ETSI ESI Workshop

Signing in the Cloud

CEN Server signing
TS 419 241 part 1

Barcelona, 14th March 2013
ETSI ESI Workshop
Signing in the Cloud

CEN Server signing
TS 419 241 part 1

CONTENTS

01 Server Signing

02 Sole Control Level 1
03 Sole Control Level 2
04 Protection Profiles

Certinomis
01 SERVER SIGNING

What is Server Signing?

This is a networked server which may process electronic certificates used by natural or legal persons for electronically signing/sealing documents.

The server signing application (SSA) is a component to be used by trust service providers (TSP) in order to provide signature generation services (SGS).
To define a:

» Trustworthy Systems Supporting Server Signing,

» With a set of security requirements and recommendations.

Drafting TS 419 241-1 a.k.a. «Server signing»

» TS 419 241 part 1, introduction and generic security requirements,

» Future PPs will be in part 2 and 3.
01 SERVER SIGNING

The place of Server Signing within the rationalized framework

TSP in the rationalized framework

- **TSP\textsubscript{QC}**
  - EN 319 411-2
  - TS 419 221

- **TSP\textsubscript{PKC}**
  - EN 319 411-3
  - TS 419 221

- **TSSP**
  - TS 419 231

- **SGSP**
  - TS 419 241

- **SVSP**
  - TS 419 261
01 SERVER SIGNING

Link with ETSI TSPs policies (STF 458)

TSP in the rationalized framework

TSP QC
EN 319 411-2
+ TS 419 221

TSP PKC
EN 319 411-3
+ TS 419 221

TSSP
EN 319 421-2
TS 419 231

SGSP
EN 319 431-2
TS 419 241

SVSP
TS 419 261
01 SERVER SIGNING

Trustworthy System Overview

Remote Signer

Signed Document

Policies

Certificates

Database

SSA

Server OS

SCDev

Cryptographic Suites

SCD
Objectives

Server side electronic signatures or electronic seals

- The remote signer can be natural or a legal person (e.g. remote application)

Need of flexibility to fit existing systems.

Need of a comparable level of assurance as it is expected with a SSCD
01 SERVER SIGNING

Strategy

2 DIFFERENT LEVELS

<table>
<thead>
<tr>
<th>Level 1</th>
<th>The remote signer authentication is enforced by the system environment.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 2</td>
<td>The remote signer authentication is enforced by the signature creation device. 2 factors for authentication are required.</td>
</tr>
</tbody>
</table>

Level 1 fits existing systems, and level 2 assurance is comparable as expected with a SSCD.
Usages

Remote signing as simple as sending an email

Web mail electronic signature
“protect an electronic email via a web mail interface as easily as done with a classic email tool.”

Contract signing
“sign a e-contract with a sustainable private key and avoid on-the-fly certification”

Equity Arbitrage
“sign a transaction on shares in a home banking web site”

Batch e-Sealing
“seal in batch electronic invoices for massive production”
Level 1: functional example

Signer authentication / Signer id

Signer

DTBS

Signed document

SSA

Signer id / SCD id bindings

SSA authentication

DTBS + SCD id

SCDev

Signer’s SCD

Signer’s SCD
ETSI ESI Workshop
Signing in the Cloud

CEN Server signing
TS 419 241 part 1

01 Server Signing
02 Sole Control Level 1
03 Sole Control Level 2
04 Protection Profiles
The Signer’s Activation Data (SAD) is functionnaly equivalent to the verification authentification data (VAD) of a SSCD (e.g. PIN)

For level 2 SAD must have 2 authentification factors
Level 2: functional example

Signer authentication / Signer id

DTBS

2 factors SAD to commit

Signed document

SSA

Signer id / SCD id bindings

DTBS + SCD id

SSA authentication

SCDev

Signer’s SCD

Signer’s SCD
03 SOLE CONTROL LEVEL 2

Signer’s Activation Data: SAD

2 DIFFERENT LEVELS

Level 1

Level 2

ANOTHER POSSIBILITY FOR LEVEL 2 IS

- Multi-factor authentication of the signer to the system,

  and in this secure channel committing is done by providing a ‘1 factor SAD’ to the SCDev.

- The 1 factor SAD must be protected against replay attack
03 SOLE CONTROL LEVEL 2

Level 2: functional example 2

Signer authentication with 2 factors

Hash (nonce + 1 factor SAD) + DTBS

Signed document

SSA

SSA authentication

Signer id / SCD id bindings

SCDev

Signer’s SCD

Signer’s SCD
ETSI ESI Workshop
Signing in the Cloud

CEN Server signing
TS 419 241 part 1

01 Server Signing
02 Sole Control Level 1
03 Sole Control Level 2
04 Protection Profiles
Proposal for drafting Server Signing PPs

Members of CEN TC 224/WG17 made the proposal to draft new PPs on Server Signing

PPs to define Sole Control Level 2 only
Level 1 system should apply TS 419 241 part 1

Two “system” PP with a similar core part (client and server sides)
- PP1 : using a SE authentication + HSM
- PP2 : using a TEE authentication + HSM
⇒ Same level for both : EAL4+ AVA_VAN.4 or AVA_VAN.5
04 PROTECTION PROFILES

Calendar

CIRCULATION OF DRAFT
TS 419 241-1 v1.0.0
2012/12/22

CEN FORMAL VOTE
2013/06/30

PPs DRAFTING
419 241-1 v2 DRAFTING
ETSI ESI Workshop : Signing in the Cloud
CEN Server signing
TS 419 241 part 1

Barcelona, 14th March, 2013

Mr. Franck Leroy
Docapost EBS / Certinomis
franck.leroy@docapost-ebs.com

Dr. Christoph Sutter
CEN TC 224 WG 17 Chairman
C.Sutter@tuвит.de