Business Requirement Description / Business Solution Description

BMISR-POS TPDU

Client	Client's Name
Reference	BRD_BSD-BMISR-POS TPDU-20150324-1.1.doc
Version	1.1
Status	Release

Africa

HPS - Casablanca Nearshore Park, Shore 1
1100, boulevard Al Qods - Sidi Maârouf
20270 Casablanca Morocco

Tel: + 212 529 045 000

Middle East & Asia

HPS - 209 / 210 Building 12, 2nd Floor, P.O. Box 500308
Dubai Internet City, Dubai

Tel: + 971 4390 0750

Europe & Americas

HPS - 65-67 rue du Faubourg St Honoré 4th Floor
75008 Paris – France

Tel: + 33 1 58 18 01 34

900, rue Ampère
Pôle d'activité d'Aix en Provence
13851 Aix en Provence Cedex 03 France

Tel: + 33 4 42 91 42 99

Document Versions

Version	Status	Author(s)	Date	Modifications
1.0		Youssef Khaloufi	24/03/2015	Initial Version
1.1		Zakaria Belhaj	25/03/2015	Quality Validation

Reference Documents

Code	Document name	Version	By

Terminology & Abbreviations

Term	Definition
RFP	Request For Proposal

Distribution List

Company	Name	Position

Summary

1 Introduction

This document is the Business Requirement Description provided by HPS to BMISR POS TPDU during the project framing, in order to ensure that business requirements are fully defined and understood by all stakeholders

It contains both business requirements and business solution descriptions. The business requirements have been gathered during workshops sessions between project team from HPS, and Business representatives from BMISR.

The business solution descriptions are closely associated to the business requirements and they provide further detail describing how the functionality requested by Business can be delivered.

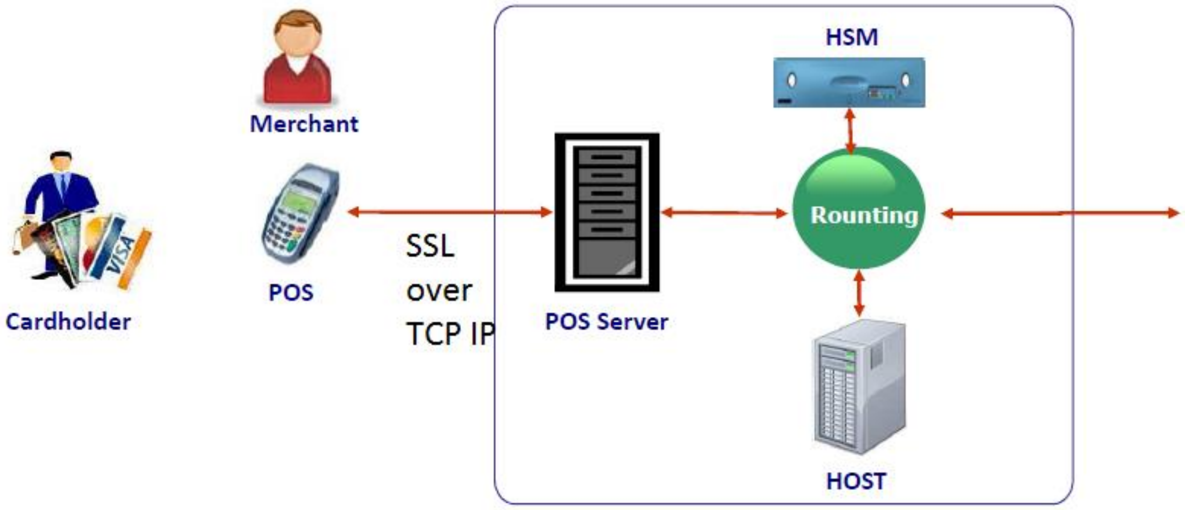
2 Project Context

Implement SSL over TCP/IP for POS ISO, using openssl library:

- Integrate ssl library over tcp/ip for POS ISO.
- Generate private Key using openssl
- Generate the CA certificate X509 with n year validation using openssl. This certificate should be installed in the terminals by POS provider tool.
- Generate PowerCARD Server certificate.

3 General Flow

The flow is standard flow between POS terminal and POS server. There is an additional requirement to exchanges the messages using the SSL over TCP/IP.



4 How to read this document

Each business requirement will have a unique reference number and is described within a table. A business requirement template will look like:

<table>
<tr><td><b>Unique Requirement Reference:</b>
<i>Unique reference given throughout the requirement description process. This reference will be used in all upcoming activities to identify it. i.e. : Project–001.1</i></td><td><b>Unique and unitary Requirement Identification:</b>
<i>Unique and unitary identification of requirement. i.e. :</i> Visa International clearing files reception</td></tr>
<tr><td><b>Priority :</b>
<i>Indicates requirement's priority level.</i>
<i>R: Required</i>
<i>P: Preferred</i>
<i>D: Preferred if the functionality is a standard one</i></td><td><b>Certification :</b>
<i>Indicates if the requirement requires a n external certification (CB, CUP, Visa, etc.).</i></td></tr>
<tr><td colspan="2"><b>Requirement description:</b>
<i>extract from Customer specifications data</i></td></tr>
<tr><td colspan="2"><b>Flows description:</b>
<i>Flow description (if necessary)</i></td></tr>
<tr><td><b>Ref. in Customer specification :</b>
<i>This zone allow to ensure that all requirement in specifications are covered by study and analysis activities</i></td><td><b>Ref. in HPS proposition:</b>
<i>Here, refer to items mentioned in HPS proposition.</i></td></tr>
<tr><td colspan="2"><b>Outputs and reports list:</b>
<i>Here list and/or describe outputs (files) and reports</i></td></tr>
<tr><td><b>Phase:</b>
<i>Project Phase(s) where the requirement is mandatory:</i>
- <i>Phase 1</i>
- <i>Phase 2</i>
- <i>Phase n</i></td><td><b>Availability :</b>
<i>Indicates if the requirement is covered by</i>
<i>- standard (S) (indicates the module and § of documentation that covers the requirement)</i>
<i>- By a planned customization (C)</i>
<i>- By a non-planned customization (E = Ecart)</i></td></tr>
<tr><td colspan="2">Understanding the requirement :
<i>This section describes how HPS understands the requirement. The information retrieved during exchanges with the Client (workshops, meetings and other documents ...) are also specified. They may even cancel and replace elements of the RFP.</i></td></tr>
<tr><td colspan="2">Description de la solution :
<i>Here you will describe the solution proposed (if HPS standard, describe how it works based on standard documentation)</i></td></tr>
</table>

5 Business requirements

5.1 Requirement: POS TPDU-001

5.1.1 Requirement: POS TPDU -001.1

Unique Requirement Reference: POS TPDU -001.1	**Unique and unitary Requirement Identification:** Integrate SSL over TCP/IP for POS ISO
Priority : *R: Required*	**Certification :** …

Requirement description:

Encrypt\Decrypt POS ISO messages using SSL.

