MasterCard International

CACR Information Security Workshop

Security issues, implementation challenges - cardholder verification methods in Electronic Commerce

November 24, 1998

John Wankmueller
Vice President, Electronic Commerce Technology

Agenda

PIN based debit transactions

- Description of current environment (ATM, POS)
- Description of electronic commerce environment
- Proposed approach - SET OAEP-2 for PIN
- Outstanding Issues/Questions

Description of current environment (POS)

Attributes

Cardholder present

- Rigid security (ISO 9564) required - banks and merchants operating ATMs and POS terminals determine the security - but cardholders and issuers hold the risks
- ISO 9564 requires tamper-resistant PIN-entry devices
- PIN pads contain CPU and memory to locally perform the PIN-encryption function

Attributes (continued)

Cardholder present

- PIN entry device are at a fixed trusted location
- All devices are “type approved” by the card scheme
- Standards exist for entry, formatting, symmetric encryption technology to deploy at public, shared, PIN entry devices (ISO 9564)
- PIN entry is hardware protected

Attributes (continued)

Cardholder present

- Basic principles of PIN Management (ISO 9564-1):

  1) Encipherment of the same PIN value using the same encipherment key for different accounts shall not predictably produce the same cipher text

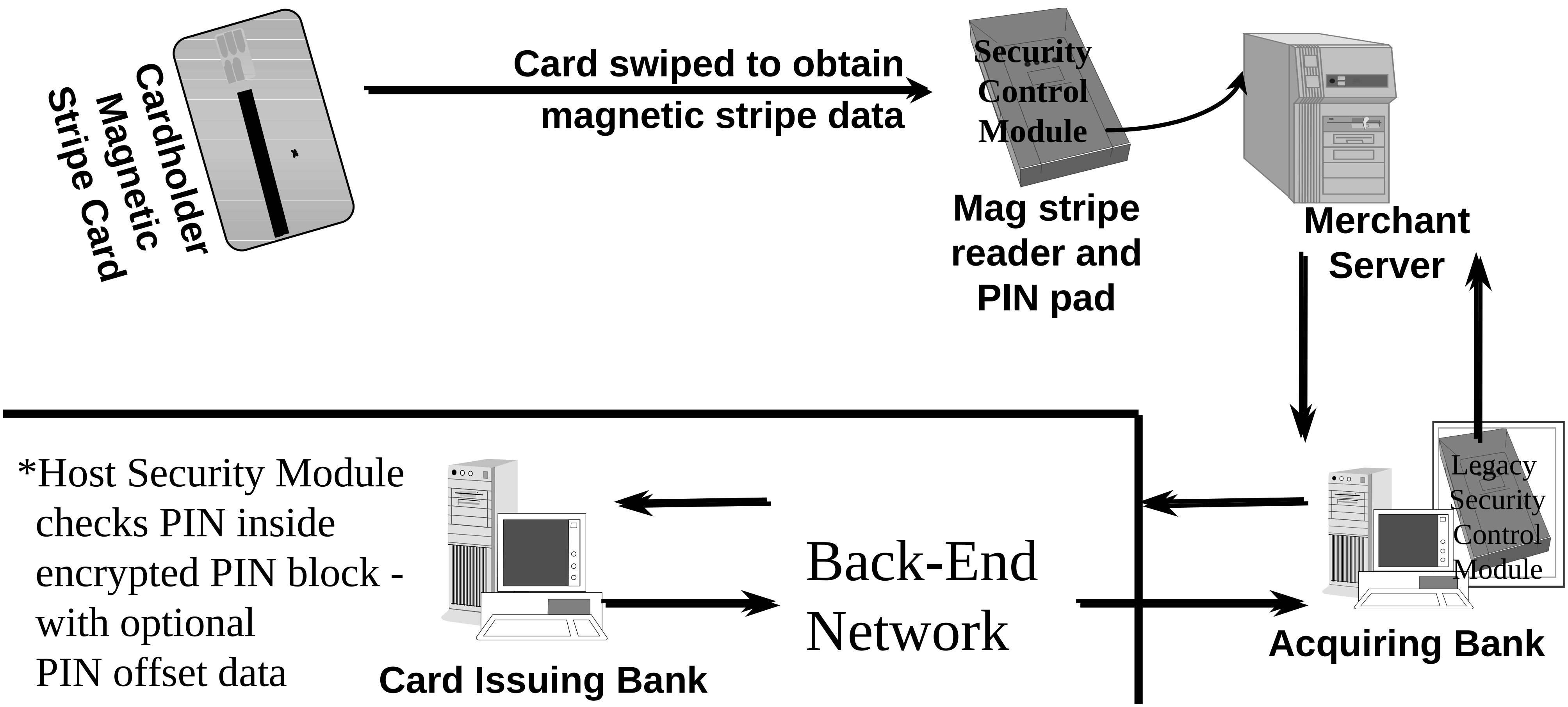
  2) Security of an enciphered PIN shall not rely on the secrecy of the encipherment design or algorithm but on a secret key

