

# Mobile Adventure



Copyright © 2008 by DoCoMo  
Communications Laboratories  
Europe GmbH All rights reserved



## Security-by-Contract for Software and Services for Mobile Systems

Specific Targeted Research Project 027004

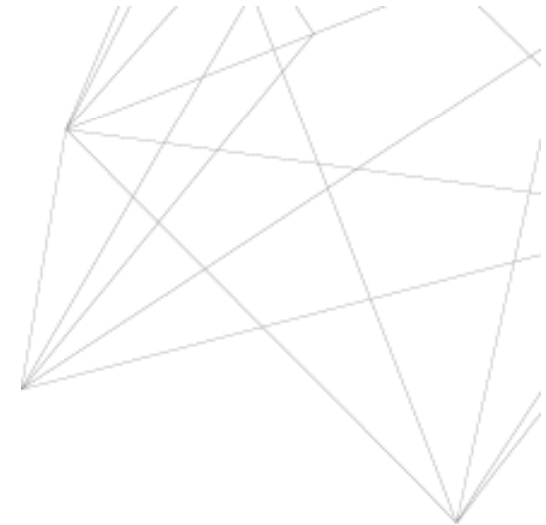
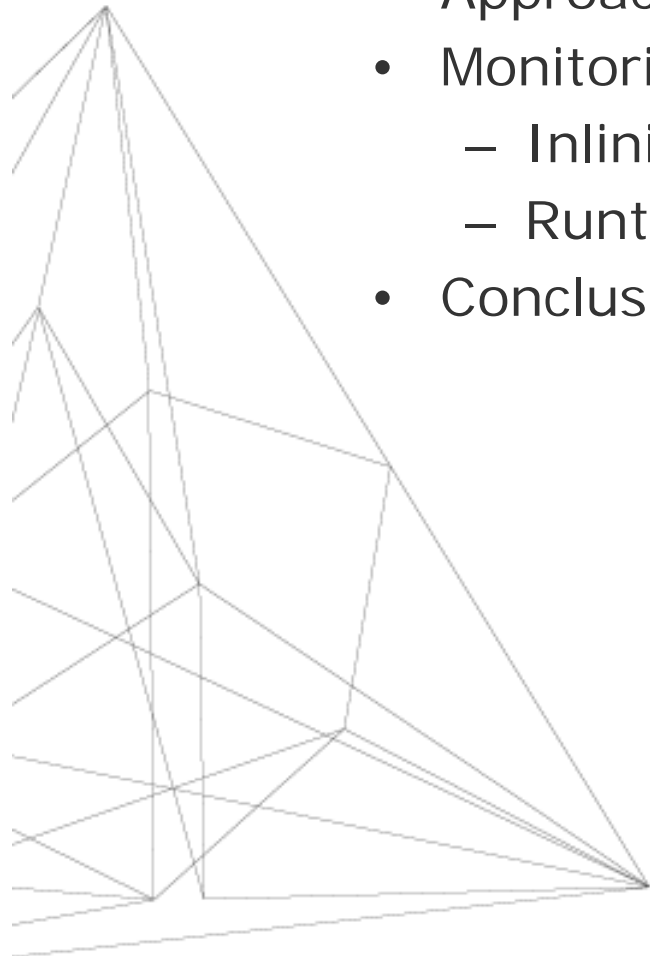
Thomas Walter, DoCoMo Euro-Labs

Smart and Secure Services Research  
and partners from the S<sup>3</sup>MS project



