NonStop Solutions by comForte:
The Natural Choice

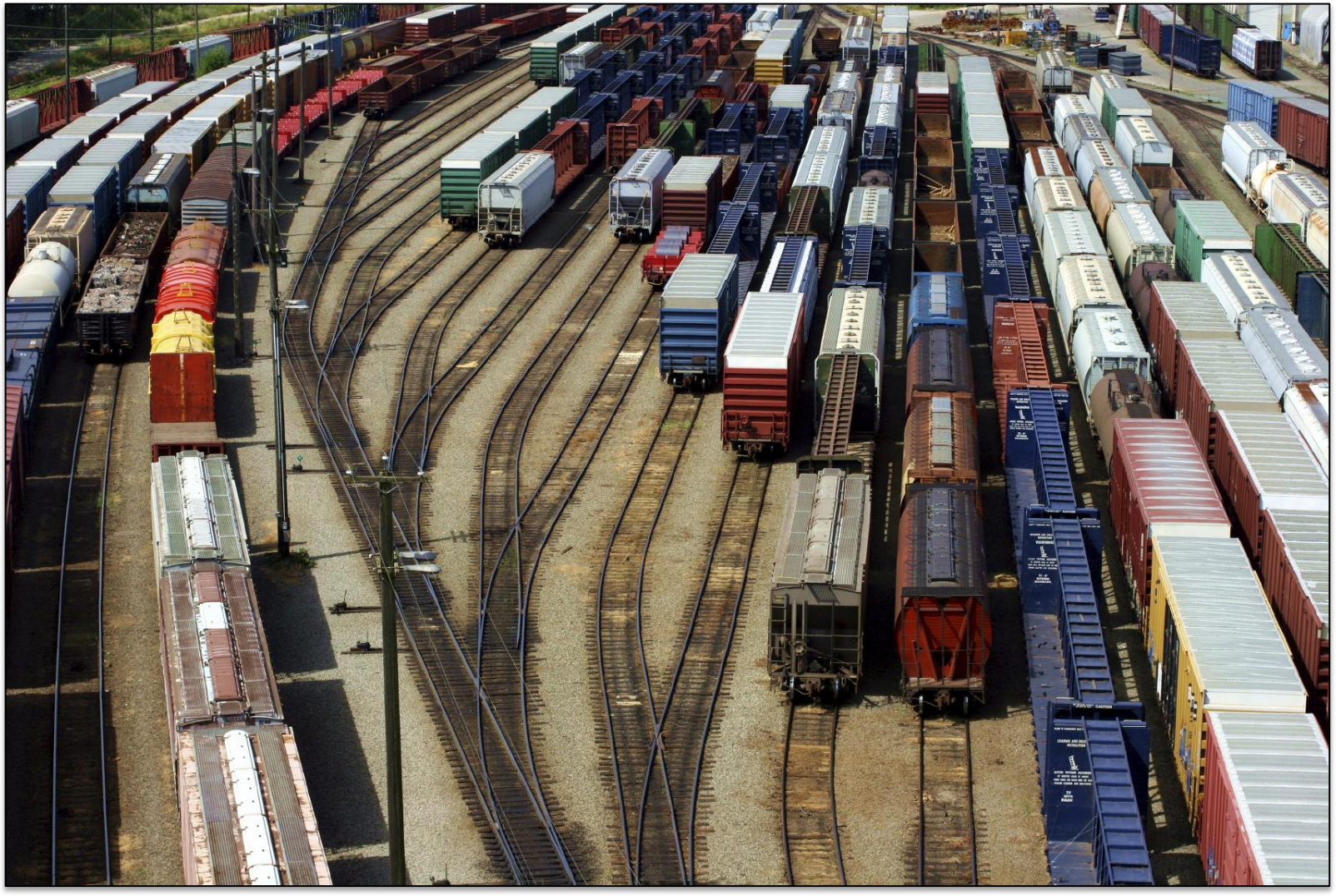
sales@comforte.com
www.comforte.com

PAN Discovery and Protection

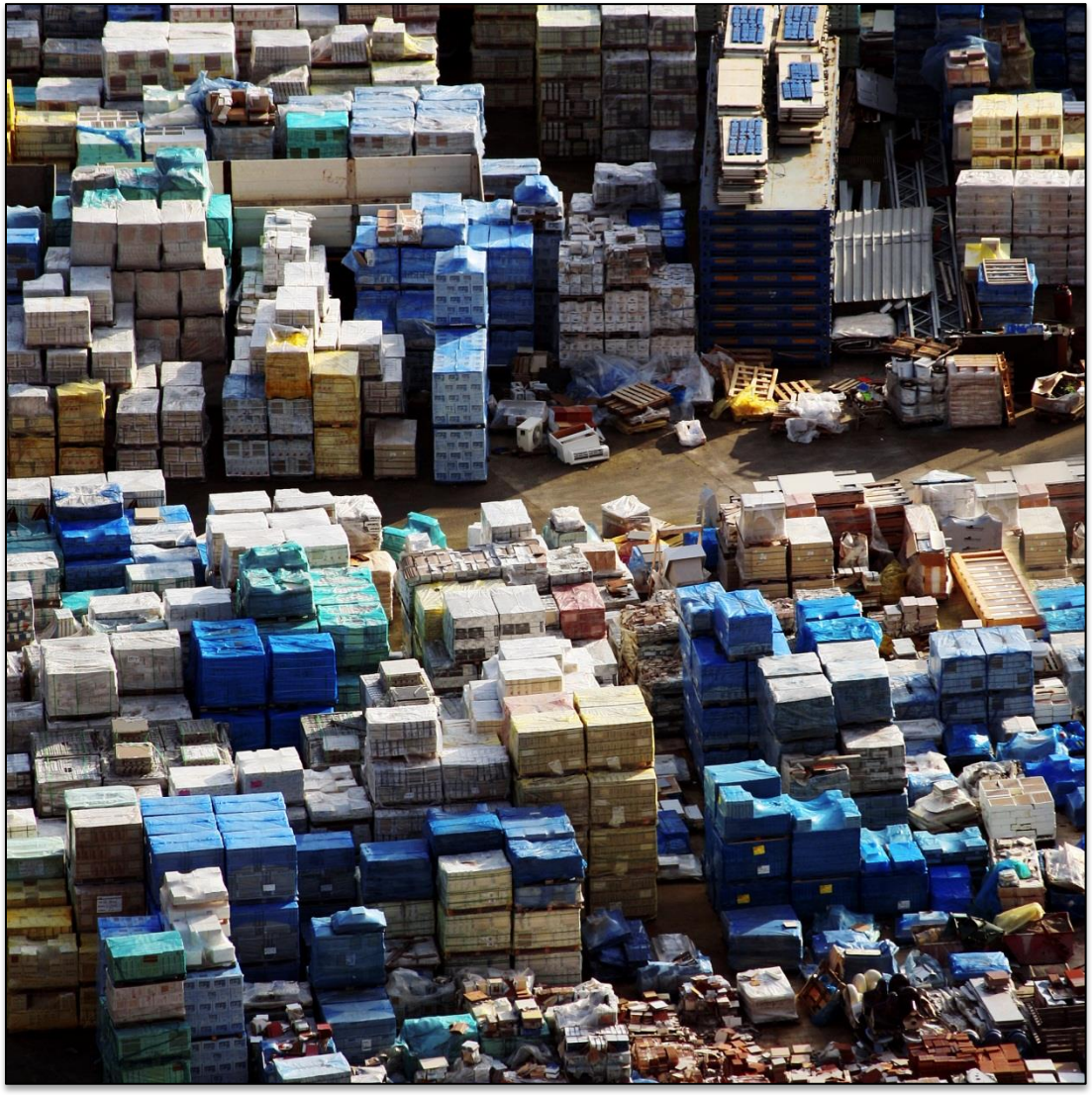
Introduction to PANFinder and SecurData

Rick Ploen, Director Business Development
INNIG October 8, 2014 Amsterdam NL

A view to a typical production system



A view to a typical test system



Pan Discovery – how would an ideal tool look like for you?

