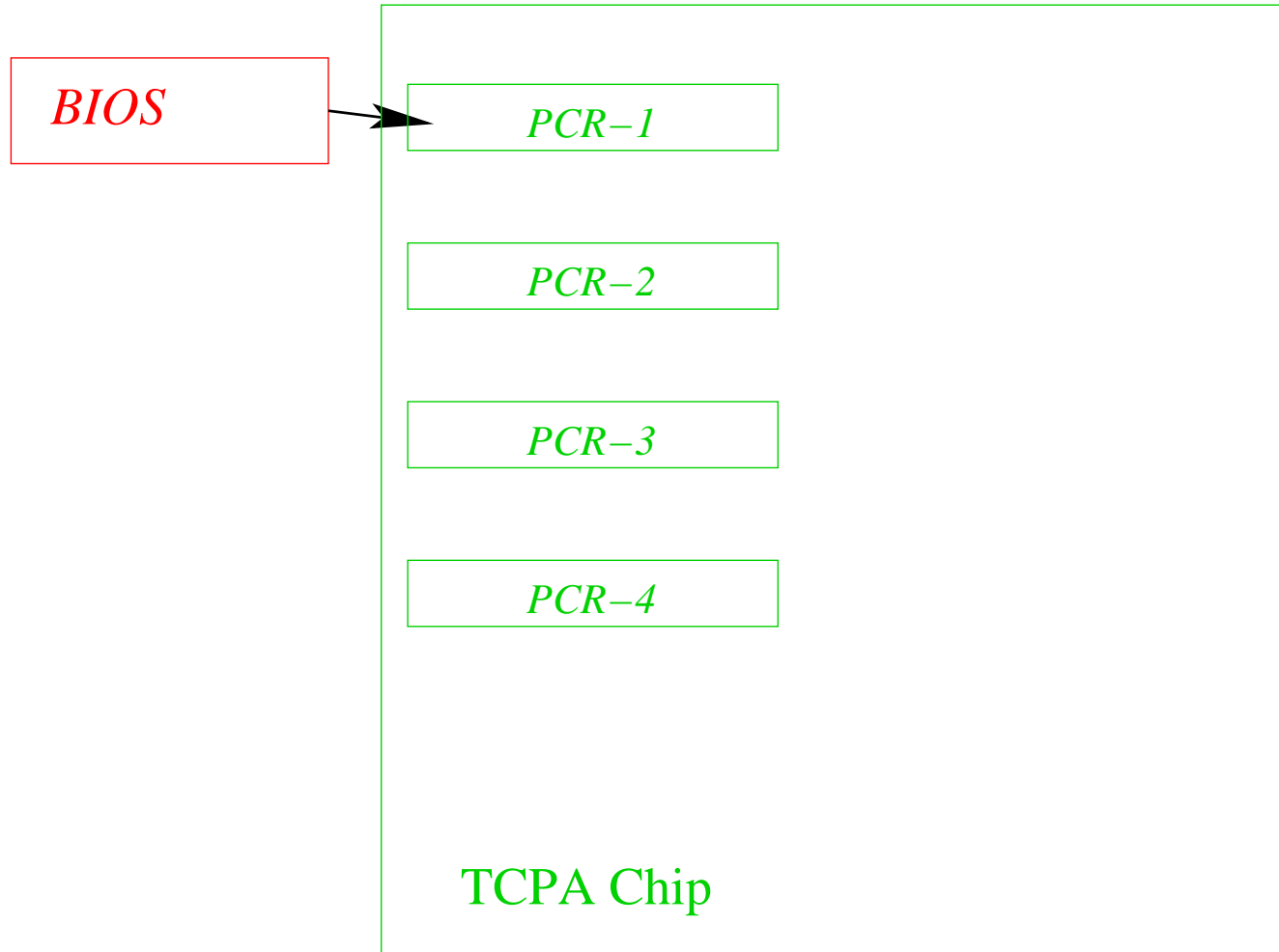
Functional Units	Non-volatile Memory	Volatile Memory
RNG	Endorsement Key (2048b)	RSA Key Slot 0 ● ● ●
Hash	Storage Root Key (2048b)	RSA Key Slot 9
HMAC	Owner Auth Secret (160b)	PCR-0 ● ● ●
RSA Key Generation		PCR-14
RSA Encrypt / Decrypt		Key Handles
		Auth Session Handles