Flows description:

Ref. in Customer specification :	**Ref. in HPS proposition:**

Outputs and reports list:

Phase	**Availability** :

Understanding the requirement :

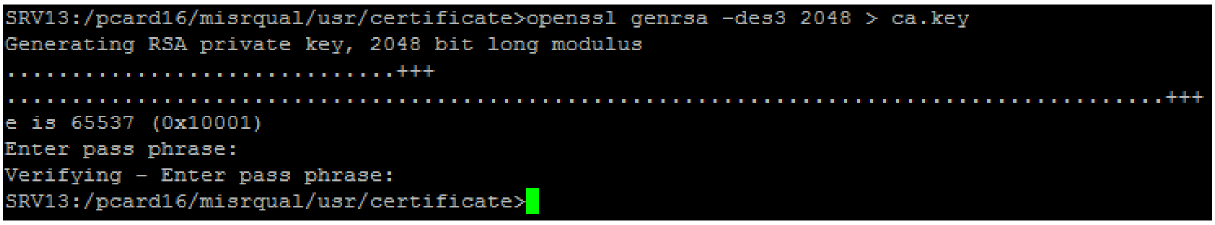
Encrypt POS ISO messages between POS ISO terminals and Server using SSL over TCP/IP.

Description de la solution :

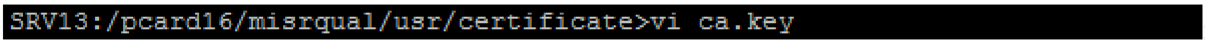
It is required to install openssl library in the PowerCARD Server.

Create new directory **usr/certificate** where you will generate the terminal and server certificates:

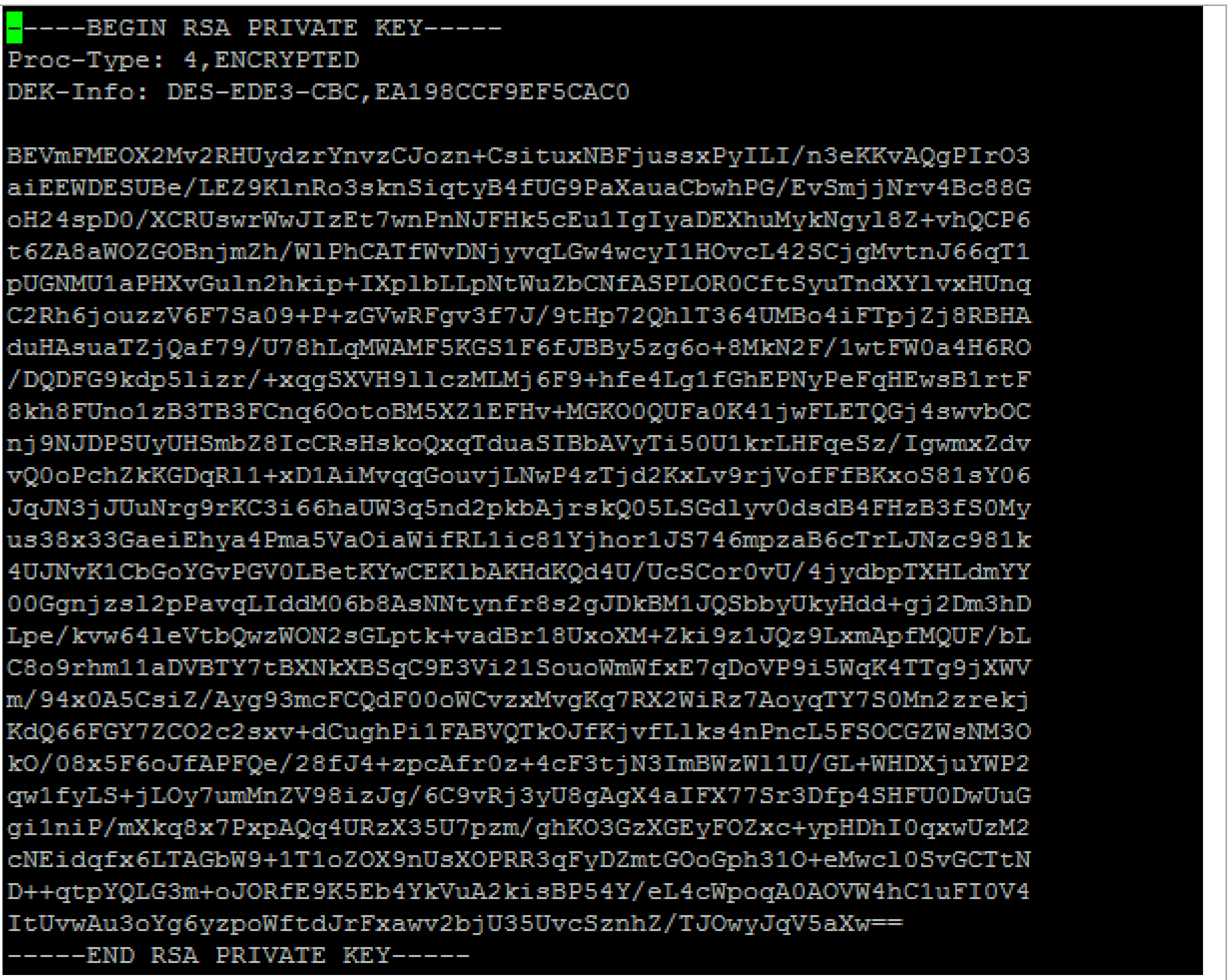
- **Step 1:** Generate the private key RSA 2048 bits for CA certificate:
  - **openssl genrsa -des3 2048 > ca.key**



```
SRV13:/pcard16/misrqual/usr/certificate>openssl genrsa -des3 2048 > ca.key
Generating RSA private key, 2048 bit long modulus
..............................+++
..........................................................................................+++
e is 65537 (0x10001)
Enter pass phrase:
Verifying - Enter pass phrase:
SRV13:/pcard16/misrqual/usr/certificate>
```



```
SRV13:/pcard16/misrqual/usr/certificate>vi ca.key
```