Attributes (continued)

Cardholder present

- Back end ATM networks use tamper-resistant, cryptographic hardware security modules for receiving and forwarding PINs
- Incoming PINs - encrypted under one DES key, are re-encrypted under a second DES key inside this secure device
- All DES keys are held in tamper-resistant, hardware security modules which can convert the PIN to different “PIN block formats” (ISO 9564-1 defines two)

Face-To-Face PIN On-Line Transaction Environment



Description:

Electronic commerce environment

PIN in electronic commerce

Cardholder not present

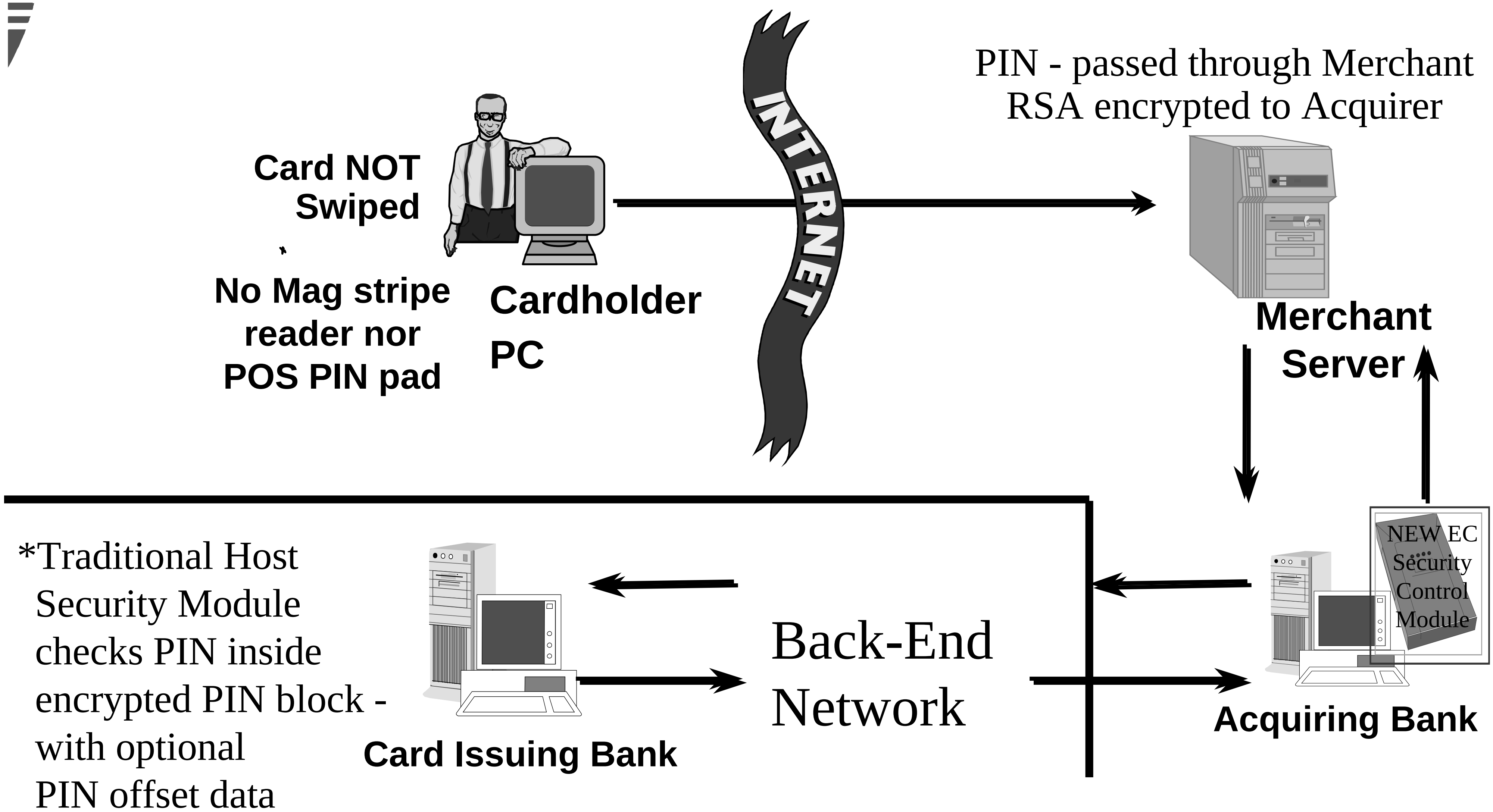
- Very different risk model - cardholders and issuers are responsible for both the risks and the PIN entry security
- Can use an established asymmetric encryption structure (SET proposed), instead of using long-lived symmetric DES keys
- Should enable acquirers and issuers to manage PIN security via their existing legacy infrastructure.