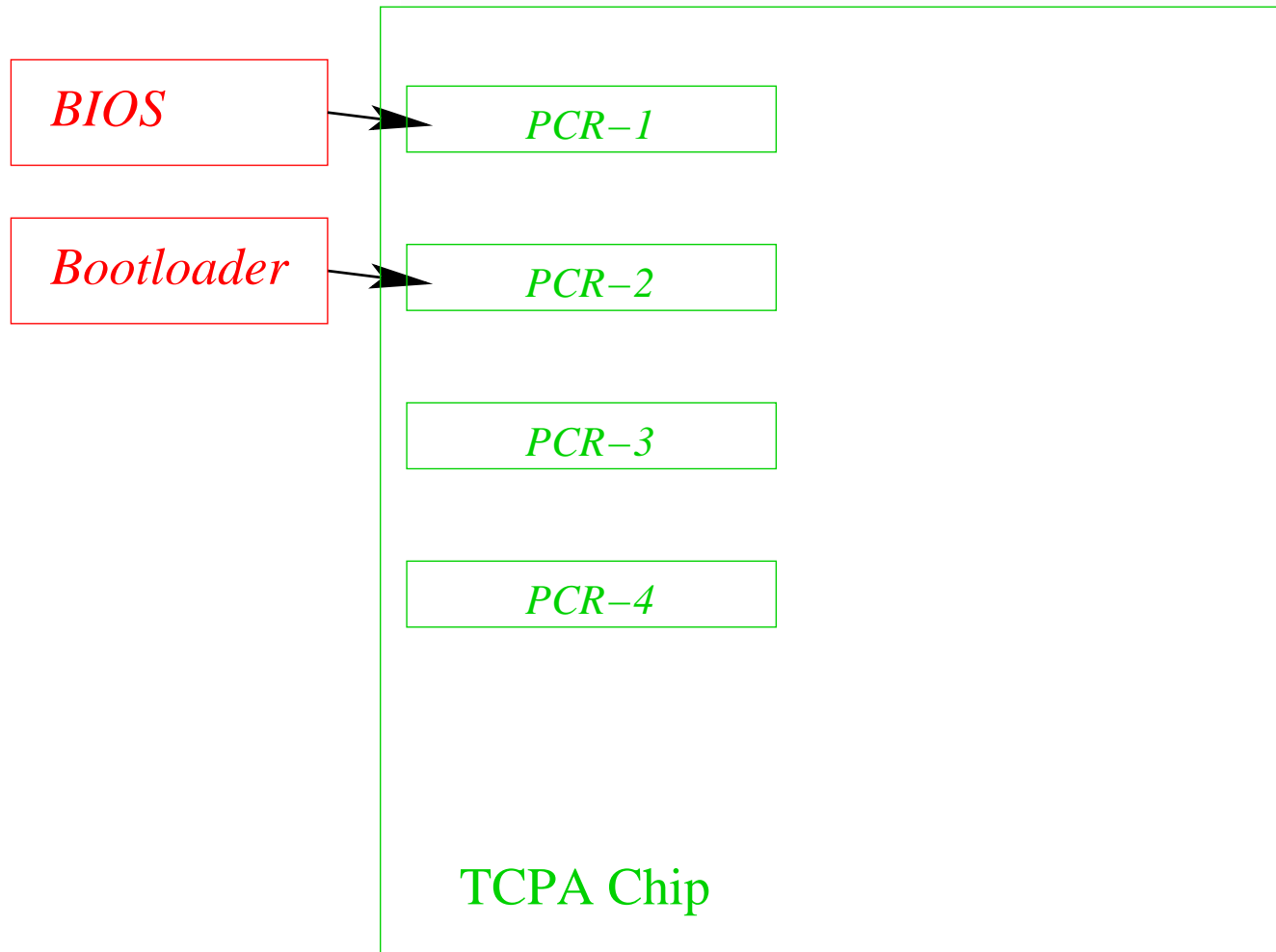
Secure Boot / Signatures



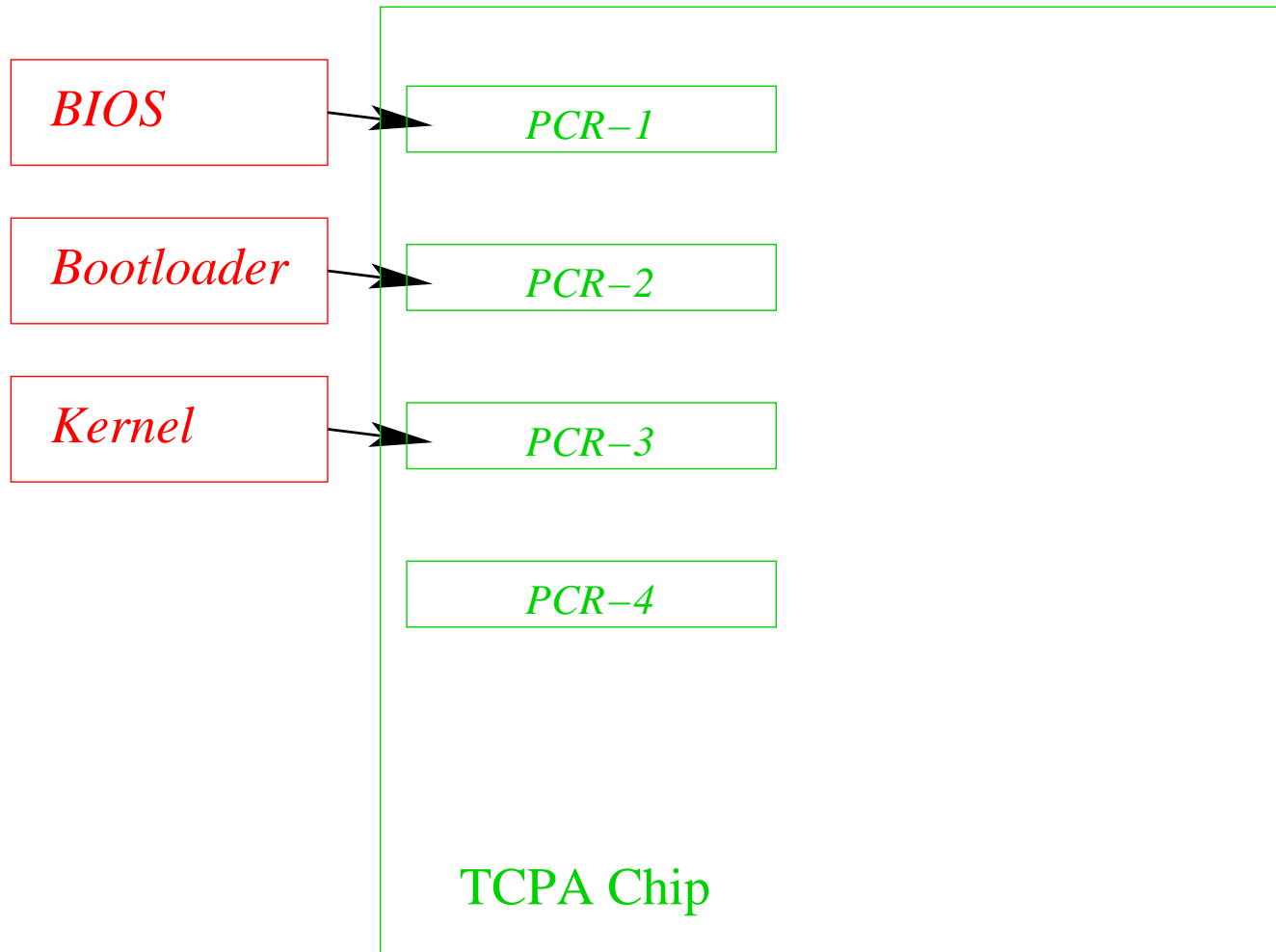
Secure Boot / Signatures



