Modeling Fraud Scenarios in a Rete-based Stateful Rule Engine with First-order Capabilities

SPRING 2009

4. Graduierten-Workshop über Reaktive Sicherheit

SYSTEMATIC THOUGHT LEADERSHIP FOR INNOVATIVE BUSINESS

Cristina Fortu

Ulrich Flegel

SAP Research Karlsruhe

September 15, 2009

Agenda

1. Customer Situation and Challenges

2. Solution Approach & Technology

3. Benefits, Best practices & Use Cases

4. Conclusion

Agenda

1. **Customer Situation and Challenges**

2. Solution Approach & Technology

3. Benefits, Best practices & Use Cases

4. Conclusion

Customer Situation and Challenges

Companies are facing:

- High volume of business transactions
- Large and quickly growing databases
- Increasing number of fraudulent activities
- Lack of real-time facilities for flagging suspicious actions

The Challenge:

- A Fraud Detection System capable of detecting fraudulent behavior

Customer Situation and Challenges

Ideal Approach

- Understanding auditors´ requirements
- Selecting the most relevant fraud scenarios
- Choosing the right language for modeling event sigantures
- Accurately specificating fraud scenario patterns

A tool based on an existing general rule engine with real world applicability based on real fraud scenarios and real business transactions.

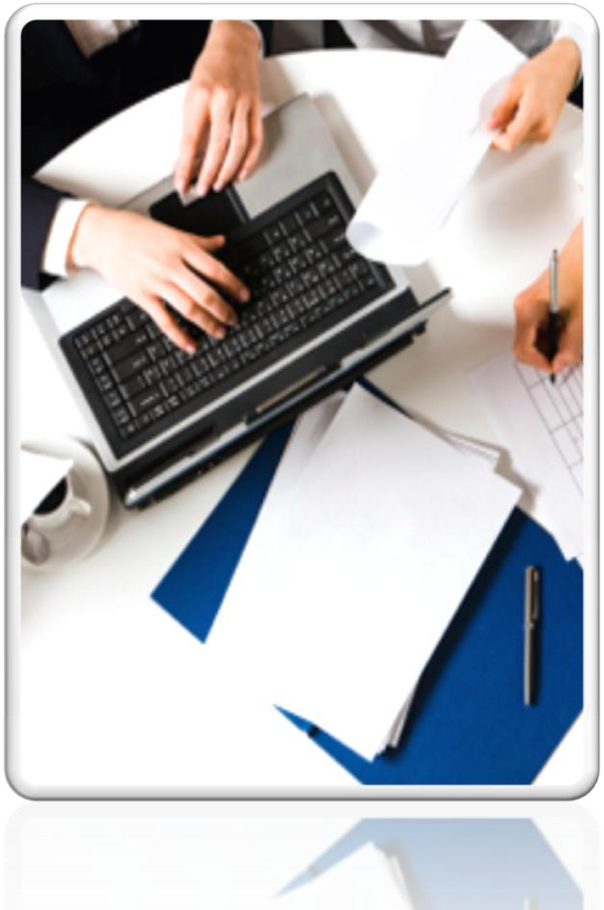
Agenda

1. Customer Situation and Challenges
2. **Solution Approach & Technology**
3. Benefits, Best practices & Use Cases
4. Conclusion

