PIN Security Management and Concerns

Susan Langford
Sr. Cryptographer

CACR Information Security Workshop

Why We Shouldn’t Study PINs

- Technology is decades olds
  - Long time for computers
  - Network is already built and tested
- Everyone knows what a PIN is
  - Personal Identification Number
  - Password made up of only numbers
  - Frequently written down
- There are a lot of new protocols to study - so why bother?

Why We Should Study PINs

- One of the few large scale implementations of cryptography in the commercial world.
  – Learn from mistakes and successes
  – New and the old systems use different mathematics, there will be new attacks, but the old attacks won’t go away.
- New Internet protocols need to inter-operate with the existing networks.
- People are trying to upgrade the existing network from single-DES to something stronger.

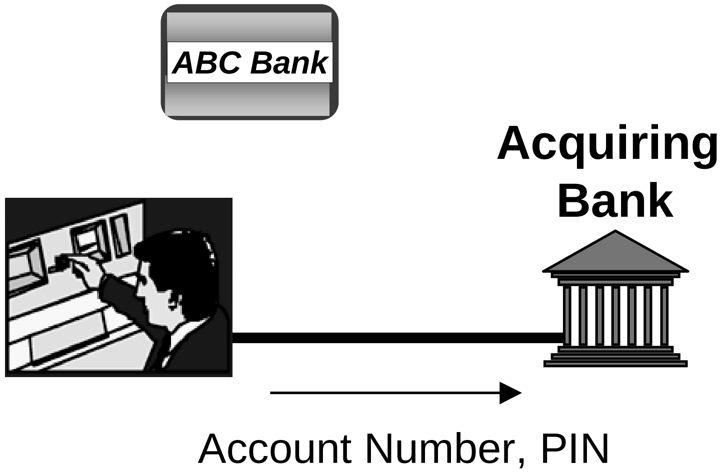
Talk Outline

- The existing network
  - Description
  - Defenses
  - Vulnerabilities
- Combining public key based networks with the existing infrastructure
  - Possible approaches
  - Vulnerabilities

The Existing Network

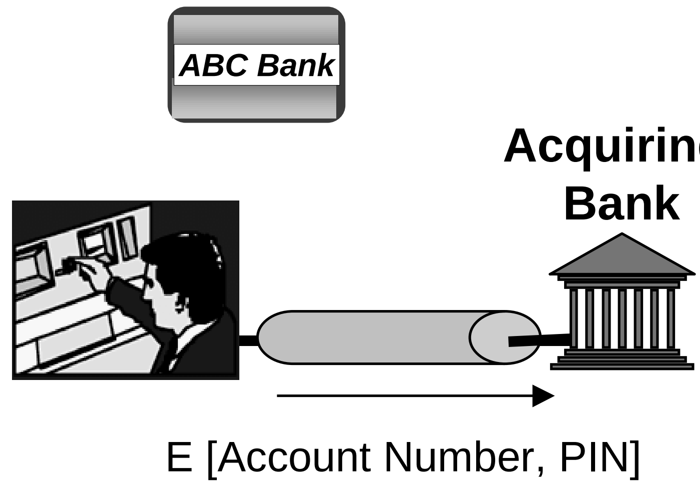
Early systems - No cryptography

- **First systems didn't even require a PIN**
- **Account number and PIN sent to bank in the clear**
- **Very little fraud protection.**
  - **Anyone that taps the line can steal from the account.**
  - **If no PIN, anyone that can write a magnetic stripe card can steal from the account.**

