

# A Security-Aware Cloud-Based Business Process Modeling and Execution Environment

Julio Damasceno, Fernando Lins, Robson Medeiros, Bruno Silva, Andre Souza, David Aragão, Paulo Maciel, Nelson Rosa

**Federal University of Pernambuco, Brazil**

Bryan Stephenson, Jun Li, Eric Wu

**HP Labs Palo Alto**



UNIVERSIDADE  
FEDERAL  
DE PERNAMBUCO



[Cln.ufpe.br](http://Cln.ufpe.br)

# Problem

- **Many stakeholders from different organizations are needed to create business processes:**
  - Business domain experts define the process
  - Security experts specify security requirements
  - Developers create the service composition
  - IT Operations deploys the service composition
- **This is difficult and time-consuming:**
  - Increasingly, multiple companies are involved in the definition and execution of business processes
  - No streamlined development environment to allow these stakeholders to work collaboratively
  - Cannot quickly create, evolve, and test business processes

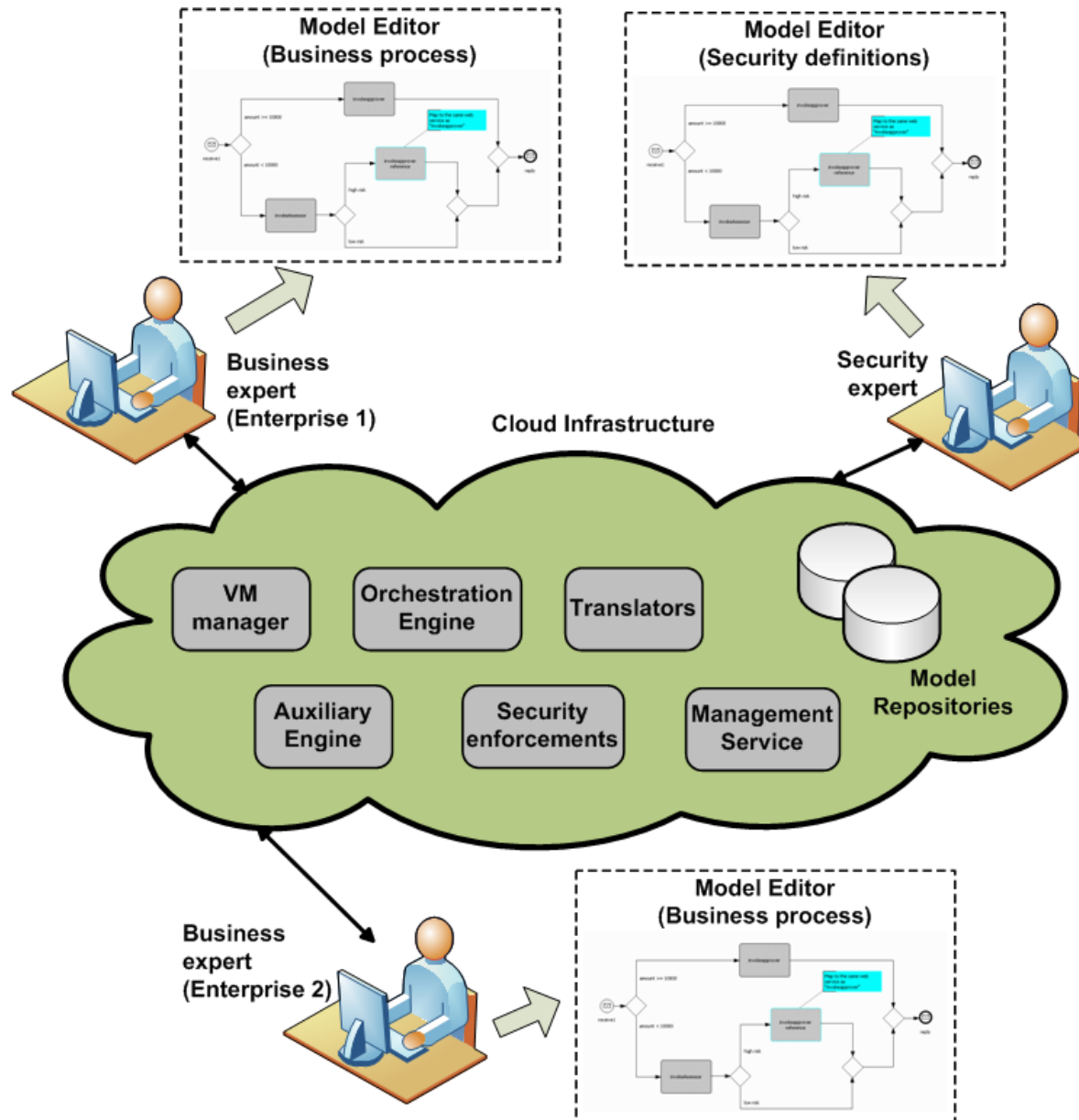
# Solution

- **A shared business process modeling workspace**
  - Stakeholders from different organizations work together
  - Supports definition of a business process model (BPM)
  - Supports definition of security requirements
- **A business process execution environment**
  - Allows a business process to be easily tested and run
  - Translates BPM into an executable service composition
  - Automatically deploys into a shared virtual machine pool
  - Enables rapid refinement

# Challenges

- **How to create a comprehensive and holistic framework to foster cross-enterprise collaboration?**
- **How to enable rapid iteration and testing?**
- **How to handle security requirements?**
  - How to express security requirements?
  - How to integrate them into the business process?
  - How to map them into enforceable security mechanisms?
  - How to support them at runtime?