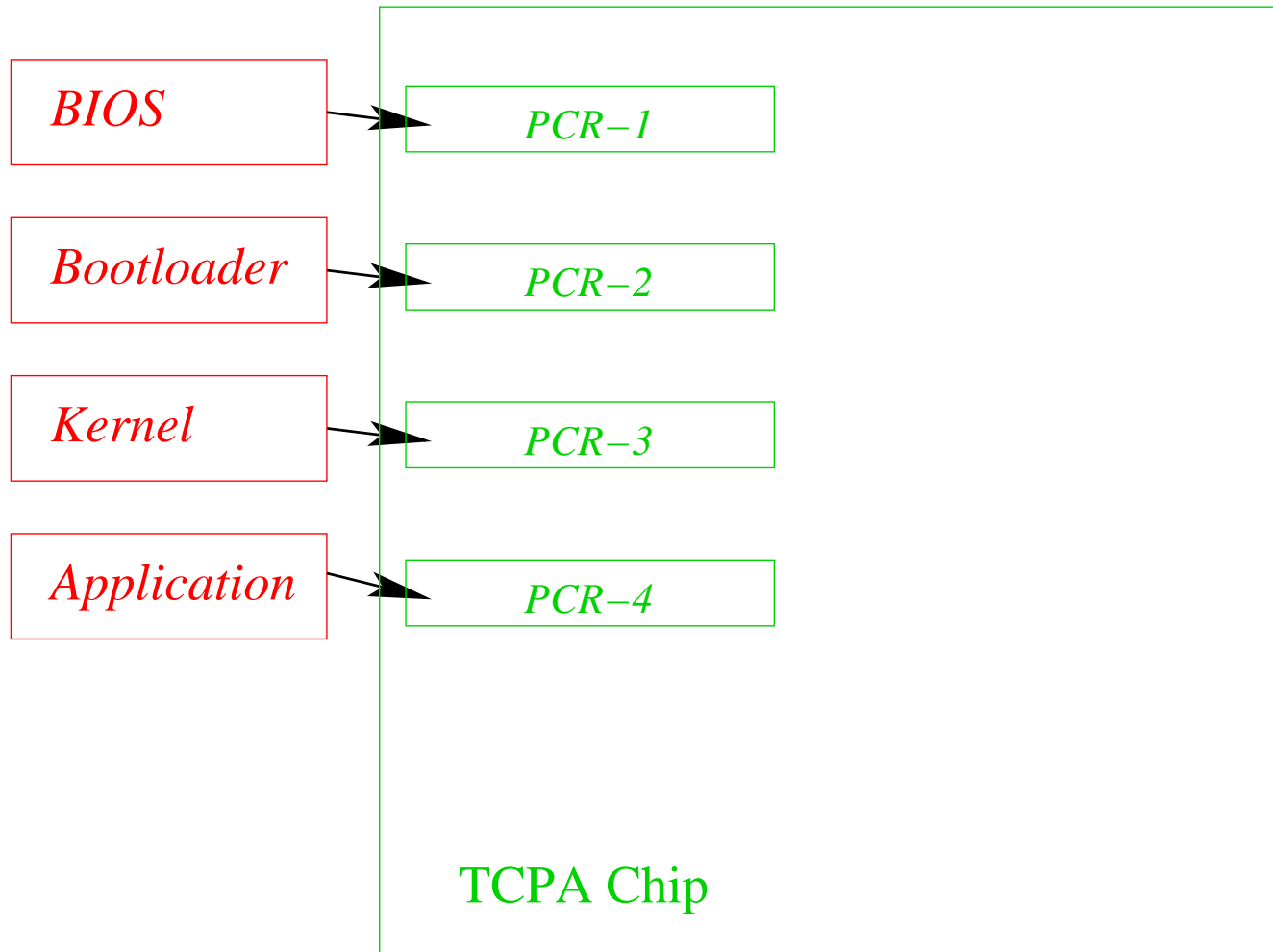
Secure Boot / Signatures



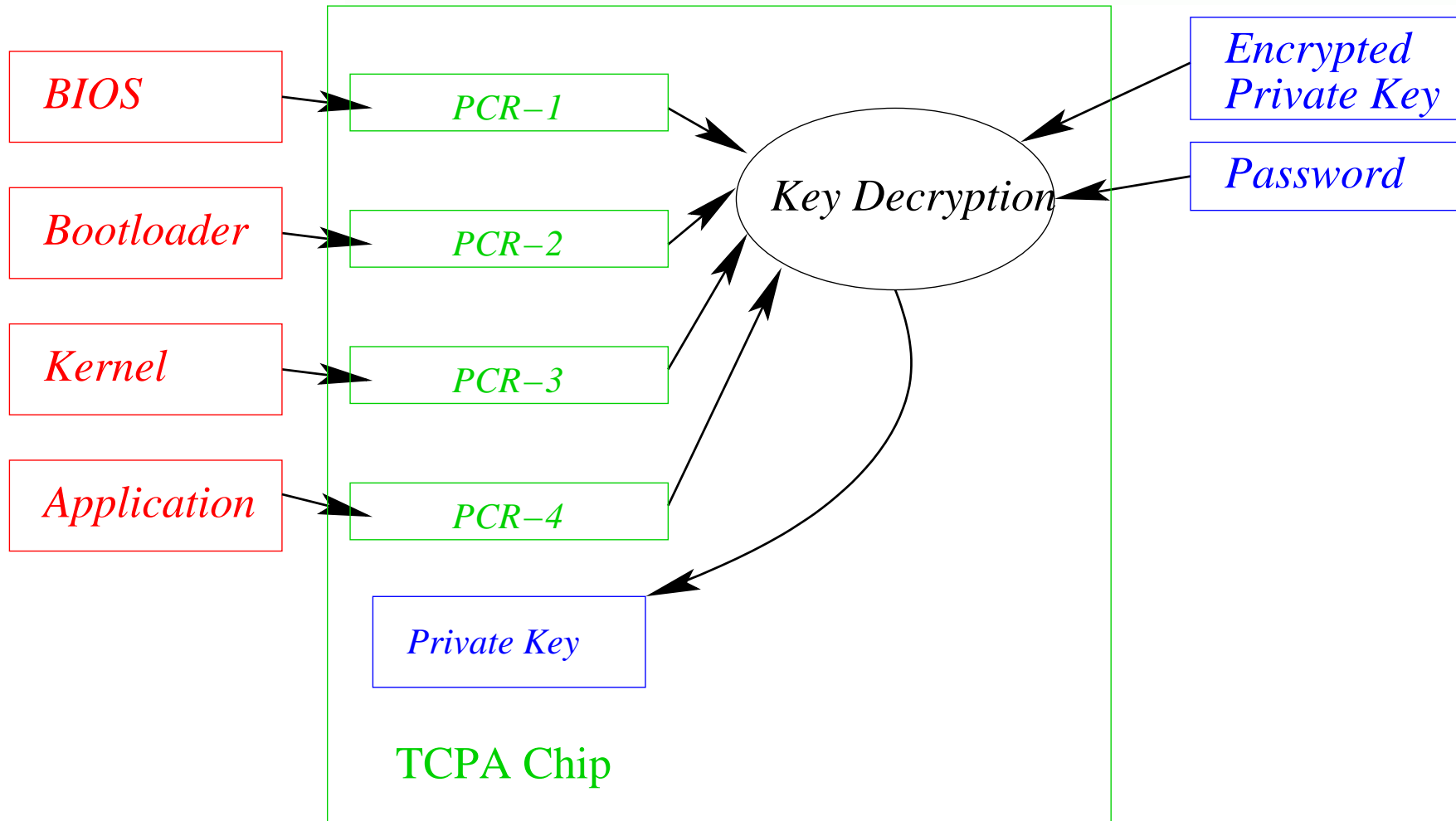