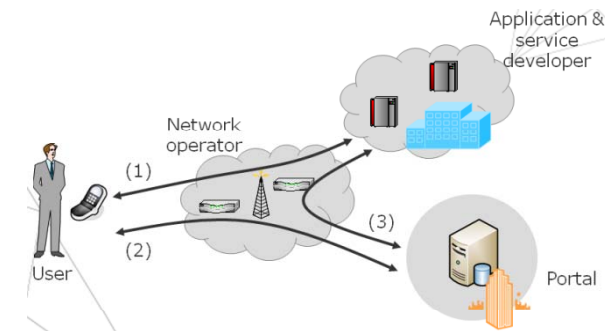
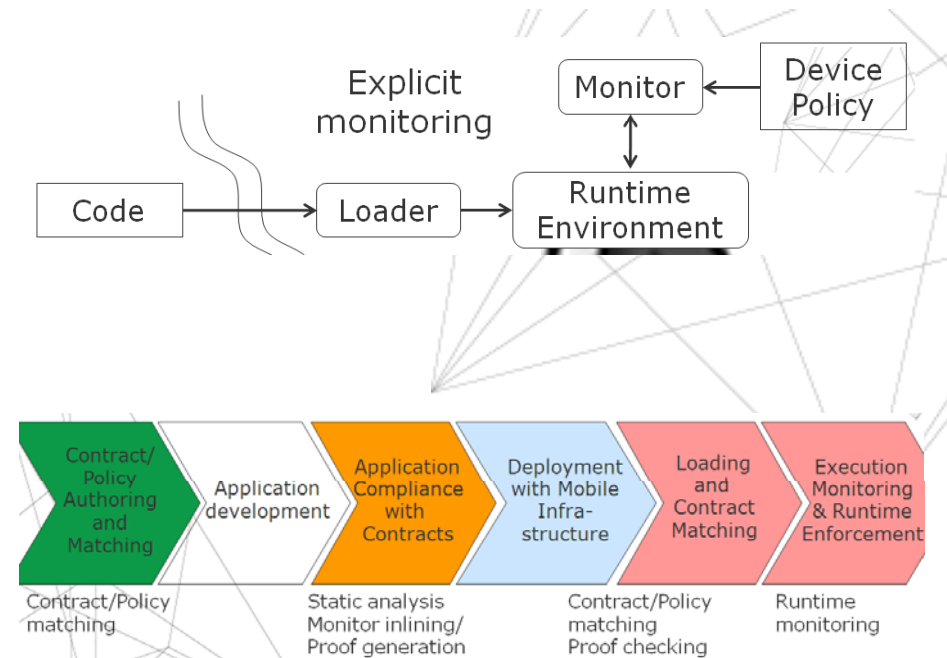
# Mobile Adventure Content

- Overview
- Goal
- Approach
- Monitoring
  - Inlining
  - Runtime monitoring
- Conclusion



# Mobile Adventure Overview

- Provide **enforcement technologies** to guarantee secure and safe execution of downloaded applications on user's mobile terminal.
- Enforcement technologies that are applicable along the **software lifecycle** from development to deployment and execution.
- Allow all **stakeholders** (users, developers and mobile network operators) to express their requirements and constraints by policies.



- Providing the infrastructure for downloading “trust-worthy” software for the benefit of all stakeholders:

- User

- Controlling the behaviour of software on his mobile system.

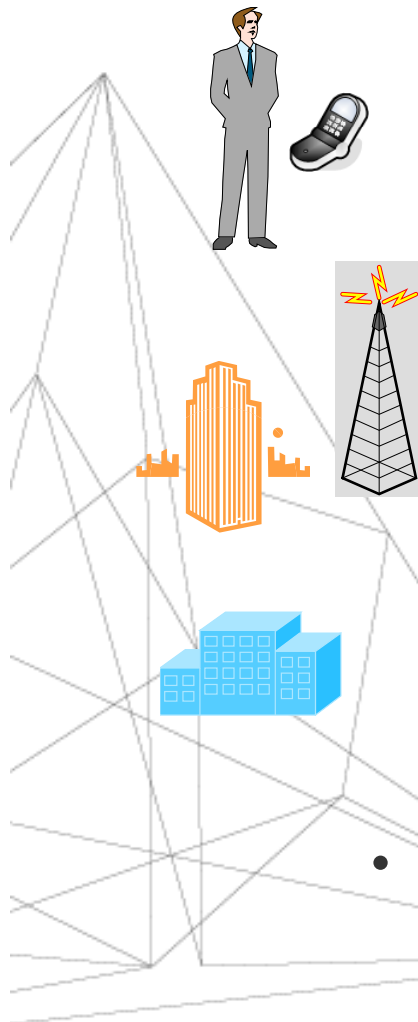
- Mobile Network Operator

- A service for its own subscribers.
- Additional source of revenues as a service for others (users, developers).
- A means for simplifying the deployment process.

- Developer

- Take advantage of the “S<sup>3</sup>MS label” for trust-worthy software.
- Software compliant to contract and MNO policy.

- Facilitate a long term market growth based on the deployment of value-added services and third party applications.

