buypass
securing transactions

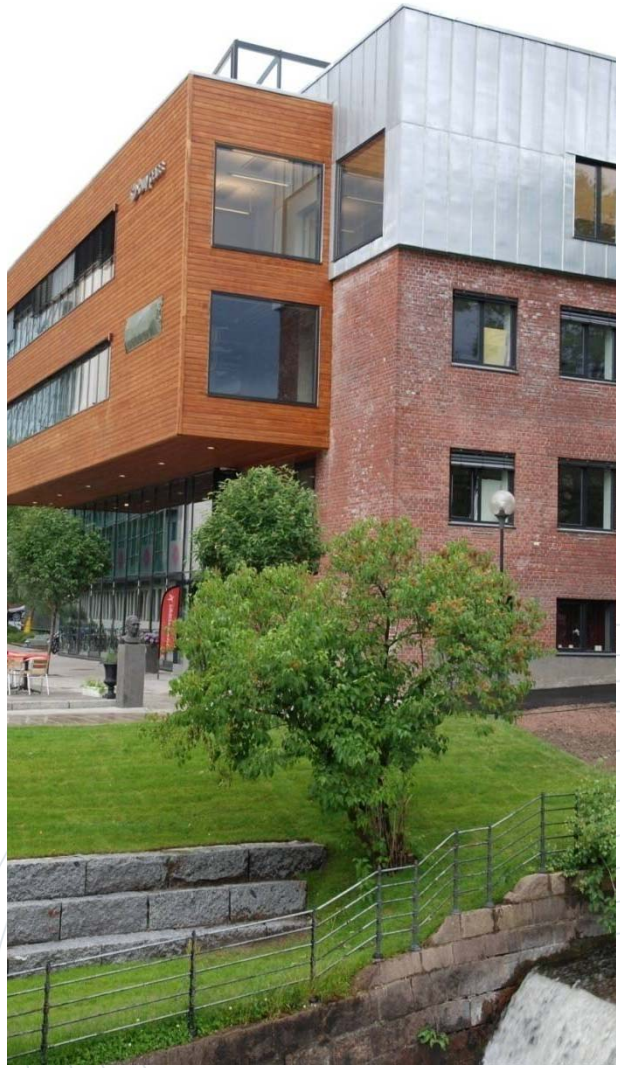
The Buypass smart card

A secure and flexible token supporting multiple electronic Ids

Mads Henriksveen

Buypass AS

- Leading national provider of solutions for the issuance, use and administration of electronic ids
  - electronic authentication
  - electronic signature
  - Buypass CA issuing Qualified Certificates
- Largest issuer of eID in Norway
  - more than 2 mill customers, generating
  - more than 13 mill transactions/month
  - supplier to all major Norwegian eGovernement projects
- Revenue 105 mill NOK (2007)
- 50 employees
- Jointly owned by Norway Post (ErgoGroup) and Norsk Tipping



The Buypass smart card - agenda

- Secure microcontroller
  - Infineon SLE66CX322P – RSA 2048
- MULTOS multiapplication OS
  - Application management
  - Isolated Execution Environment
  - Accredited to ITSEC E6 high
- Buypass MULTOS applications
  - Buypass ID (BID) : symmetric cryptography
  - Buypass PKI (BPKI): asymmetric cryptography
- Buypass products and services
  - Buypass BID only cards
  - Buypass PKI cards
  - Buypass Activate service – enabling PKI over internet