does not impact CPU usage

provides meaningful results

is FAST

can be configured for my specific needs

is powerful

does not create a PCI violation itself

Introducing Panfinder

does not impact CPU usage

- can be configured to use all available CPU or to always stay at a low CPU usage
- several parameters for fine-tuning

provides meaningful results

- minimizes "false positives" (file not containing real PANs is marked as containing PANs)
- minimizes "false negatives" (file containing real PANs is not found)

is FAST

- Summary scans stop after 'X' PANs found
- Use of change detection monitoring
- Configurable Include/Exclude wild carded file sets
- Re-run file list

can be configured for my specific needs

- i.e. credit card prefixes I actually use

is powerful

- Searches multiple file formats (Enscribe, SQL/MP)
- Searching of open and locked files
- Configurable resource utilisation (maximum scan speed v minimum system impact)
- Scheduled searches (Netbatch)
- Syslog output, SIEM/enterprise logging solution integration (Arcsight, RSA enVision etc.)

does not create a PCI violation itself

- PCI-DSS compliant reports (suspected PANs are appropriately masked)

➡ See http://www.comforte.com/products/protect/panfinder/ for details

How to protect your sensitive information then?

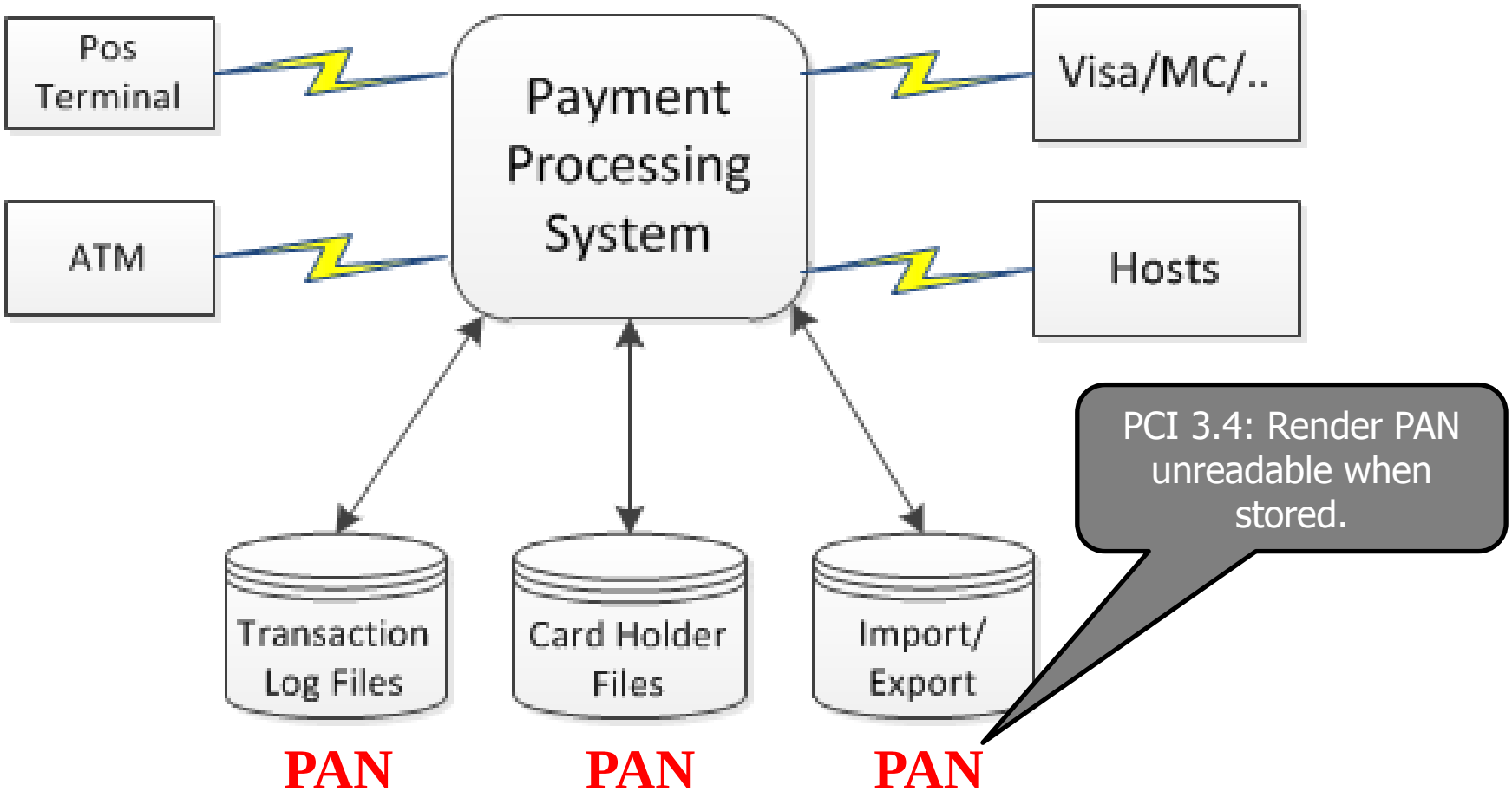
"I'm sure there are better ways to disguise sensitive information"

Does Volume Level Encrytion (VLE) Pass PCI Test?