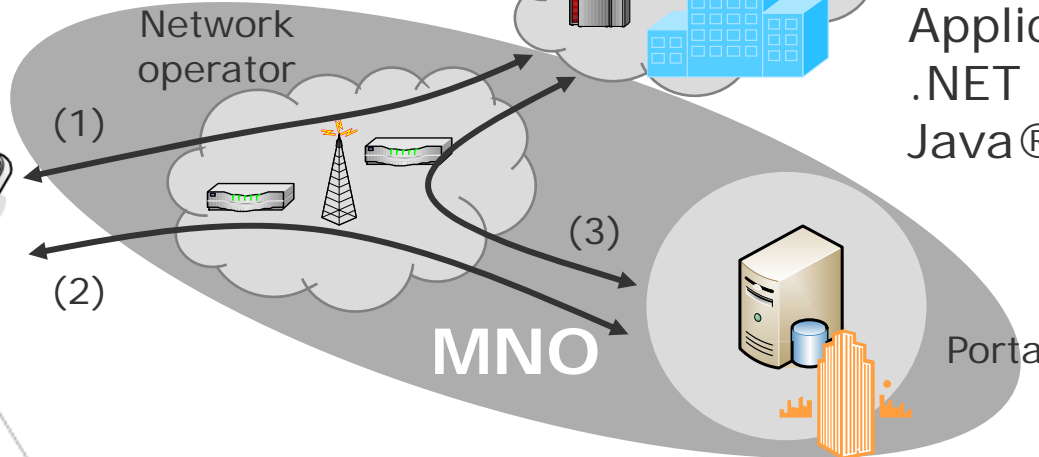


# Approach – Security-by-Contract

**Attack:** Harming the mobile terminal by not obeying policies; unauthorised use of API, data leakage, spending for (communication) resource use, etc.

**Contract:** Behavioural specification of the security relevant actions of the application/service. Contract is defined by developer (in co-operation with network operator).

