Supporting the secure Deployment of OSGi Bundles

Pierre Parrend, Stéphane Frénot
Pierre.parrend@insa-lyon.fr
Lab. CITI, 21, Avenue J. Capelle
69621 Vileurbanne Cedex

Context

- The OSGi Platform
  - Extensible at runtime
    - Based on Java
    - Components are called 'bundles'
  - A versatile Platform
    - IBM Websphere 6.1, JBoss
    - Home Set top Boxes (ADSL Modems), Automotive Media Systems
    - Soon in the Sun JVM ? JSR 277, 291
  - A new Attack Vector
    - Seemless install code from the environment

The problem

- OSGi Security
  - How to make actual code secure
    - Formal approaches is not relevant
  - Requires a very pragmatic view
    - Java Developpers usually do not accept to put (too much) constraints on their code
    - Execution environments are often resource-restricted devices
  - Boom on Functionalities
    - Need a strong secure environment

This Work

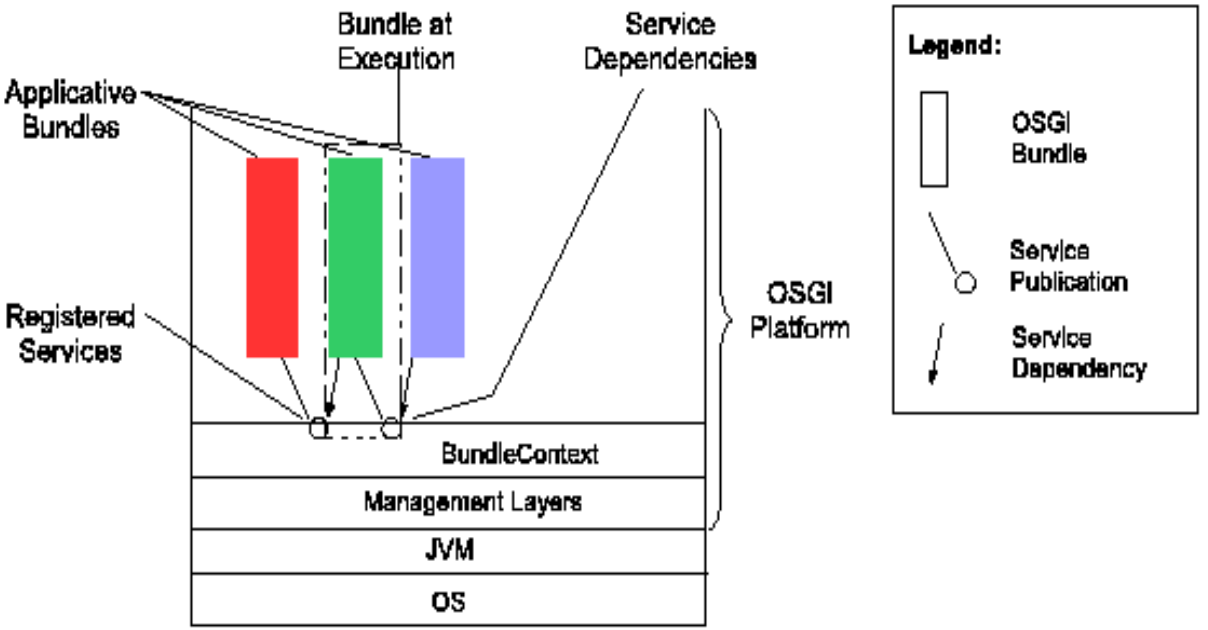
- Identification of the threats over OSGi Platforms
- A convenient tool for supporting life-cycle long security in OSGi-based Systems
  - Bundle Signature
  - Publication
  - (Download)
  - Signature Verification – OSGi R4 compliant
- Objective
  - Provide tools for OSGi users
  - Provide a Spec-compliant basis to support further research