Secure Boot / Signatures



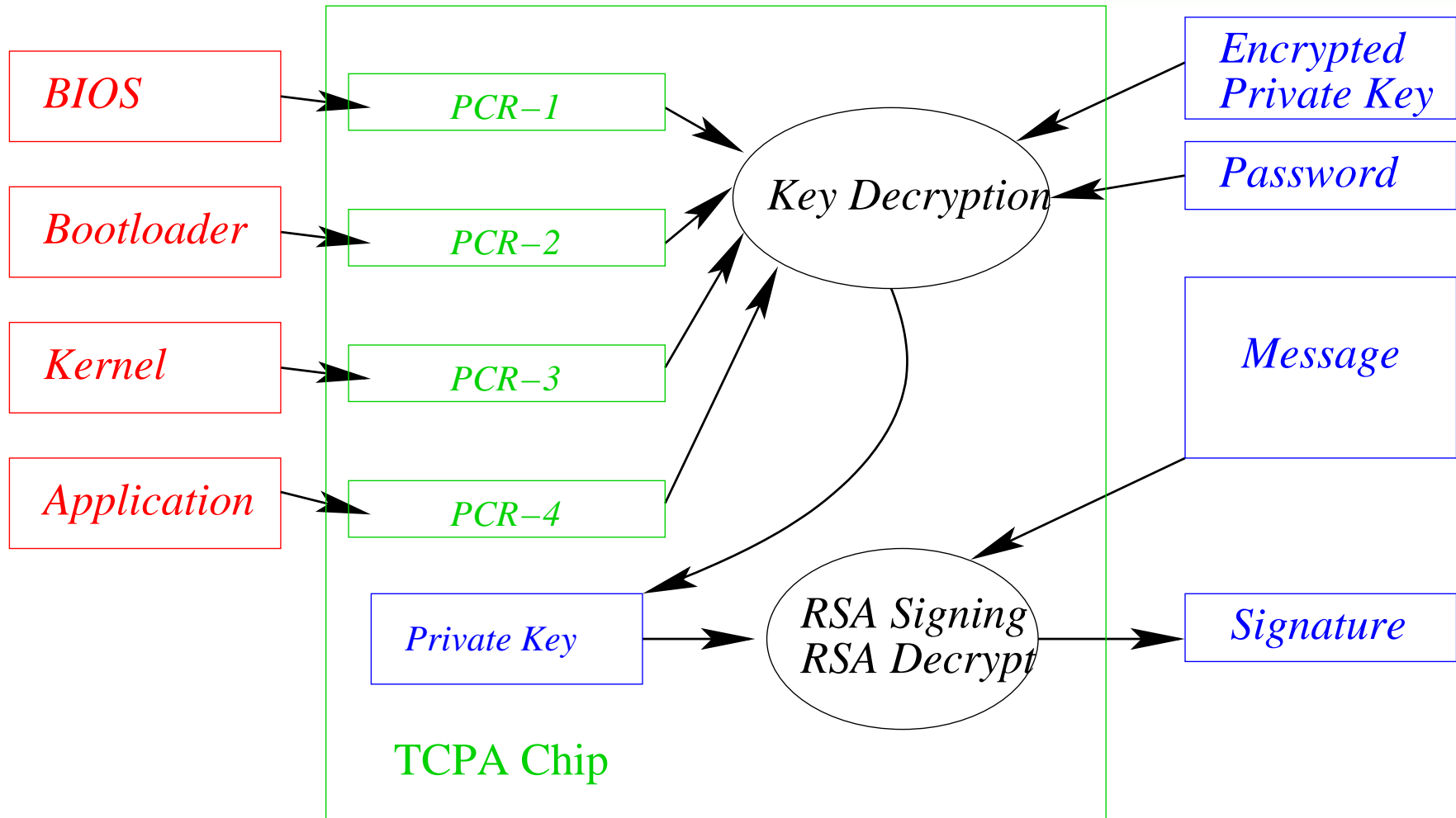
Secure Boot / Signatures



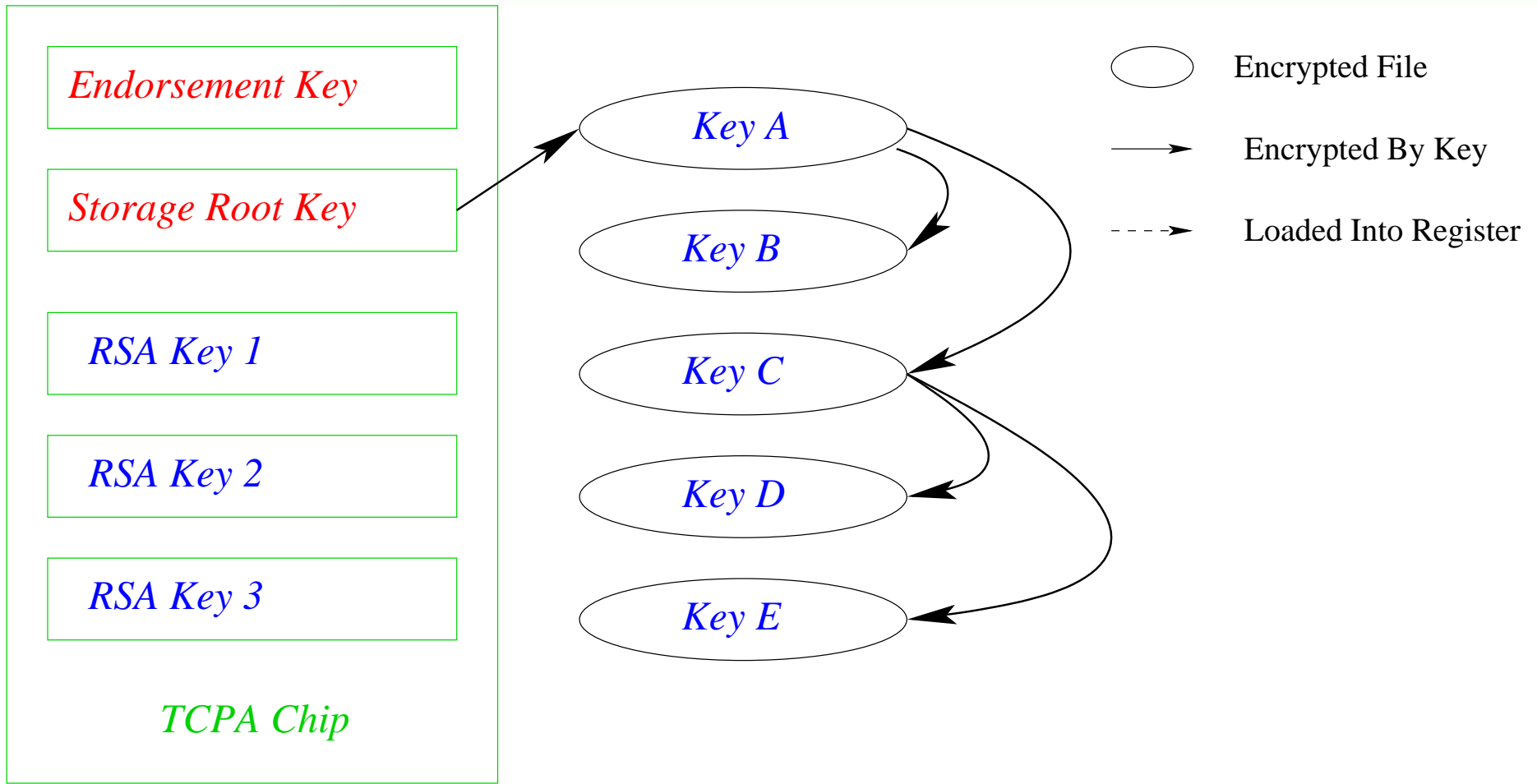