## Security-By-Contract

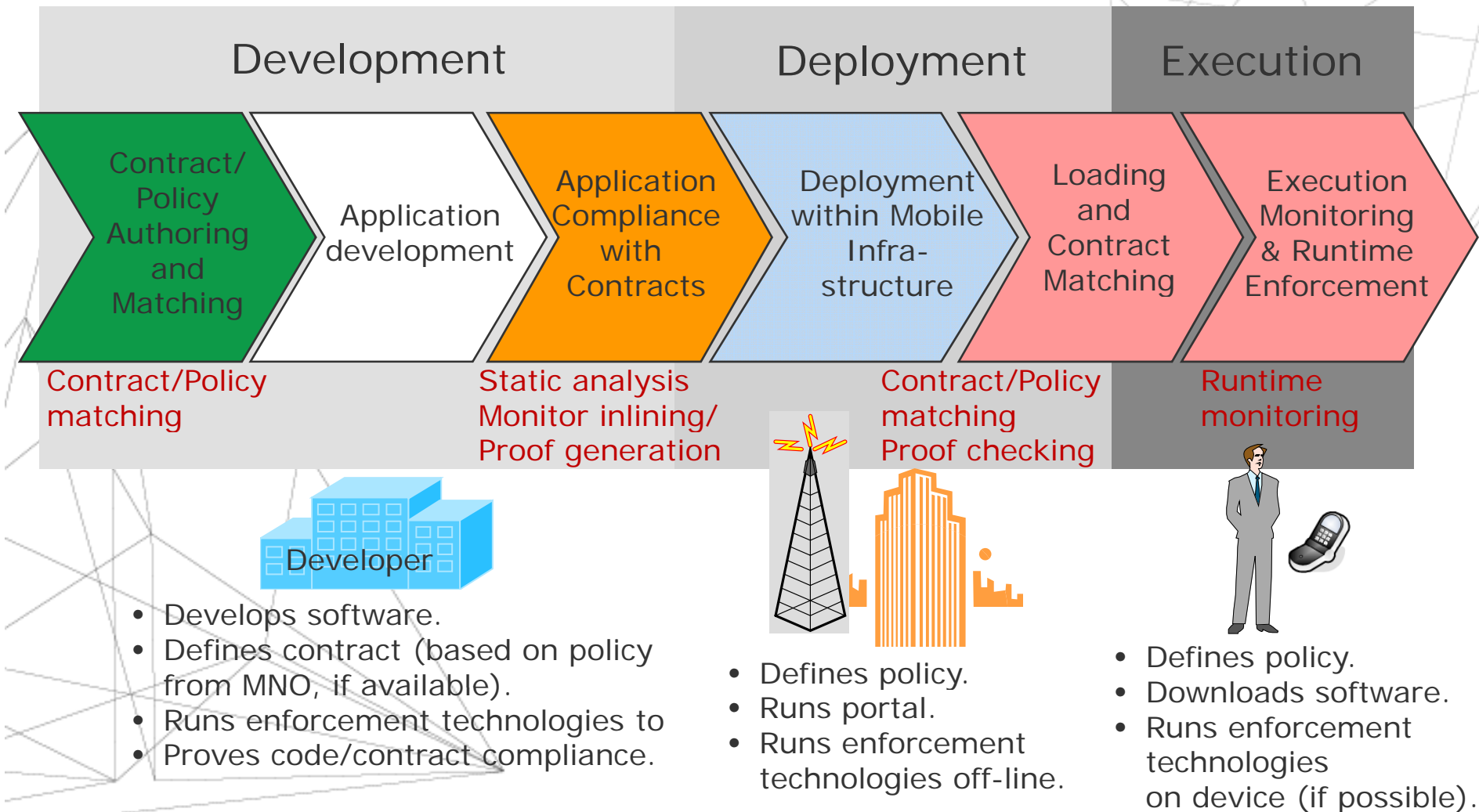