# Our Solution::Overview



# Mapping the Problem to Open Cirrus

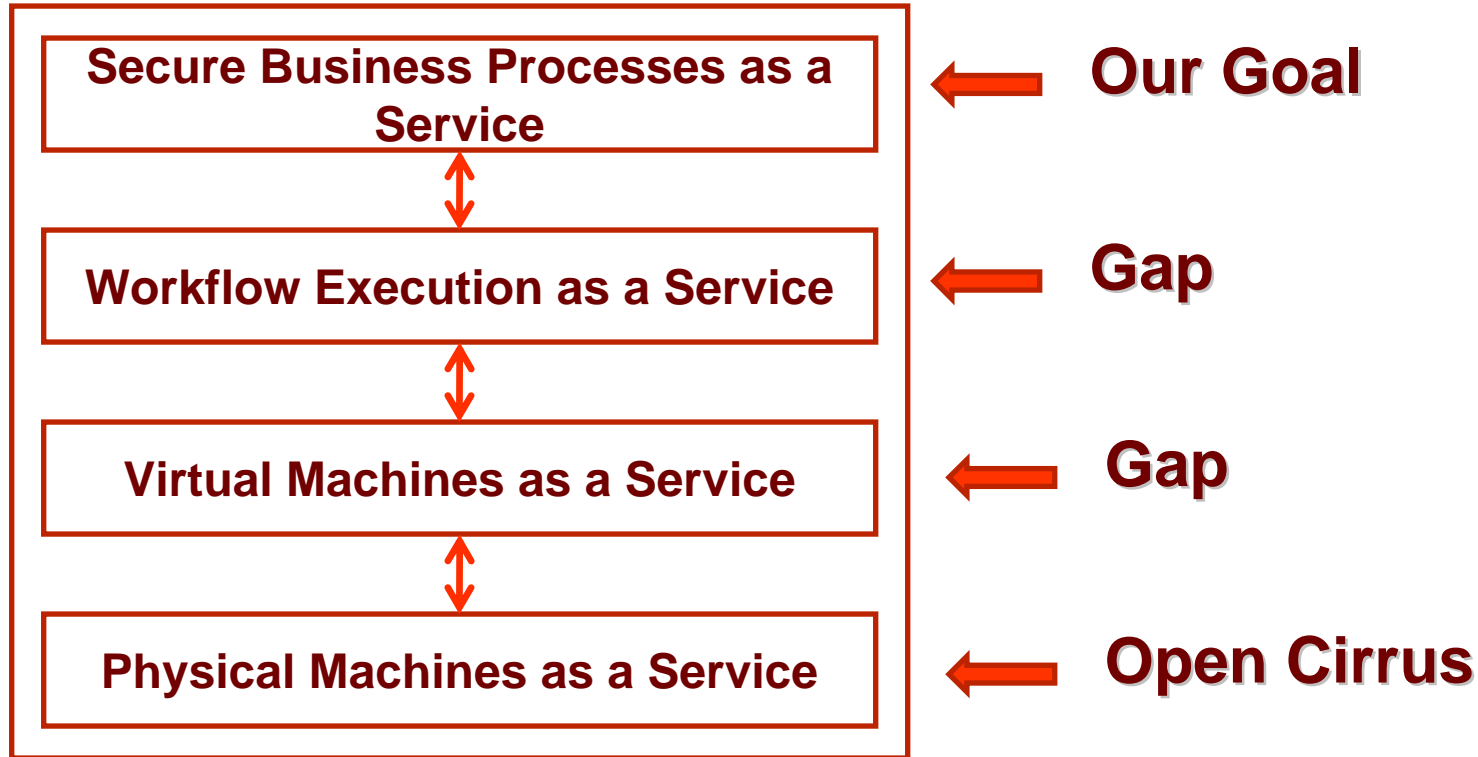
**Secure Business Processes as a Service**

← **Our Goal**

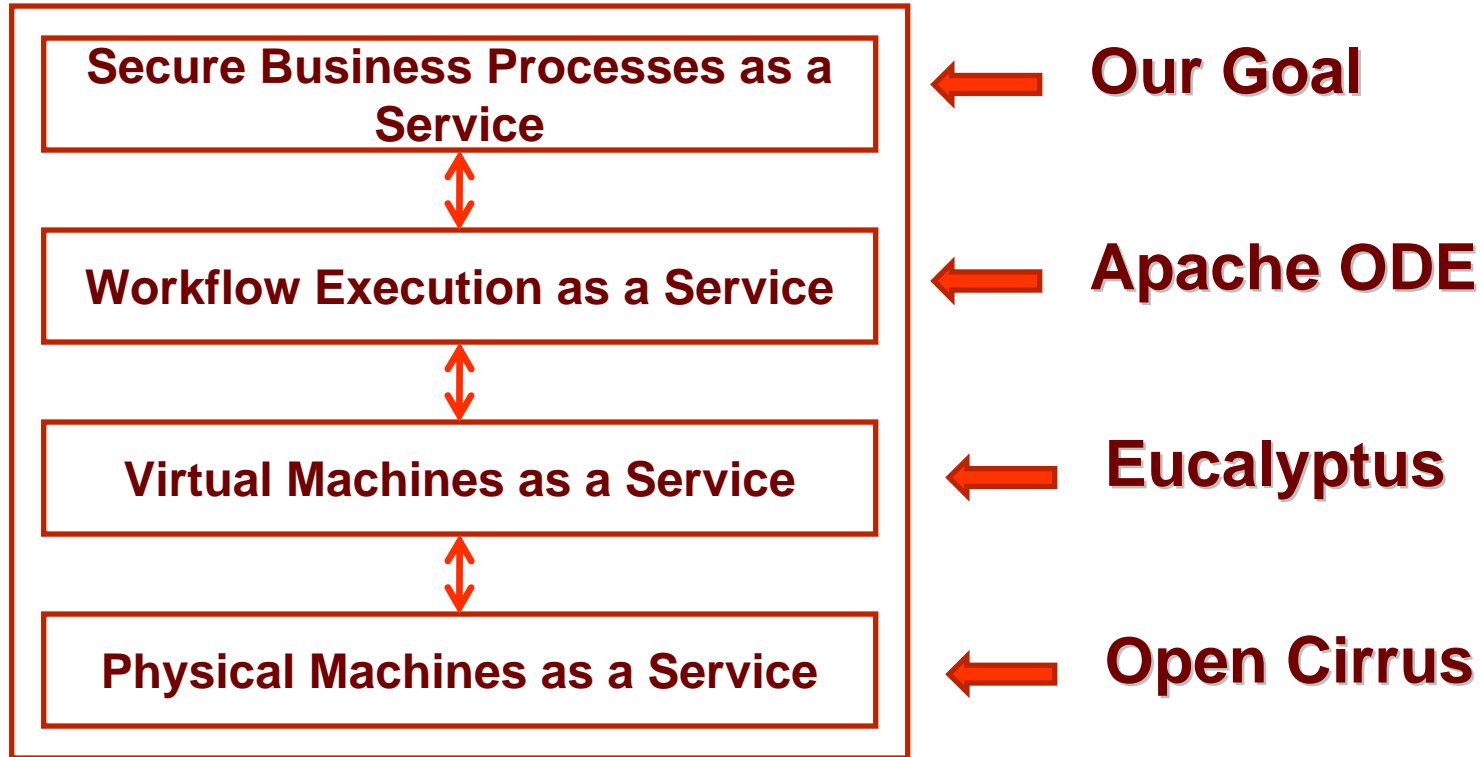
**Physical Machines as a Service**

← **Open Cirrus**

# Mapping the Problem to Open Cirrus::Gaps



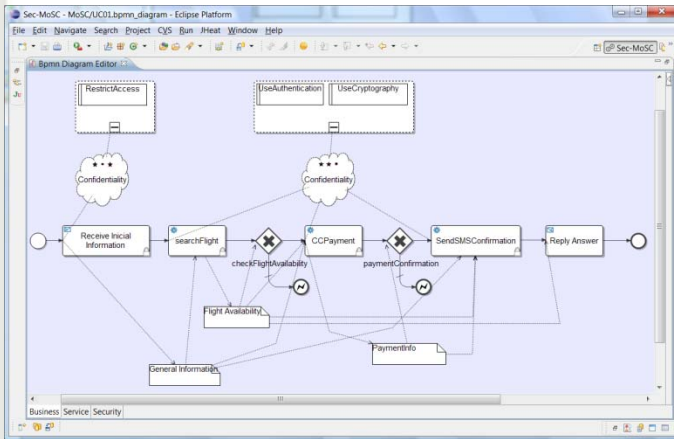
# Mapping the Problem to Open Cirrus::Solution