Secure Boot / Signatures



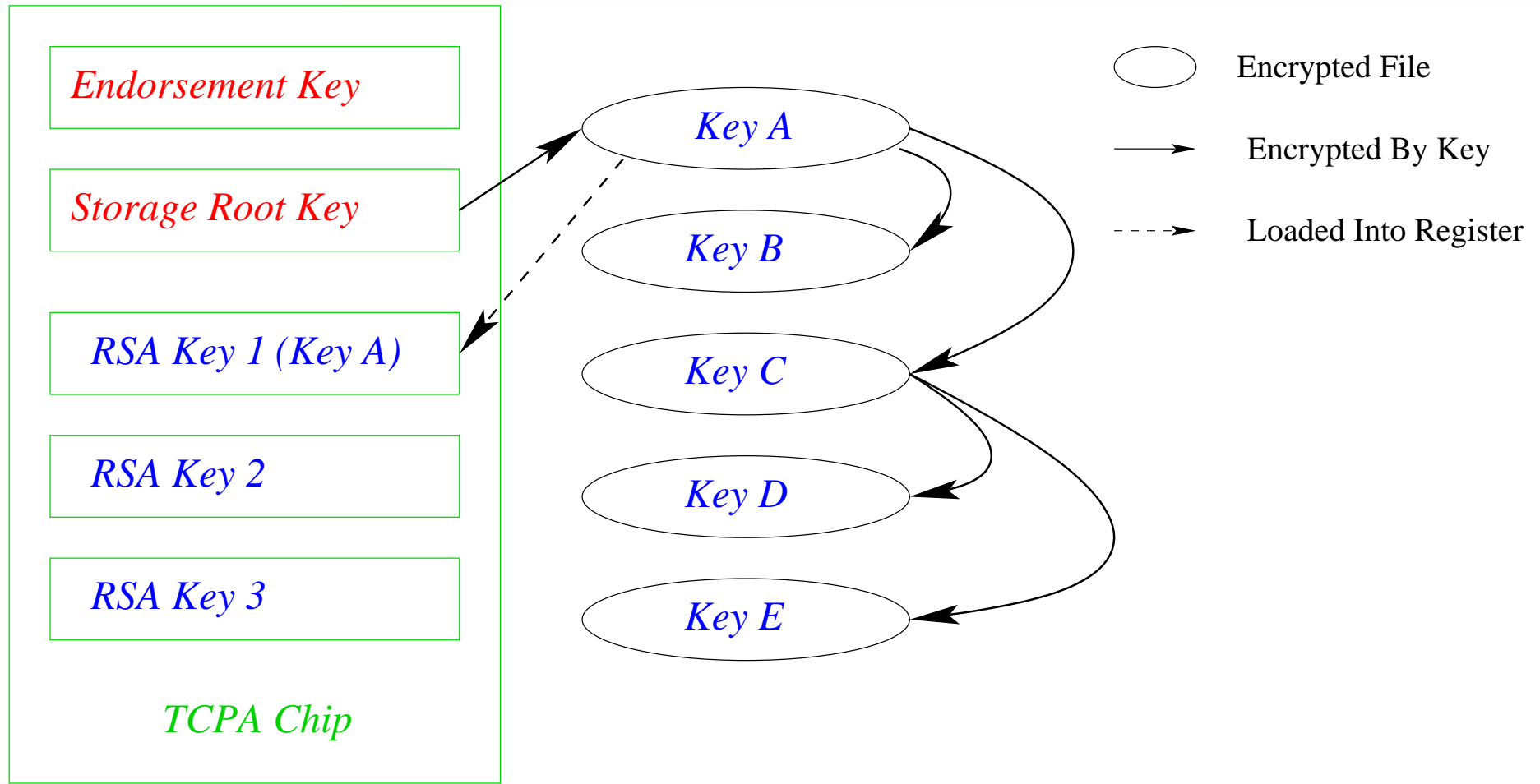
Secure Boot / Signatures



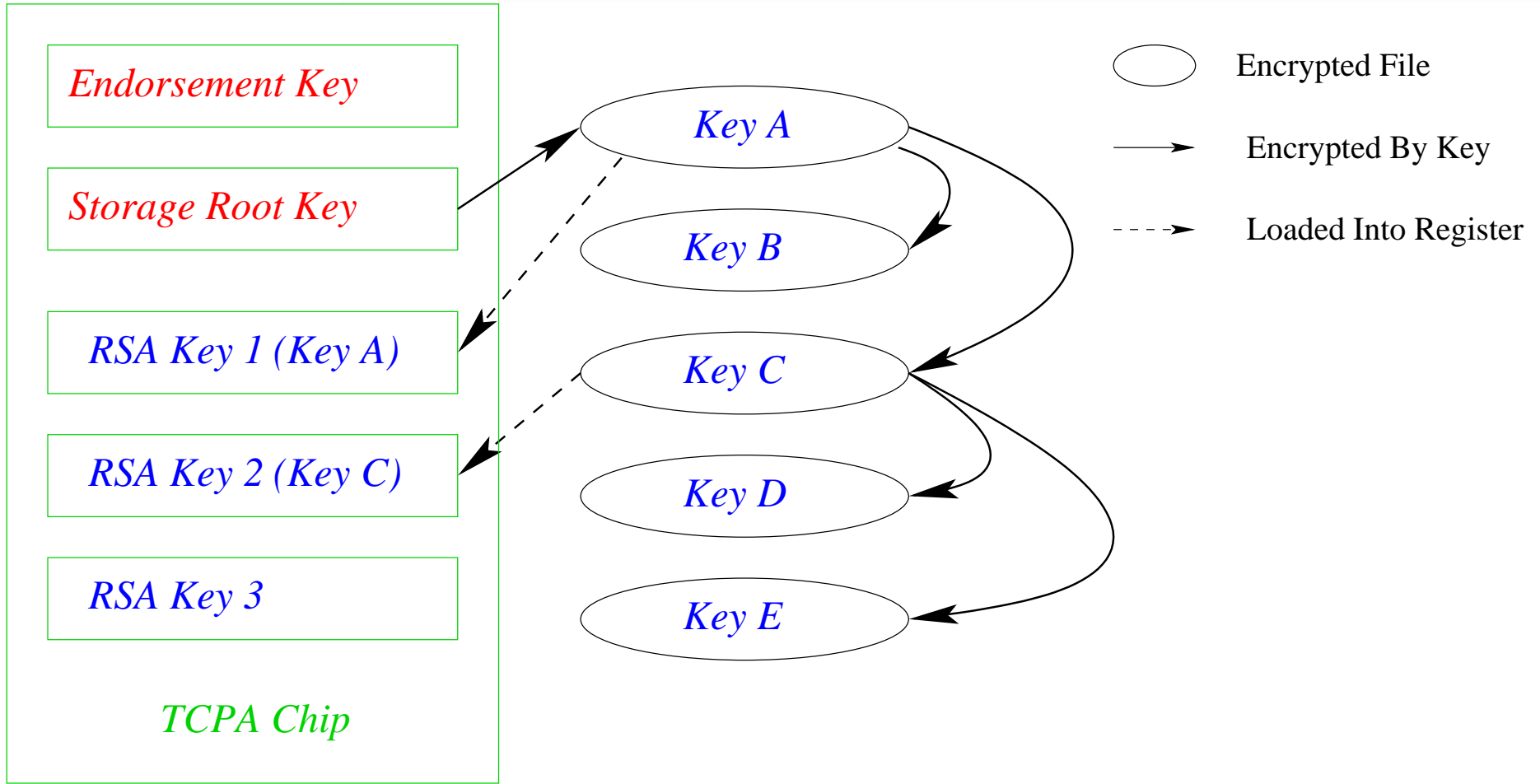
