

SignServer

PrimeKey Solutions AB

Markus Kilås

<http://www.primekey.se>

markus@primekey.se

www.signserver.org

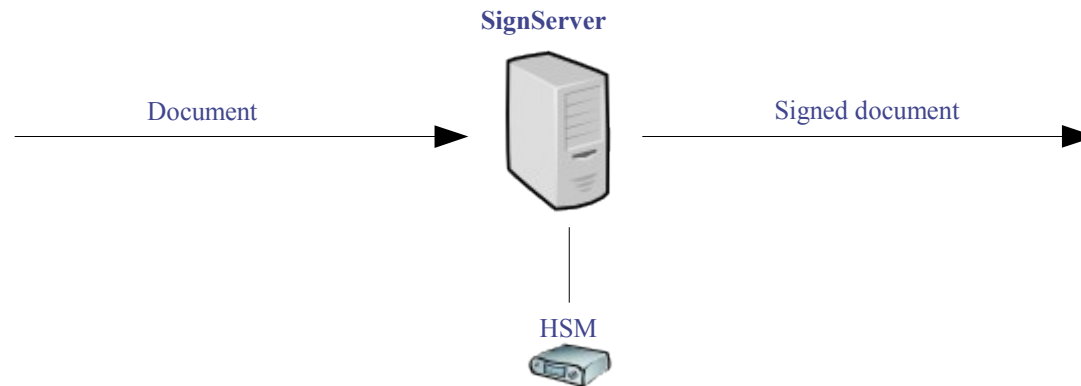
Outline

1. SignServer basics
2. Latest Releases
3. Future SignServer

What is SignServer?

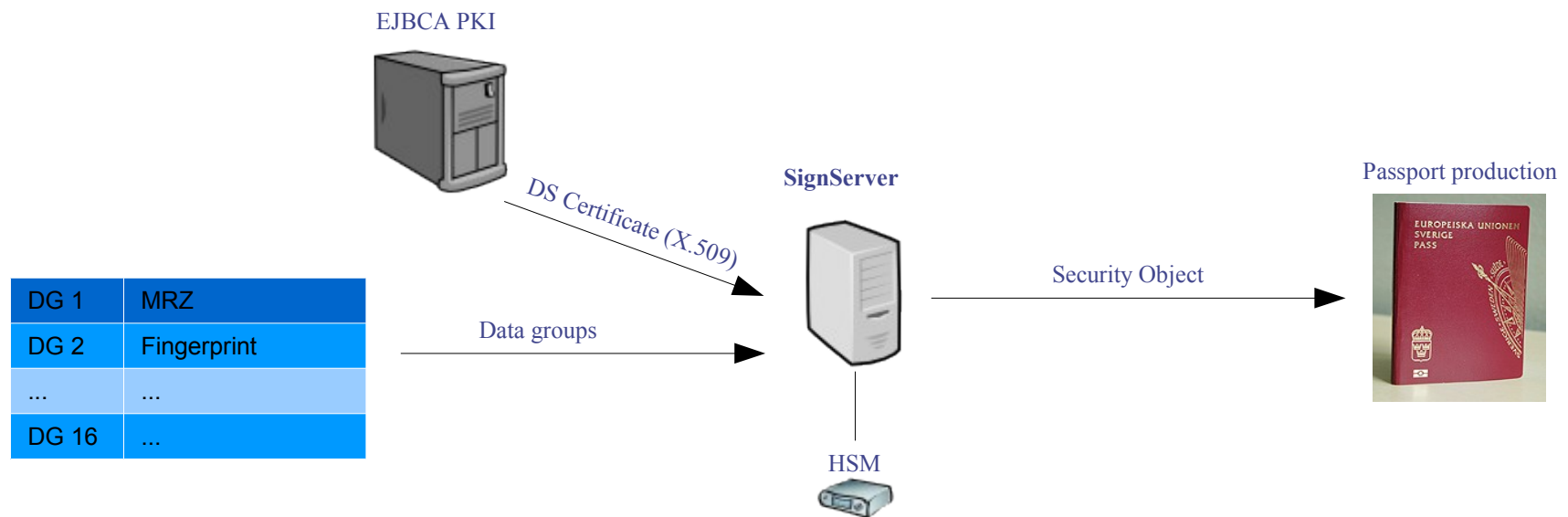
- ◆ "Application framework performing cryptographic operations for other applications"
- ◆ Central server

Document signing



Document signing

◆ ePassport



What is SignServer?