Description of electronic commerce environment (continued)

Cardholder not present

- PINs are entered at private PC's (not shared public devices)
- Systemic risk at cardholder PC is smaller than at ATM or POS terminals

Electronic Commerce PIN On-Line Transaction Environment



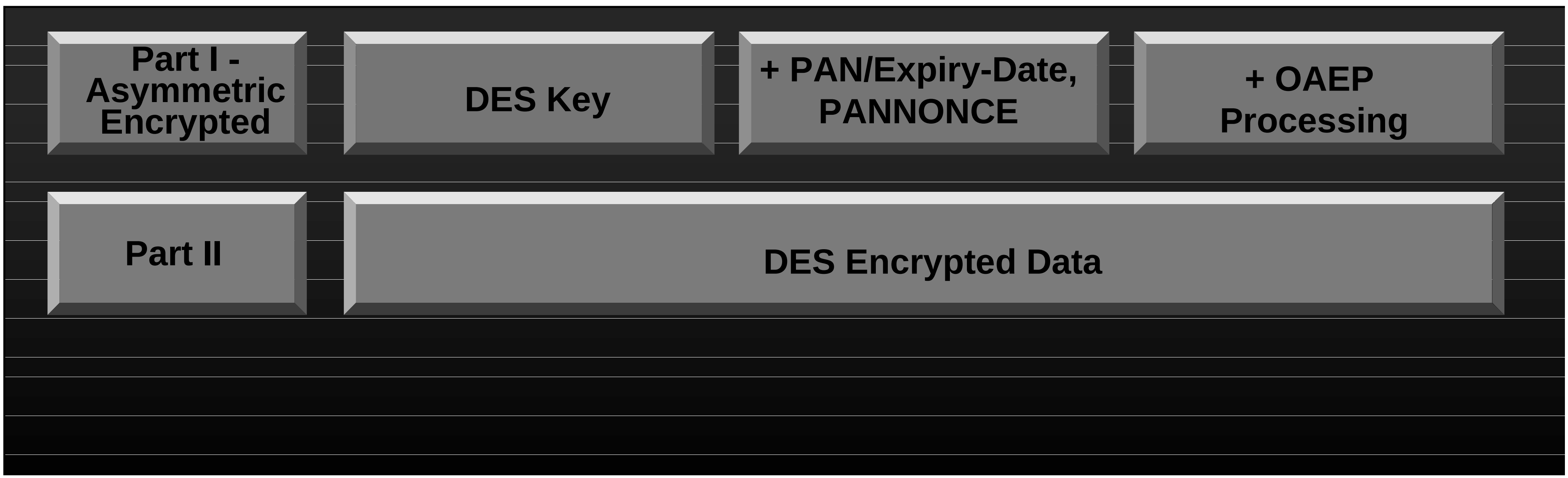
Proposed approach -

SET OAEP-2 for PIN

Current SET V1.0 OAEP Block

(Protects PAN, no PIN)