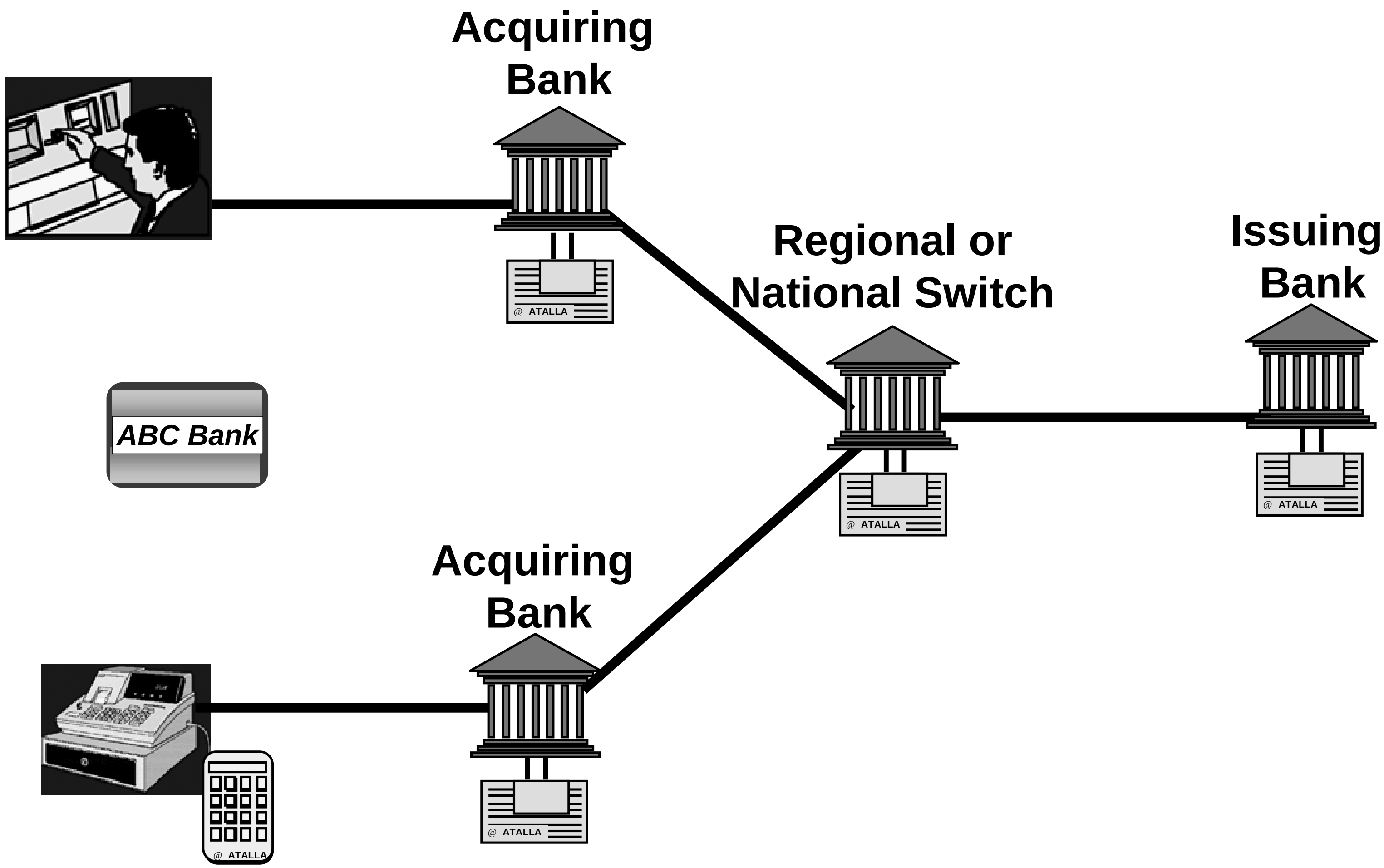


Link Encryption

- Encrypt the traffic from the device to the bank.
- Bank verifies PIN in software.
- Better fraud protection.
  - Tapping the line does not provide useful information.
  - Vulnerable within the bank. Employees can see PIN.
  - Networks require banks to trust other's employees.



The Existing Network



The Existing Network

ABM (ATM) or POS device sends data to its bank

- **PIN block always DES encrypted, under PIN key**
- **Track 2 may be DES encrypted under a general traffic key.**
  - **Track 2 contains 40 digits (0-9), 37 usable**
  - **Primary Account Number (PAN), 16 - 19 digits**
  - **Exp. Date (4 digits)**
  - **Varying fields - service code, language indicator, member number**
  - **Data to verify PIN (ex. IBM 3624 offset) Usually only 4-5 digits.**