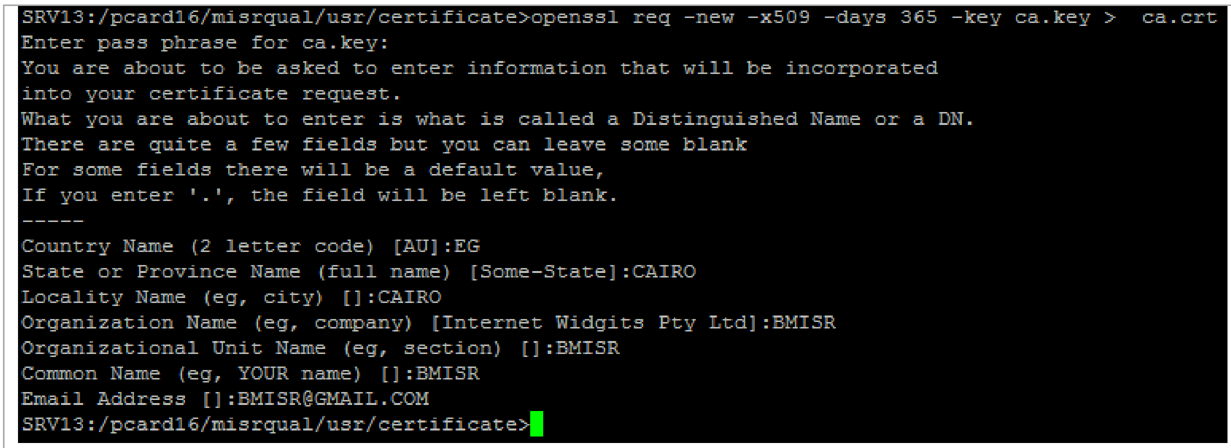
```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,EA198CCF9EF5CAC0

BEVmFMEOX2Mv2RHUydzrYnvzCJozn+CsituxNBFjussxPyILI/n3eKKvAQgPIrO3
aiEEWDESUBe/LEZ9KlnRo3sknSiqtyB4fUG9PaXauaCbwhPG/EvSmjjNrv4Bc88G
oH24spD0/XCRUswrWwJIzEt7wnPnNJFHk5cEu1IgIyaDEXhuMykNgyl8Z+vhQCP6
t6ZA8aWOZGOBnjmZh/WlPhCATfWvDNjyvqLGw4wcyI1HOvcL42SCjgMvtnJ66qT1
pUGNMU1aPHXvGuln2hkip+IXplbLLpNtWuZbCNfASPLOR0CftSyuTndXYlvxHUnq
C2Rh6jouzzV6F7Sa09+P+zGVwRFgv3f7J/9tHp72QhlT364UMBo4iFTpjZj8RBHA
duHAsuaTZjQaf79/U78hLqMWAMF5KGS1F6fJBBy5zg6o+8MkN2F/1wtFW0a4H6RO
/DQDFG9kdp5lizr/+xqgSXVH9llczMLMj6F9+hfe4Lg1fGhEPNyPeFqHEwsB1rtF
8kh8FUno1zB3TB3FCnq6OotoBM5XZ1EFHv+MGKO0QUFa0K41jwFLETQGj4swvbOC
nj9NJDPSUyUHSmbZ8IcCRsHskoQxqTduaSIBbAVyTi50U1krLHFqeSz/IgwmxZdv
vQ0oPchZkKGDqRl1+xD1AiMvqqGouvjLNwP4zTjd2KxLv9rjVofFfBKxoS81sY06
JqJN3jJUuNrg9rKC3i66haUW3q5nd2pkbAjrskQ05LSGdlyv0dsdB4FHzB3fS0My
us38x33GaeiEhya4Pma5VaOiaWifRL1ic81Yjhor1JS746mpzaB6cTrLJNzc981k
4UJNvK1CbGoYGvPGV0LBetKYwCEKlbAKHdKQd4U/UcSCor0vU/4jydbpTXHLdmYY
00Ggnjzsl2pPavqLIddM06b8AsNNtynfr8s2gJDkBM1JQSbbyUkyHdd+gj2Dm3hD
Lpe/kvw64leVtbQwzWON2sGLptk+vadBr18UxoXM+Zki9z1JQz9LxmApfMQUF/bL
C8o9rhm11aDVBTY7tBXNkXBSqC9E3Vi21SouoWmWfxE7qDoVP9i5WqK4TTg9jXWV
m/94x0A5CsiZ/Ayg93mcFCQdF00oWCvzxMvgKq7RX2WiRz7AoyqTY7S0Mn2zrekj
KdQ66FGY7ZCO2c2sxv+dCughPi1FABVQTkOJfKjvfLlks4nPncL5FSOCGZWsNM3O
kO/08x5F6oJfAPFQe/28fJ4+zpcAfr0z+4cF3tjN3ImBWzWl1U/GL+WHDXjuYWP2
qw1fyLS+jLOy7umMnZV98izJg/6C9vRj3yU8gAgX4aIFX77Sr3Dfp4SHFU0DwUuG
gi1niP/mXkq8x7PxpAQq4URzX35U7pzm/ghKO3GzXGEyFOZxc+ypHDhI0qxwUzM2
cNEidqfx6LTAGbW9+1T1oZOX9nUsXOPRR3qFyDZmtGOoGph31O+eMwcl0SvGCTtN
D++qtpYQLG3m+oJORfE9K5Eb4YkVuA2kisBP54Y/eL4cWpoqA0AOVW4hC1uFI0V4
ItUvwAu3oYg6yzpoWftdJrFxawv2bjU35UvcSznhZ/TJOwyJqV5aXw==
-----END RSA PRIVATE KEY-----
```

This has the effect of creating the private key of the certification authority. In this case, it is better to add -des3 the option that introduced the use of a "passphrase" (long password that can even contain white) because it is the private key that will sign all issued certificates. This "passphrase" will be applied to each key usage.

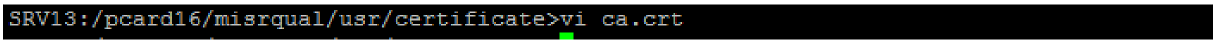
- **Step 2:** Generate the CA certificate X509 with 1 year validation using the private key:
    - **openssl req -new -x509 -days 365 -key ca.key > ca.crt**

You have to enter the passphrase used since ... "ca.key" is protected.

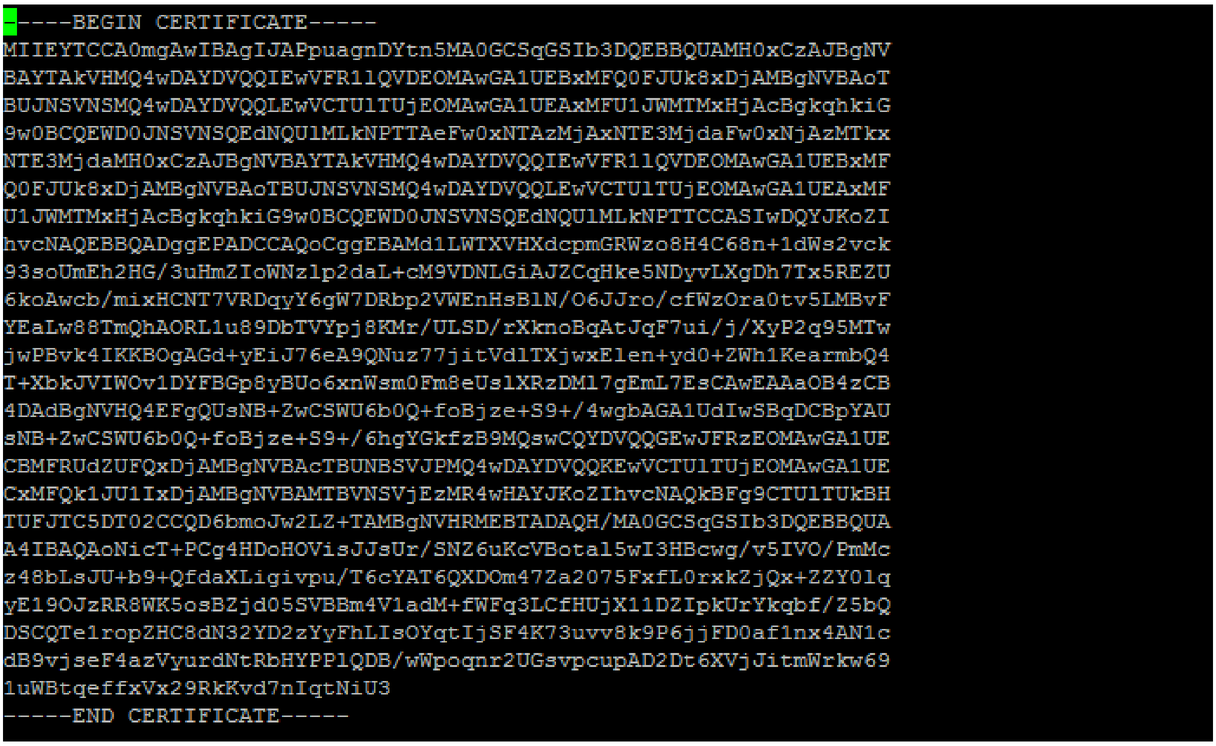
The system will ask to enter the field, this represents X.509 attributes of the certificate (not mandatory, but recommended). The information given on this time the certification authority except for the "**Common Name" field should match the host name of your virtual server:** The expected output is as follows:



```
SRV13:/pcard16/misrqual/usr/certificate>openssl req -new -x509 -days 365 -key ca.key >  ca.crt
Enter pass phrase for ca.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:EG
State or Province Name (full name) [Some-State]:CAIRO
Locality Name (eg, city) []:CAIRO
Organization Name (eg, company) [Internet Widgits Pty Ltd]:BMISR
Organizational Unit Name (eg, section) []:BMISR
Common Name (eg, YOUR name) []:BMISR
Email Address []:BMISR@GMAIL.COM
SRV13:/pcard16/misrqual/usr/certificate>
```



```
SRV13:/pcard16/misrqual/usr/certificate>vi ca.crt
```