Infineon Secure microcontroller

RNG: Random Number Generator

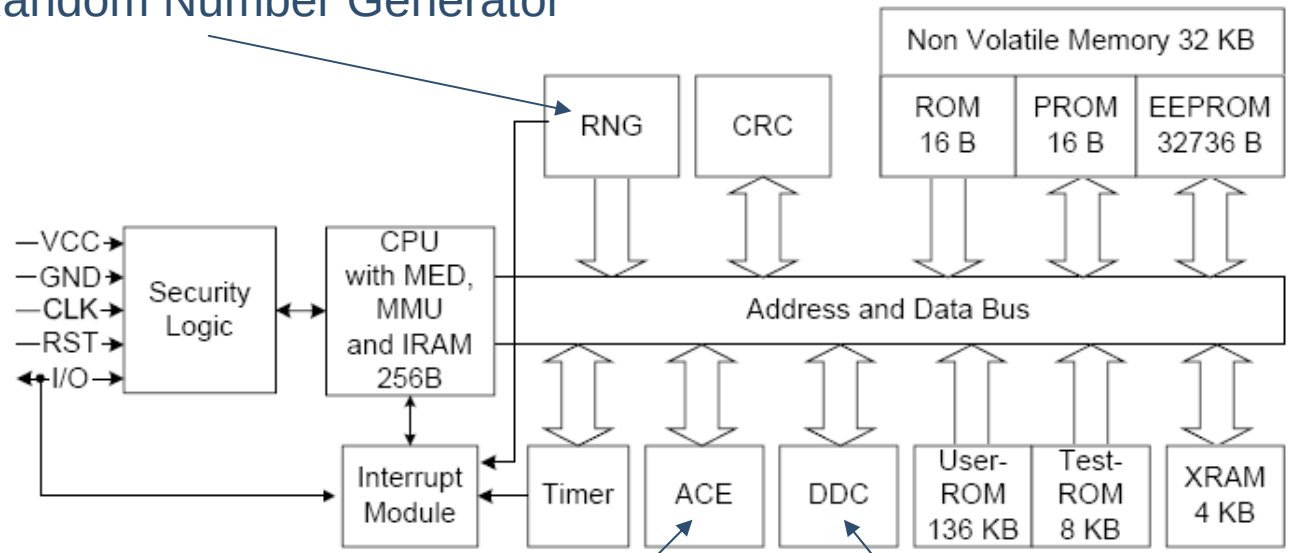


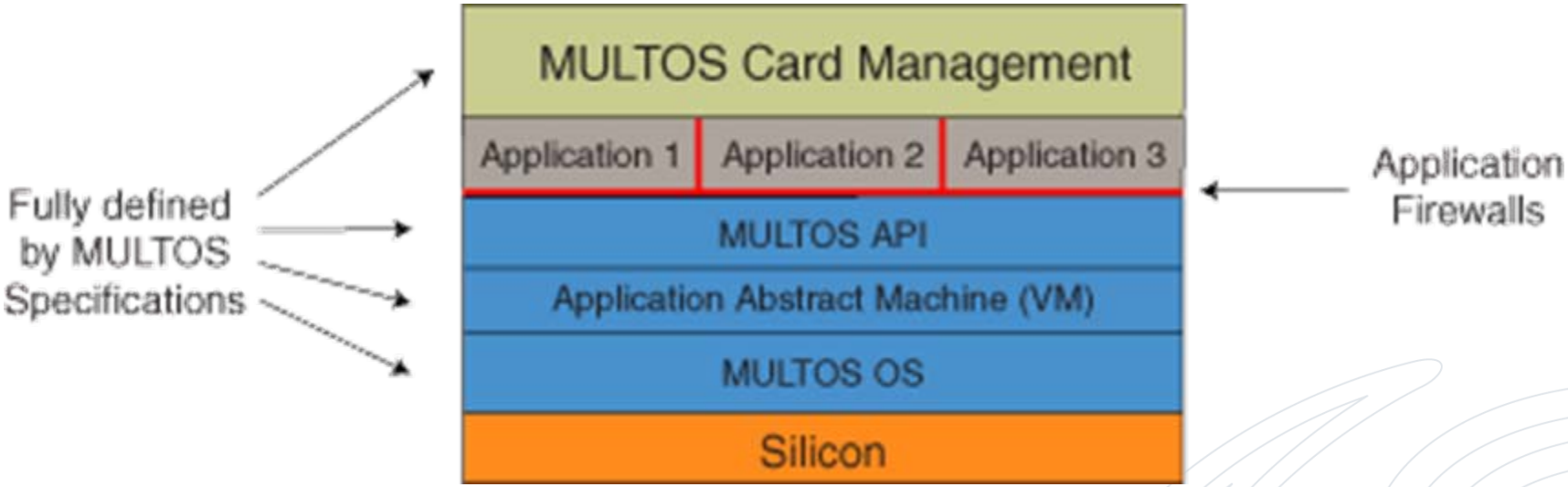
Figure 1: Block diagram of the SLE66CX322P with RSA2048

ACE: Advanced Crypto Engine (RSA)

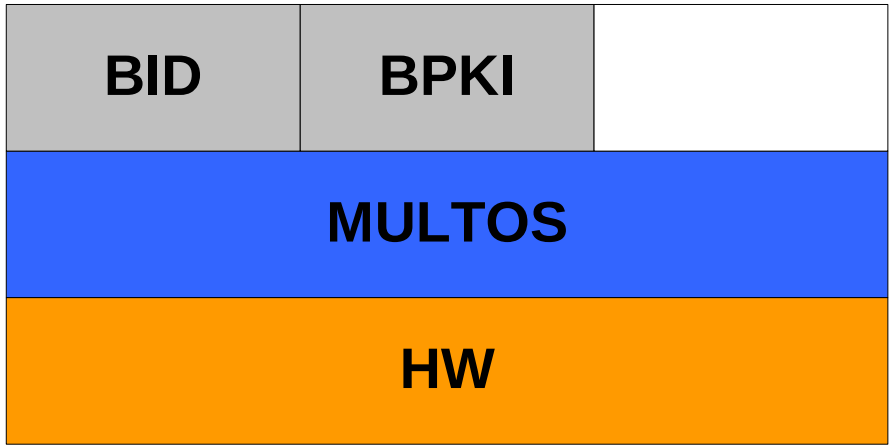
DDC: DES Accelerator (DES, EC)

Certified according to CC to EAL5+, includes RSA 2048.