The Existing Network - transport

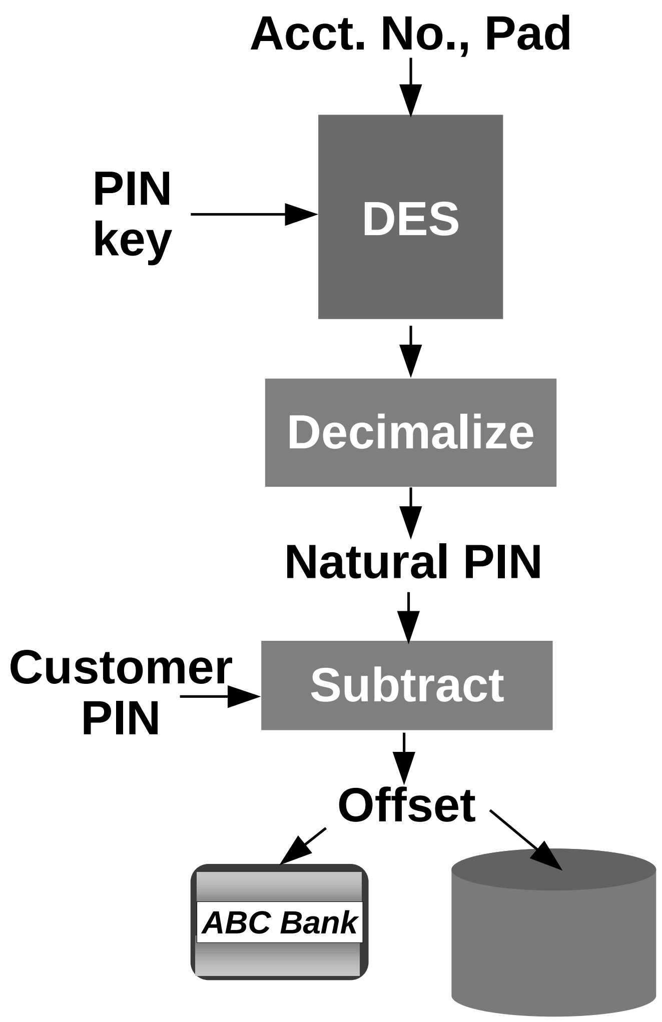
- **If the transaction is “not on us”, Bank A’s customer using Bank B’s device, the bank forwards the transaction to a switch.**
- **The switch then routes the transaction to the correct bank or processor.**
- **At each stage, the PIN is translated - decrypted and re-encrypted in a key known by the recipient.**

The Existing Network - Verification

- At the issuing bank, the PIN is verified.
- Verification is a DES-based function involving the PIN, a PIN verification key, and a verification string. The verification string is stored on the card, on the local database, or both.
- Verification returns a yes or no. It never returns the verification string.
- Two main types of verification (many others)
  - IBM 3624 offset
  - VISA PVV