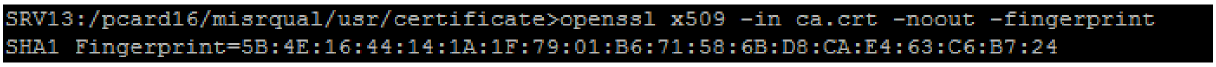
```
-----BEGIN CERTIFICATE-----
MIIEYTCCA0mgAwIBAgIJAPpuagnDYtn5MA0GCSqGSIb3DQEBBQUAMH0xCzAJBgNV
BAYTAkVHMQ4wDAYDVQQIEwVFR1lQVDEOMAwGA1UEBxMFQ0FJUk8xDjAMBgNVBAoT
BUJNSVNSMQ4wDAYDVQQLEwVCTU1TUjEOMAwGA1UEAxMFU1JWMTMxHjAcBgkqhkiG
9w0BCQEWD0JNSVNSQEdNQU1MLkNPTTAeFw0xNTAzMjAxNTE3MjdaFw0xNjAzMTkx
NTE3MjdaMH0xCzAJBgNVBAYTAkVHMQ4wDAYDVQQIEwVFR1lQVDEOMAwGA1UEBxMF
Q0FJUk8xDjAMBgNVBAoTBUJNSVNSMQ4wDAYDVQQLEwVCTU1TUjEOMAwGA1UEAxMF
U1JWMTMxHjAcBgkqhkiG9w0BCQEWD0JNSVNSQEdNQU1MLkNPTTCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBAMd1LWTXVHXdcpmGRWzo8H4C68n+1dWs2vck
93soUmEh2HG/3uHmZIoWNzlp2daL+cM9VDNLGiAJZCqHke5NDyvLXgDh7Tx5REZU
6koAwcb/mixHCNT7VRDqyY6gW7DRbp2VWEnHsBlN/O6JJro/cfWzOra0tv5LMBvF
YEaLw88TmQhAORL1u89DbTVYpj8KMr/ULSD/rXknoBqAtJqF7ui/j/XyP2q95MTw
jwPBvk4IKKBOgAGd+yEiJ76eA9QNuz77jitVdlTXjwxElen+yd0+ZWh1KearmbQ4
T+XbkJVIWOv1DYFBGp8yBUo6xnWsm0Fm8eUslXRzDM17gEmL7EsCAwEAAaOB4zCB
4DAdBgNVHQ4EFgQUsNB+ZwCSWU6b0Q+foBjze+S9+/4wgbAGA1UdIwSBqDCBpYAU
sNB+ZwCSWU6b0Q+foBjze+S9+/6hgYGkfzB9MQswCQYDVQQGEwJFRzEOMAwGA1UE
CBMFRUdZUFQxDjAMBgNVBAcTBUNBSVJPMQ4wDAYDVQQKEwVCTU1TUjEOMAwGA1UE
CxMFQk1JU1IxDjAMBgNVBAMTBVNSVjEzMR4wHAYJKoZIhvcNAQkBFg9CTU1TUkBH
TUFJTC5DT02CCQD6bmoJw2LZ+TAMBgNVHRMEBTADAQH/MA0GCSqGSIb3DQEBBQUA
A4IBAQAoNicT+PCg4HDoHOVisJJsUr/SNZ6uKcVBotal5wI3HBcwg/v5IVO/PmMc
z48bLsJU+b9+QfdaXLigivpu/T6cYAT6QXDOm47Za2075FxfL0rxkZjQx+ZZY01q
yE19OJzRR8WK5osBZjd05SVBBm4V1adM+fWFq3LCfHUjX11DZIpkUrYkqbf/Z5bQ
DSCQTe1ropZHC8dN32YD2zYyFhLIsOYqtIjSF4K73uvv8k9P6jjFD0af1nx4AN1c
dB9vjseF4azVyurdNtRbHYPP1QDB/wWpoqnr2UGsvpcupAD2Dt6XVjJitmWrkw69
1uWBtqeffxVx29RkKvd7nIqtNiU3
-----END CERTIFICATE-----
```

This is the certificate authority certificate that will allow you to sign all certificates created.

To not make mistakes, we define the fingerprint, by typing:

- **openssl x509 -in ca.crt -noout -fingerprint**

The expected output is as follows:

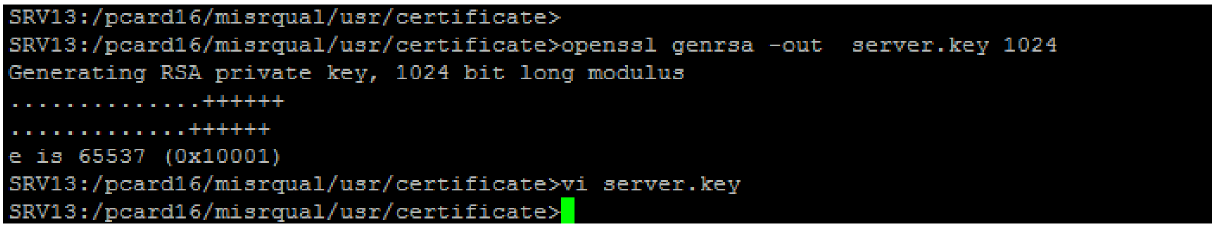


```
SRV13:/pcard16/misrqual/usr/certificate>openssl x509 -in ca.crt -noout -fingerprint
SHA1 Fingerprint=5B:4E:16:44:14:1A:1F:79:01:B6:71:58:6B:D8:CA:E4:63:C6:B7:24
```