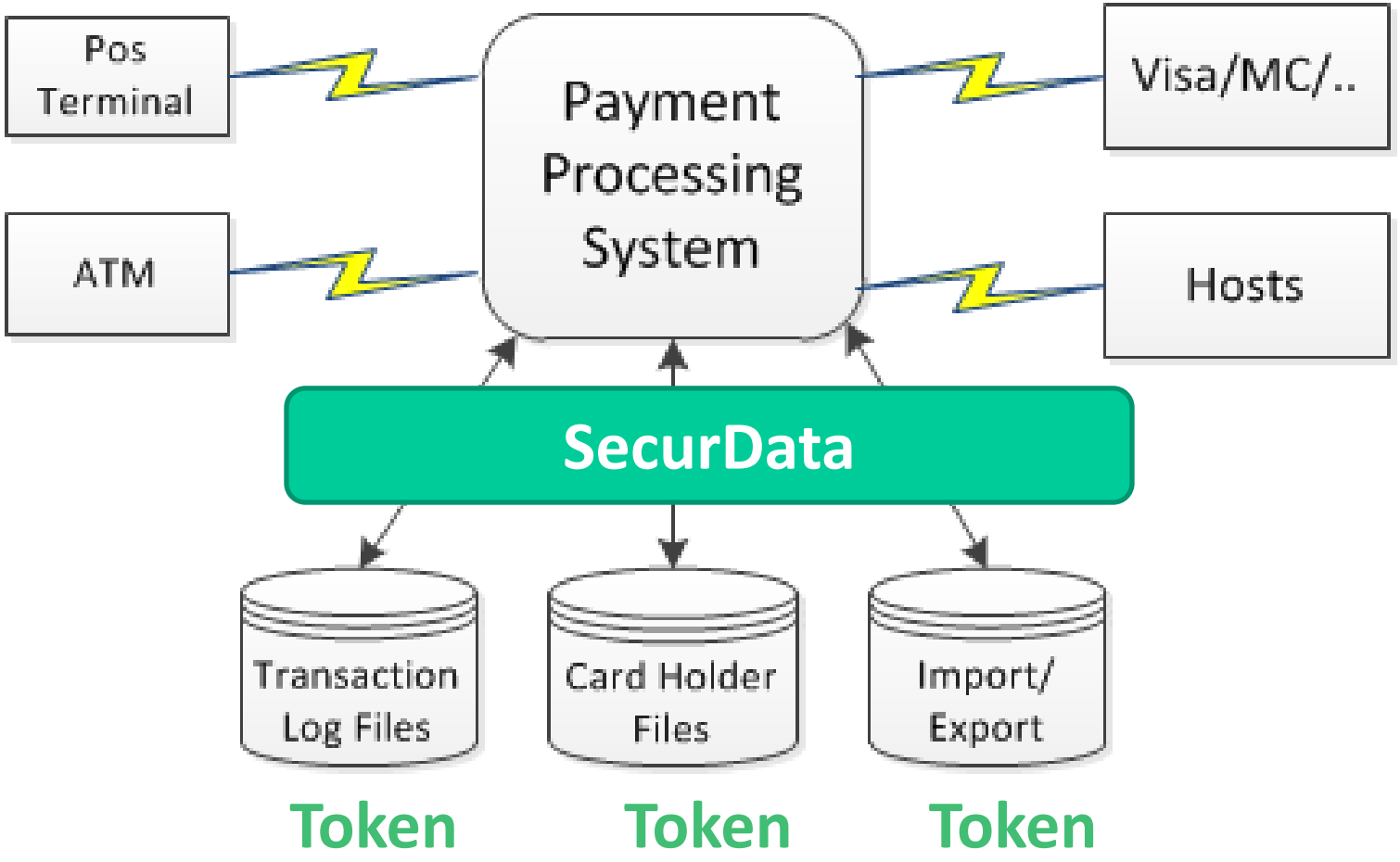
Logical access for disk encryption must be managed ***separately and independently*** of the native operating system authentication and access control mechanisms, and that decryption keys **must not be *associated*** *with* user accounts.

THE ANSWER IS NO!

A typical payment system

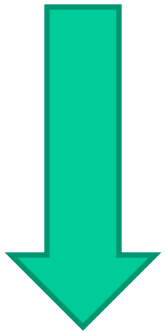


Payment System Secured with SecurData



Tokenization – the concept

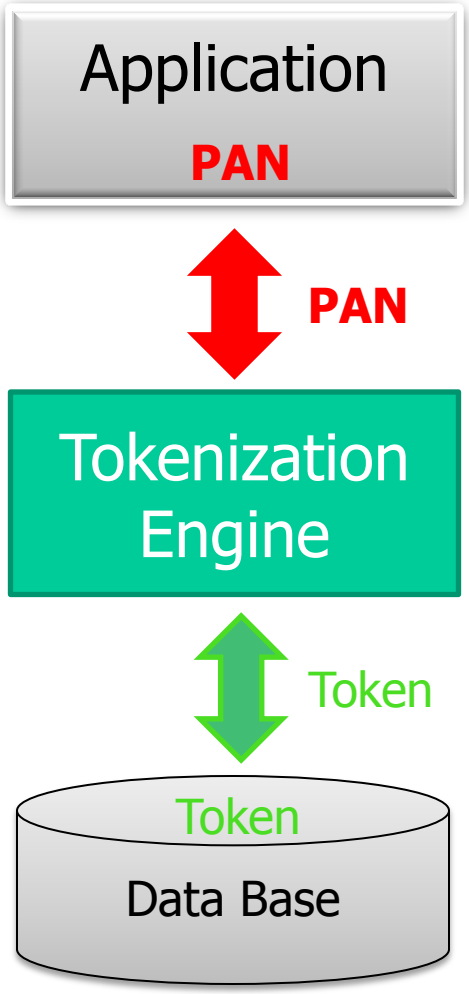
4026157151401408 (PAN)



4026xExn12VT0258 (Token)

Tokenization Engine

Tokenization – The concept



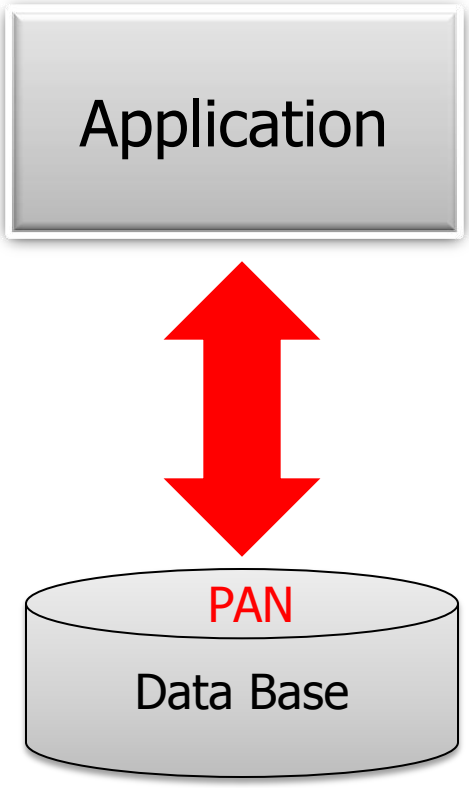
Transaction Log before Tokenization

```
$B2402.RYN1PTLF.PO110114  RECORD 11  KEY 12290 (%30002)  LEN 1066

   0:  ....S...01VISAVISA4026157151401408   000RYN1AIB10015001588888830
  35:       88888830        001001RYN1AIB188888830        1026410088888830
  70:       588888830           11111100210001399....S...................1101
 105:  14102641001101140000001101140000000005605TEST TERMINAL ASSET ML   JOE
 140:  DOE              NEW YORK  IE IE0000   ..630493000000000000000007011
 175:  1111000000000005999B24 B24 100000V                    050............
 210:  ....1306M4026157151401408=1306?
 245:                           P1A^APACS^02    9001000        6910000000000
 280:                     02000001501109789786100000097861000000........1220
 315:  00     00000000000
 350:    0000                                 00
 385:                  & ....! 04..             0     Y ! C0..111     2
 420:    7  1    ! C1..S1A^APACS^AST^02! C4..20351000061 ! B4..011500..
 455:  15060 ! P0.&                    88888830           ! B8."
 490:    POS               ! B9.<                              ISO000000
 525:
```