1024 Bits
or higher



PIN - Electronic Commerce Using a Second OAEP Block

Attributes

– PINs entered at cardholder PCs via

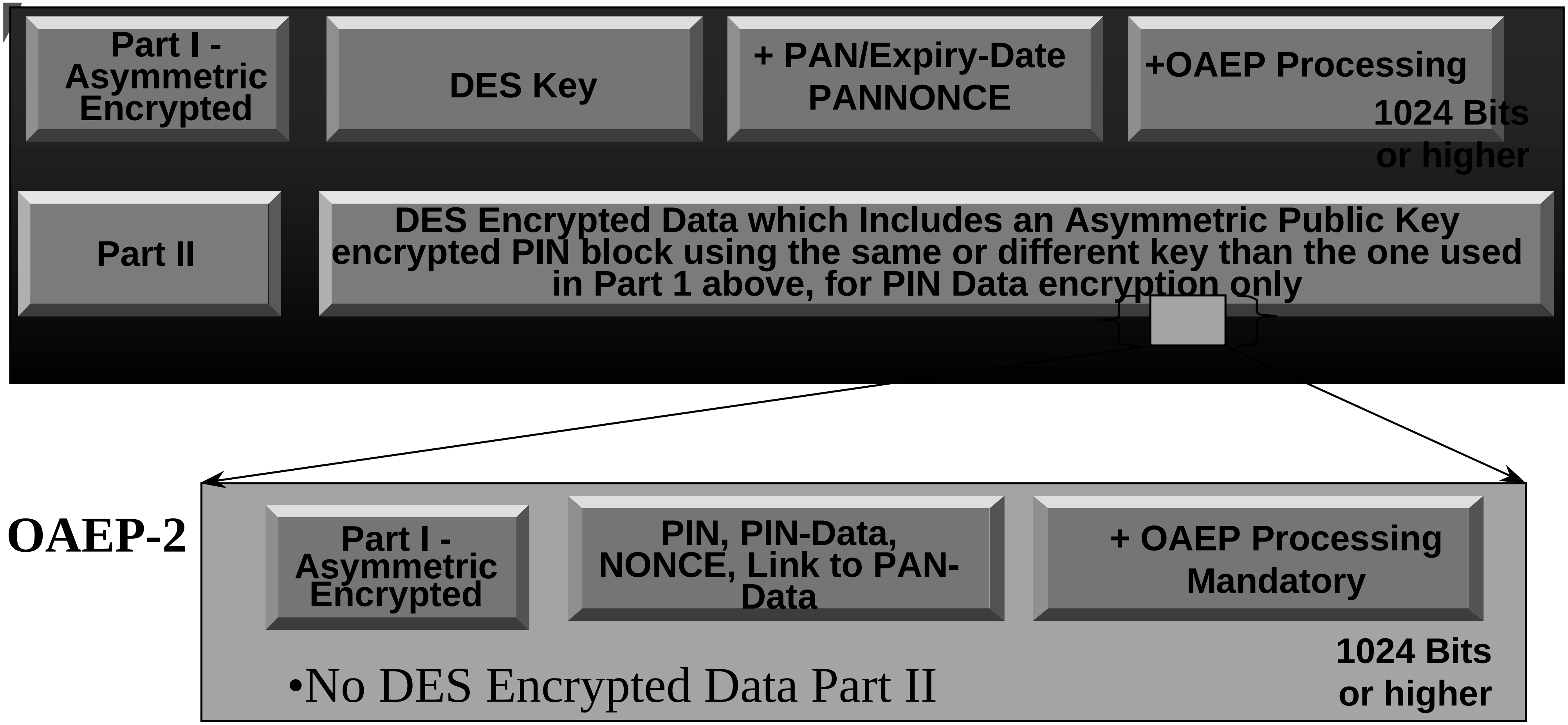
1) functionally-secure encrypting PIN pads, or

2) via PC keyboard entry with software encryption

– PINs placed into a second OAEP block, specially for a PIN, protected via asymmetric encryption under the public key of payment gateways which bypasses the merchant

– The payment gateway decrypts PIN data, converts the PIN to a standard PIN block format, re-encrypts it using its outbound symmetric key to legacy debit networks

Proposed OAEP-2 PIN Block



Outstanding Issues/Questions

PIN in Electronic Commerce

Issues

– PINs at “public” PCs (e.g. in libraries, kiosks, cyber cafes) are not allowed since a “private” PC might masquerade as a public one

– PCs are not bank “type approved” - how to control and protect PIN, in current PCs and deployed operating systems

– Use of PINs in payment transactions for cardholders who do not have a digital certificate related to an account

– Attaching magnetic stripe readers to private PCs to simplify the entry of PANs, card expiration, and other track 2 data

PIN in Electronic Commerce

Issues (continued)

Security risks of PIN in a PC:

- entered through an unmodified PC keyboard
- entered into an in-line keyboard-connecting device
- entered through a numeric key pad device attached to a serial port
- entered into a device using the PC's own electrical power
- while the PIN travels the internal PC data bus
- H/W, S/W, OS security profile differences

Security risks for other devices: (WEB TV, Direct TV, cable set-top boxes, mobile phones, PDA's)

PIN in Electronic Commerce

Issues (continued)

- Providing a low cost, tamper-resistant PC PIN entry device
- No established/approved asymmetric PIN encryption standard
- Solution must link into established legacy systems to minimize changes to back end systems
- Security profile of alternative entry methods (GUI entered PIN, voice recognition entered PIN, …)
- Methods to validate that the cardholder is employing correct PKI root public key
- Possible poor response times due to additional asymmetric encryption steps

PIN in Electronic Commerce

Issues (continued)

- Biometric CVM’s as alternative to PIN- any more secure
  - Fingerprint on the PC keyboard
  - In a smart card
  - In a serially attached device
  - Off line PIN checked locally by a smart card
- Export issues with OAEP-2 approach
  - Double encryption restriction?
- Any conflicts with emerging international asymmetric PIN encryption standards

PIN in Electronic Commerce

Issues (continued)

– Is the use of OAEP blocks and 1024 bit asymmetric encryption to transport PINs over the Internet secure enough?

– Use of asymmetric encryption - what are the practical business risks with lower exponents, 512 bits

– H/W Requirements and security procedures at Internet acquiring banks