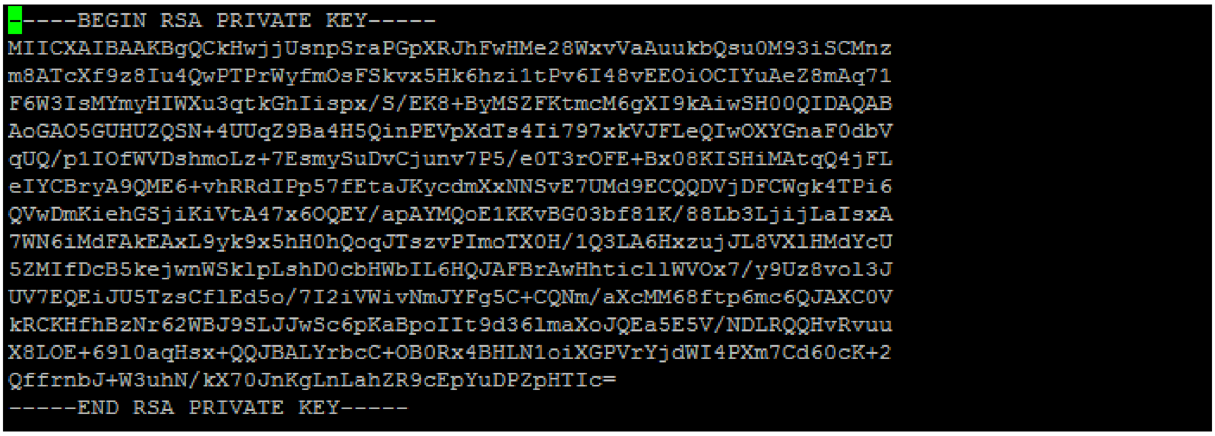
These 20 bytes are listed footprint of the certificate and allow verification that it is not corrupt.

The CA certificate is now created.

- **Step 3:** Generate private key for SSL certificate:
  - **openssl genrsa -out server.key 1024**



```
SRV13:/pcard16/misrqual/usr/certificate>
SRV13:/pcard16/misrqual/usr/certificate>openssl genrsa -out  server.key 1024
Generating RSA private key, 1024 bit long modulus
..............++++++
.............++++++
e is 65537 (0x10001)
SRV13:/pcard16/misrqual/usr/certificate>vi server.key
SRV13:/pcard16/misrqual/usr/certificate>
```

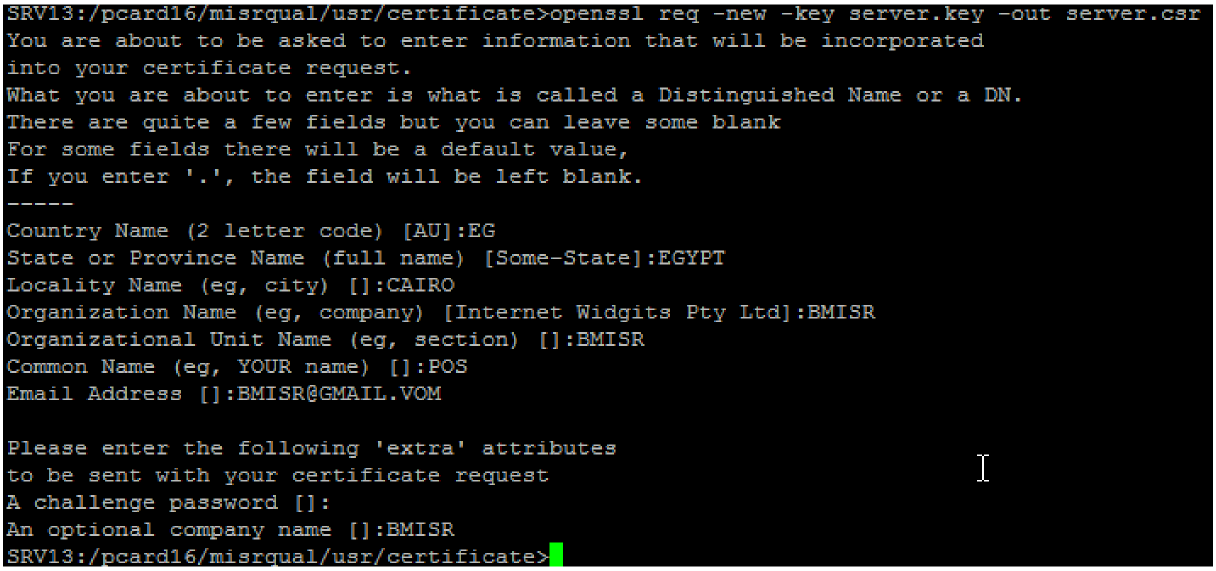


```
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQCkHwjjUsnpSraPGpXRJhFwHMe28WxvVaAuukbQsu0M93iSCMnz
m8ATcXf9z8Iu4QwPTPrWyfmOsFSkvx5Hk6hzi1tPv6I48vEEOiOCIYuAeZ8mAq71
F6W3IsMYmyHIWXu3qtkGhIispx/S/EK8+ByMSZFKtmcM6gXI9kAiwSH00QIDAQAB
AoGAO5GUHUZQSN+4UUqZ9Ba4H5QinPEVpXdTs4Ii797xkVJFLeQIwOXYGnaF0dbV
qUQ/p1IOfWVDshmoLz+7EsmySuDvCjunv7P5/e0T3rOFE+Bx08KISHiMAtqQ4jFL
eIYCBryA9QME6+vhRRdIPp57fEtaJKycdmXxNNSvE7UMd9ECQQDVjDFCWgk4TPi6
QVwDmKiehGSjiKiVtA47x6OQEY/apAYMQoE1KKvBG03bf81K/88Lb3LjijLaIsxA
7WN6iMdFAkEAxL9yk9x5hH0hQoqJTszvPImoTX0H/1Q3LA6HxzujJL8VX1HMdYcU
5ZMIfDcB5kejwnWSklpLshD0cbHWbIL6HQJAFBrAwHhticl1WVOx7/y9Uz8vol3J
UV7EQEiJU5TzsCflEd5o/7I2iVWivNmJYFg5C+CQNm/aXcMM68ftp6mc6QJAXC0V
kRCKHfhBzNr62WBJ9SLJJwSc6pKaBpoIIt9d361maXoJQEa5E5V/NDLRQQHvRvuu
X8LOE+6910aqHsx+QQJBALYrbcC+OB0Rx4BHLN1oiXGPVrYjdWI4PXm7Cd60cK+2
QffrnbJ+W3uhN/kX70JnKgLnLahZR9cEpYuDPZpHTIc=
-----END RSA PRIVATE KEY-----
```

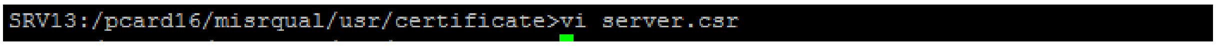
Its effect is to create an SSL key (server.key file), it is the private key.