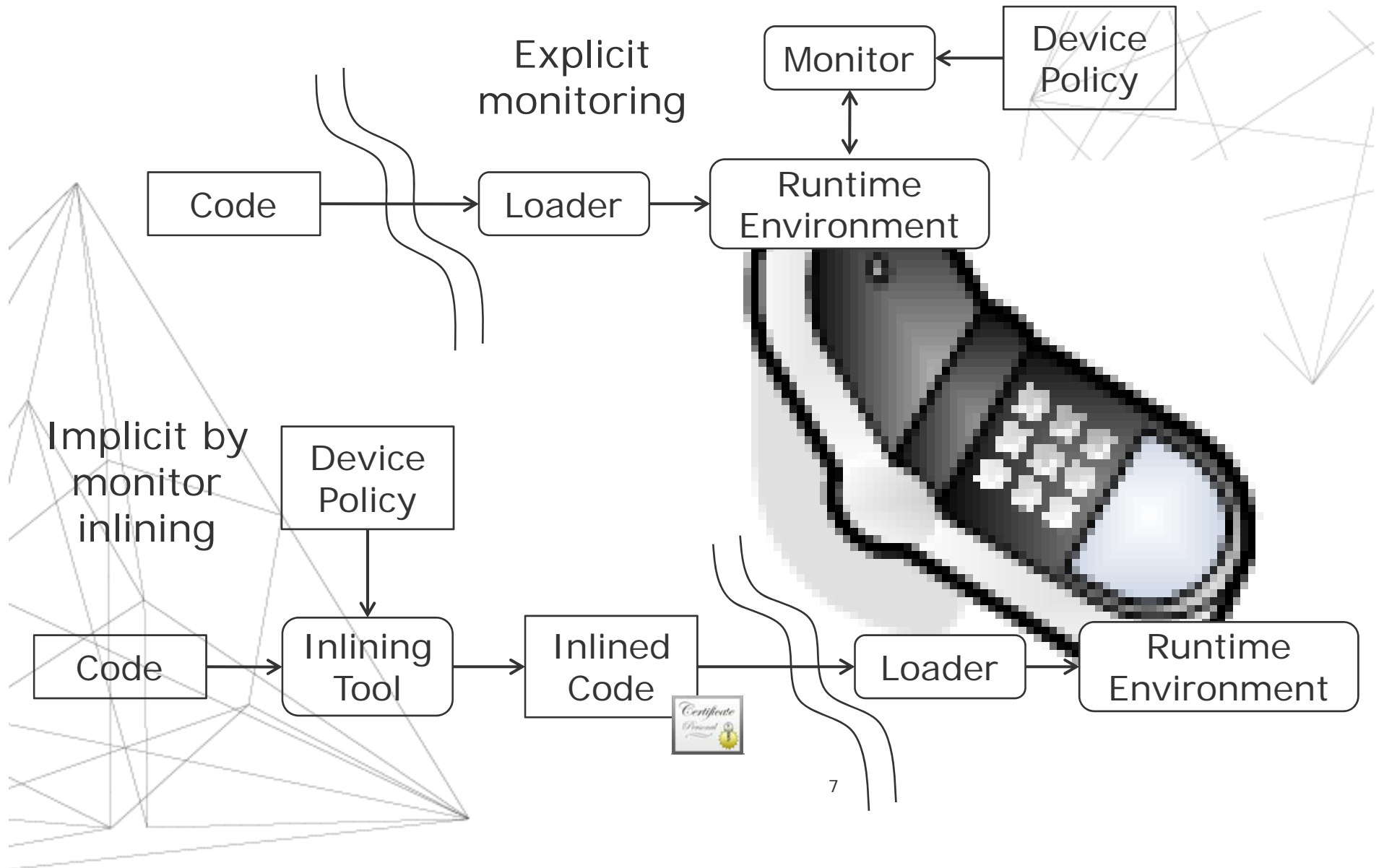
Application/Service  
.NET CLR  
Java® Byte Code