Summary

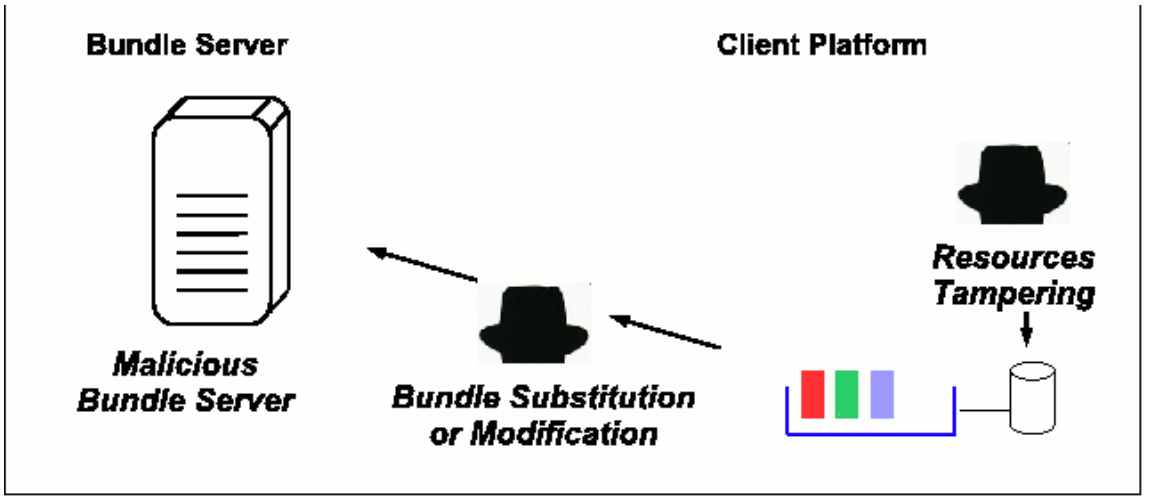
- OSGi Platforms and Threats
- Secure OSGi Tool Suite
  - SFelix
  - SF-JarSigner
- Comparisons