- **Step 4:** Generate Certificate Signing Request:
  - **openssl req -new -key server.key -out server.csr**

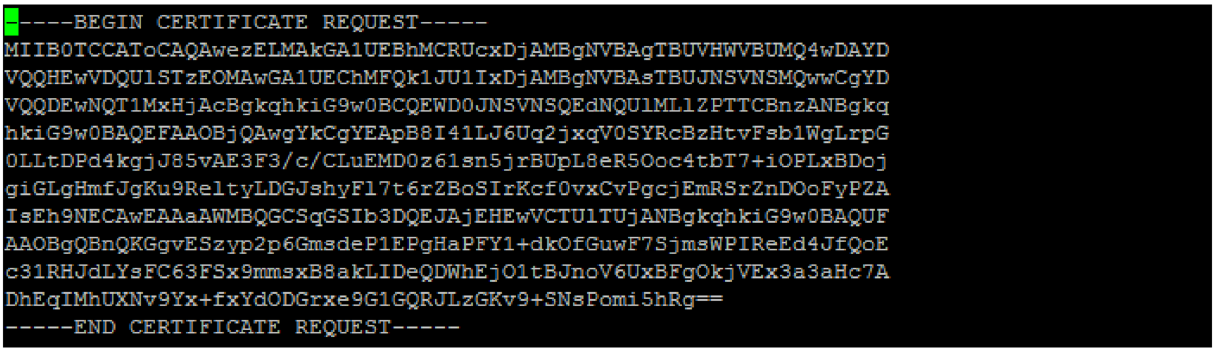
Warning: the "Common Name" must be different from that which was given to the key CA.



```
SRV13:/pcard16/misrqual/usr/certificate>openssl req -new -key server.key -out server.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:EG
State or Province Name (full name) [Some-State]:EGYPT
Locality Name (eg, city) []:CAIRO
Organization Name (eg, company) [Internet Widgits Pty Ltd]:BMISR
Organizational Unit Name (eg, section) []:BMISR
Common Name (eg, YOUR name) []:POS
Email Address []:BMISR@GMAIL.VOM

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:BMISR
SRV13:/pcard16/misrqual/usr/certificate>
```



```
SRV13:/pcard16/misrqual/usr/certificate>vi  server.csr
```

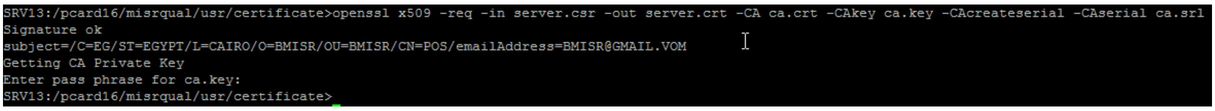


```
-----BEGIN CERTIFICATE REQUEST-----
MIIB0TCCAToCAQAwezELMAkGA1UEBhMCRUcxDjAMBgNVBAgTBUVHWVBUMQ4wDAYD
VQQHEwVDQU1STzEOMAwGA1UEChMFQk1JU1IxDjAMBgNVBAsTBUJNSVNSMQwwCgYD
VQQDEwNQT1MxHjAcBgkqhkiG9w0BCQEWD0JNSVNSQEdNQU1MLlZPTTCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwgYkCgYEApB8I41LJ6Uq2jxqV0SYRcBzHtvFsb1WgLrpG
OLLtDPd4kgjJ85vAE3F3/c/CLuEMD0z61sn5jrBUpL8eR5Ooc4tbT7+iOPLxBDoj
giGLgHmfJgKu9ReltyLDGJshyFl7t6rZBoSIrKcf0vxCvPgcjEmRSrZnDOoFyPZA
IsEh9NECAwEAAaAWMBQGCSqGSIb3DQEJAjEHEwVCTU1TUjANBgkqhkiG9w0BAQUF
AAOBgQBnQKGgvESzyp2p6GmsdeP1EPgHaPFY1+dkOfGuwF7SjmsWPIReEd4JfQoE
c31RHJdLYsFC63FSx9mmsxB8akLIDeQDWhEjO1tBJnoV6UxBFgOkjVEx3a3aHc7A
DhEqIMhUXNv9Yx+fxYdODGrxe9G1GQRJLzGKv9+SNsPomi5hRg==
-----END CERTIFICATE REQUEST-----
```

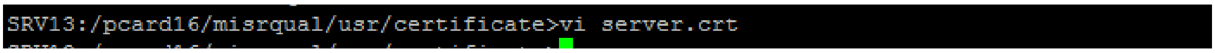
Its effect is to create the certificate request form (server.csr) from our key Private previously created.

- **Step 5:** Signature of certificate with certificate authority:
  - **openssl x509 -req -in server.csr -out server.crt -CA ca.crt -CAkey ca.key -CAcreateserial -CAserial ca.srl**

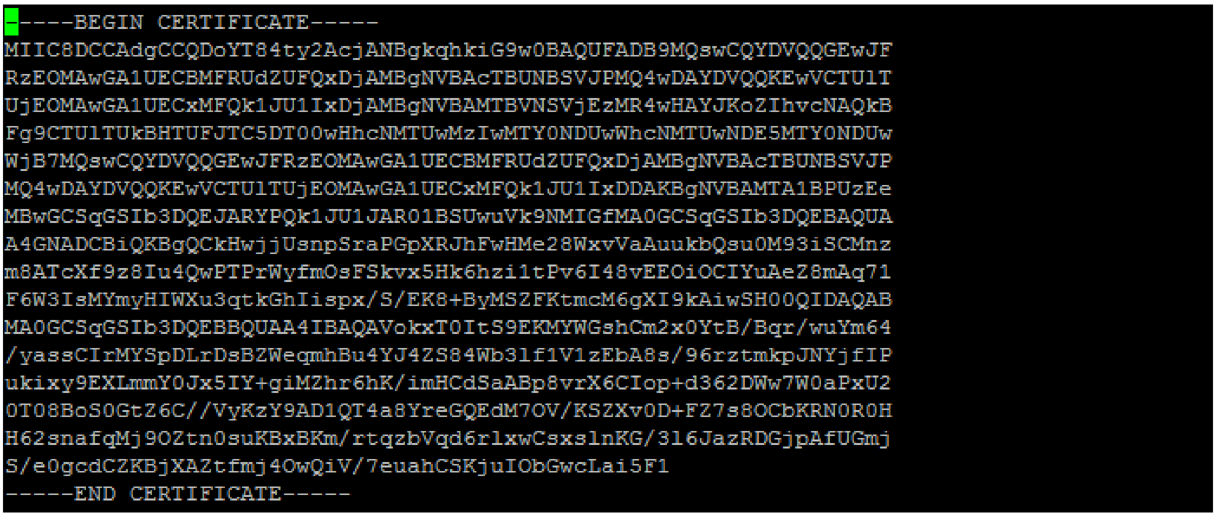
The CAcreateserial option is only necessary for the first time.



```
SRV13:/pcard16/misrqual/usr/certificate>openssl x509 -req -in server.csr -out server.crt -CA ca.crt -CAkey ca.key -CAcreateserial -CAserial ca.srl
Signature ok
subject=/C=EG/ST=EGYPT/L=CAIRO/O=BMISR/OU=BMISR/CN=POS/emailAddress=BMISR@GMAIL.VOM
Getting CA Private Key
Enter pass phrase for ca.key:
SRV13:/pcard16/misrqual/usr/certificate>
```