# Our Solution::Overview

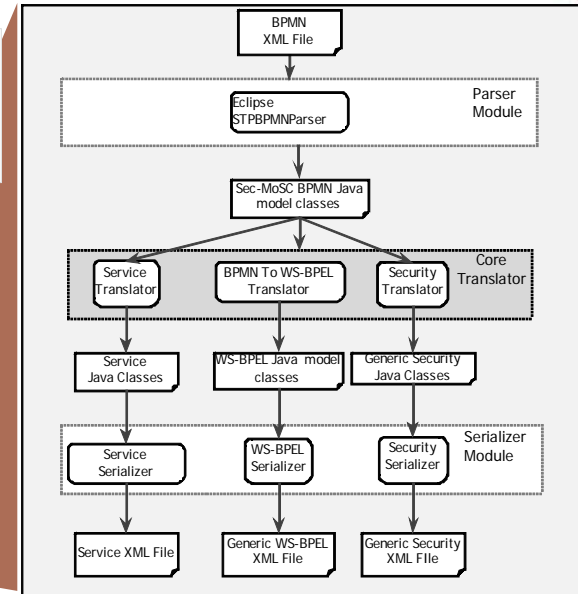
## Design support



## Tool Support

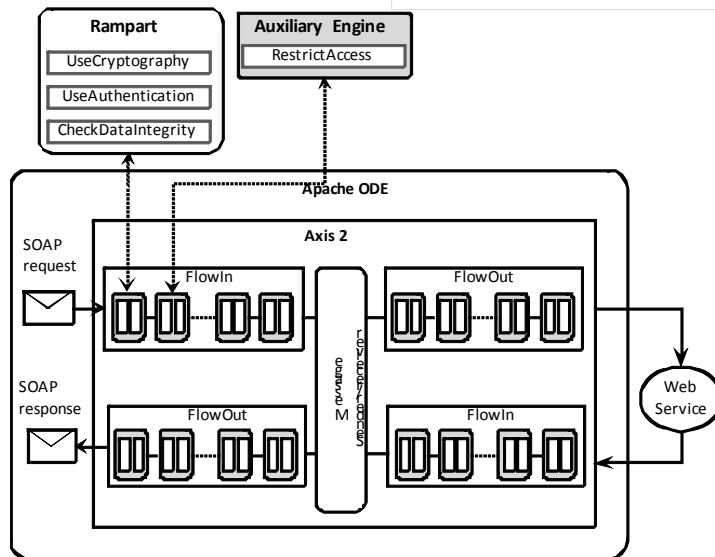
- ✓ BPMN
- ✓ Security annotations
- ✓ Views

## Translation support



## Runtime support

- ✓ BPMN to WS-BPEL translation
- ✓ Security requirement translation
- ✓ MDA principles



- ✓ Deploy into Open Cirrus
- ✓ Interact with orchestration engines at runtime
- ✓ Enforce security requirements

# Our Solution::Overview

## ■ Set of abstractions

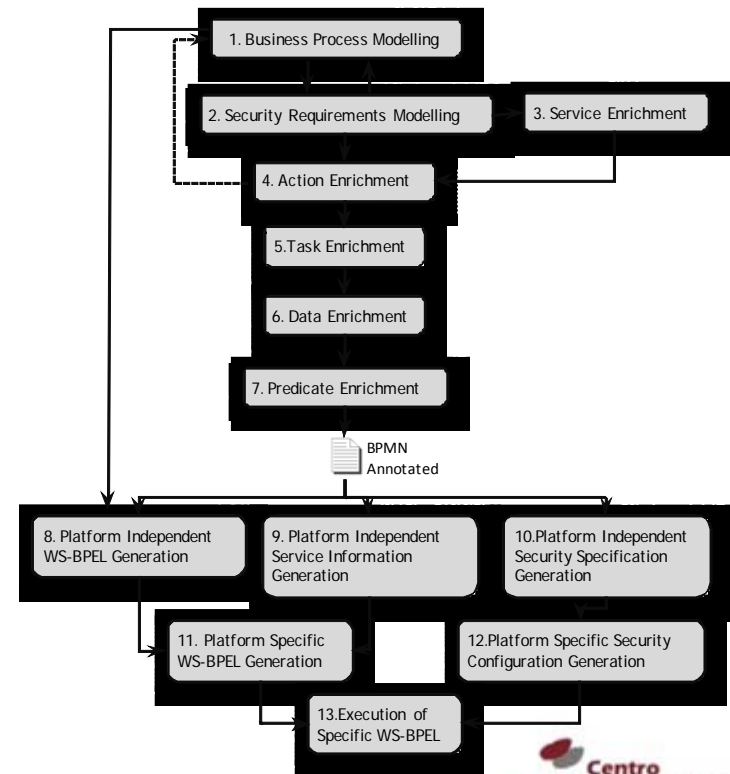
- To express and refine security requirements



Abstraction	Notation
NF-Attribute	
NF-Statement	 Low      Medium      High      Customised
NF-Action	
NF-Property	Encryption Type <input type="text" value="Asymmetric"/>
NF-Group	
NF-Bind	-----

## ■ Methodology

- Guides the treatment of security requirements from business process to runtime



# Our Solution::Abstractions

## ■ **NF-Attribute**

- Models non-functional characteristics that either can be precisely measured or not quantified
- Two kinds: primitive, composite
- e.g., *Confidentiality*

## ■ **NF-Statement**

- High-level constraint described in terms of levels (High, Medium, Low, Customized)
- e.g., *High Confidentiality*

## ■ **NF-Action**

- Models either any software aspects or any hardware characteristics that realise the NF-Attribute
- e.g., *UseCryptography*

# Our Solution::Abstractions

## ■ **NF-Group**

- It enables us to group NF-Actions in such way that facilitates their reuse
- e.g., *UseCryptography, UseAuthentication*

## ■ **NF-Property**

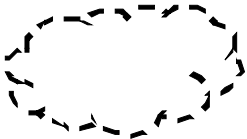
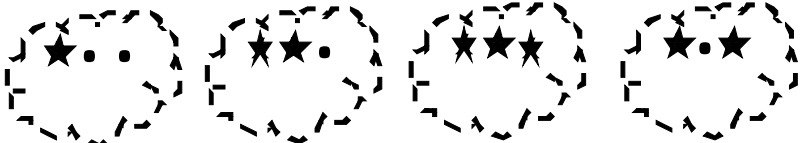




- It is associated to NF-Actions and allows more detailed definition of an NF-Action
- e.g., *encryption type*

## ■ **NF-Bind**

- It captures the integration of these NF-\* abstractions with BPMN (tasks/data objects)
- e.g., *High Confidentiality* associated to BPMN Task “*Credit Card Payment*”