**Policy:** Specification of the acceptable behaviour of application/service on the platform. Policy is set by user or network operator.

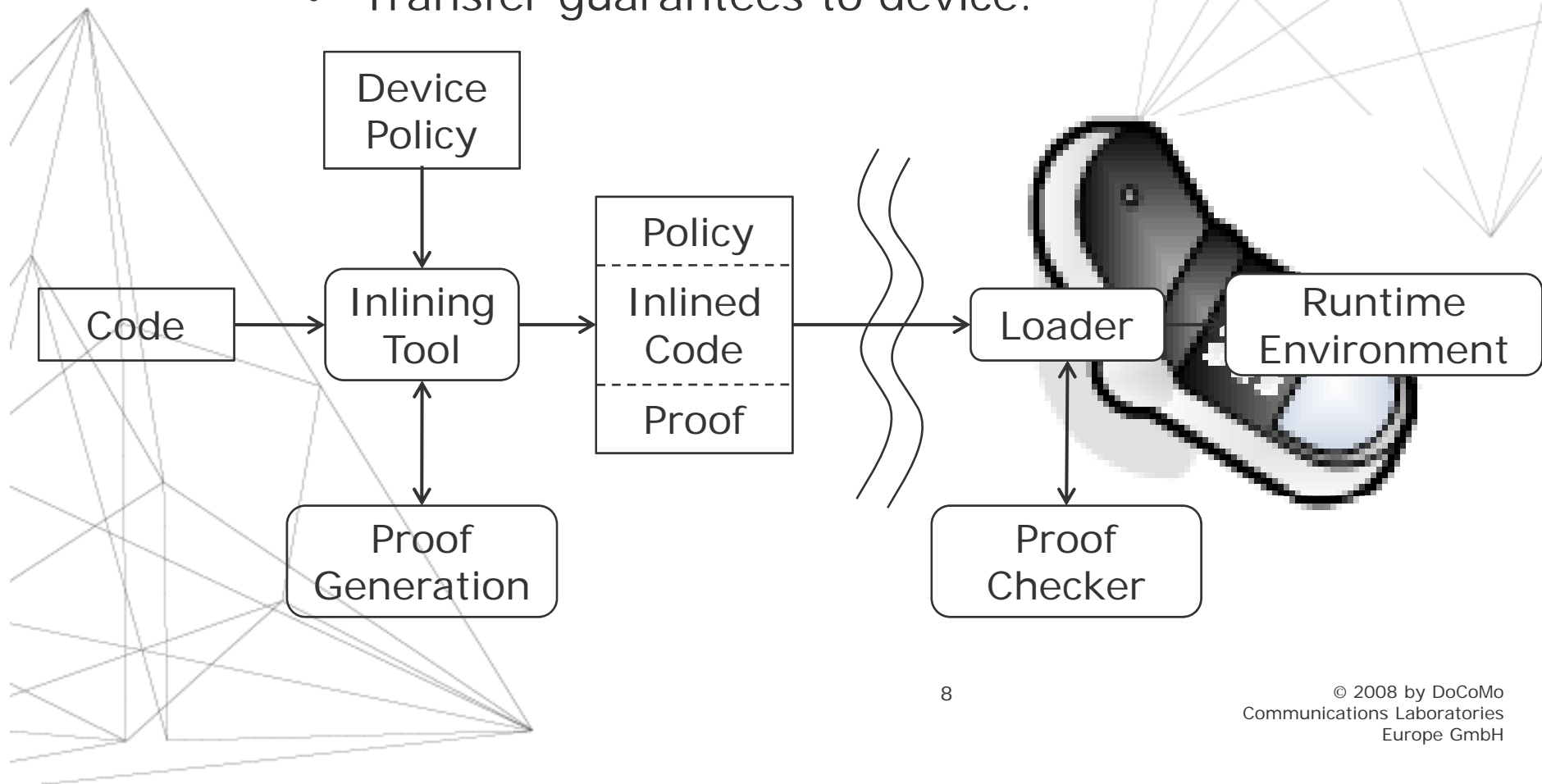
- Interaction:
- (1) User – Developer
  - (2) User – Portal
  - (3) Portal - Developer