OSGi Platforms and Threats

- Overview of the OSGi Platform

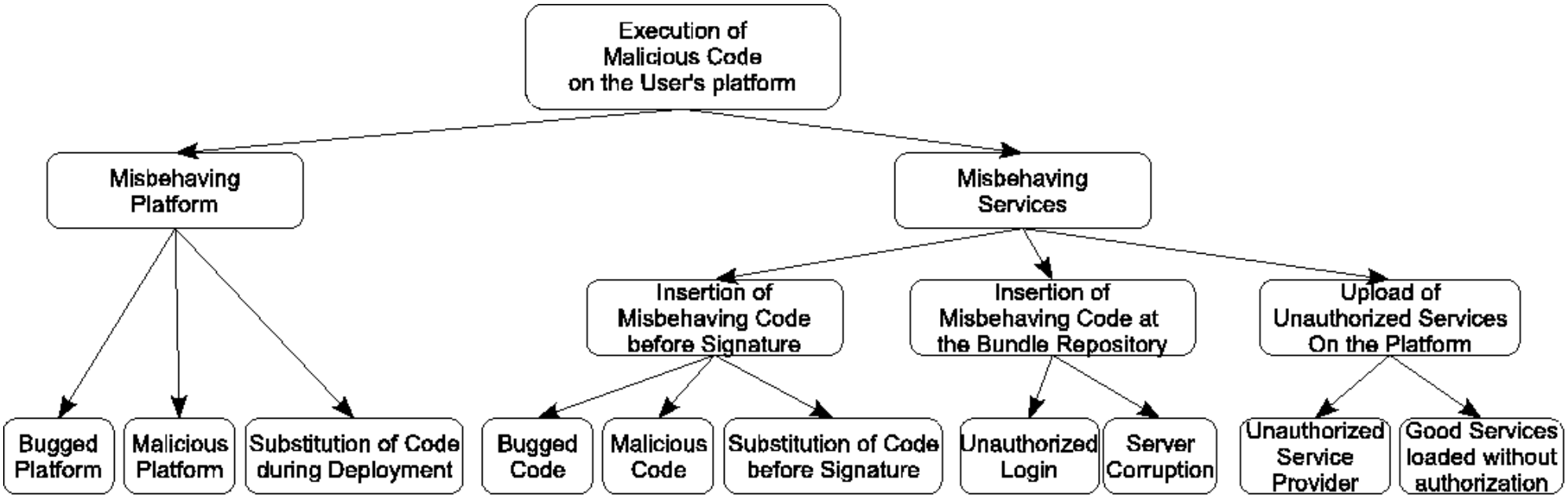


OSGi Platforms and Threats



OSGi Platforms and Threats

- Attack Vector - Execution of Malicious Code

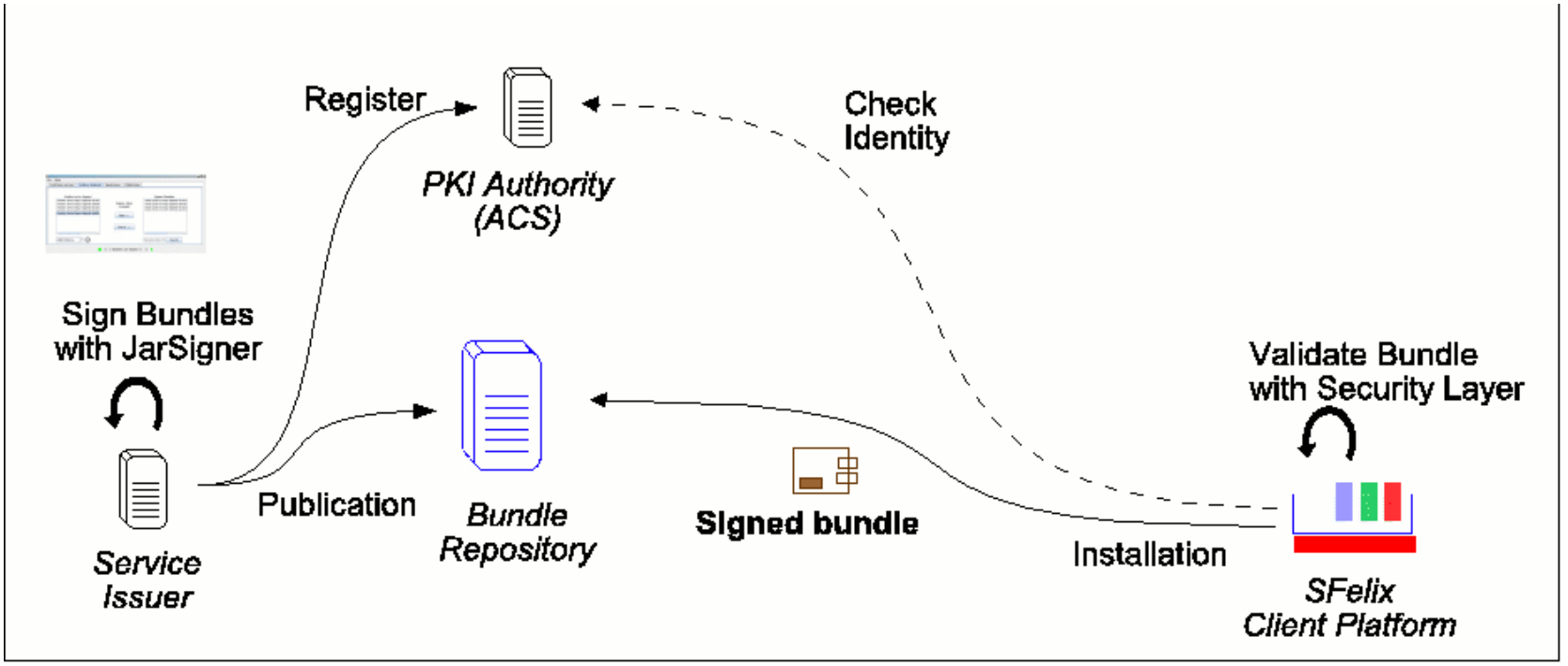


Summary

- Threats over OSGi Platforms
- Secure OSGi Tool Suite
  - SFelix
  - SF-JarSigner
- Comparisons

Secure OSGI Tool Suite

- Overview



Secure OSGI Tool Suite

- Sfelix
  - http://sfelix.gforge.inria.fr/
  - Sfelix v0.1
    - OSGi Release 4 Implementation of the Bundle Signature Validation Process
    - Beware of JVM-only solutions !
  - Sfelix v0.2
    - Robust against ill-coded Bundles
    - In a near future – still need to be published