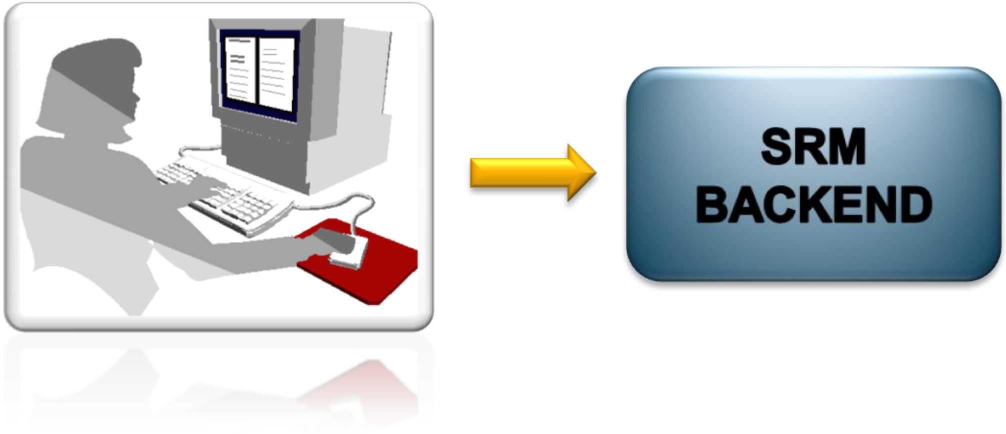
Solution Approach & Technology

Methodology

- Understand the reference fraud scenarios provided by auditors
- Investigate the expressiveness of WANF for modeling fraud scenarios
- Provide working constructions of event signatures
- Test the system using real world data and business transactions