Transaction Log after Tokenization

```
$B2402.RYN1PTLF.PO110114  RECORD 11  KEY 12290 (%30002)  LEN 1066

   0:  ....S...01VISAVISA4026xExn12VT0258   000RYN1AIB10015001588888830
  35:       88888830        001001RYN1AIB188888830        1026410088888830
  70:       588888830           11111100210001399....S...................1101
 105:  14102641001101140000001101140000000005605TEST TERMINAL ASSET ML   JOE
 140:  DOE              NEW YORK  IE IE0000   ..630493000000000000000007011
 175:  1111000000000005999B24 B24 100000V                    050............
 210:  ....1306M4026xExn12VT0258=1306?
 245:                           P1A^APACS^02    9001000        6910000000000
 280:                     02000001501109789786100000097861000000........1220
 315:  00     00000000000
 350:    0000                              00
 385:                  & ....! 04..            0     Y ! C0..111     2
 420:    7  1    ! C1..S1A^APACS^AST^02! C4..20351000061 ! B4..011500..
 455:  15060 ! P0.&                   88888830           ! B8."
 490:    POS               ! B9.<                              ISO000000
 525:
```

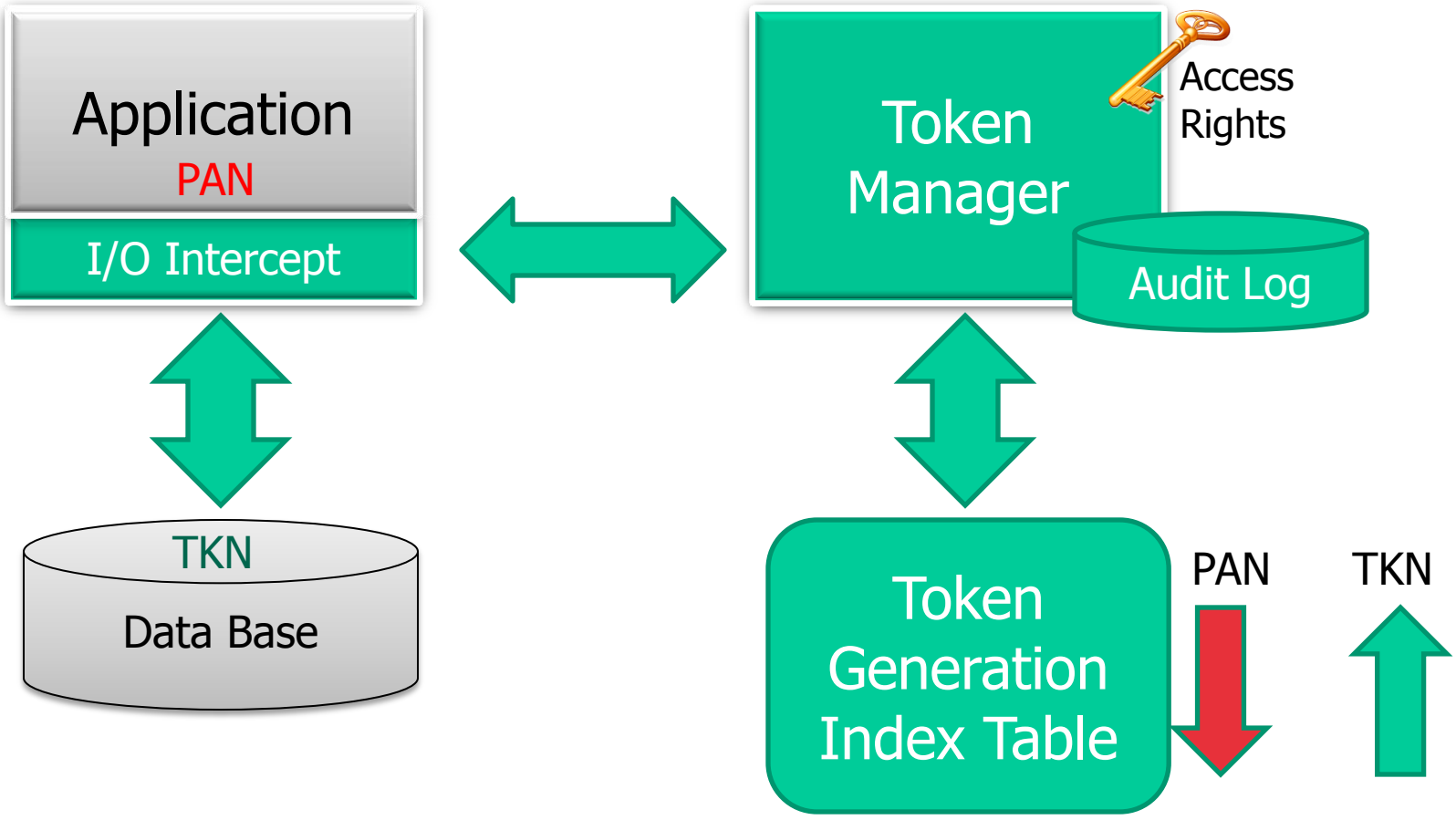
Tokenization for NonStop Applications



Considerations for introducing Tokenization

- What will I have to do with my application?
- What about latency ?
- Is it a one off for every additional application ?
- Does it cover the whole picture?