Secure OSGI Tool Suite

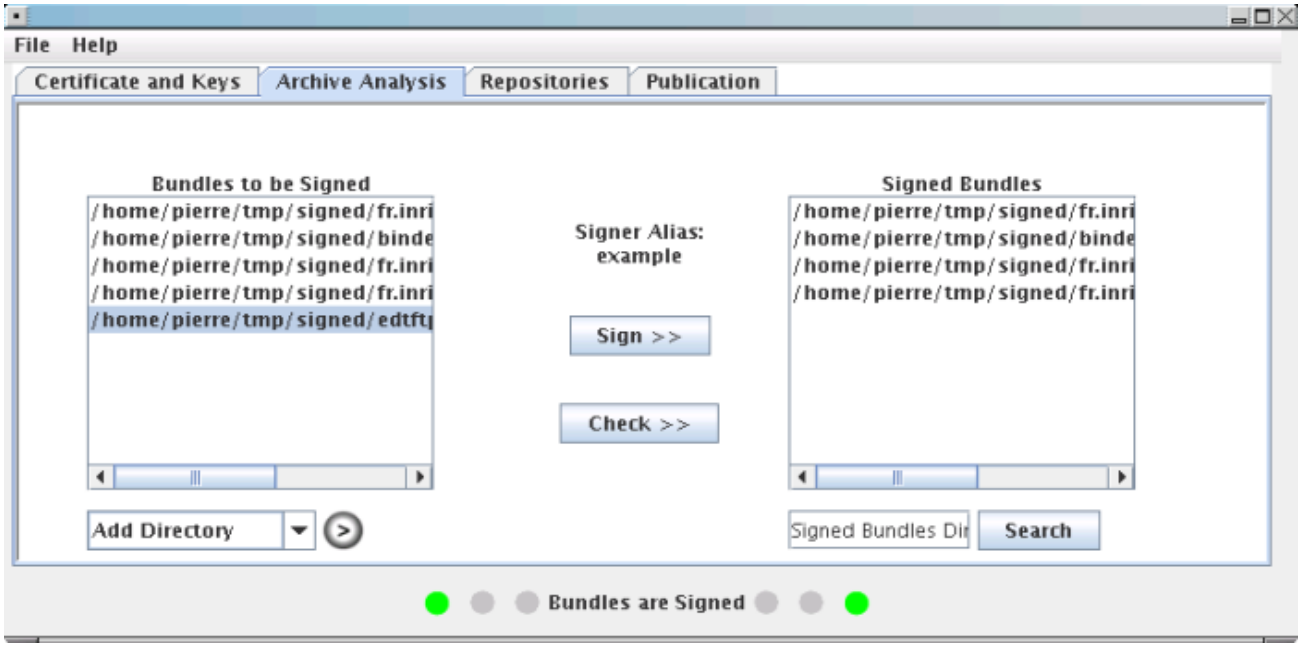
- Sfelix

```
-> obr start "HTTP Service"
Target resource(s):
-------------------
   HTTP Service (0.8.0.SNAPSHOT)

Deploying...Resolver: Install error - org.apache.felix.http.jetty
org.osgi.framework.BundleException: Could not create bundle object.
        at org.apache.felix.framework.Felix.installBundle(Felix.java:1947)
        at org.apache.felix.framework.Felix.installBundle(Felix.java:1822)
        at org.apache.felix.framework.BundleContextImpl.installBundle(BundleContextImpl.java:90)
        at org.apache.felix.bundlerepository.ResolverImpl.deploy(ResolverImpl.java:457)
        at org.apache.felix.bundlerepository.ObrCommandImpl._deploy(ObrCommandImpl.java:356)
        at org.apache.felix.bundlerepository.ObrCommandImpl.deploy(ObrCommandImpl.java:294)
        at org.apache.felix.bundlerepository.ObrCommandImpl.execute(ObrCommandImpl.java:108)
        at org.apache.felix.shell.impl.Activator$ShellServiceImpl.executeCommand(Activator.java:253)
        at org.apache.felix.shell.tui.Activator$ShellTuiRunnable.run(Activator.java:165)
        at java.lang.Thread.run(Thread.java:595)
Caused by: org.osgi.framework.BundleException: Bundle Unsecure
        at fr.inria.ares.framework.cache.DefaultSecuredBundleArchive.checkArchiveValidity(DefaultSecuredBundleArchive.java:73)
        at org.apache.felix.framework.Felix.installBundle(Felix.java:1823)
        ... 9 more
done.
->
->
```