- ◆ Two different modes:
 - SignServer
 - MailSigner
- ◆ Also:
 - Certificate validation
 - Document validation

Architecture

- ◆ Based on components
 - Workers
 - CryptoTokens

Workers

◆ Signers

- PDF, TSA, XML, ODF, OOXML, MRTD, ...

◆ Document validators

- XML, ODF?

◆ Certificate validators

- CRL, OCSP

Worker configuration

- ◆ Configuration per worker instance
- ◆ Ex: PDFSigner properties:

CLASSPATH=org.signserver.module.pdfsigner.PDFSigner

NAME=MyPDFSigner

AUTHTYPE=NOAUTH

REASON=Officially issued document

RECTANGLE=400,700,500,800

CryptoTokens

◆ Workers use CryptoTokens

- PKCS12 (soft)
- PKCS11 (hard)

◆ Ex: P12CryptoToken properties:

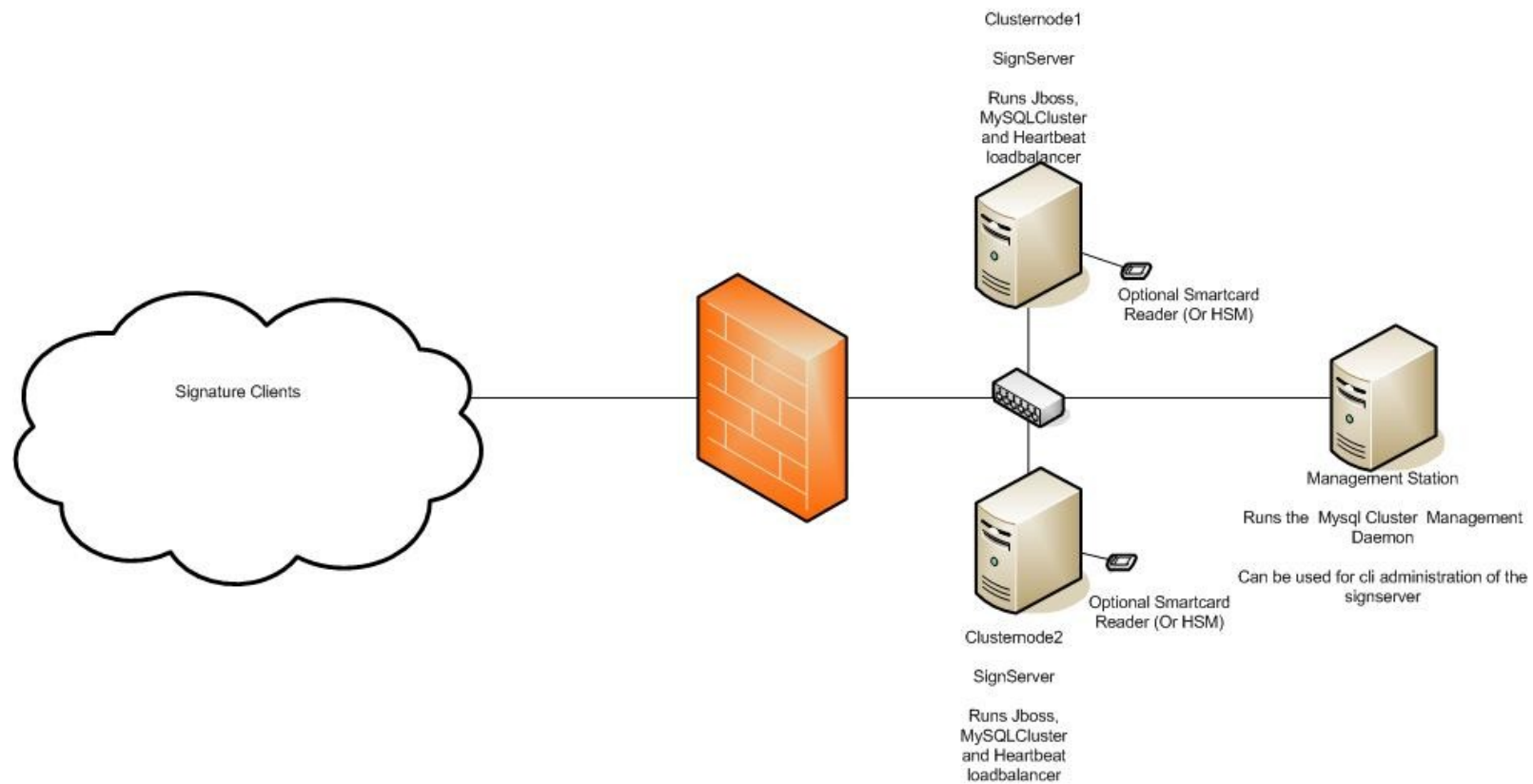
```
SIGNERTOKEN.CLASSPATH =  
    org.signserver.server.cryptotokens.P12CryptoToken  
KEYSTOREPATH=/etc/signserver/signer.p12  
KEYSTOREPASSWORD=foo123
```