SecurData: Transparent Tokenization for NonStop

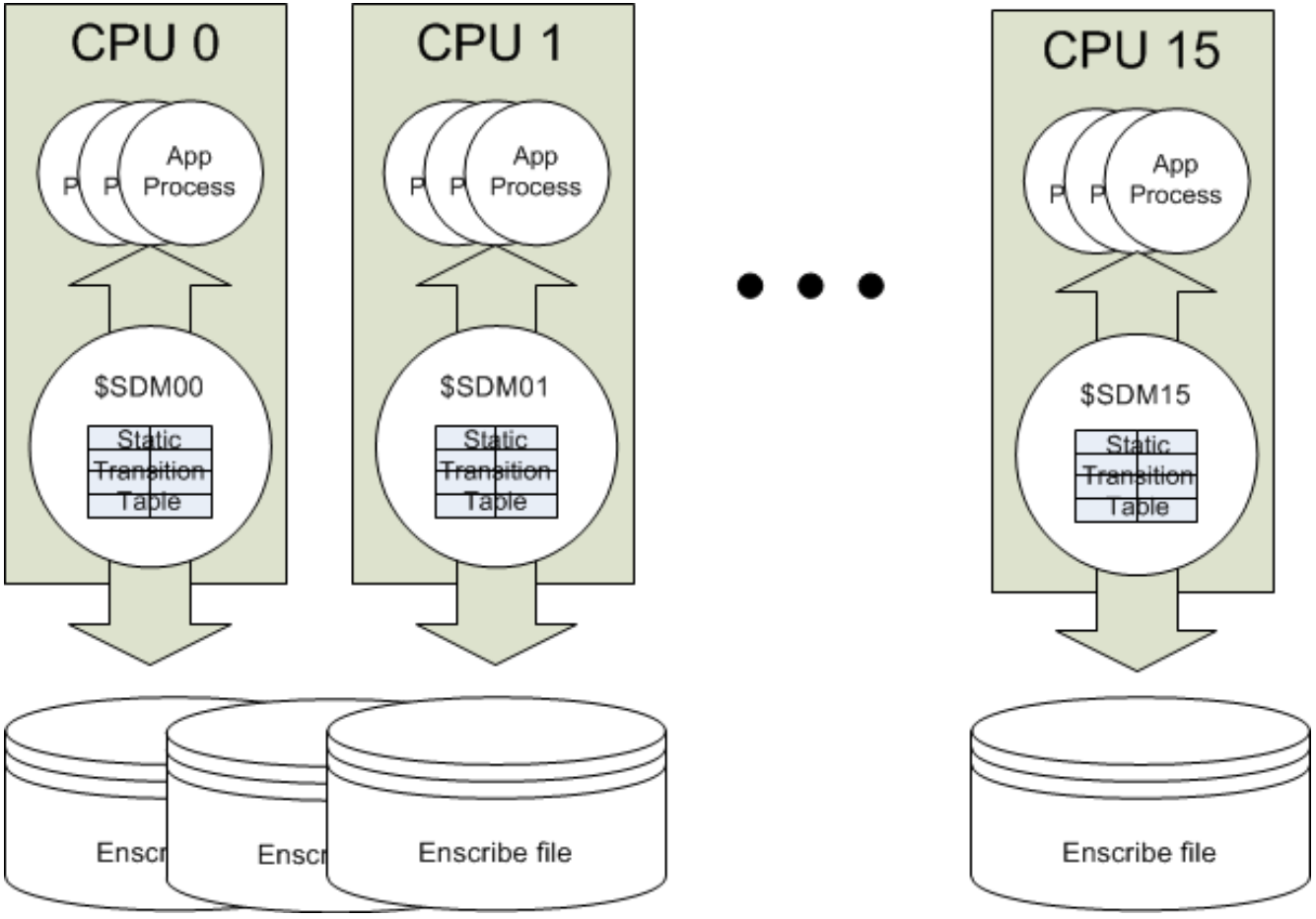


SecurData Tokenization Scheme

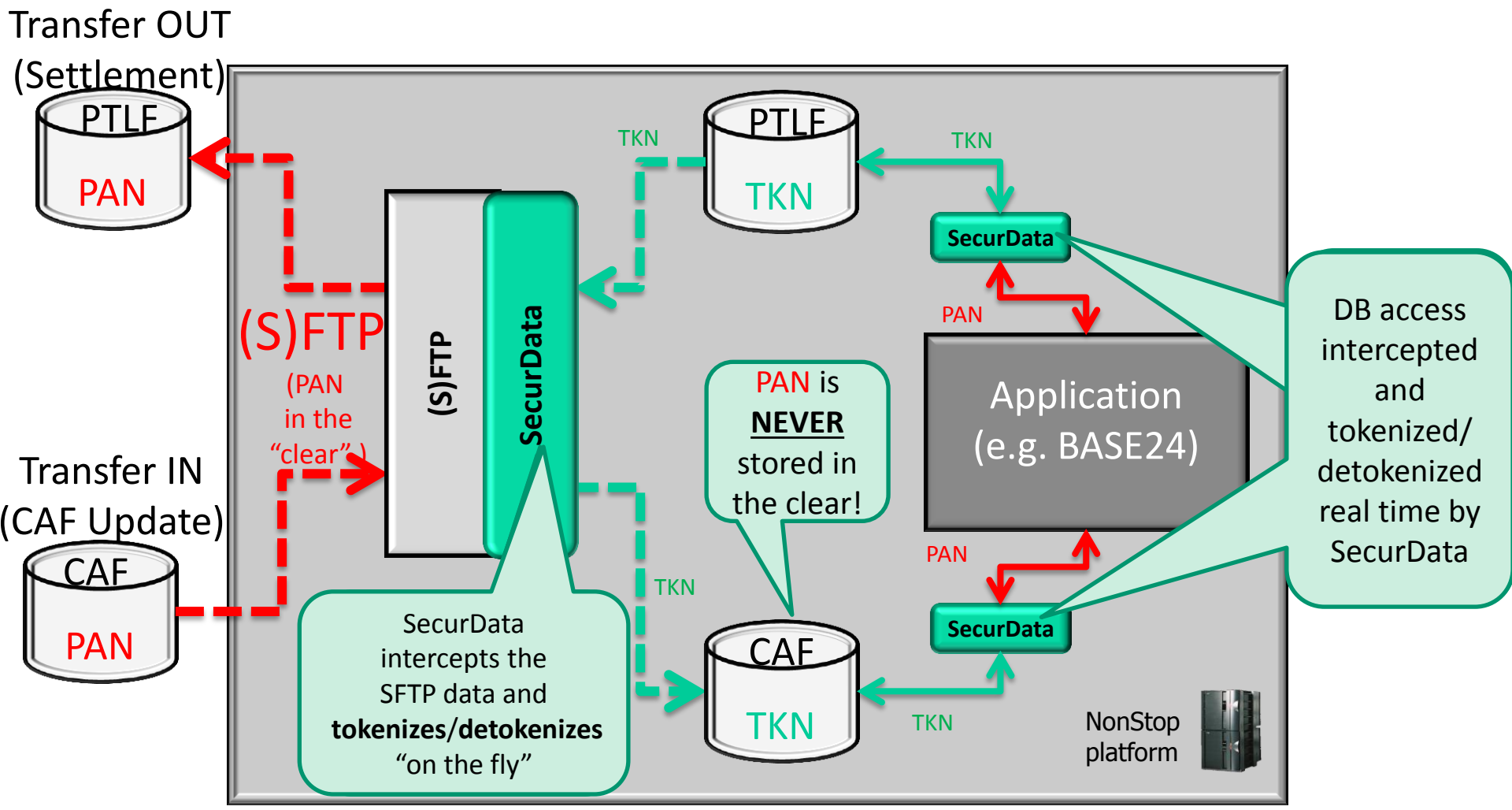
- Token Generation Index Table (TGIT) is a large table of random numbers
  - Customer specific
  - Generated during installation of SecurData at the customer side
  - Encrypted while residing on disk, loaded completely into memory during SecurData startup and kept there
  - Easily replicated

- Special two-way deterministic algorithm using the TGIT to generate tokens from PANs and obtaining back PANs from tokens
  - Security validated
  - Algorithm available under NDA
  - Adhering to Kerckhoffs' principle: security does **NOT** depend on keeping algorithm secure
  - Patent pending