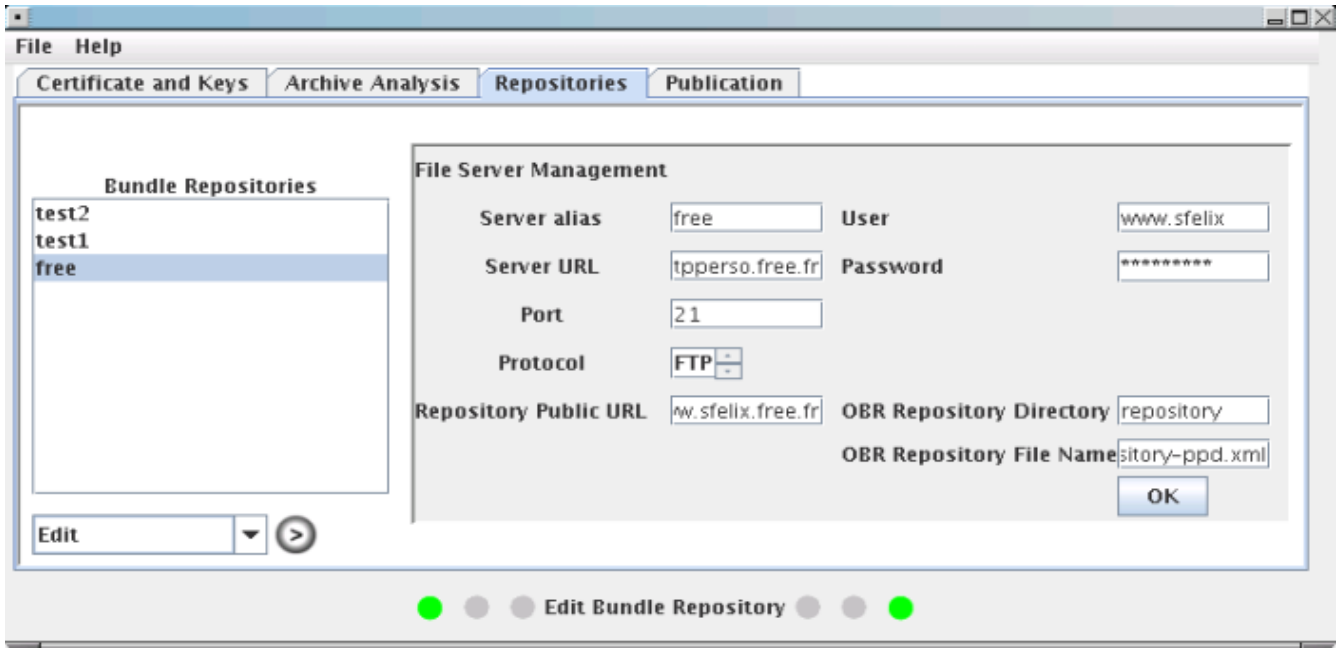
Secure Deployment

- The SF-JarSigner Tools
  - http://sf-jarsigner.gforge.inria.fr/
  - The Archive Analysis Panel