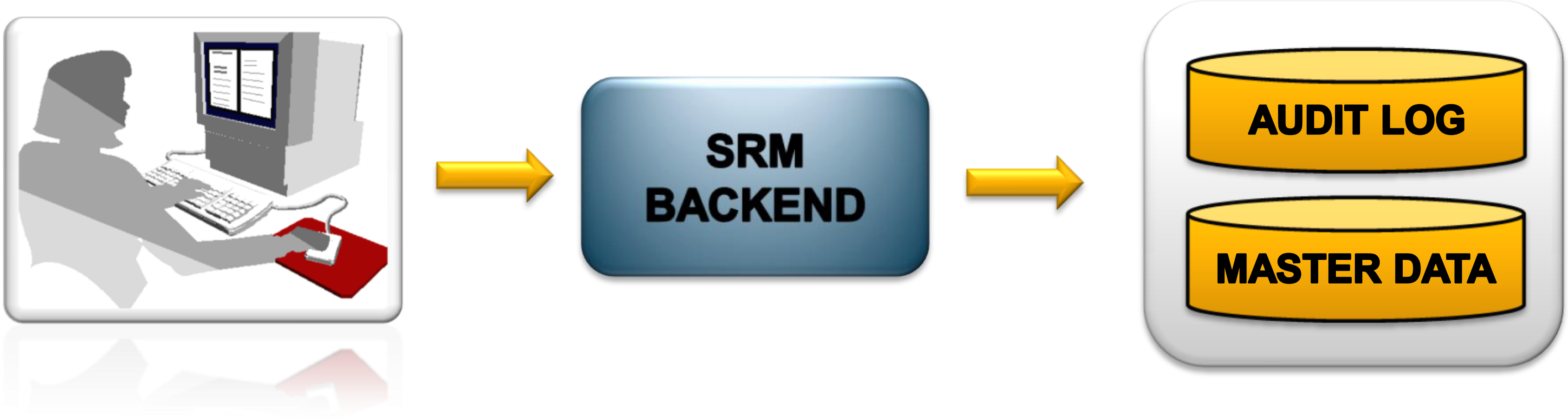


Solution Approach & Technology



SRM
BACKEND

Solution Approach & Technology

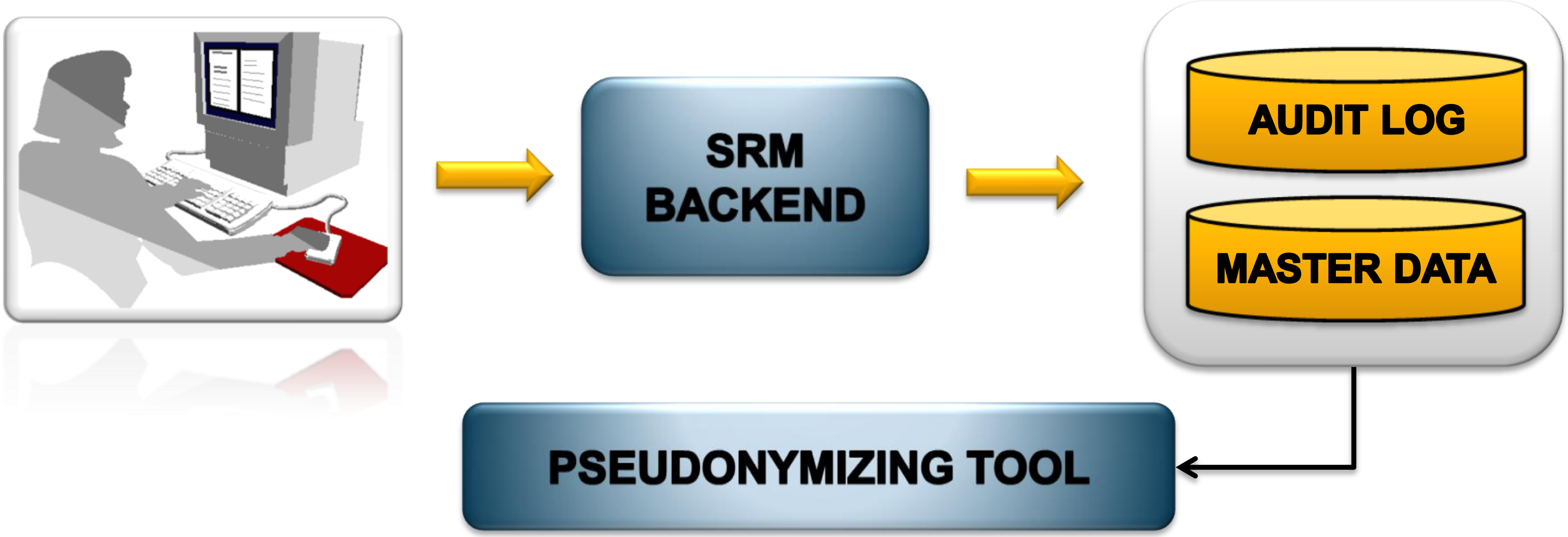


SRM BACKEND

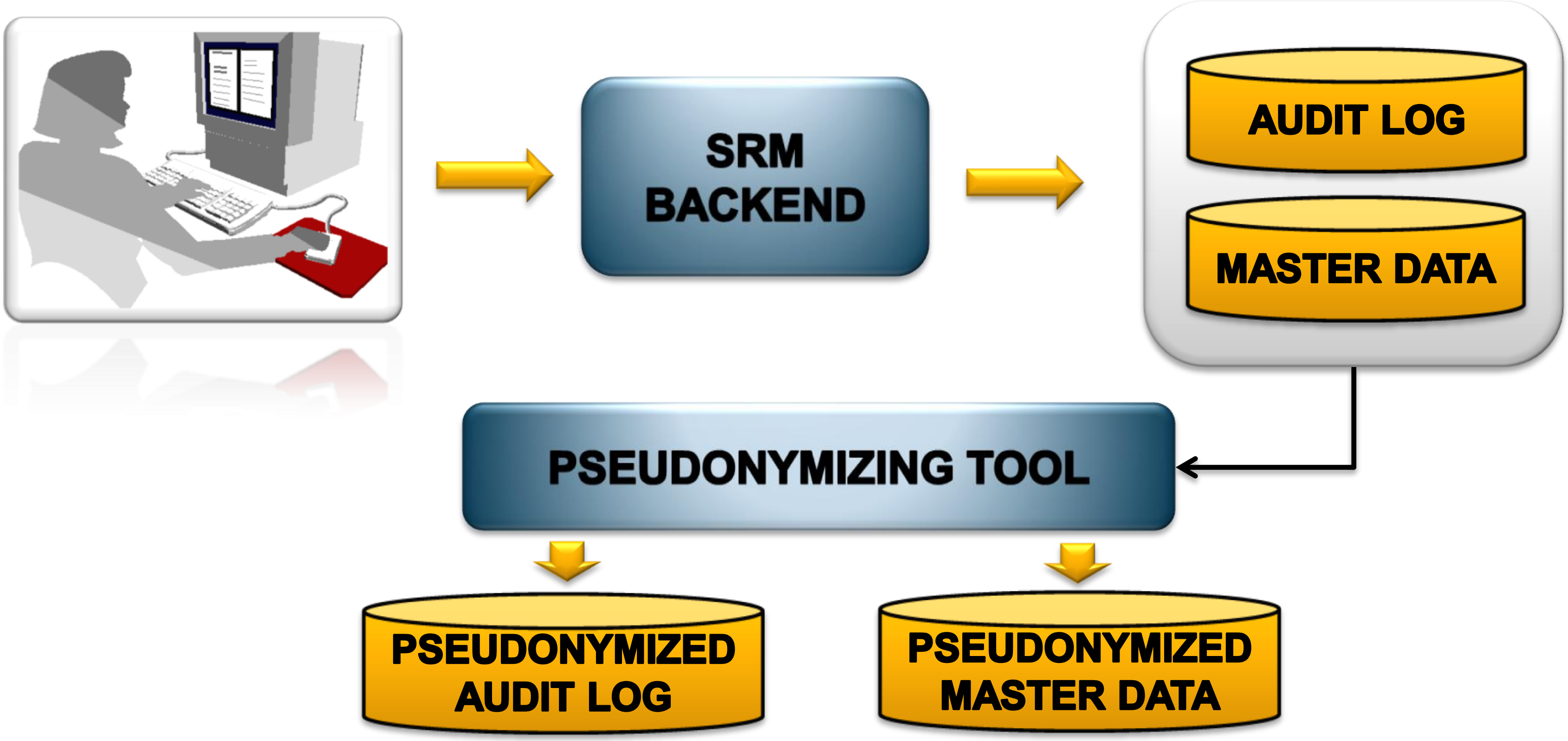
AUDIT LOG

MASTER DATA

Solution Approach & Technology



Solution Approach & Technology