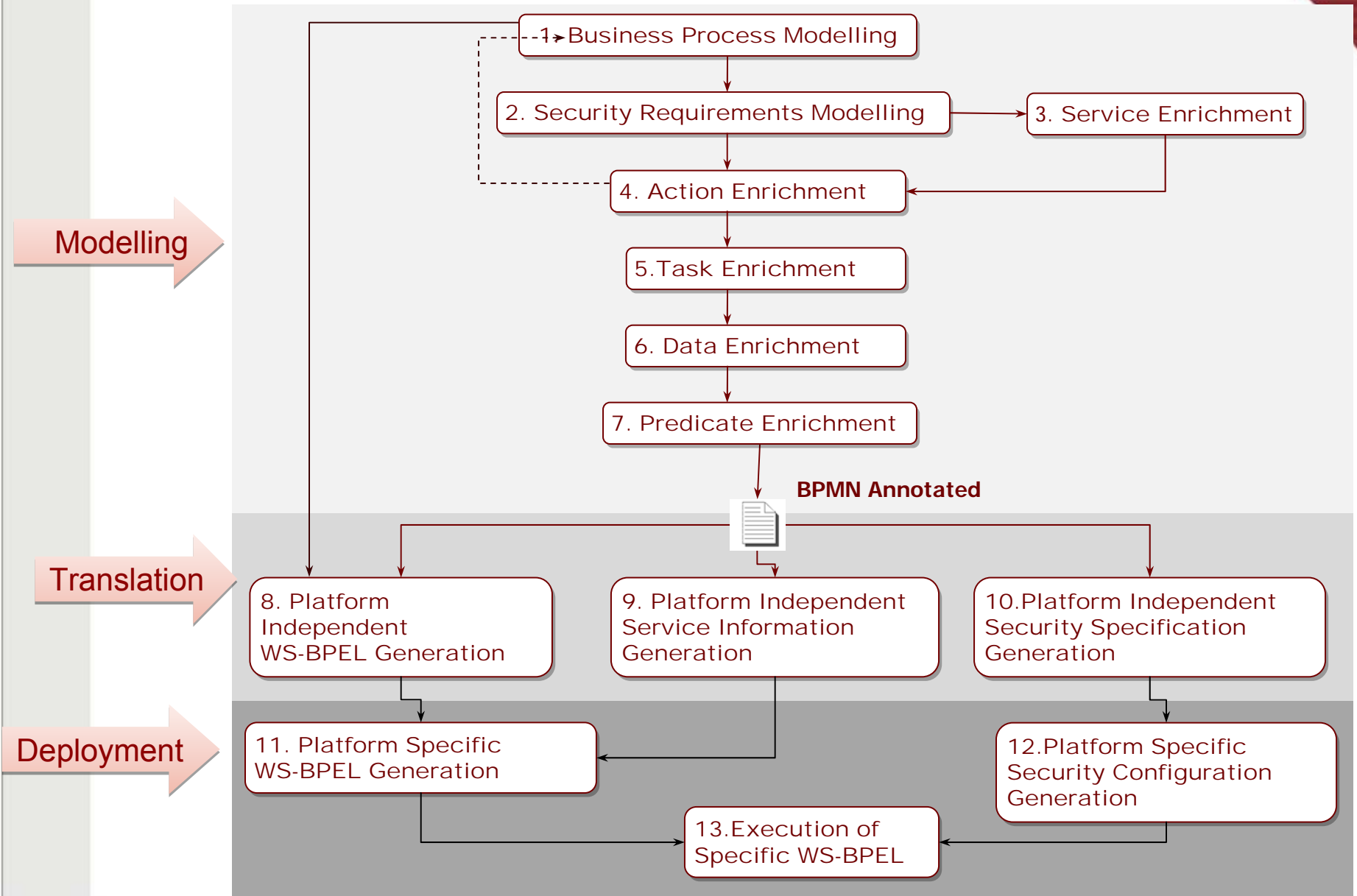
# Our Solution::Abstractions Graphical Notation

---

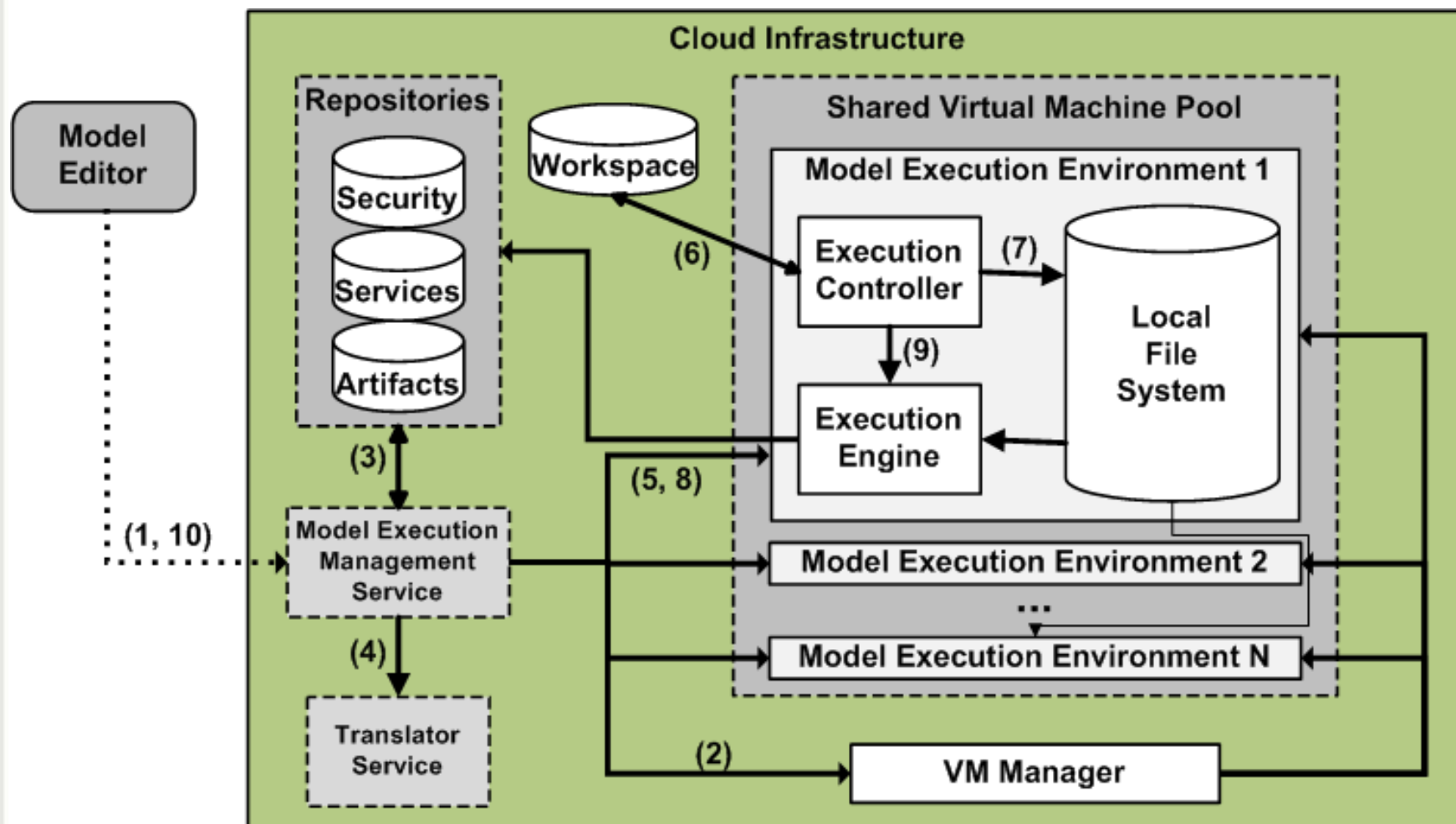
Abstraction	Notation
NF-Attribute	
NF-Statement	 <p>Low      Medium      High      Customised</p>
NF-Action	
NF-Property	
NF-Group	
NF-Bind	