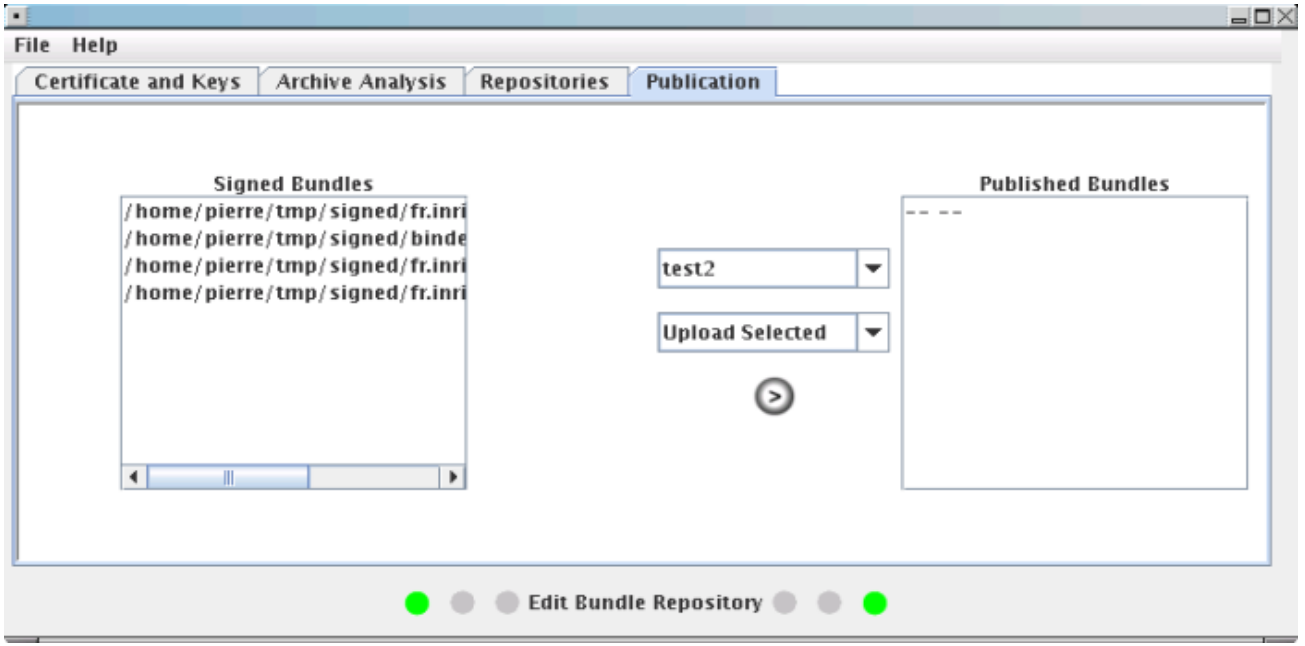
Secure Deployment

- The SF-JarSigner Tools
  - The BundleRepository Management Panel



Secure Deployment

- The SF-JarSigner Tools
  - The Publication Panel



Summary

- Threats over OSGi Platforms
- Secure OSGi Tool Suite
  - SFelix
  - SF-JarSigner
- Comparisons

Digital Signature Validation

- Validity Criteria

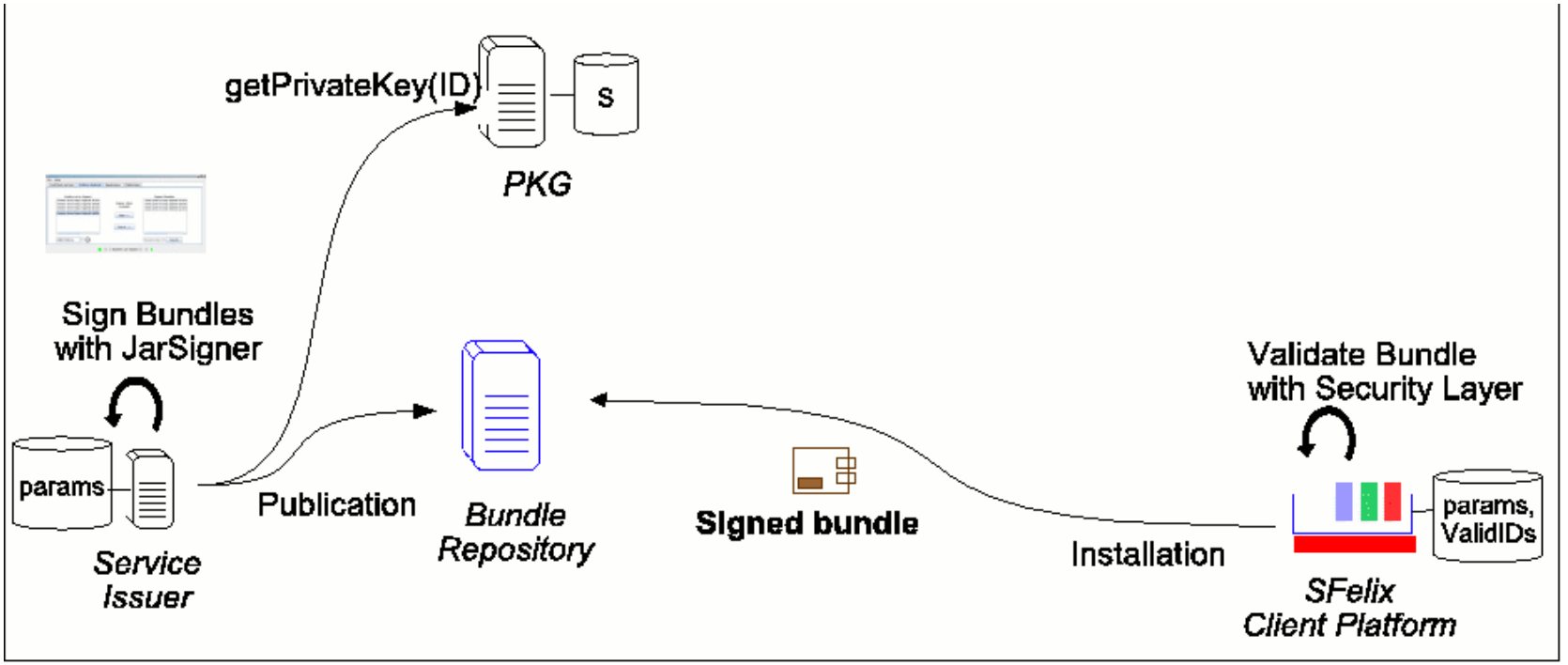
Table 1. Behavior of several tools and frameworks in the presence of unvalid archives