SRM BACKEND

AUDIT LOG

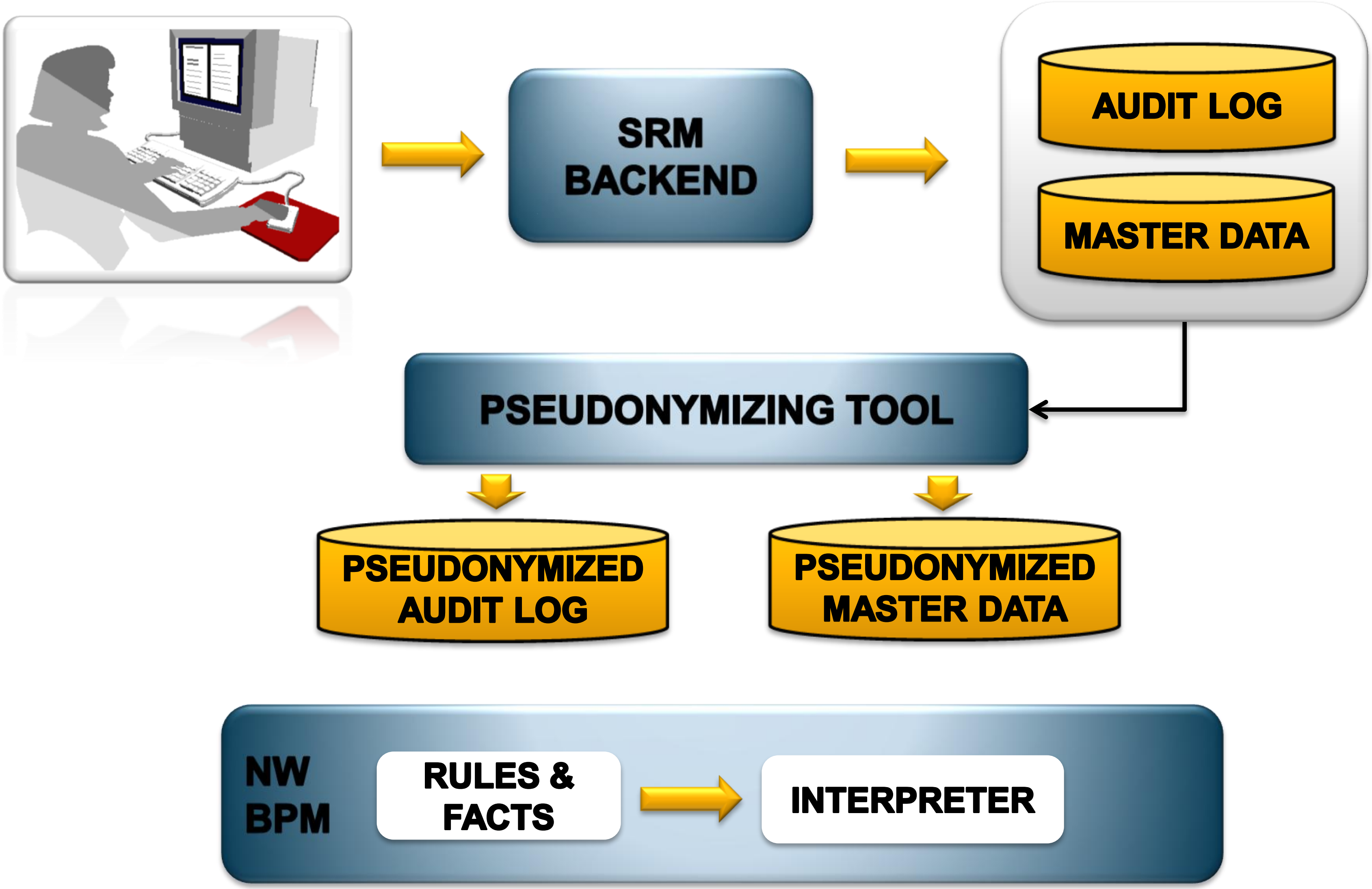
MASTER DATA

PSEUDONYMIZING TOOL

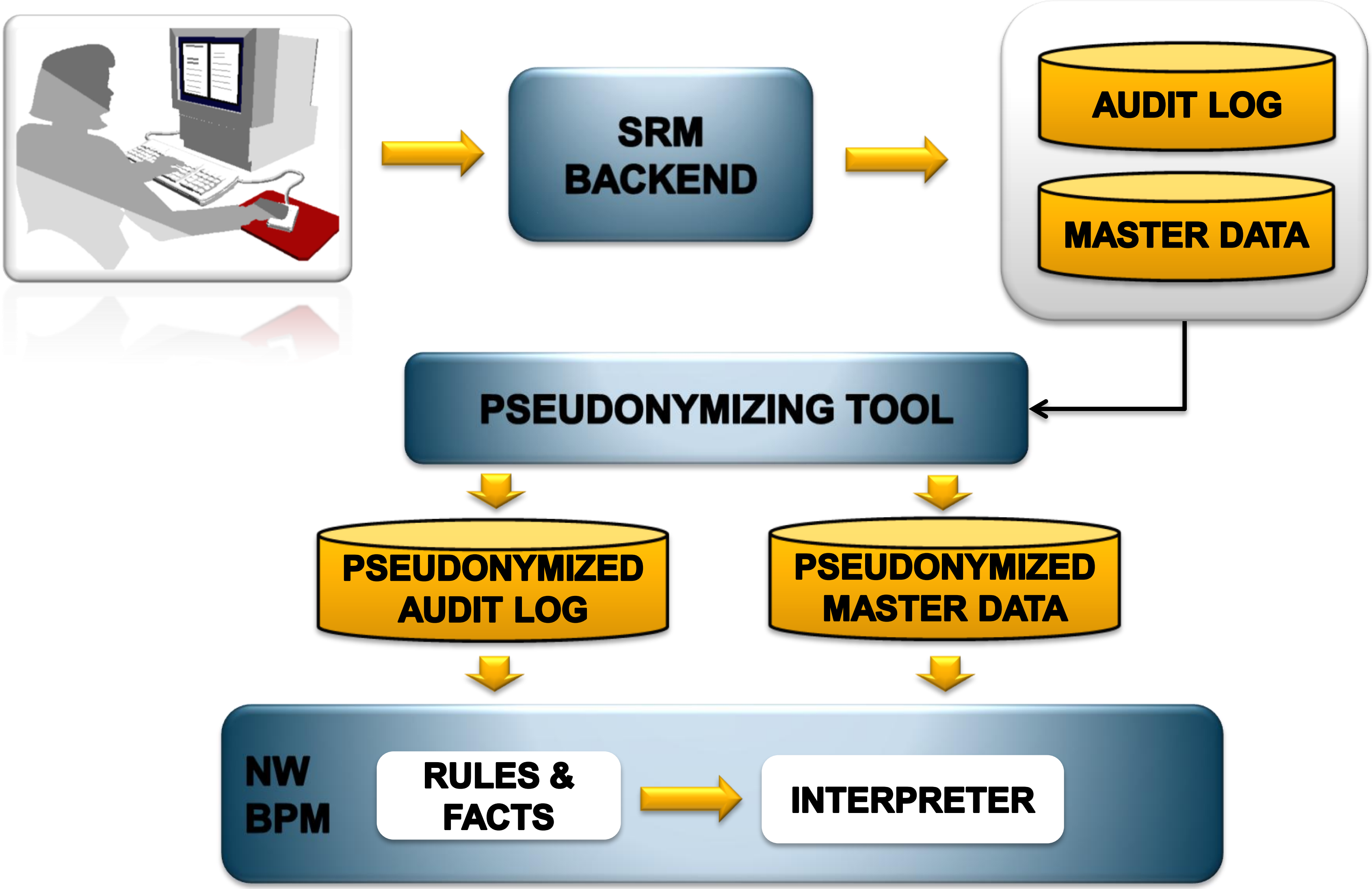
PSEUDONYMIZED AUDIT LOG

PSEUDONYMIZED MASTER DATA

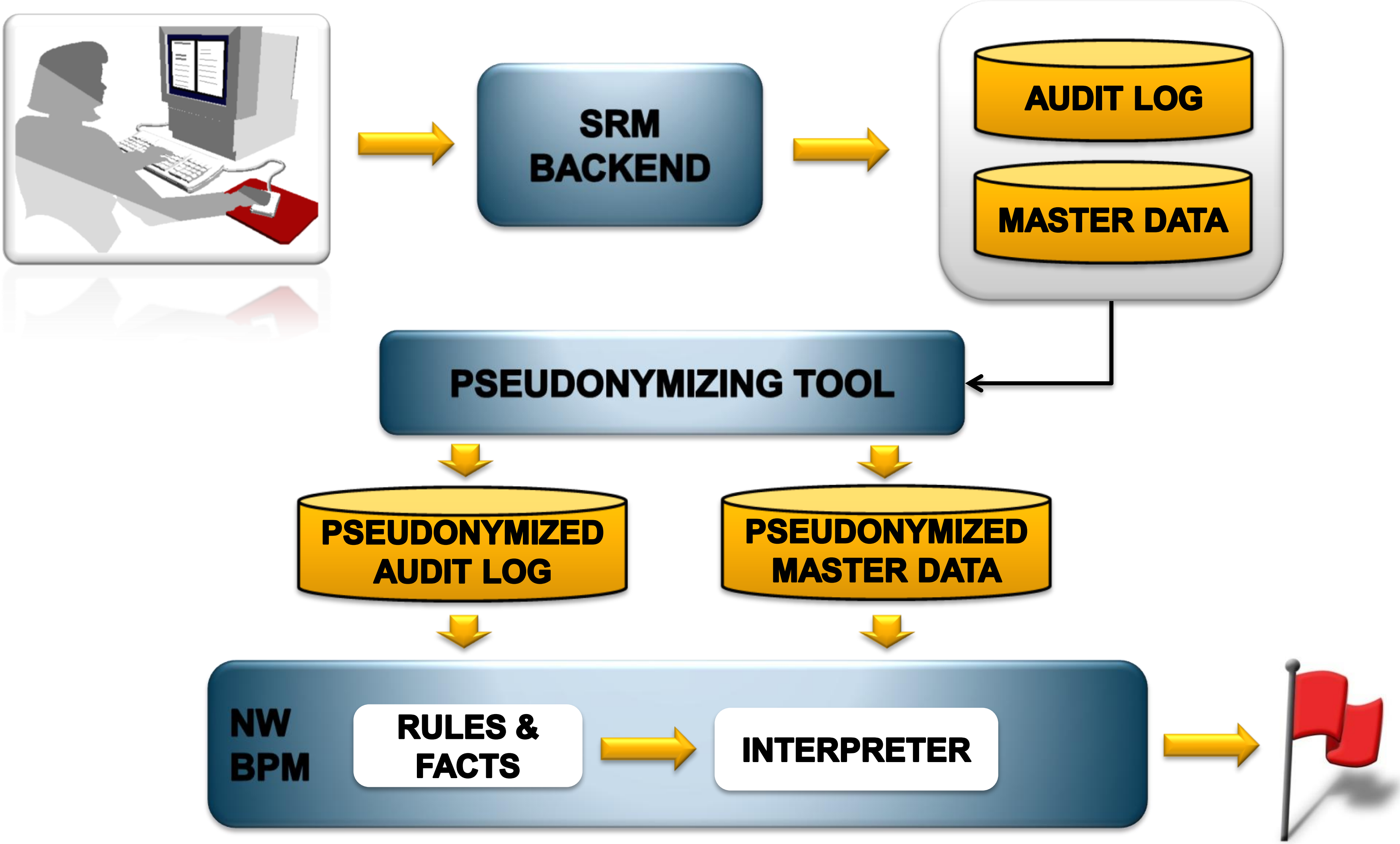
Solution Approach & Technology



Solution Approach & Technology