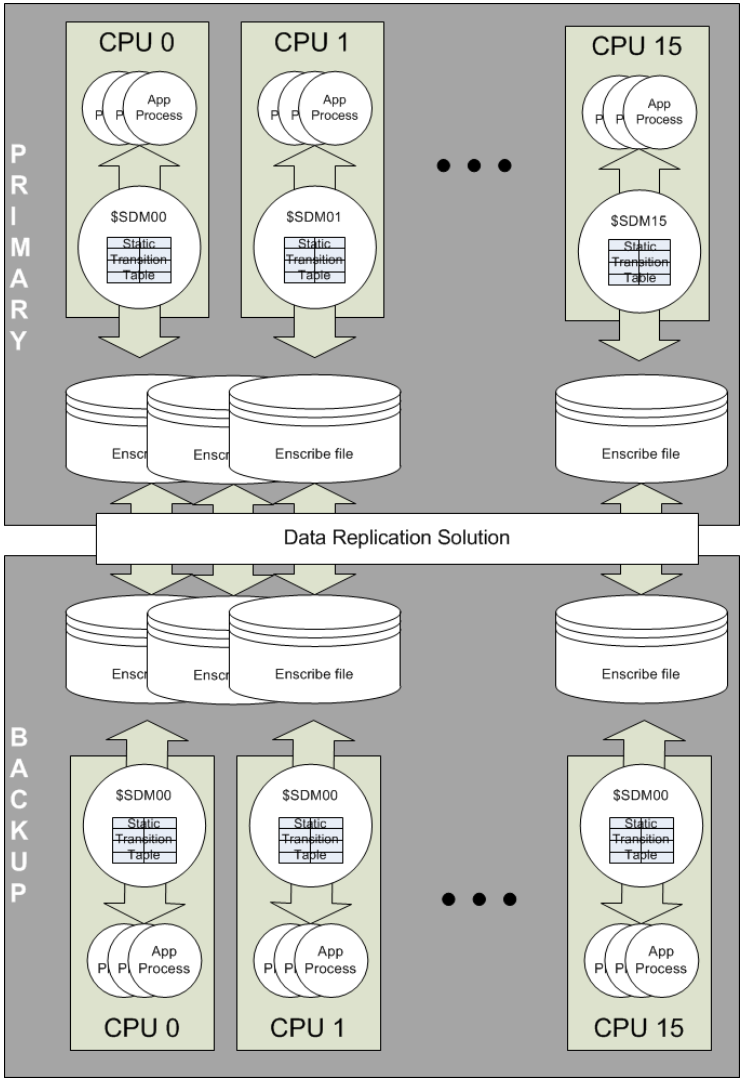
SecurData Runtime Environment



Does it cover the full picture?



SecurData with DR solution

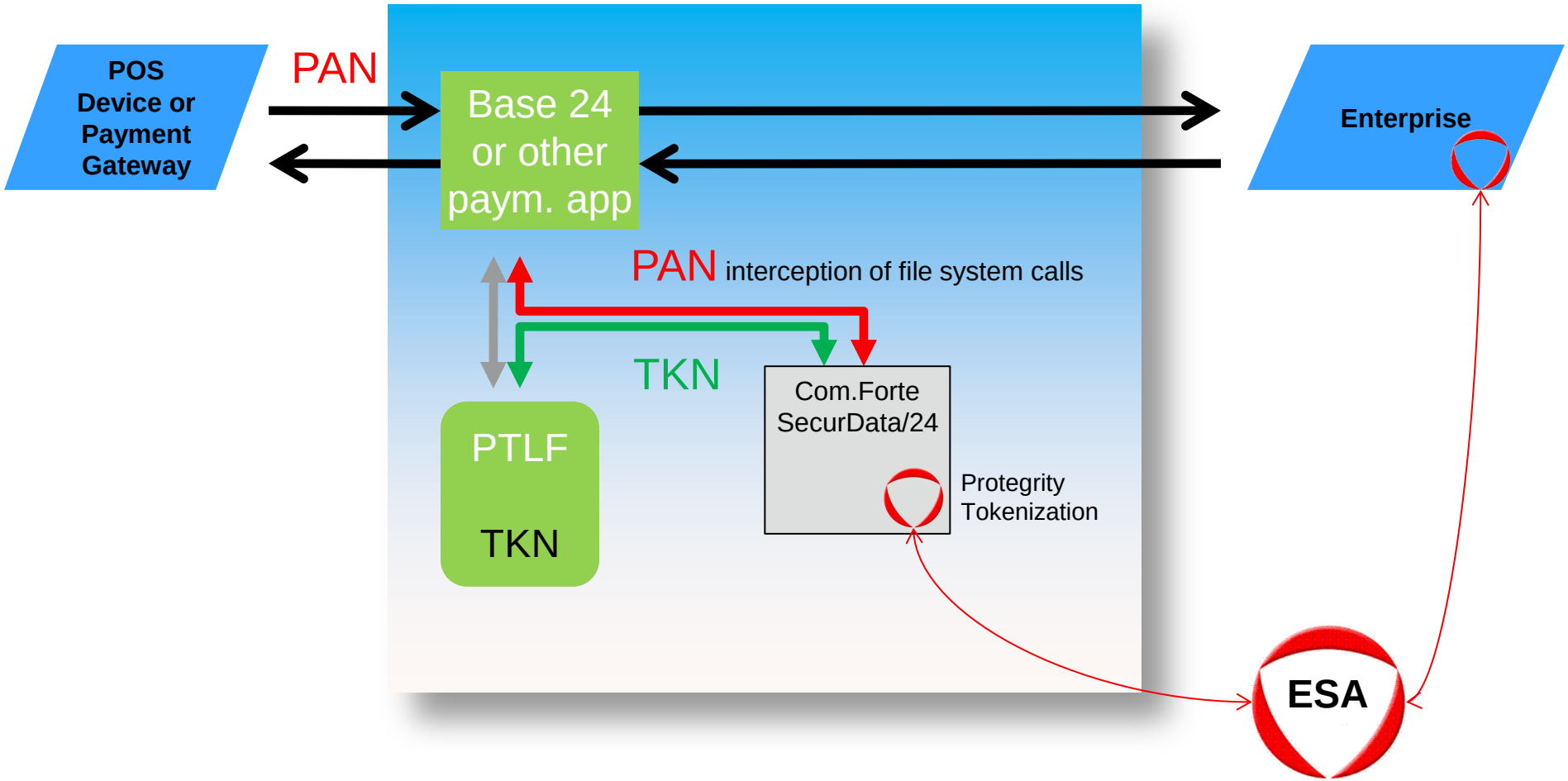


- stateless SecurData configuration
  => easily replicated
- Pre-generated Token Generation Index Table
  => No risk of collisions
  => easily replicated