Error Type	Sun Jarsigner	Java with Security Manager	Felix	SFelix
Unsigned Archive	W	A	R	R
Unknown Signer	A	A	R	R
Addition of Resource	A	A	A	R
Removal of Resource	A	A	A	R
Modification of Resource	R	R	W	R
Unvalid Order of Resources	A	A	A	R
Signature of Embedded Archive Unvalid	R	R	W	R
Time Of Check	Test	Exec	Exec	Install

A: Accept; R: Reject; W: Warning;

Perspectives
Secure Deployment

- Key Management with Identity Based Cryptography



Perspectives
Safe execution

- What if a Bundle Issuer provides ill-tested Code ?
  - The whole system is impacted
  - What are OSGi Weaknesses
  - To be released very soon
- What guarantees on OSGi Code ?
  - Code Validation for better code (e.g. Findbugs)
  - Formal Code Analysis (e.g. PCC)
  - Sandboxing (e.g. Java Permissions)

Conclusions

- Current Threat Model for OSGi
  - Untrusted Network
  - Trusted Platform Issuer
  - Trusted Bundle Issuer
  - Trusted Host
- Future Threat Model
  - Untrusted Network
  - Trusted Platform Issuer
  - Untrusted Bundle Issuer ??
  - Untrusted Host ??

Questions ?

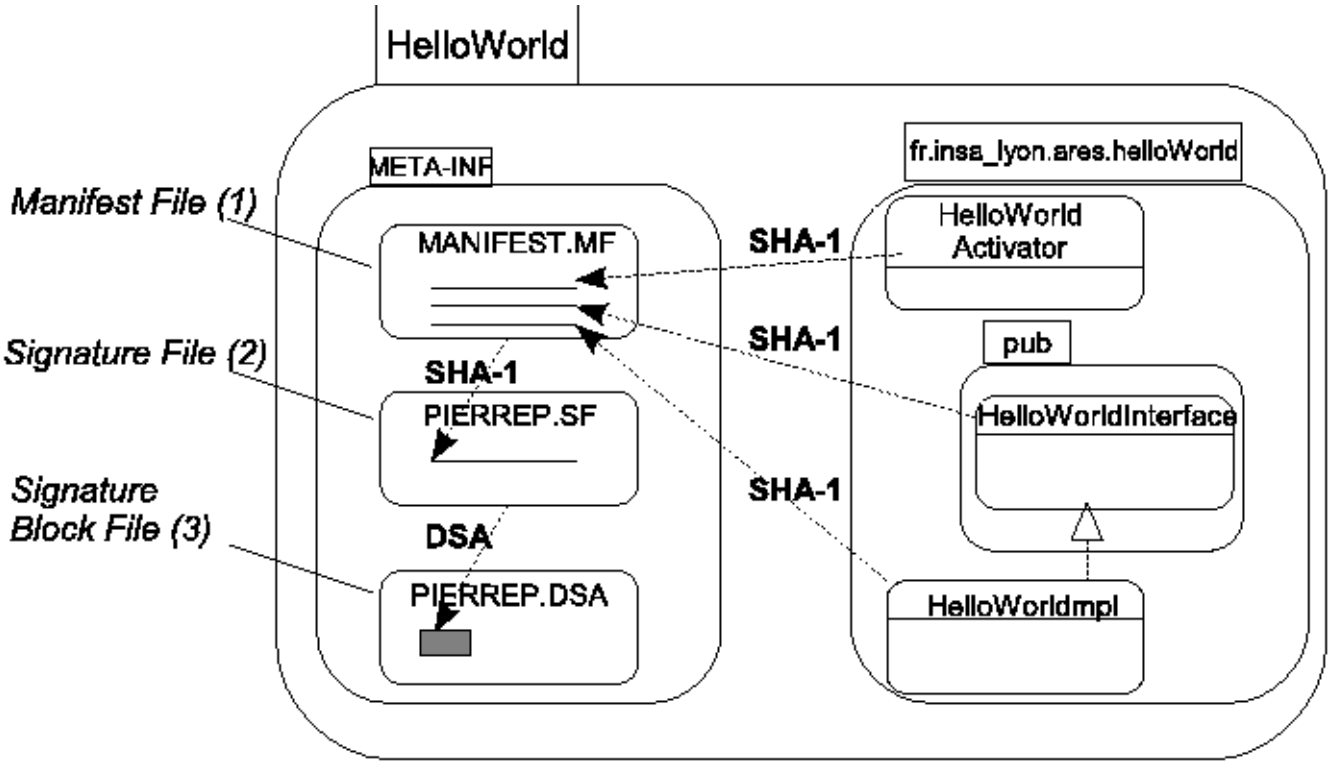
For more informations

Secure Component Deployment in the OSGi(tm) Release 4 Platform , http://www.rzo.free.fr/parrend06deployment.php