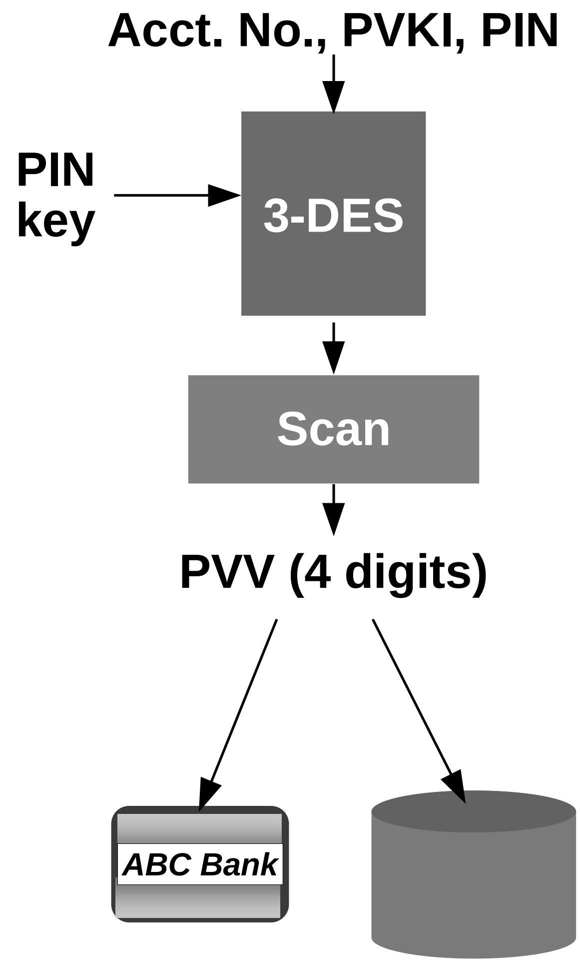
IBM 3624 PIN Verification Algorithm

- Calculate a “natural PIN” by DES encrypting Account Number
- For customer selected PIN, calculate an offset
  – Customer PIN - Natural PIN
- The length of the verified PIN is limited to the length of the offset. Leftmost digits ignored.
- Bank can change the PIN key if offset is stored on the data base.



VISA PIN Verification Value (PVV)

- **3DES encryption**
- **Verified PIN limited to 4 digits, ignore rightmost digits**
- **PIN Verification Key Indicator (PVKI) selects key from table of 6.**
- **Scan start at leftmost character and finds hex character 0-9. If fewer than 4 are found, create the rest of the PVV by decimalizing remaining characters starting at the left.**



Defenses

Protect the PIN

- PINs in the clear only within trusted hardware
  - Trusted entry devices are more difficult to tap.
  - No PIN decryption capability in system. Hardware only decrypts with one key and re-encrypt with another or verifies encrypted PIN with verification value.
- Make PIN search difficult
  - Clear PIN entry only possible manually.
  - Requires keyed, trusted device.
  - Velocity checks against account numbers.

Defenses

Protect the Key that protects the PIN

- Encrypting a PIN under a known key is the same as decrypting the PIN into the clear.
- Clear Keys are entered only under split knowledge. Two or more people must collude to know the key.
- Keys exist in the clear only within secure hardware.
- No Key decryption, only translation.
- Less secure hardware (PIN pads) should limit the exposure from the compromise of a device key.
  - Devices should not share keys.
  - Limit exposure of previous transactions.

Defenses

- Keep the system from being confused.
  - If the PIN looks like data, system will decrypt it.
  - If the PIN looks like a key, system will encrypt things with it.
  - Distinction must be cryptographic and quick. BER encoding will not help.
- Other
  - Change keys frequently to limit exposure.
  - Limit the amount that can be withdrawn per day.

Vulnerabilities - Physical

- Some of the attacks on the system are very basic
  - Pickup truck pulling out the ABM (ATM)
  - Pointing a gun at the customer
- These threats are not unique to this network.
  - Attacks against older systems are generally tried against the new systems.
- Defenses are physical, not cryptographic
  - This talk focusing on logical security.
  - Other defenses are equally important.

Vulnerabilities - Customer

- Customer reveals PIN and Account number directly
  - Security guard attack
  - Help at the ATM
- PIN is easily guessed or written on card
- Customer is watched entering PIN
  - "Shoulder-surfing" plus theft of card
  - Camera plus monitor the line
  - Card + PIN to get access to ATM
- Customer forgets PIN

Vulnerabilities - Network

- **Rogue device**
  - **Fake ABM (ATM)**
  - **Altered PIN pad**
- **Attacker monitors the connection between device and bank.**
  - **PINs are encrypted**
  - **Account numbers & balances are often not encrypted, which may help social engineering attacks.**

Vulnerabilities - Banks and Switches

- **An attacker within a bank has the most opportunities to defeat the system.**
- **A single transaction may run through many systems.**
  - **Many different insiders have opportunity.**
  - **Exposure at one point can harm many other points.**
- **Insider fraud is the main danger. All other types of attacks are a subset of insider attacks.**