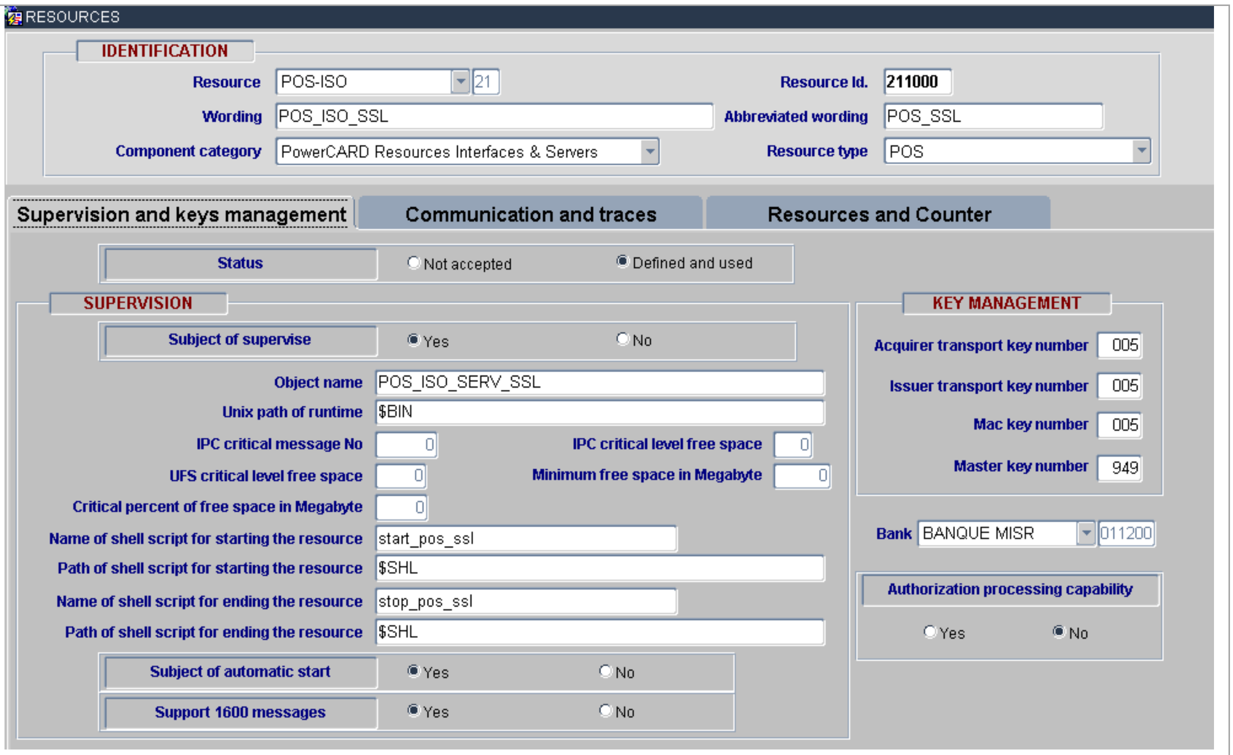
```
SRV13:/pcard16/misrqual/usr/certificate>vi  server.crt
```



```
-----BEGIN CERTIFICATE-----
MIIC8DCCAdgCCQDoYT84ty2AcjANBgkqhkiG9w0BAQUFADB9MQswCQYDVQQGEwJF
RzEOMAwGA1UECBMFRUdZUFQxDjAMBgNVBAcTBUNBSVJPMQ4wDAYDVQQKEwVCTU1T
UjEOMAwGA1UECxMFQk1JU1IxDjAMBgNVBAMTBVNSVjEzMR4wHAYJKoZIhvcNAQkB
Fg9CTU1TUkBHTUFJTC5DT00wHhcNMTUwMzIwMTY0NDUwWhcNMTUwNDE5MTY0NDUw
WjB7MQswCQYDVQQGEwJFRzEOMAwGA1UECBMFRUdZUFQxDjAMBgNVBAcTBUNBSVJP
MQ4wDAYDVQQKEwVCTU1TUjEOMAwGA1UECxMFQk1JU1IxDDAKBgNVBAMTA1BPUzEe
MBwGCSqGSIb3DQEJARYPQk1JU1JAR01BSUwuVk9NMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCkHwjjUsnpSraPGpXRJhFwHMe28WxvVaAuukbQsu0M93iSCMnz
m8ATcXf9z8Iu4QwPTPrWyfmOsFSkvx5Hk6hzi1tPv6I48vEEOiOCIYuAeZ8mAq71
F6W3IsMYmyHIWXu3qtkGhIispx/S/EK8+ByMSZFKtmcM6gXI9kAiwSH00QIDAQAB
MA0GCSqGSIb3DQEBBQUAA4IBAQAVokxT0ItS9EKMYWGshCm2x0YtB/Bqr/wuYm64
/yassCIrMYSpDLrDsBZWeqmhBu4YJ4ZS84Wb31f1V1zEbA8s/96rztmkpJNYjfIP
ukixy9EXLmmY0Jx5IY+giMZhr6hK/imHCdSaABp8vrX6CIop+d362DWw7W0aPxU2
0T08BoS0GtZ6C//VyKzY9AD1QT4a8YreGQEdM7OV/KSZXv0D+FZ7s8OCbKRN0R0H
H62snafqMj9OZtn0suKBxBKm/rtqzbVqd6rlxwCsxslnKG/316JazRDGjpAfUGmj
S/e0gcdCZKBjXAZtfmj4OwQiV/7euahCSKjuIObGwcLai5F1
-----END CERTIFICATE-----
```

We now have a certificate naming server.crt.

- Give the certificate ca.crt to POS provider to integrate in the POS.
- POS resource parameters:



RESOURCES

IDENTIFICATION

Resource: POS-ISO 21
Resource Id.: 211000
Wording: POS_ISO_SSL
Abbreviated wording: POS_SSL
Component category: PowerCARD Resources Interfaces & Servers
Resource type: POS