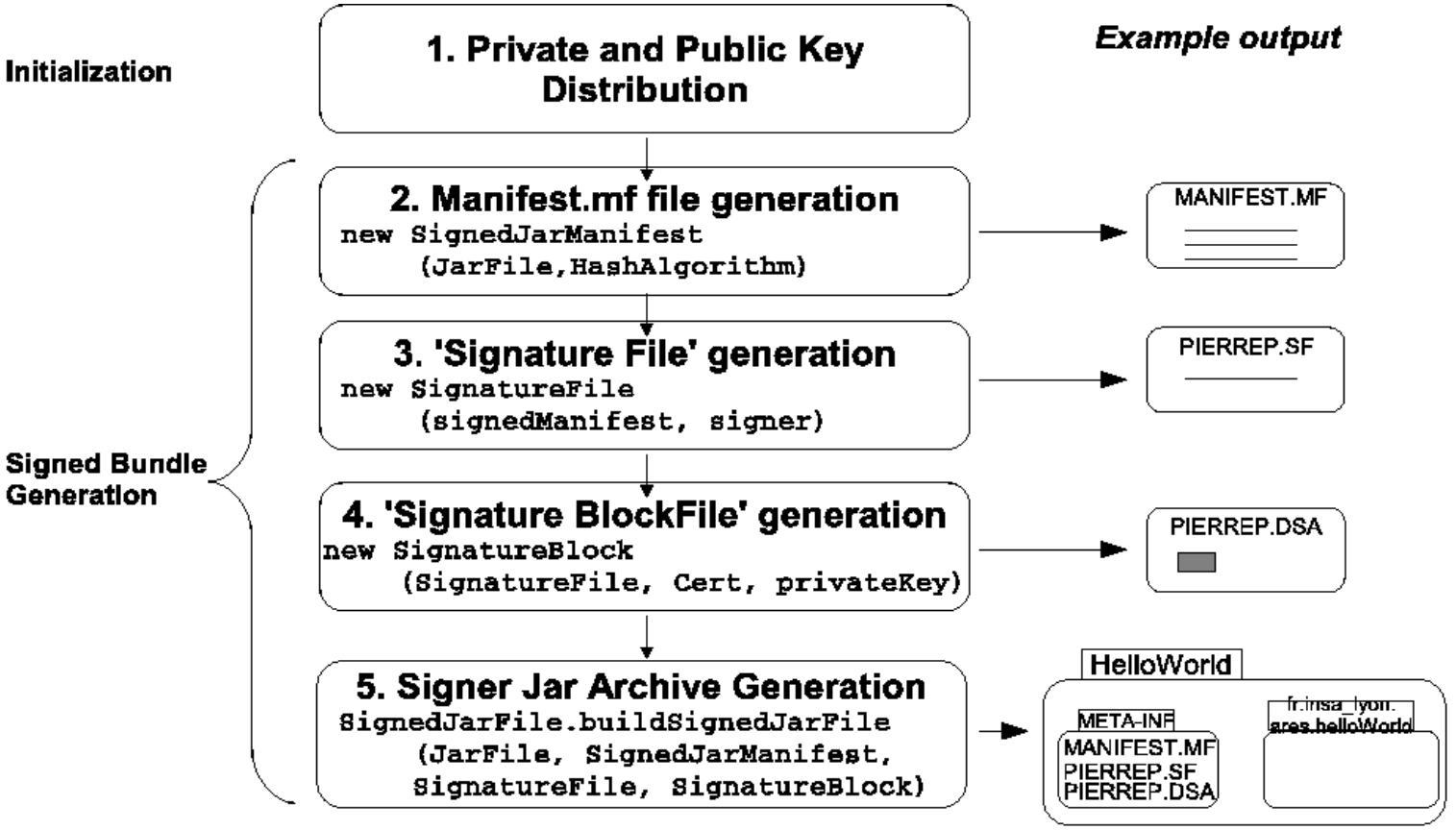
http://sfelix.gforge.inria.fr/

http://sf-jarsigner.gforge.inria.fr/

- OSGi Signed Bundle



- Signing OSGi Bundles



- OSGi Bundles Signature Verification