Solution Approach & Technology



SRM BACKEND

AUDIT LOG

MASTER DATA

PSEUDONYMIZING TOOL

PSEUDONYMIZED AUDIT LOG

PSEUDONYMIZED MASTER DATA

NW BPM

RULES & FACTS

INTERPRETER

WANF & Meier's Semantic Model
- Investigation Outcome -

Aspect		Characteristic	WANF
Event Pattern	**Type and Order**	Sequence	✓
		Disjunction	✓
		Conjunction	✓
		Simultaneity	✗
		Negation	✓
	Repetition	Exactly	✓
		At least	✓
		At most	✓
	Continuity	Continous	✓
		Non-Continous	✓
	Concurrency	Overlapping	✓
		Non-Overlapping	✓
	Context Condition	Inter-Event Condition	✓
		Intra-Event Condition	✓
Step Instance Selection		First	✓
		Last	✗
		All	✗
Step Instance Consumption		Consuming	✓
		Non-Consuming	✓

Agenda

1. Customer Situation and Challenges

2. Solution Approach & Technology

3. **Benefits, Best practices & Use Cases**

4. Conclusion

SAP RESEARCH

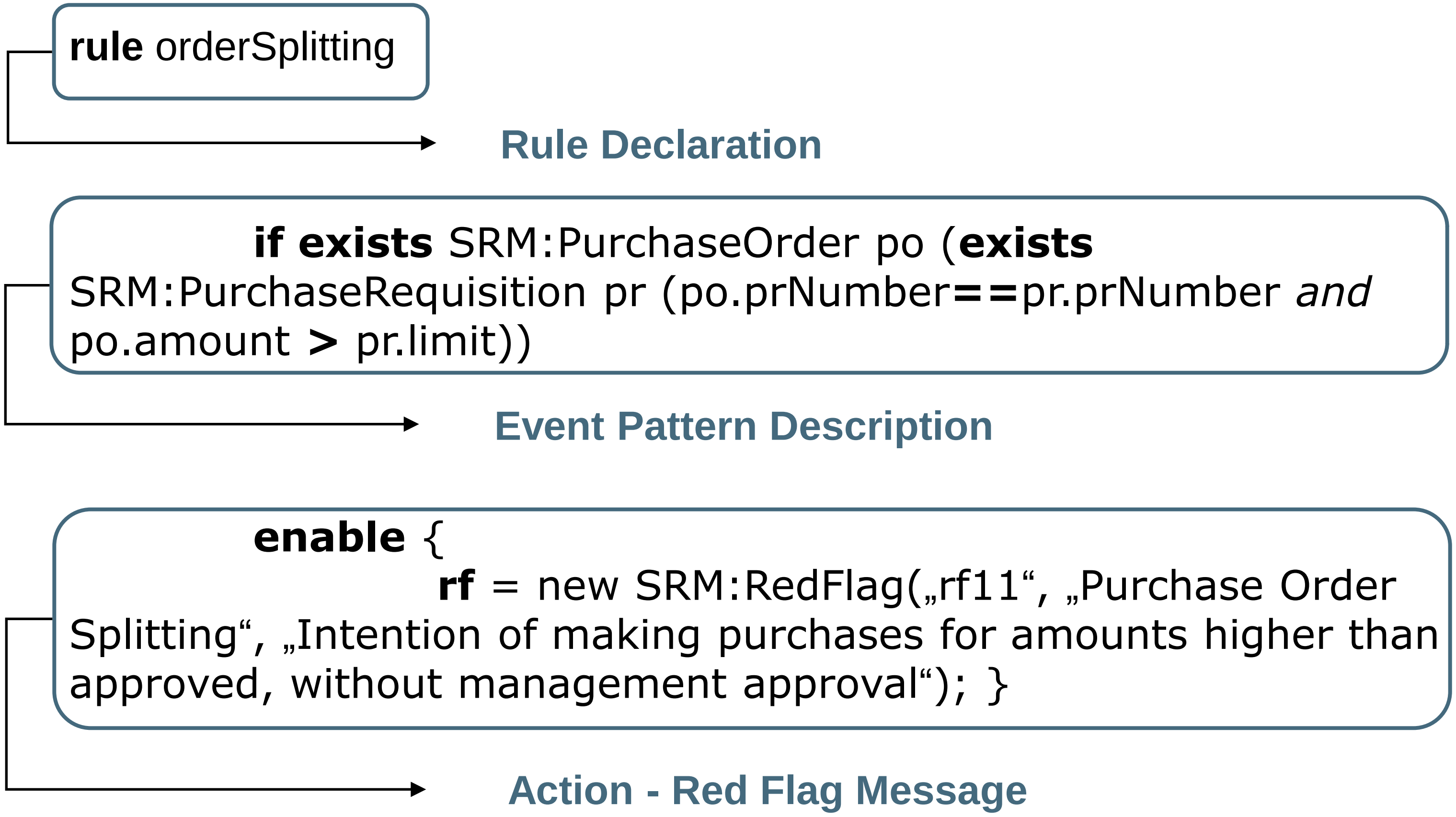
Benefits, Best practices & Use Cases
Practical example