---

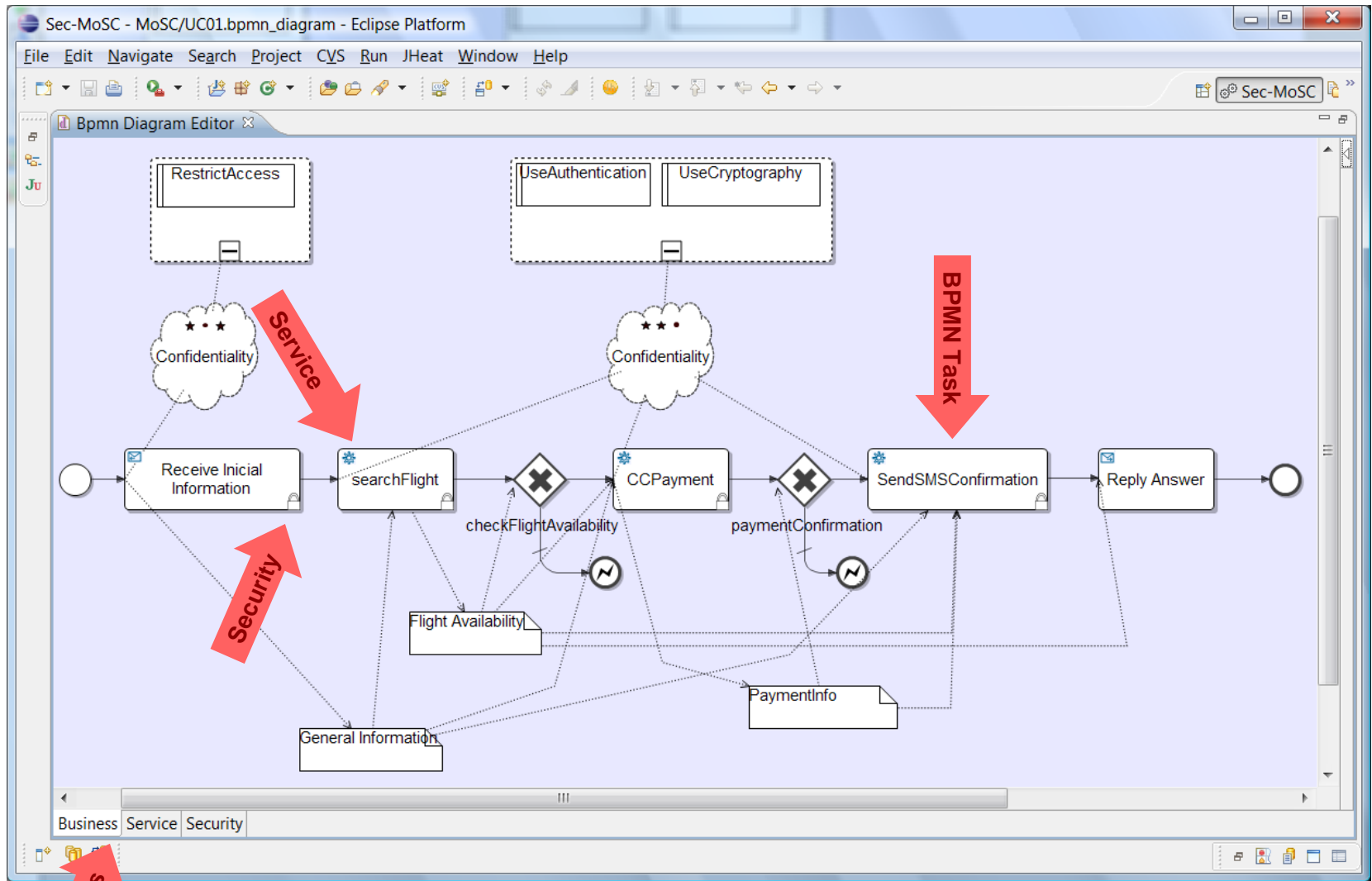
# Our Solution::Methodology



# Our Solution::Architecture



# Our Solution::Tools::Editor Business View



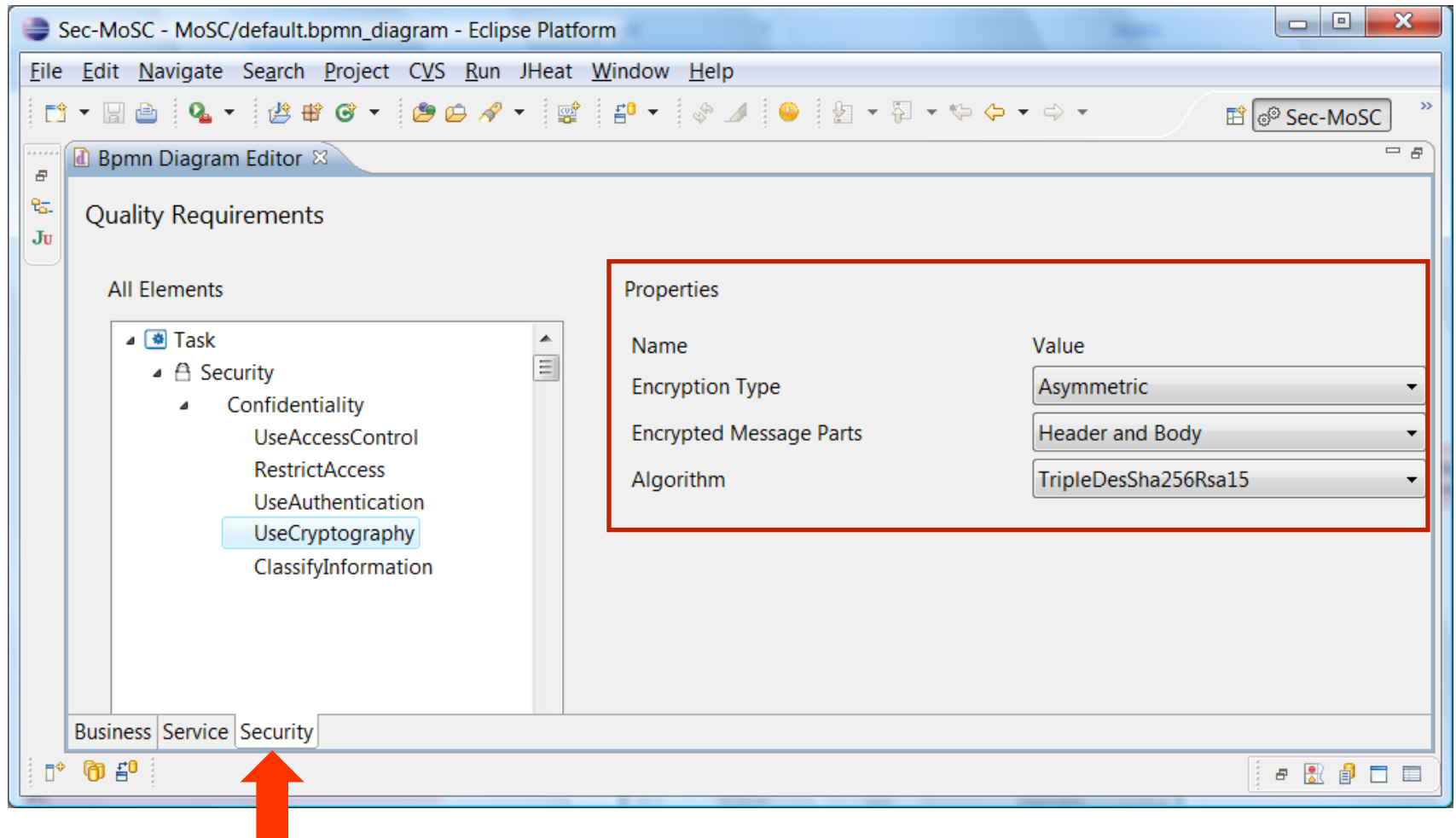


# Our Solution::Tools::Editor Service View

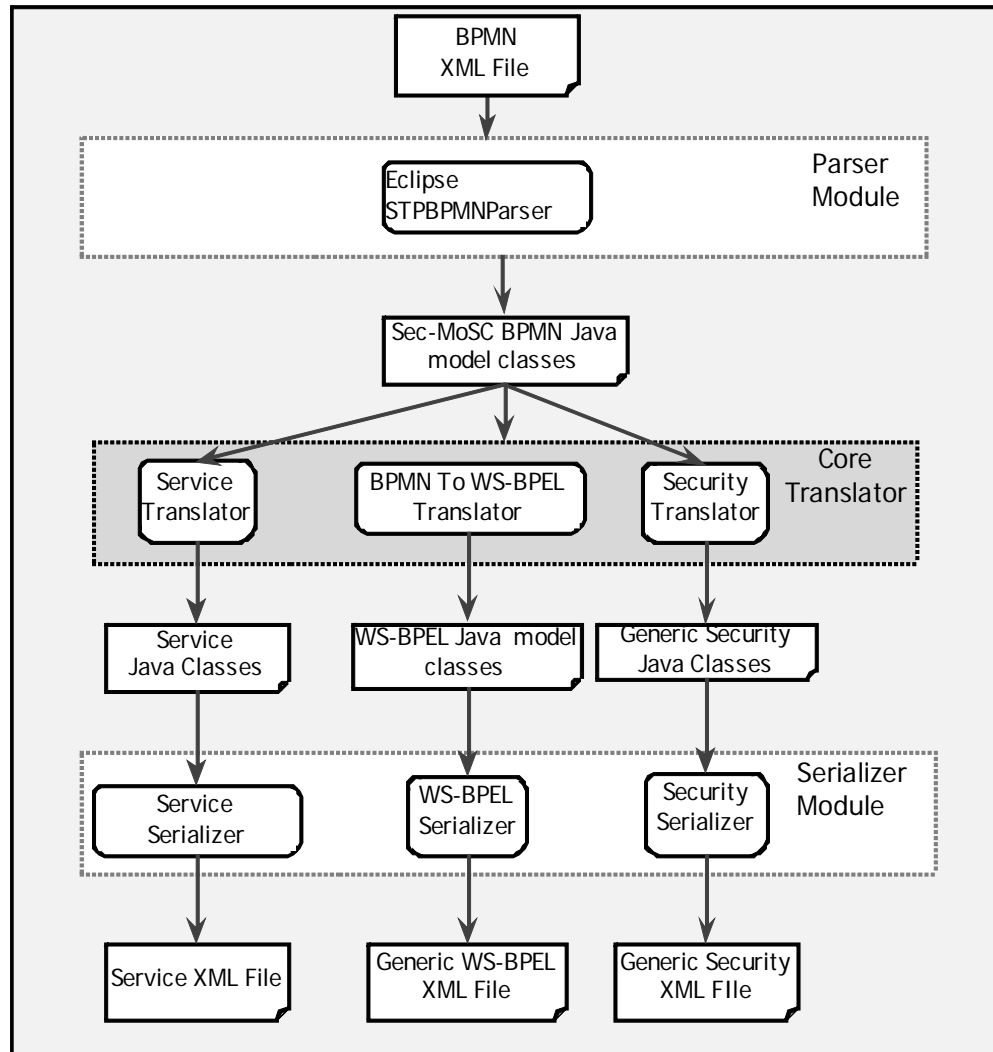
The screenshot shows the Eclipse Platform interface for editing a BPMN diagram. The main window is titled "Sec-MoS - MoSC/UC01.bpmn\_diagram - Eclipse Platform". The "Services" view is active, showing a tree of elements under "Service". The "searchFlight" service is selected, and its properties are displayed in the "Properties" tab. A red box highlights the "Properties" tab and its content. A red arrow points to the "Service" tab in the bottom navigation bar.

Property	Value
Task Type	Service
URI	http://172.17.110.210:6060/Sec-MoS-GDS-Service/services/SecMoSC_GD...
Service Name	SecMoSC_GDS
Service Description	WS Air
Business Type	Air Company
Operation Name	searchPrices