The MULTOS platform



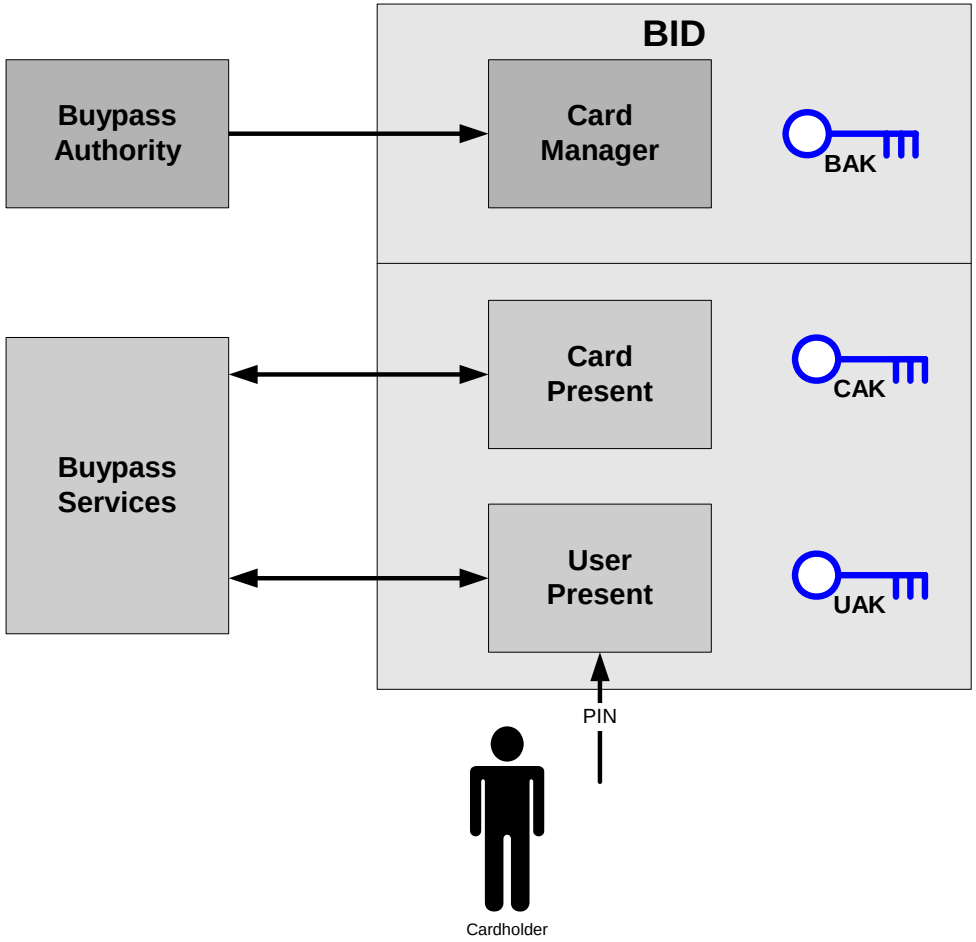
Buypass MULTOS applications



BID – Buypass ID (symmetric)
3TDES – 168 bits

BPKI – Buypass PKI (asymmetric)
RSA 1024/1536/2032 bits

Buypass ID (BID) – symmetric cryptography



BAK – Buypass Authority Key

CAK – Card Authentication Key

UAK – User Authentication Key

Buypass PKI – pocket concept

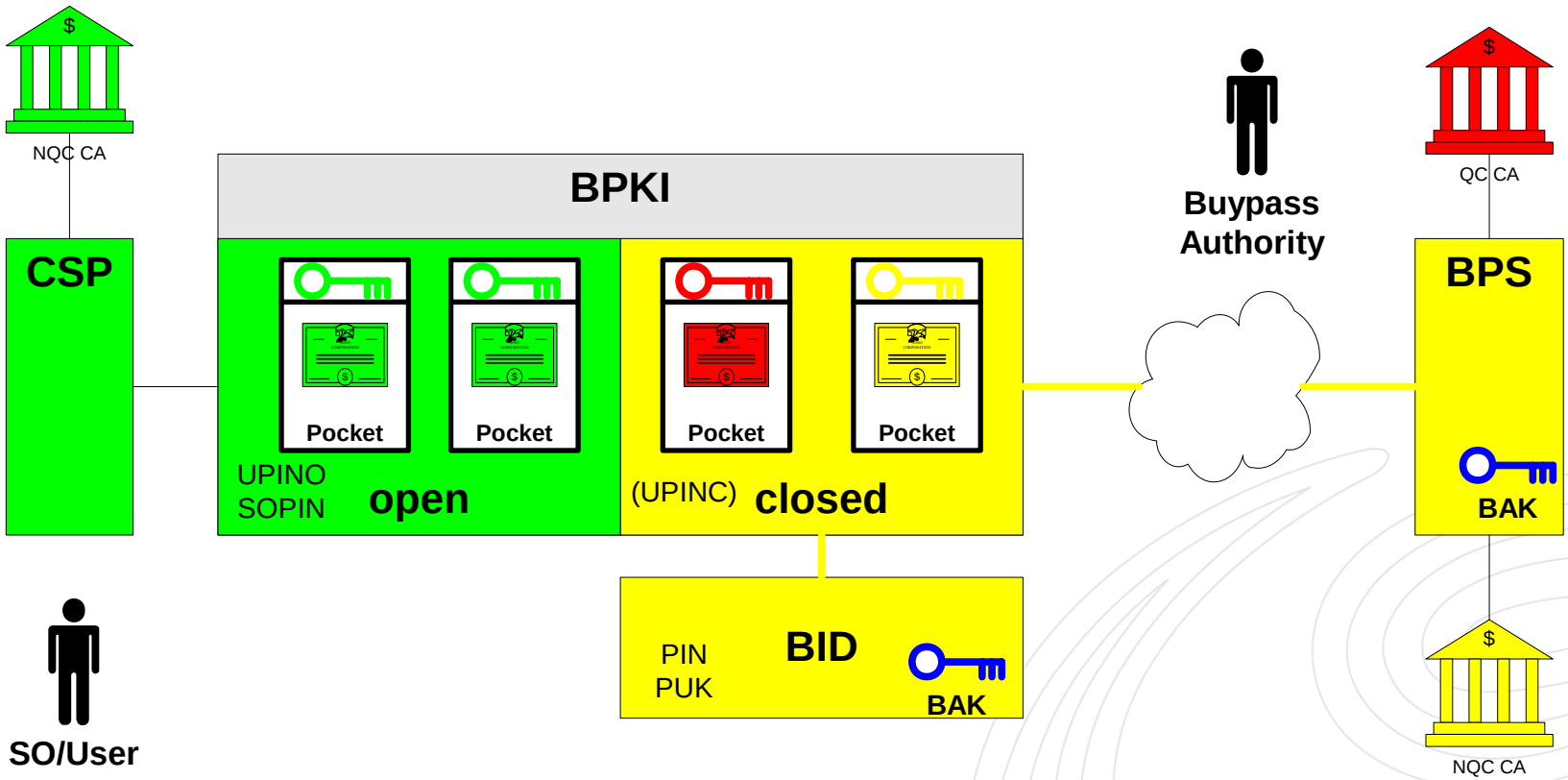
POCKET properties:
- PIN: reference to PIN file
- Open/Closed
- Locked/Unlocked

Administrative Key operations:
- Import Key Pair
- Generate Key Pair
- Export Public Key
- Delete Key
- Sign (CertReq)

Administrative Certificate operations
- Import Certificate
- Delete Certificate

User operations:
- Sign (PIN required)
- Decrypt (PIN required)

Buypass PKI – multi pocket application



Buypass Activate – enabling PKI over internet

- Pre condition
  - Card with BID preloaded
- Secure Messaging – SM
  - Secure Channel between Buypass Central Systems and chip
- Post issuance application loading
  - MULTOS confidential ALU - BPKI
- Buypass Activate
  - On-card key generation (SM)
  - Export of public key (SM)
  - Certificate generation – Buypass CA
  - Certificate import and installation (SM)
- Post condition
  - Card with PKI, qualified certificates

A flexible and secure token

- Multiple electronic IDs in one single card
  - Symmetric eID - BID
  - Qualified certificates - BPKI
  - Local certificates – BPKI
- Different issuance models supported
  - Local certificates only (for internal organisation only)
  - Qualified certificates for advanced users
  - BID only when PKI is not required
- Additional Ids may be added post issuance
  - E.g. Buypass Activate
- Users choice

buypass™

securing transactions