# Software Lifecycle

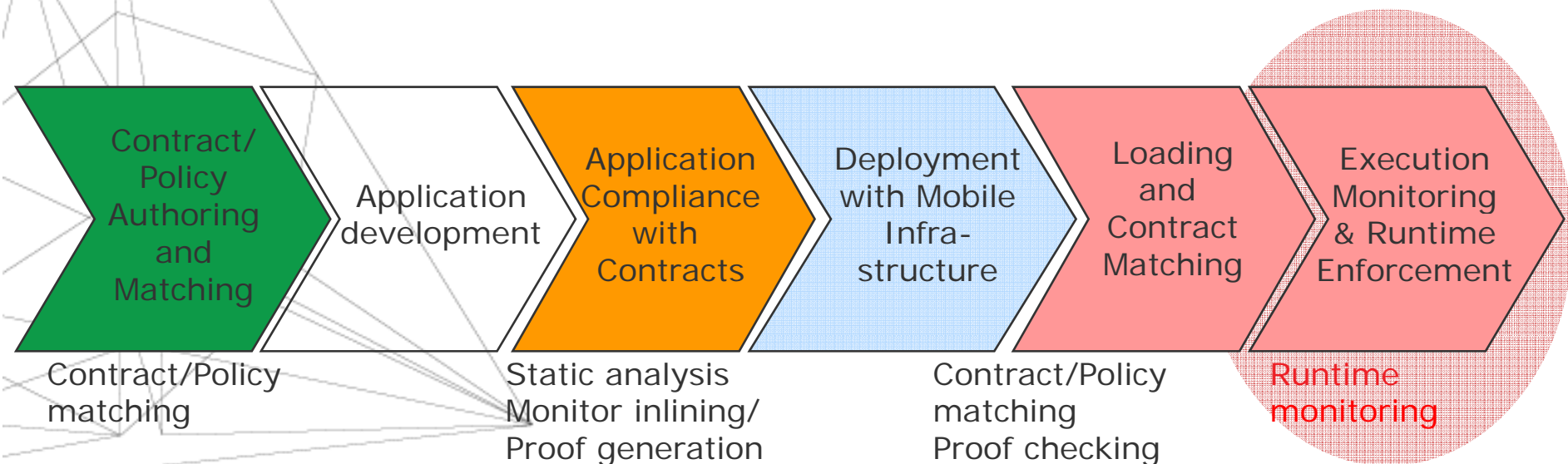




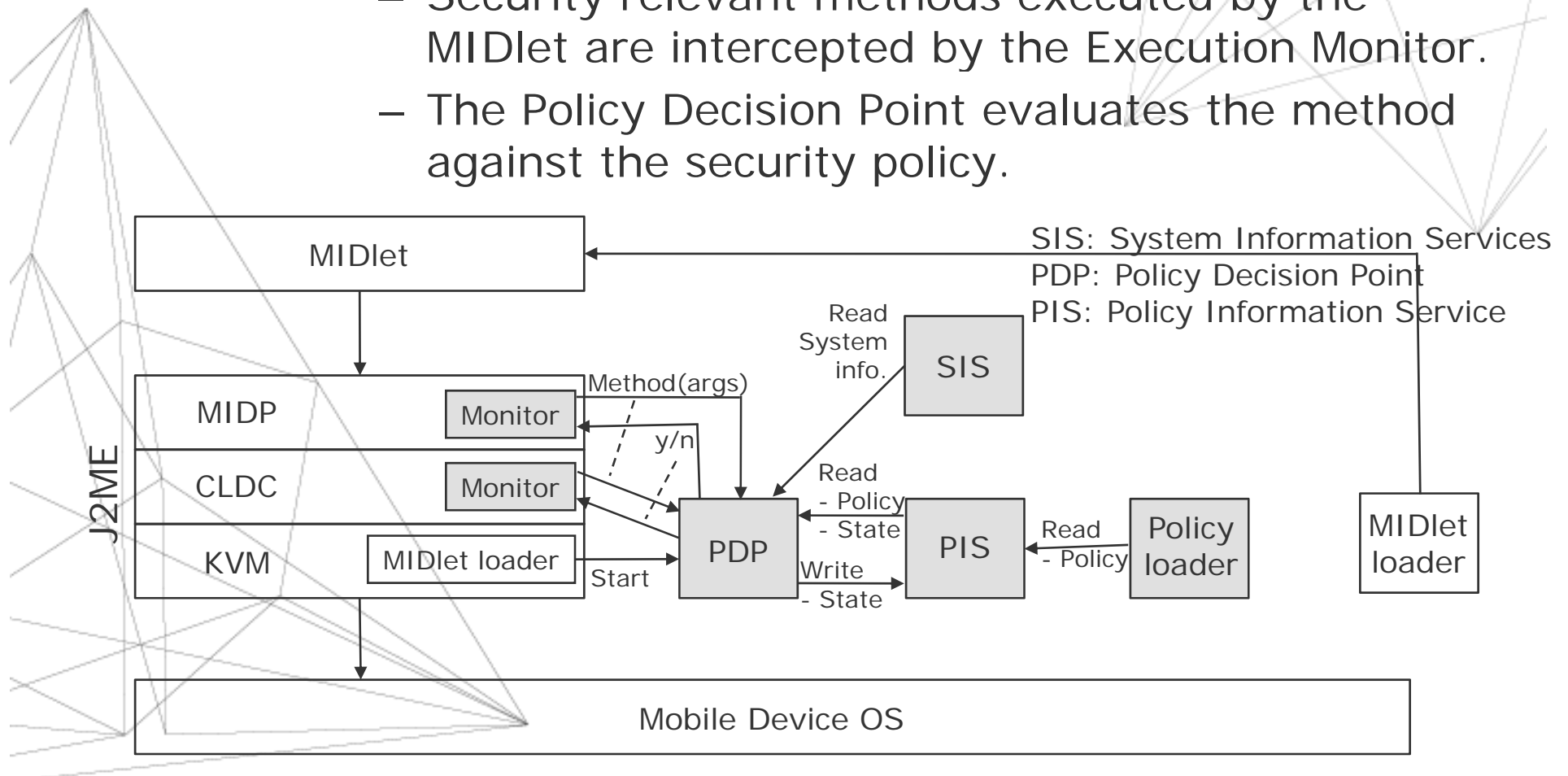
- Monitor inlined into code at development time.
- Guarantee application policy compliance.
- Transfer guarantees to device.



- External monitoring component is implemented, e.g., for the Java Virtual Machine.
- Code is inserted into the libraries to call the monitor.
- When a program uses a JVM API the external monitor checks if this usage is correct with respect to the security policy.



- Steps
  - Monitoring of the MIDlet while running.
  - Security relevant methods executed by the MIDlet are intercepted by the Execution Monitor.
  - The Policy Decision Point evaluates the method against the security policy.