Other features

◆ Archiving of signed documents

Other features

◆ Easy clustering



Interacting with SignServer

◆ Interfaces

- Command line interface (CLI)
- Web Services
- HTTP
- Client libraries/applications

HTTP interface

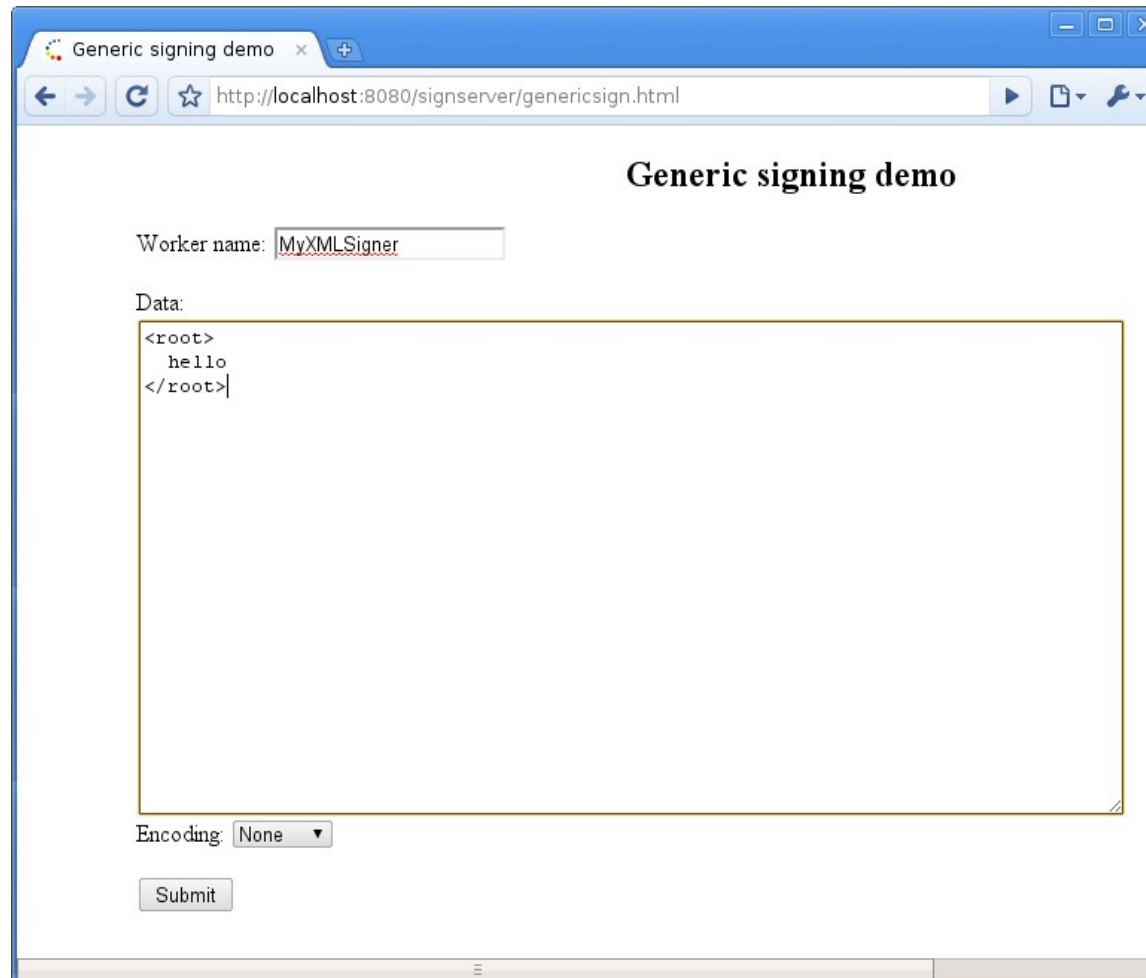
◆ Example with worker MyXMLSigner

`http://localhost:8080/signserver/process?
workerName=MyXMLSigner&data=<root>hello</root>`

```
<root>  
hello  
</root>
```

```
<root>  
hello  
  <Signature>  
    <SignedInfo>...</SignedInfo>  
    <SignatureValue>BYr49...</SignatureValue>  
    <KeyInfo>  
      <X509Data>  
        <X509Certificate>MIICtjC....</X509Certificate>  
      </X509Data>  
    </KeyInfo>  
  </Signature>  
</root>
```

HTTP interface



Generic signing demo

Worker name:

Data:

```
<root>
  hello
</root>
```

Encoding:

What is SignServer?