Tree of Keys



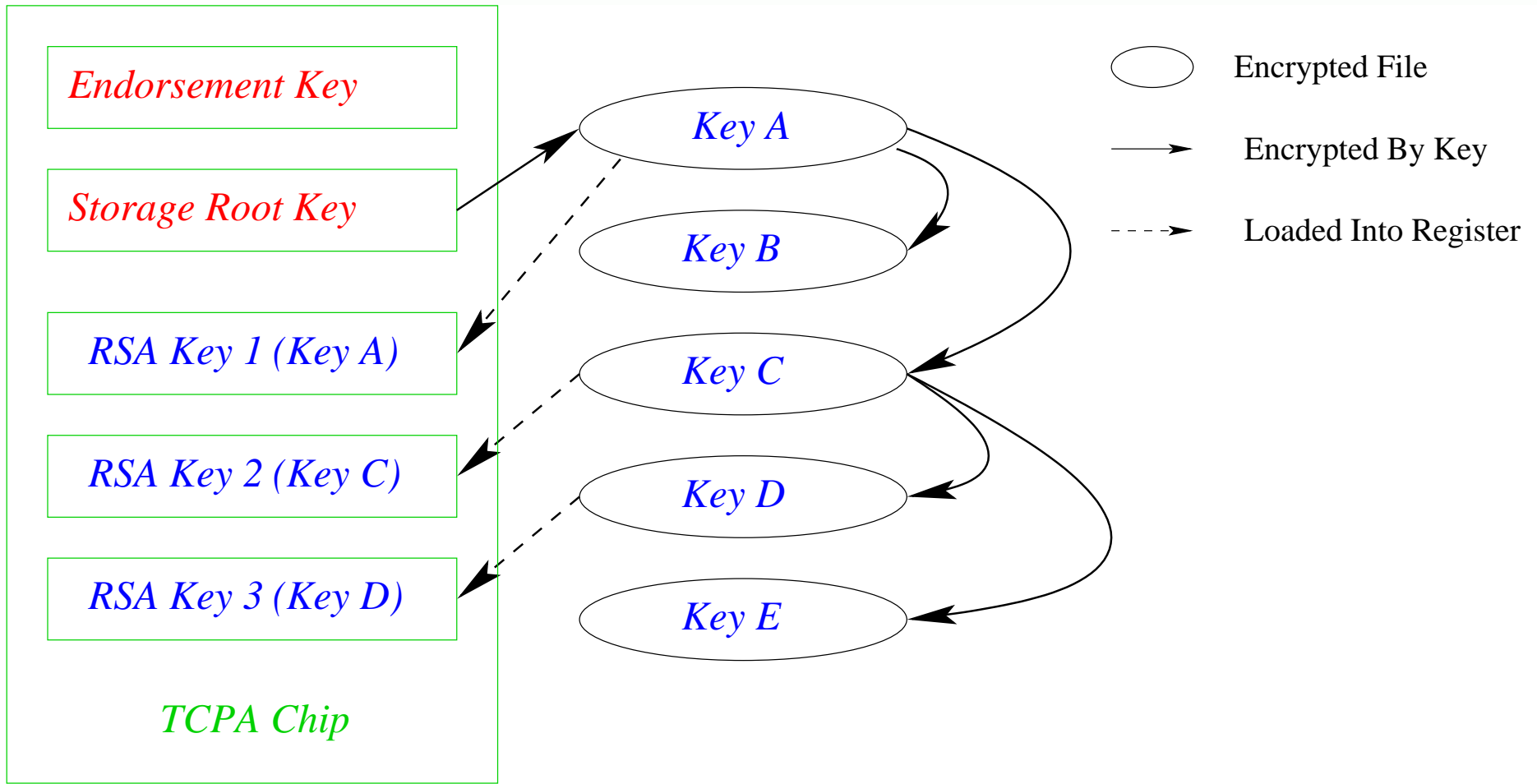
Tree of Keys



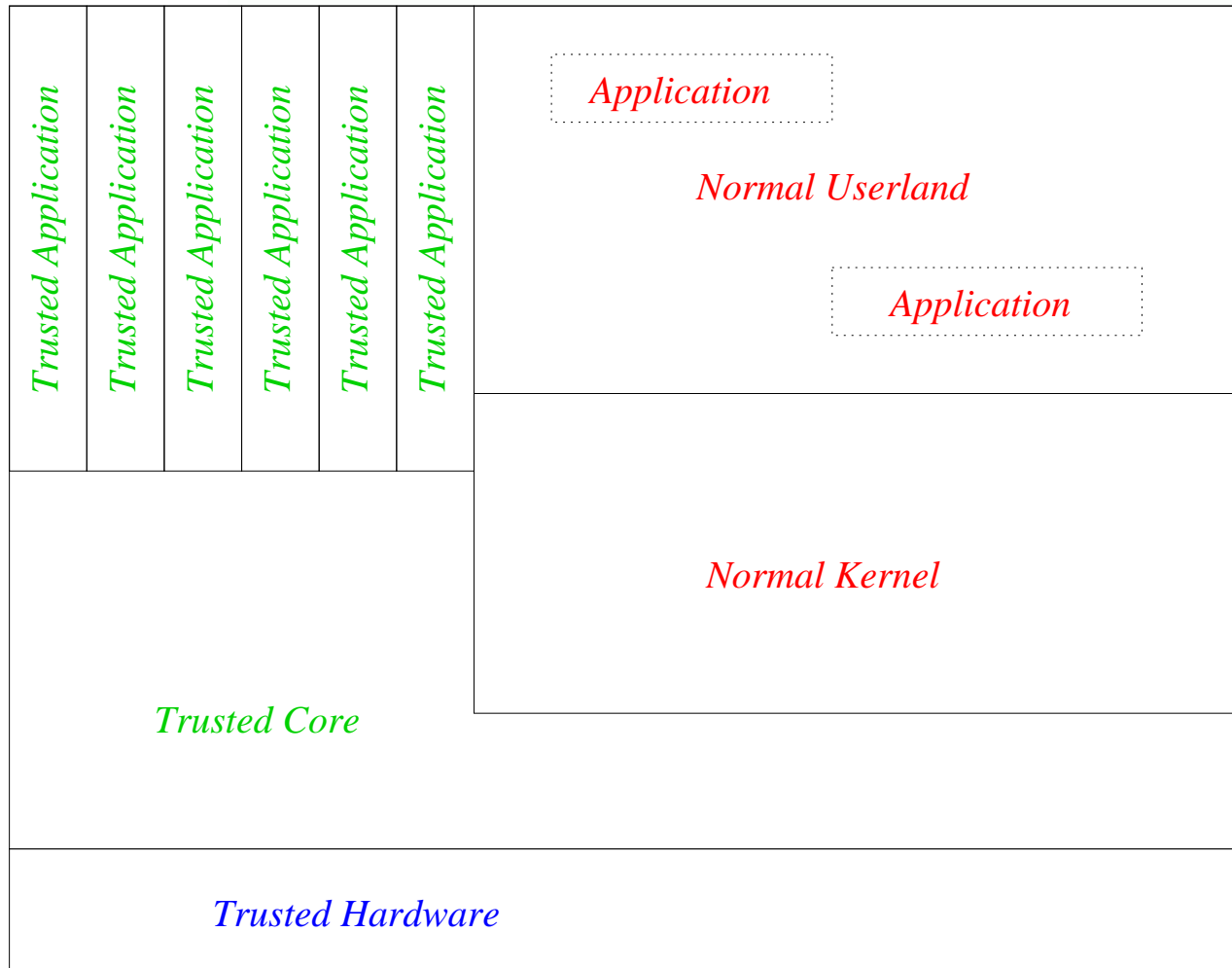
Tree of Keys



Tree of Keys



Trusted OS Architecture





What it Does NOT Do

- ⑥ Prevent Buffer Overflows, etc.
- ⑥ Make Software More Secure
- ⑥ Eliminate Open Source
- ⑥ Prevent Copying

The End



The Security of Trusted Computing

Rick Wash

`rwash@citi.umich.edu`