Operation Description	searchPrices
Organization Name	WS Air
Target Namespace	http://gds.hp.ufpe.cin.br
Port Name	SecMoSC_GDSHttpSoap11Endpoint
Port Type	SecMoSC_GDSPortType
Port Namespace	http://gds.hp.ufpe.cin.br
Partner Link Type	SecMoSC_GDSPartnerLinkType
Partner Role	gdsCompany

# Our Solution::Tools::Editor Security View

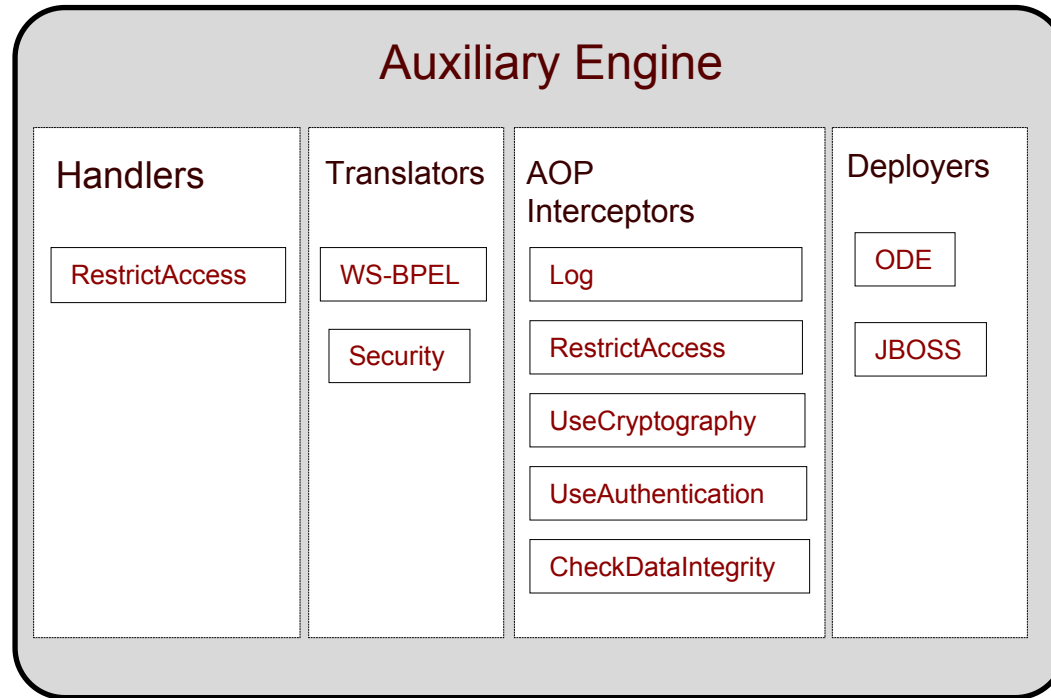


# Our Solution::Tools::Translator



- BPMN to WS-BPEL translation (mapping rules)
- Translation of class models (not XML representations)
- Core translator decoupled from a particular XML representation of BPMN
- Automatic generation of security configurations

# Our Solution::Tools::Auxiliary Engine



► Support provided by orchestration engines to enforce security requirements varies

**So, the Auxiliary Engine ...**

- Needs to provide either full or partial support to security enforcement
- Serves as a uniform interface to enforce security requirements
- Currently integrated with Apache ODE, JBOSS