Vulnerabilities - Cryptographic

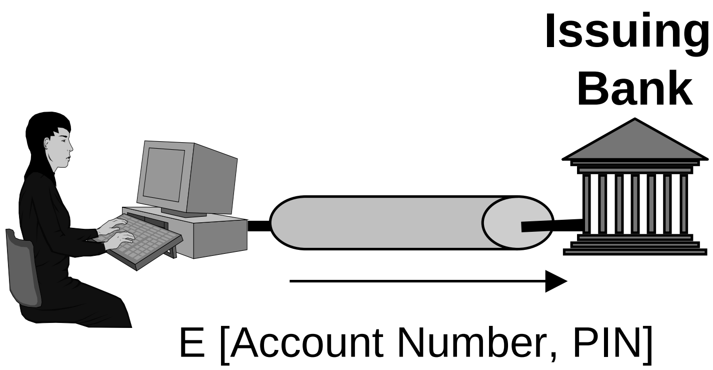
- Most of the network uses single-DES encryption
  - Vulnerable to search
  - Key management is sometimes done with 3-DES
  - IBM 3624 PIN verification key can be recovered with about 6 known PINs and track 2 data.
- Verification values are frequently only 4 digits.
- Most systems only verify 4 digits of the PIN, even if the customer is using a longer PIN.
- With IBM 3624, if the PIN is compromised, changing the PIN does not help.

Combining Public Key Protocols with PIN Networks

Approach 1 - Home Banking

Link Encryption

- Encrypt the traffic from the PC to the bank using SSL.
- Tapping the line does not provide useful information.
- Difficult to get track 2 data.
- PIN in the clear in software at the bank.
- Some banks use a separate password rather than a PIN.



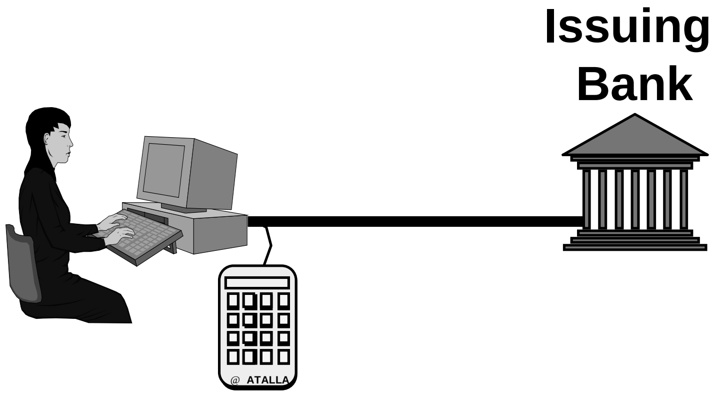
Approach 1 - Vulnerabilities

- **Easy to modify a PC to compromise PIN.**
- **PIN is in the clear within the Bank, which could compromise a PIN using this scheme.**
- **Bank systems have to be modified to allow verification of these PINs, allowing the possible compromise of the rest of the system.**
- **PIN search is very easy to implement, no good way to add velocity checks.**
- **Treating PINs like data.**

Approach 2 - Treat the PC as a PIN Pad

PIN processing ignores the public key protocol

- Create a standard PIN block at the PC by one of the following:
  – Software program with key to emulate a PIN pad.
  – Provide customer with low cost PIN pad.
  – Provide cryptogram.
- Track 2 data read by device or loaded in program.
- Sent by SSL or other protocol.



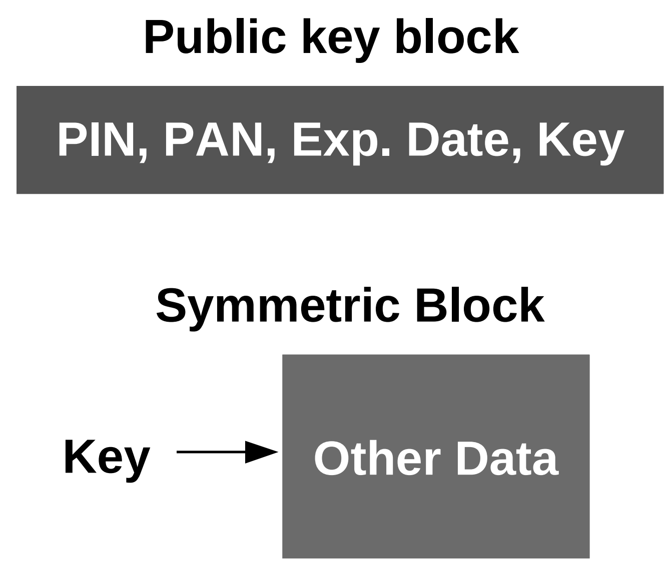
Approach 2 - Vulnerabilities

- **Emulating the PIN pad in software**
  - **Easy to modify the PC to compromise the PIN.**
  - **PIN search is possible, but the bank can use velocity checks by key.**
- **PIN pads**
  - **Tamper-resistant, but not tamper-proof. People will modify these devices and recover keys.**
  - **Difficult to manage and support the PIN pads.**
- **Cryptogram**
  - **Could be copied and used by someone else.**