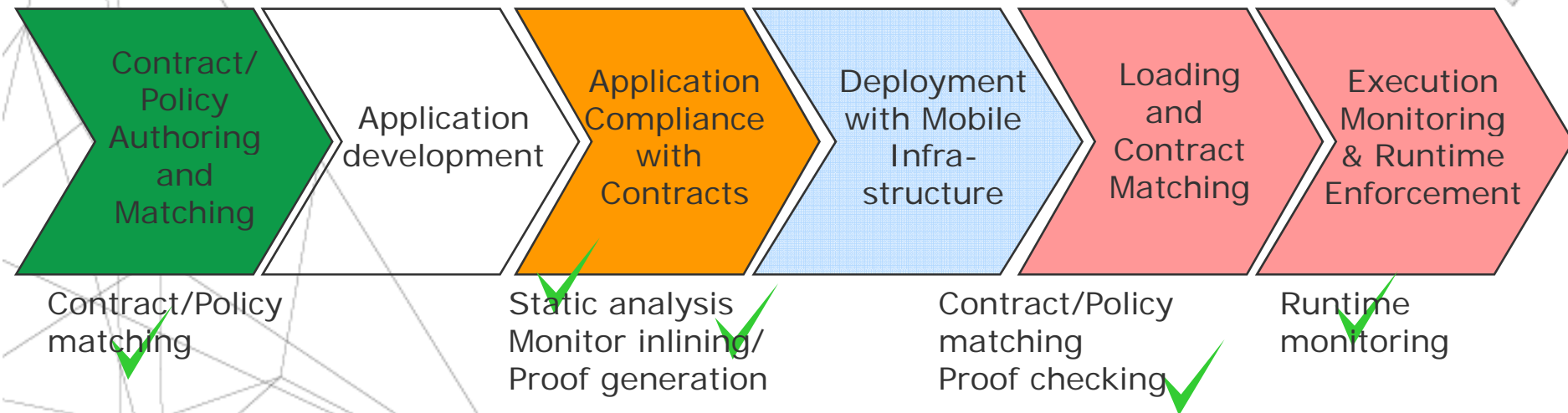
# Mobile Adventure Results

## ConSpec Contract/Policy Language

```
MAXINT 5 MAXLEN 10
RuleID Rule1
Version 1.0

SCOPE Session
SECURITY STATE ✓

BEFORE Connection.open(String url)
PERFORM
url.startsWith("http://www.google.ie") -
> {skip;}
```



# Mobile Adventure

Copyright © 2008 by DoCoMo  
Communications Laboratories  
Europe GmbH All rights reserved

S3MS  
 Security of Software and Services for Mobile Systems

Search  >>

You are here: [Home](#)



## Security of Software and Services for Mobile Systems



Application

- :: Would you **trust** to download any kind of mobile application onto your mobile device?
- :: Do you feel your personal and business data stored in your device are completely **safety**?
- :: Have you ever thought a malicious behaviour of an application might have **hazarded** to the normal behaviour of your mobile platform?
- :: Have you ever felt frustrated because you didn't know whether a mobile application you wished to download could be considered **trustable**?
- :: Have you ever felt **frustrated** once you discovered you had to pay for a very expensive phone bill, because the last mobile application you have downloaded used to make phone call to an international number without your prior acknowledgment?

The S3MS Research Project provides a solution by allowing you to know a-priori if a mobile application is trustable or not. [CLICK HERE TO KNOW HOW >>](#)

**Project start date:** 1st March 2006  
**Project end date:** 29th February 2008

Towards a global dependability and security framework



Information Society Technologies

Specific Targeted Research Project - 6th Framework Programme



### Last Accepted Publications

<p><b>10/12/2007</b>                      Extending the Java Virtual Machine to Enforce Fine-Grained Security Policies in Mobile Devices                      @ Annual Computer Security Applications Conference (ACSAC'07)</p>	<p><b>09/09/2007</b>                      Enhancing Java Security with History Based Access Control                      @ Foundations of Security Analysis and Design (FOSAD '07)</p>
<p><b>19/07/2007 A</b>                      Security-by-Contract Architecture for Pervasive Services                      @ 3rd International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing (SEC 07)</p>	<p><b>28/06/2007</b>                      Security-by-Contract: Toward a Semantics for Digital Signatures on Mobile Code                      @ 4th European PKI Workshop: Theory and Practice (EuroPKI 2007)</p>

### Flash news

[Home](#)  
[Restricted Area](#)  
[Project Objectives](#)  
[Project Activities](#)  
[Expected results](#)  
[Public Deliverables \(all\)](#)  
[Publications](#)  
[Participants](#)  
[Industry Board](#)  
[News & Events](#)  
[Utilities](#)

www.s3ms.org