# Running Example:: Virtual Travel Agency

## ■ VTA

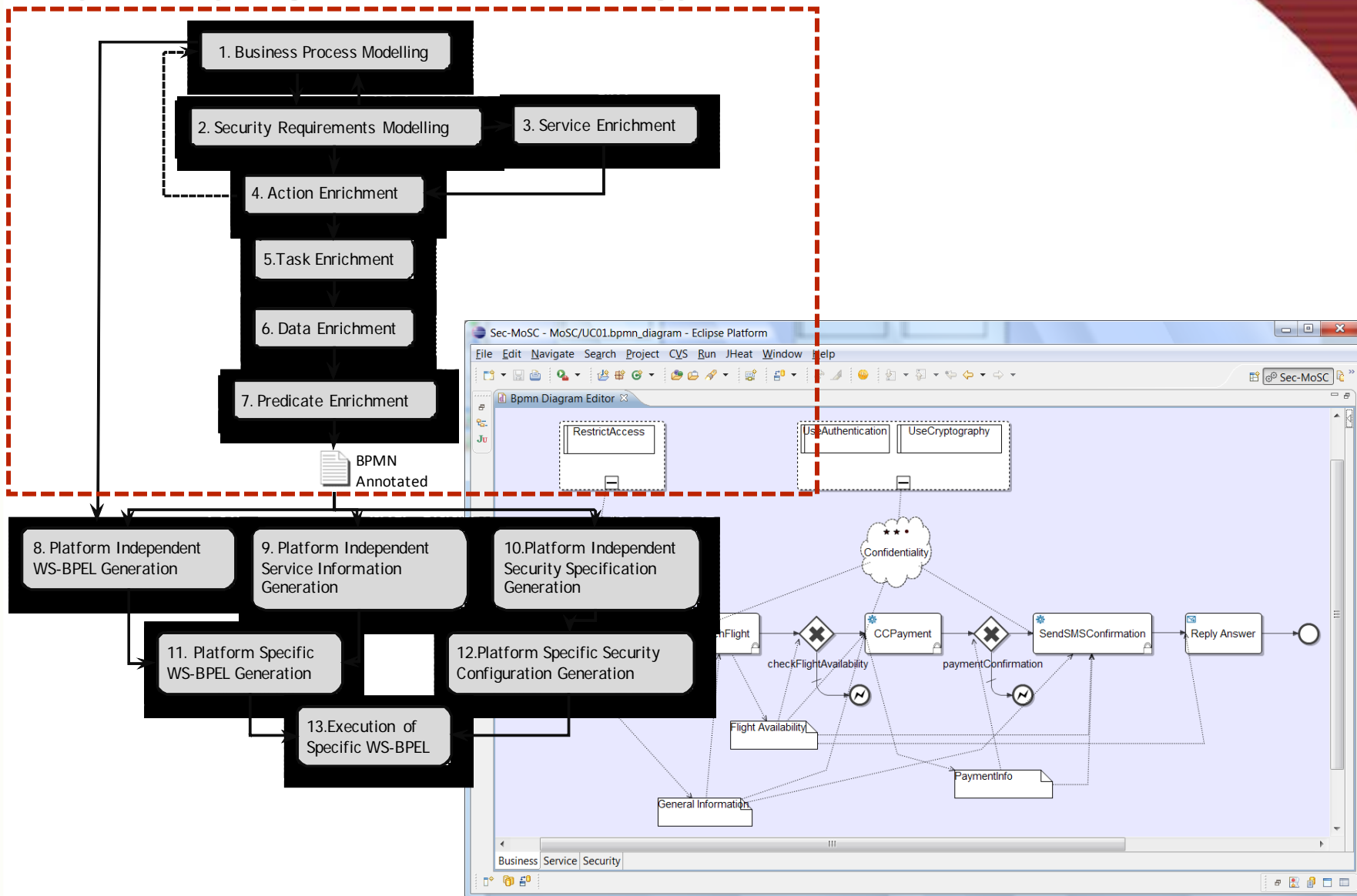
- Internet portal
- Companies, government services and end-users interested in travel
- Runs through the composition of services available in the Internet

## ■ **Customers interact with VTA for service usage, payment and non-computational assets**

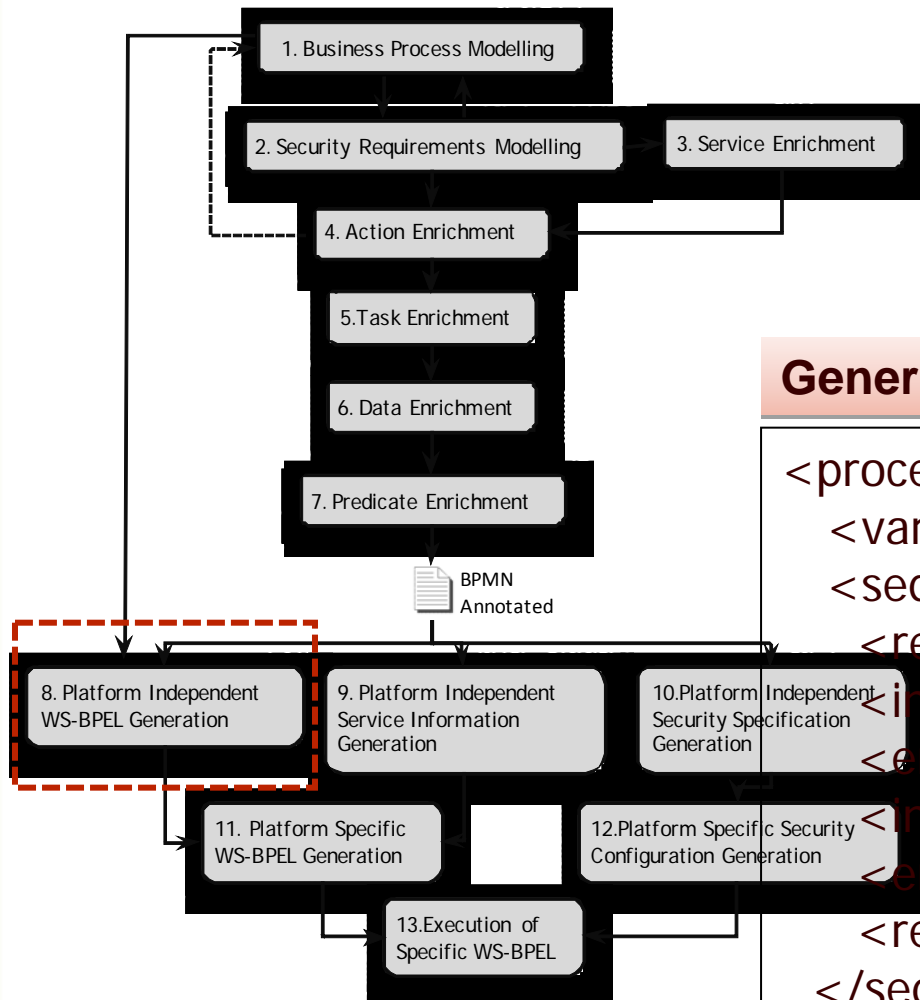
## ■ **Security requirements**

- Encrypt credit card information in all communications
- VTA and its partners need valid digital signatures
- Authentication mechanisms must be used in all interactions among web services
- Log all operations for auditing purposes
- VTA / partners restrict access to specific IP addresses / domains