Approach 3a: Public Key PIN Protocols

Within the public key block

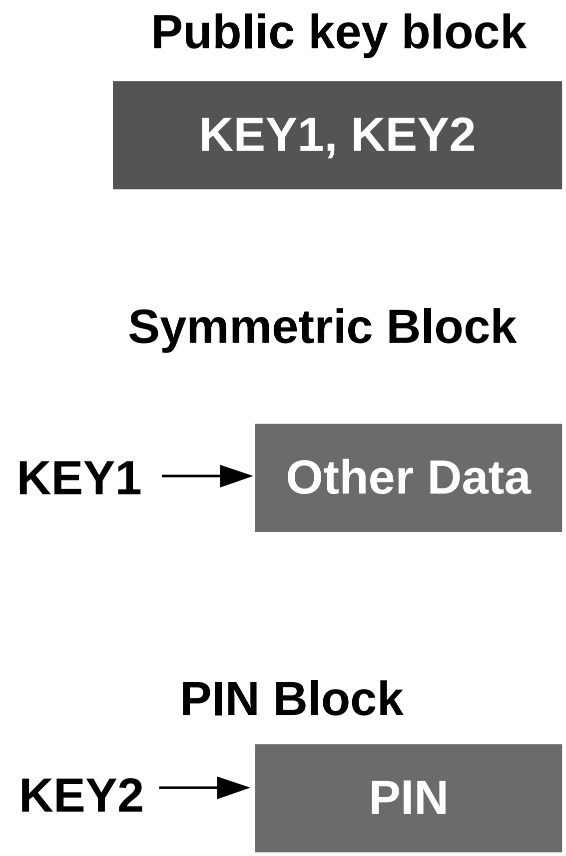
- Encrypt the PIN and the symmetric key with the public key.
  - Add PAN, Expiration date, etc. depending on space.
- Encrypt other parts of message with the symmetric key.
- Must have a way to know the PIN is within the public key envelope, and to tell which bits are part of the PIN.
  - Example: SET’s Block Content



Approach 3b: Public Key PIN Protocols

Add a separate PIN block

- Encrypt the symmetric key(s) with the public key.
- Encrypt other parts of message with symmetric key KEY1.
- Encrypt the PIN block with a second key, either KEY2 as sent, or KEY2 equals a function of KEY1.
- Must know the public key block has 2 keys, and which is which, or
- Must never compute KEY2 as data key.



Approach 3 - Vulnerabilities

- Note that the two approaches have similar security properties
  - Both can be implemented fairly securely.
  - Both can be poorly implemented, revealing PINs.
  - Approach 2b, with KEY2 = function (KEY1) may be slightly easier to implement
- Still have the problem of not trusting the PC.
  - Easy to alter.
  - Many people know how to attack.

Vulnerabilities - PIN Search Machine

- Easy for attacker to use the Internet as a PIN search machine.
  - Automated attack.
  - Try lots of account number and different banks to avoid velocity checks.
- One possible solution is to require a signature, which includes the clear PIN value.
  - Public key must be tied to account number.
  - Still difficult to avoid internal PIN search.

Vulnerabilities - Known Keys

- **The existing network was built on the assumption that no single person knows the clear value of a key.**
- **With public key cryptography, that assumption is wrong. Anyone can send a key encrypted under a public key.**
  - **Not a problem with a data encryption key.**
  - **Definite problem for PIN keys (Approach 3b).**
- **There are ways to implement this securely, but the problem is not widely understood.**

Comment about cryptographic APIs

- Banking systems would like to use standard cryptographic APIs.
- Most of the current APIs were not designed to allow a banking system to work.
  - Need to have distinctions between PINs and data, PIN keys and Data keys.
  - PINs need to be exportable under trusted symmetric keys (only PIN keys, not data keys), but not under an untrusted public key.
  - Need a secure translation function for hundreds of PINs per second.