◆ Technical facts:

- Enterprise Java Beans 3
- Application server: JBoss 4
- Hibernate
- MySQL, HypersonicSQL, ...

Outline

1. SignServer basics
- 2. Latest releases**
3. Future SignServer

Latest releases

Evolution:

- ◆ SignServer 2.0 – 2007
 - Time Stamp Authority and MRTD signer
 - EJB2
- ◆ SignServer 3.0 – 2008
 - EJB3
 - PDF signer, Webservice, Validation API, Group key API, PKCS#11 crypto tokens

Latest releases

- ◆ SignServer 3.1 (next release)
 - Dynamic module loading
 - New modules:
 - ◆ XMLSigner/Validator
 - ◆ ODFSigner
 - ◆ OOXMLSigner
 - ◆ CRLValidator
 - ◆ OCSPValidator
 - ◆ MRTDSODSigner

Outline

1. What is SignServer?
2. Latest releases
- 3. Future SignServer**

Future SignServer

- ◆ Ideas for future versions
 - Web-GUI
 - Divide source code in sub-projects
 - Other?













Web GUI

- ◆ Could give a better overview of the workers and their configuration
- ◆ Could simplify normal workflows that today requires multiple steps:
 - ◆ Set up worker
 - ◆ Create certificate signing request
 - ◆ Send request to CA
 - ◆ Upload the returned certificate

Sub projects

- ◆ Divide source code in sub-projects
 - Easier to see which code belongs to which part of SignServer
 - Get control of internal/external dependencies
 - You can choose to only have the part that you are working on open in the IDE
 - Rebuild only the parts that changed
 - Simplified build scripts
 - Easier to create new modules

Sub projects

-  **SignServer-ear**
-  SignServer-ejb
-  SignServer-war
-  SignServer-war-admin
-  SignServer-lib-common
-  SignServer-lib-common-mailsigner
-  SignServer-client-cli
-  SignServer-client-cli-mailsigner
-  SignServer-client-ws
-  SignServer-client-wsra
-  SignServer-client-timestamp
-  SignServer-client-performancetesttool
-  SignServer-lib-client-ws
-  SignServer-lib-client-api