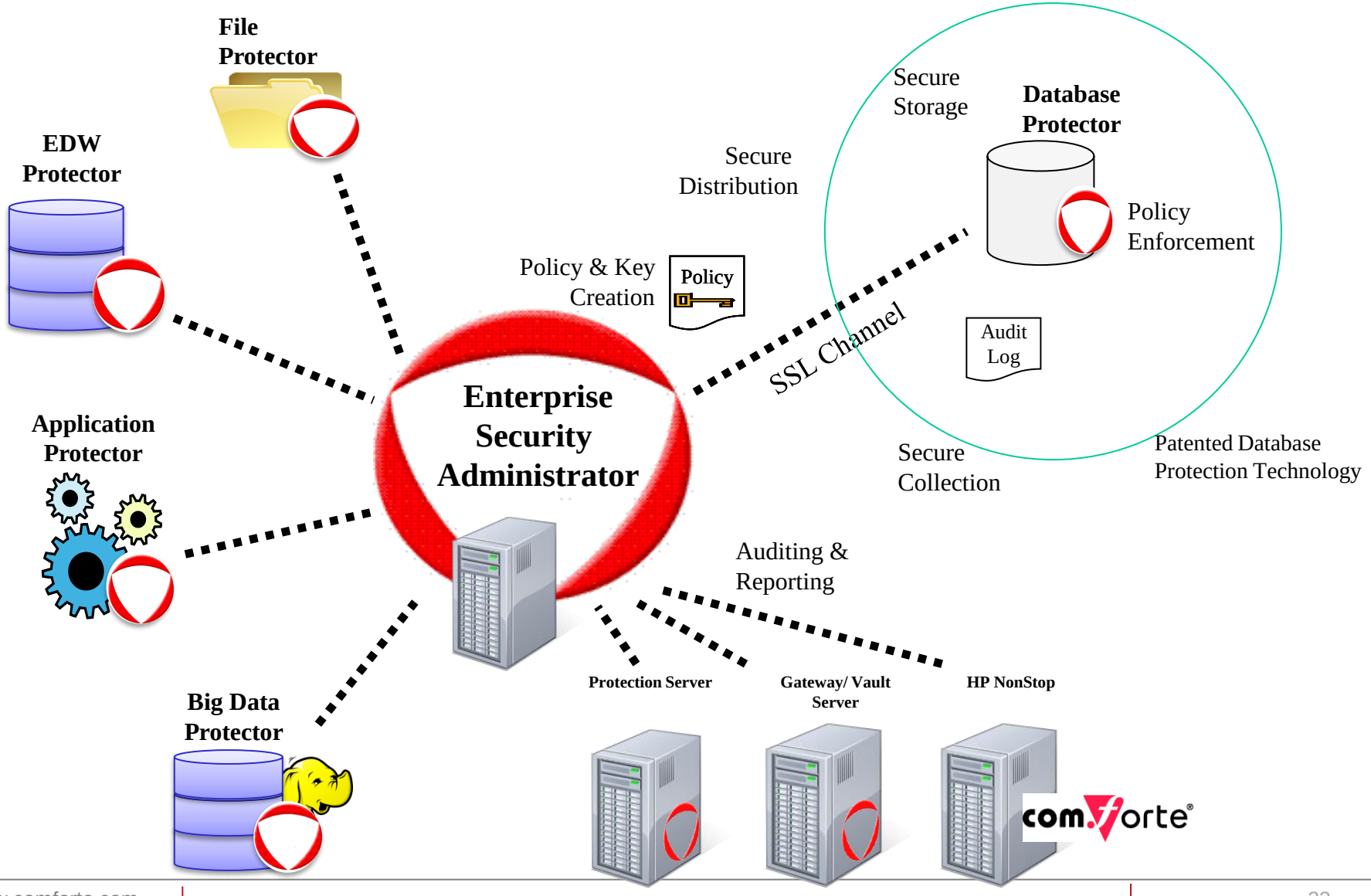
Enterprise Integration

- SecurData Enterprise options:
  - NonStop as central Enterprise tokenization server
    - Control everything at the heart of the payment environment
    - Availability, Scalability, Reliability
    - Might have quicker ROI
  - Integration with Protegrity
    - Integrating the NonStop into Protegrity‘s Enterprise Service Administrator environment
    - Central Administration entity with point and click

SecurData: Enterprise Integration with Protegriy



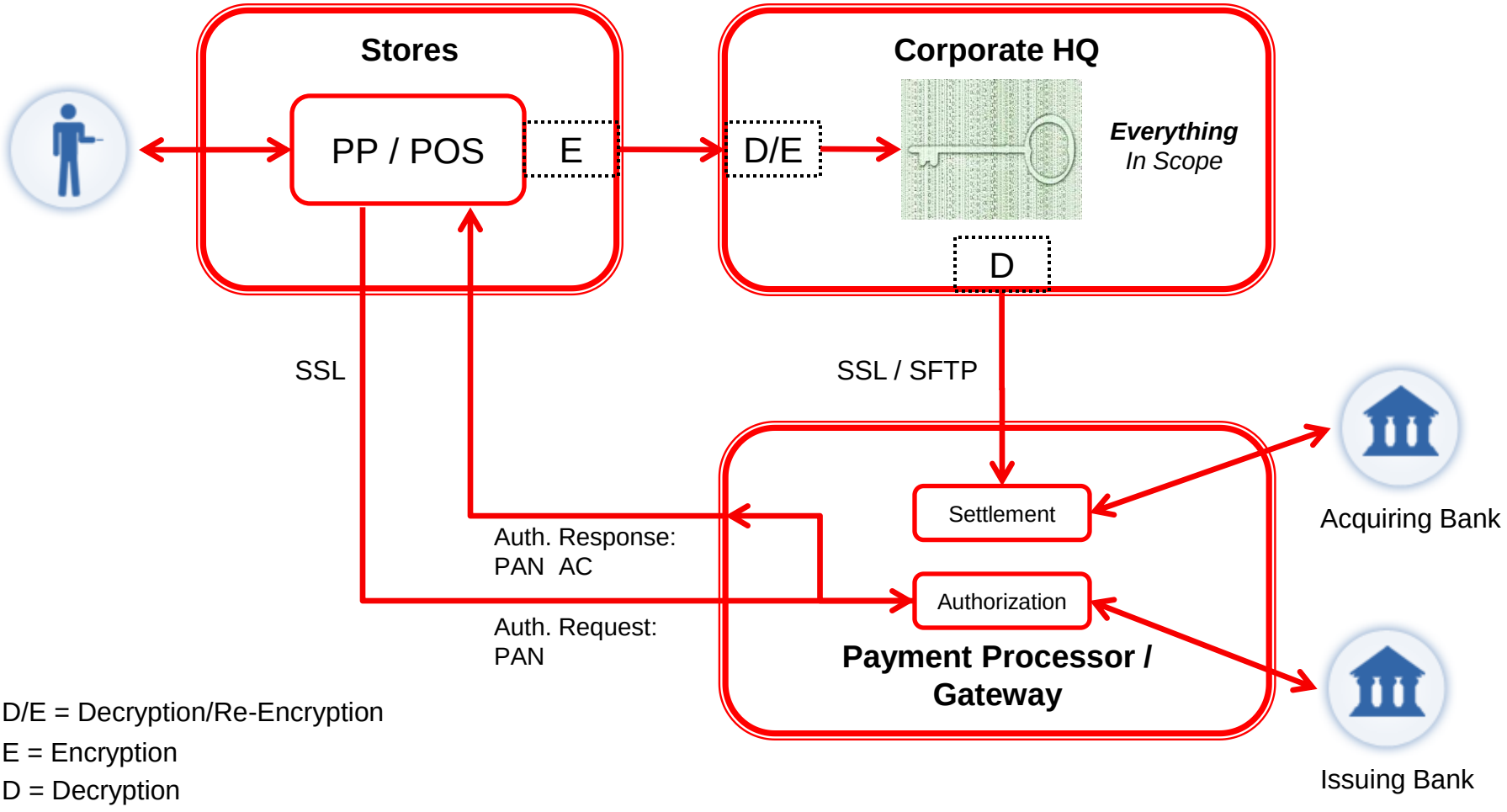
SecurData: Enterprise tokenization with Protegrity



sales@comforte.com
www.comforte.com

Questions ?