# By applying the methodology...



# By applying the methodology...

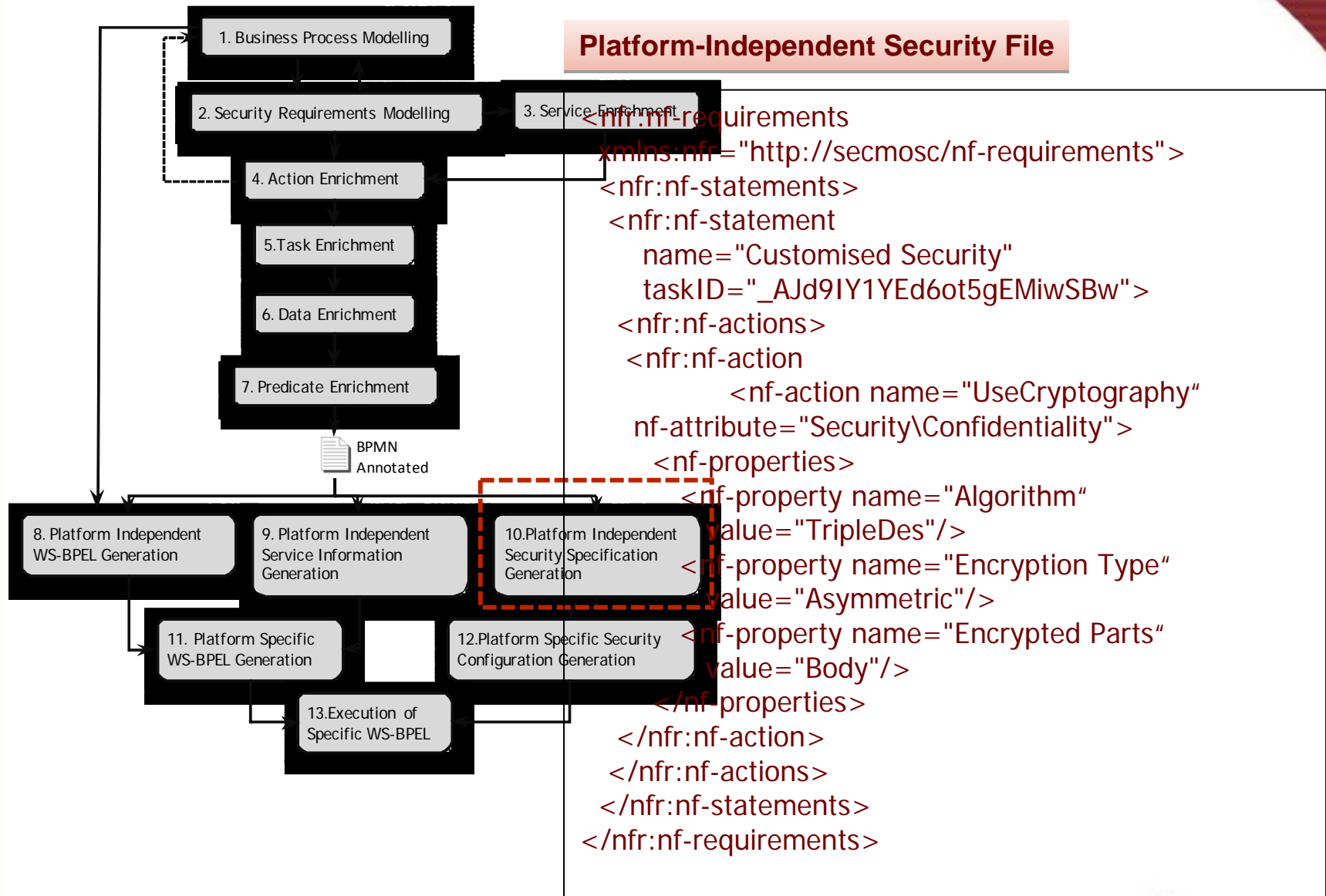


## Generic WS-BPEL

```

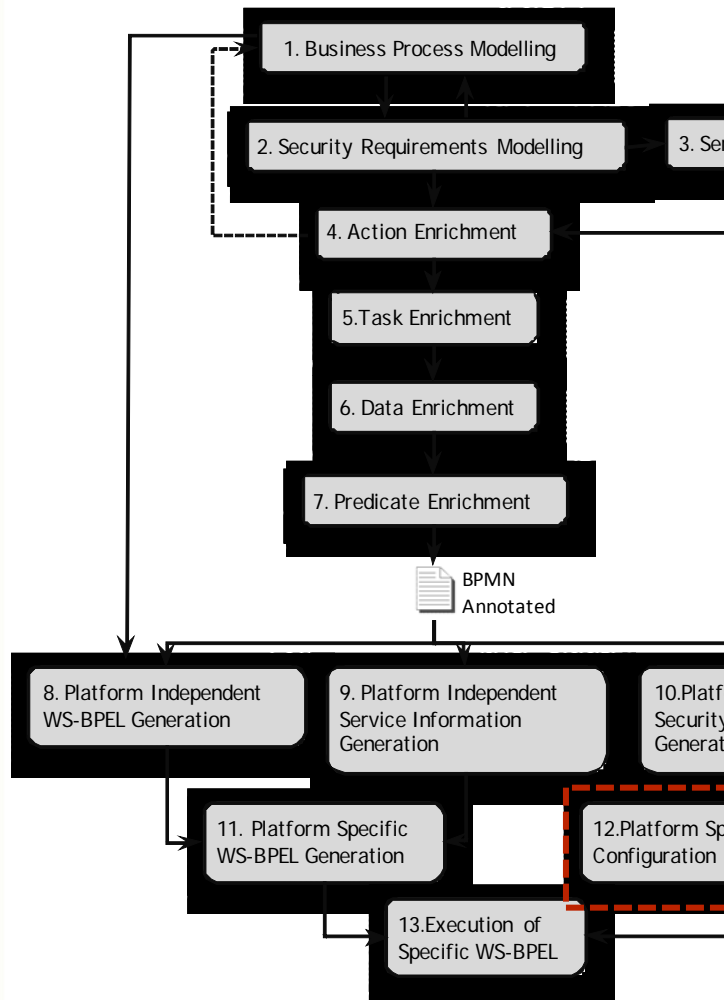
<process name="VTAProcess">
  <variables/>
  <sequence name="main">
    <receive name="_ssld1"/>
    <invoke name="_ssld2"/>
    <empty/>
    <invoke name="_ssld3"/>
    <empty/>
    <reply name="_ssld4"/>
  </sequence>
</process>
  
```

# By applying the methodology...





# By applying the methodology...



## Platform-Specific Security File (JBoss)

```
<jboss-ws-security>
  <key-store-file>
    repository/engine.ks
  </key-store-file>
  <key-store-type>
    Jks
  </key-store-type>
  <key-store-password>
    engineKS
  </key-store-password>
  <config>
    <timestamp ttl="300" />
    <encrypt type="x509v3" alias="payment"
      algorithm="tripledes"/>
    <requires>
      <encryption />
    </requires>
  </config>
</jboss-ws-security>
```

# Open Cirrus Wish List

- **Save and restore the disk images we created**
- **Reserve and easily use machines from more than one Open Cirrus site**
- **Better documentation of Open Cirrus**
- **Community document repository**
- **Remote power-cycle to recover hung machines**
- **Ability to install an OS on the machine remotely**
- **Ability to see consoles of machines**
- **Services above the infrastructure level**

# Conclusion & Future Work

## ■ Contributions

- Novel holistic model-driven approach
- Enables cross-enterprise collaboration of business experts, security experts and service composition developers
- Toolset supports business process and security requirement modelling, automatic code generation, and cloud deployment

## ■ Future Work

- Extend the binding of security requirements to other BPMN element types beyond tasks, task groups, and data objects
- Define and realize additional security requirements
- Monitor security requirements at runtime