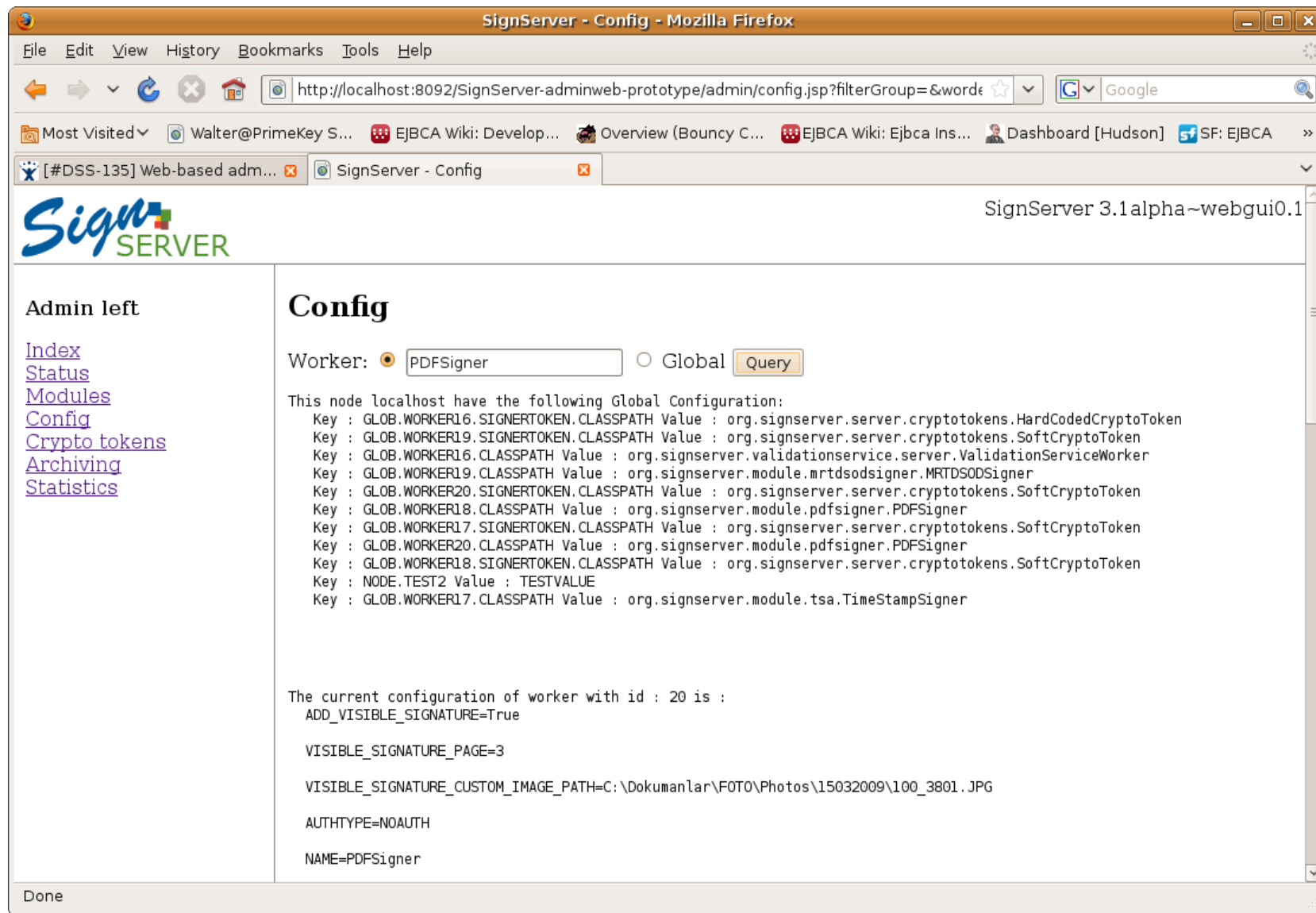
Future SignServer

- ◆ Statistics
- ◆ Integration with CA

Future SignServer

◆ Other ideas?

- New requirements?
- Support for other application servers?
- New module?
- Different kind of documents?



The screenshot shows a Mozilla Firefox browser window titled "SignServer - Config". The address bar shows the URL: `http://localhost:8092/SignServer-adminweb-prototype/admin/config.jsp?filterGroup=&word=`. The browser tabs include "[#DSS-135] Web-based adm...", "SignServer - Config", and several others. The page content is divided into two main sections:

- Admin left:** A sidebar menu with links for [Index](#), [Status](#), [Modules](#), [Config](#), [Crypto tokens](#), [Archiving](#), and [Statistics](#).
- Config:** The main content area. It features a "Worker:" label with two radio buttons: "PDFSigner" (selected) and "Global". A "Query" button is next to it. Below this, it displays the configuration for the selected worker on the local host. The configuration is as follows:

```
This node localhost have the following Global Configuration:  
Key : GLOB.WORKER16.SIGNERTOKEN.CLASSPATH Value : org.signserver.server.cryptotokens.HardCodedCryptoToken  
Key : GLOB.WORKER19.SIGNERTOKEN.CLASSPATH Value : org.signserver.server.cryptotokens.SoftCryptoToken  
Key : GLOB.WORKER16.CLASSPATH Value : org.signserver.validationsservice.server.ValidationServiceWorker  
Key : GLOB.WORKER19.CLASSPATH Value : org.signserver.module.mrtdsodsigner.MRTDSODSigner  
Key : GLOB.WORKER20.SIGNERTOKEN.CLASSPATH Value : org.signserver.server.cryptotokens.SoftCryptoToken  
Key : GLOB.WORKER18.CLASSPATH Value : org.signserver.module.pdfsigner.PDFSigner  
Key : GLOB.WORKER17.SIGNERTOKEN.CLASSPATH Value : org.signserver.server.cryptotokens.SoftCryptoToken  
Key : GLOB.WORKER20.CLASSPATH Value : org.signserver.module.pdfsigner.PDFSigner  
Key : GLOB.WORKER18.SIGNERTOKEN.CLASSPATH Value : org.signserver.server.cryptotokens.SoftCryptoToken  
Key : NODE.TEST2 Value : TESTVALUE  
Key : GLOB.WORKER17.CLASSPATH Value : org.signserver.module.tsa.TimeStampSigner
```

Below the global configuration, it shows the current configuration for worker with id : 20:

```
The current configuration of worker with id : 20 is :  
ADD_VISIBLE_SIGNATURE=True  
  
VISIBLE_SIGNATURE_PAGE=3  
  
VISIBLE_SIGNATURE_CUSTOM_IMAGE_PATH=C:\Dokumanlar\FOTO\Photos\15032009\100_3801.JPG  
  
AUTHTYPE=NOAUTH  
  
NAME=PDFSigner
```

Source tree