Protegrity HQ Encryption (Level 1&2)

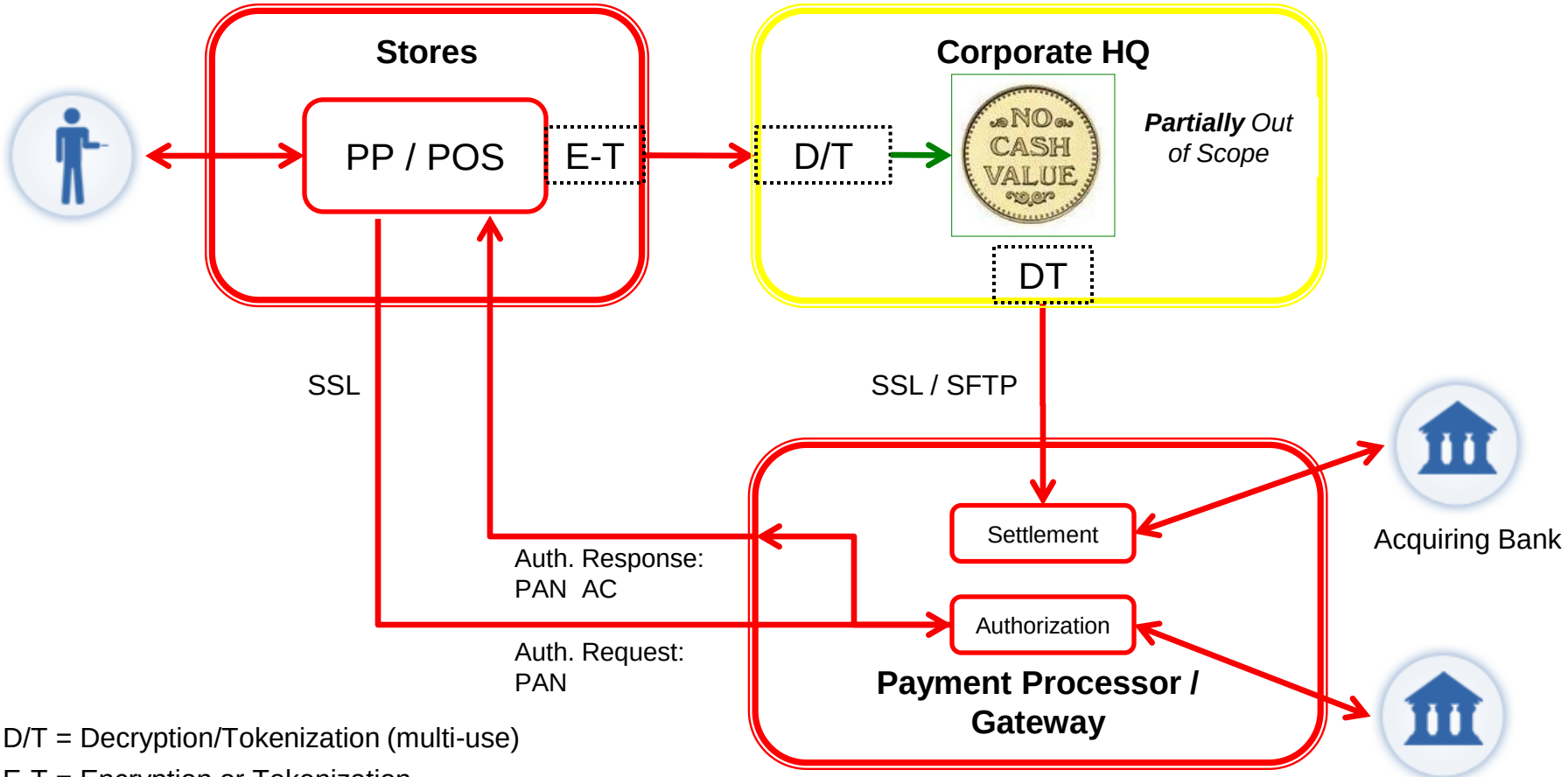


D/E = Decryption/Re-Encryption

E = Encryption

D = Decryption

Protegrity HQ Encryption (Level 1&2)

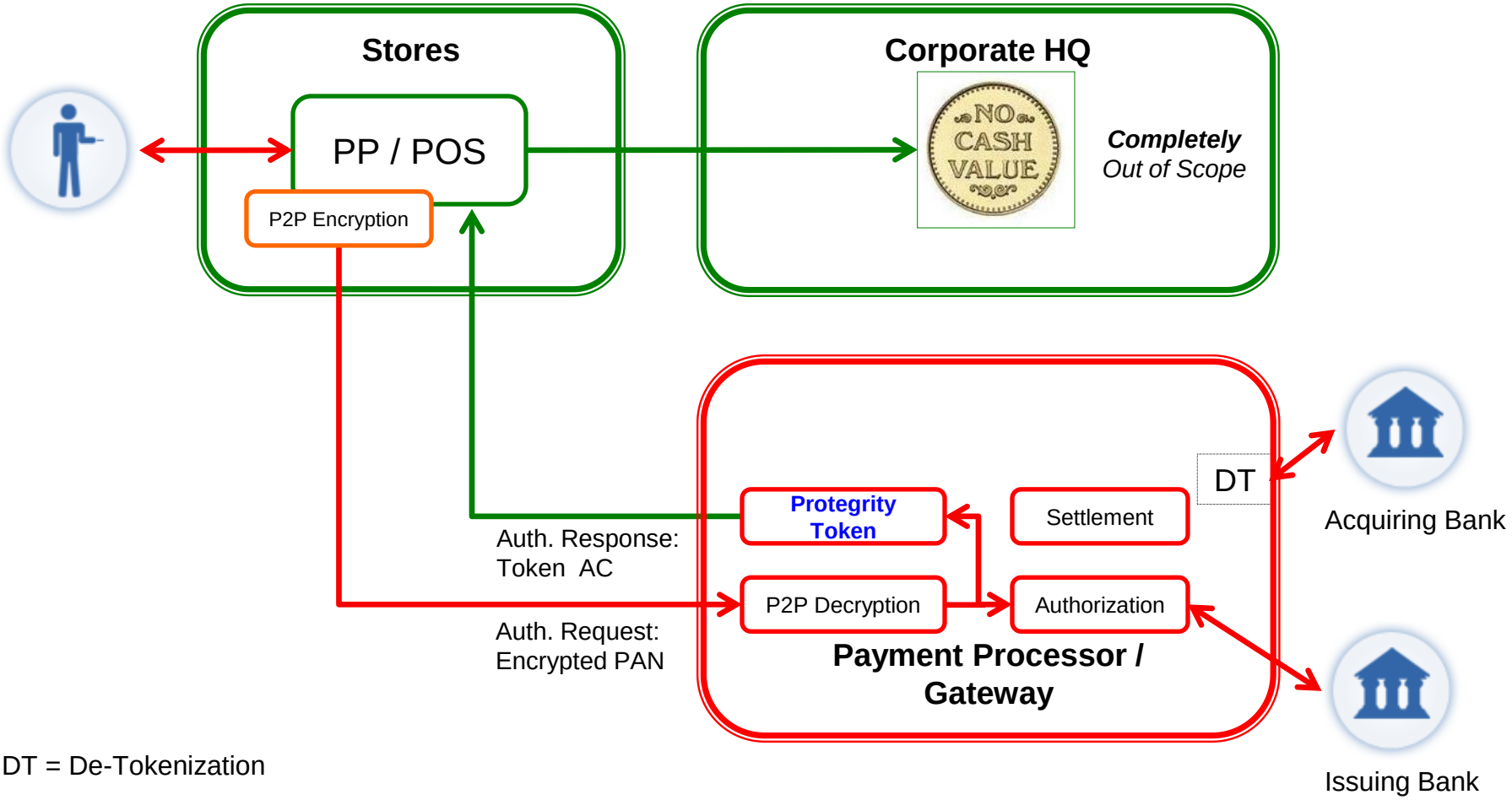


D/T = Decryption/Tokenization (multi-use)

E-T = Encryption or Tokenization

DT = De-Tokenization

PP/GW Tokenization – (Level 1-4)



DT = De-Tokenization

Common Payment processor environment