Case Description - „Order Splitting“:

- An employer intends to make purchases higher than the imposed limit without supplementary approval.
- Purchasers split up large orders to qualify them within the limit imposed
- Purchase Requisitions issued by the same employer, approved by the same person, involving the same vendor, with the same identification numbers.

Benefits, Best practices & Use Cases

WANF Rule – „Order Splitting“:



```
rule orderSplitting
```

Rule Declaration

```
            if exists SRM:PurchaseOrder po (exists
SRM:PurchaseRequisition pr (po.prNumber==pr.prNumber and
po.amount > pr.limit))
```

Event Pattern Description

```
            enable {
                        rf = new SRM:RedFlag(„rf11“, „Purchase Order
Splitting“, „Intention of making purchases for amounts higher than
approved, without management approval“); }
```

Action - Red Flag Message

Benefits, Best practices & Use Cases

Sample Input Data

Purchase Requisition

PR Number: 23655384

Total Value: 8 500

Currency: €

Limit: 10 000

Recipient: ID652798

Purchase Order

PO Number: 745126

PR Number: 23655384

Net Price: 17 000

Currency: €

Recipient: ID652798

Benefits, Best practices & Use Cases

Sample Output Data

Intrusion Detection Message Exchange Format – „Order Splitting“:

Red Flag: RF-11-1-PO		
Analyzer	ID	rule OrderSplitting
	Name	Rule for detecting Purchase „Order Splitting“
Classification	ID	**rf11**
	Description	Multiple Purchase Requisitions made by the same employee which refer to the same Purchase Order number but sum up to an amount of money ordered higher than approved
Source	Node Name	Audit Log
	Process ID	PurchaseOrder.ident
	Process Name	Purchase Order
	User ID	Identification Number of the employee who sent the Purchase Order: employee.ident
	User Name	Name of the employee who sent the Purchase Order: employee.name
Assessment	Impact	Intention of making purchases higher than approved, without seeking management approval
	Actions Taken	- Notification sent - Mark the employee who created the Purchase Order as fraudulent
	Confidence	High – It is clear indication of the fact that the employee attempts to make purchases which exceed the allowed purchasing amount

Agenda

1. Customer Situation and Challenges
2. Solution Approach & Technology
3. Benefits, Best practices & Use Cases
4. **Conclusion**

Conclusion

Current Status:

- **Investigation** of Meier´s Semantic Model
- **Documentation** of the expressiveness of the language used for expressing event patterns *WANF*
- **Research** of the most relevant fraud scenarios
- **Translation** of the reference fraud scenarios into *WANF*

Future Work:

- **Implementation** of I/O Adapters
- **Pseudonymization** of sensitive data for compliance with the Federal Data Protection Act

Thank you!