Status: ○ Not accepted ● Defined and used

SUPERVISION

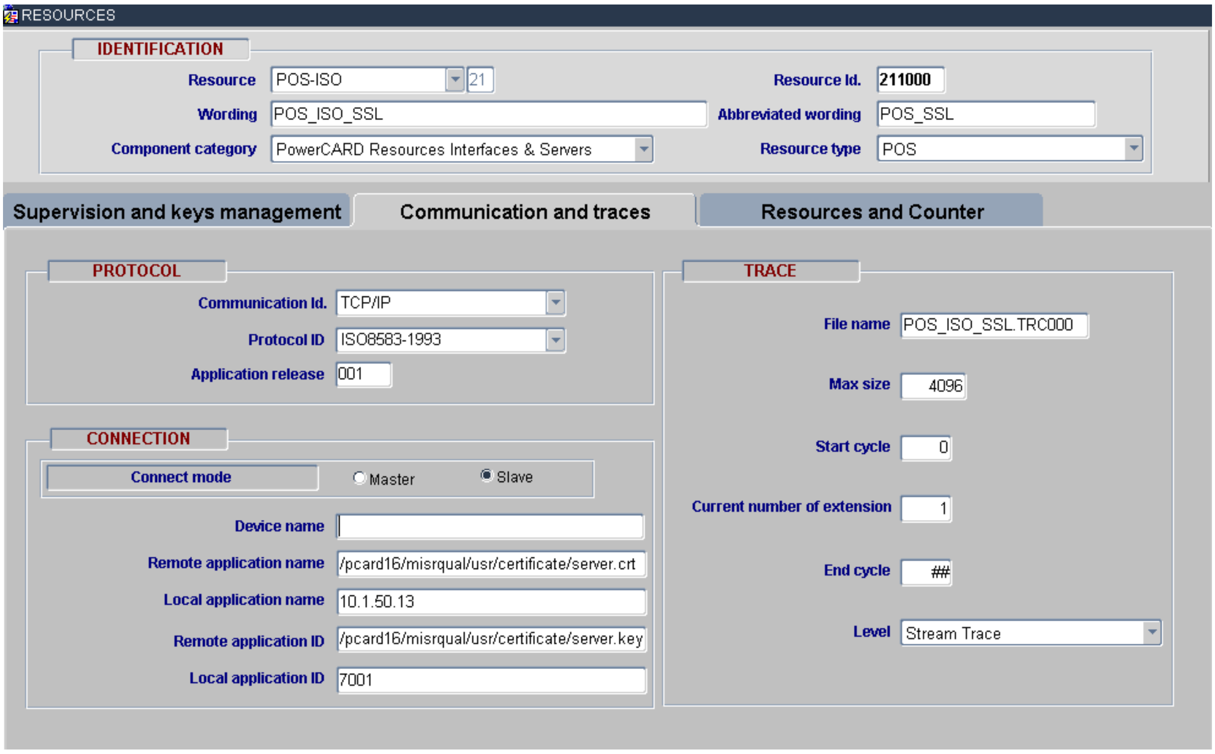
Subject of supervise: ● Yes ○ No
Object name: POS_ISO_SERV_SSL
Unix path of runtime: $BIN
IPC critical message No: 0
IPC critical level free space: 0
UFS critical level free space: 0
Minimum free space in Megabyte: 0
Critical percent of free space in Megabyte: 0
Name of shell script for starting the resource: start_pos_ssl
Path of shell script for starting the resource: $SHL
Name of shell script for ending the resource: stop_pos_ssl
Path of shell script for ending the resource: $SHL
Subject of automatic start: ● Yes ○ No
Support 1600 messages: ● Yes ○ No

KEY MANAGEMENT

Acquirer transport key number: 005
Issuer transport key number: 005
Mac key number: 005
Master key number: 949

Bank: BANQUE MISR 011200

Authorization processing capability: ○ Yes ● No



RESOURCES

IDENTIFICATION

Resource: POS-ISO 21
Resource Id.: 211000
Wording: POS_ISO_SSL
Abbreviated wording: POS_SSL
Component category: PowerCARD Resources Interfaces & Servers
Resource type: POS

PROTOCOL

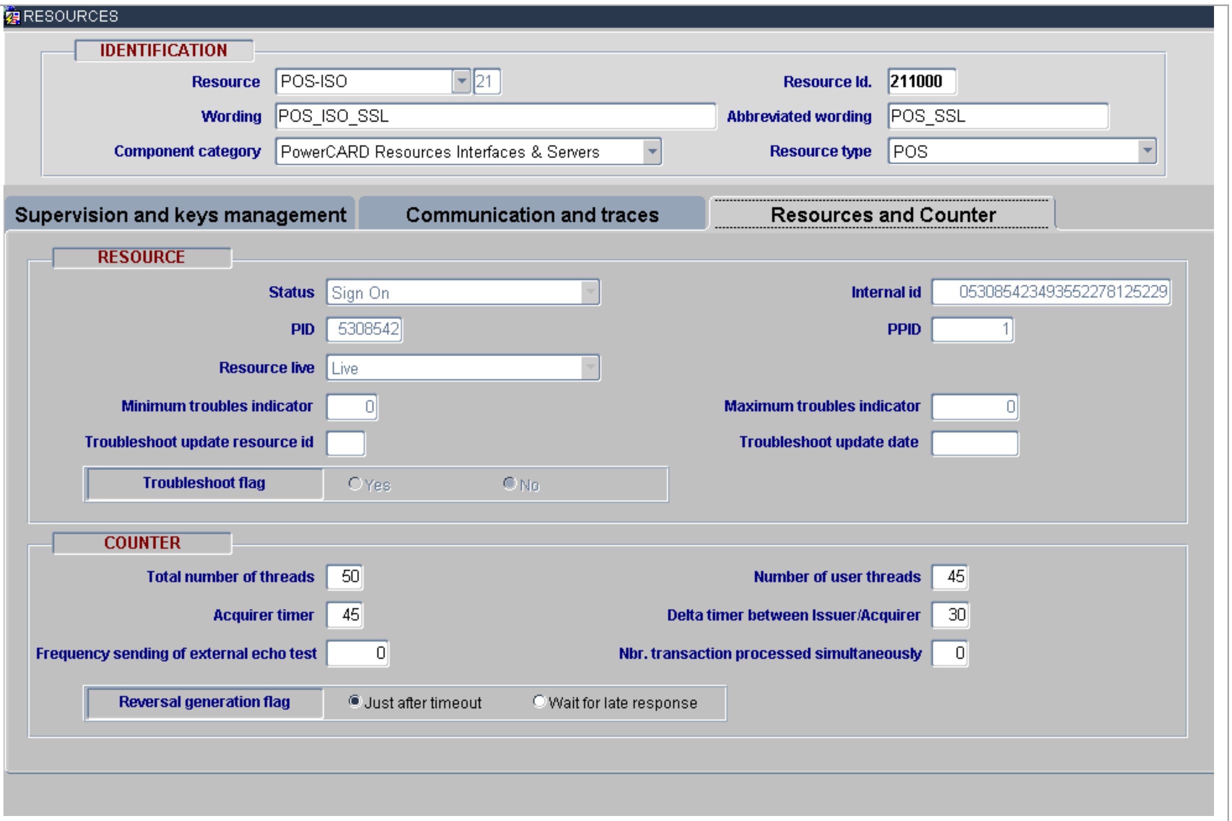
Communication Id.: TCP/IP
Protocol ID: ISO8583-1993
Application release: 001

CONNECTION

Connect mode: ○ Master ● Slave
Device name:
Remote application name: /pcard16/misrqual/usr/certificate/server.crt
Local application name: 10.1.50.13
Remote application ID: /pcard16/misrqual/usr/certificate/server.key
Local application ID: 7001

TRACE

File name: POS_ISO_SSL.TRC000
Max size: 4096
Start cycle: 0
Current number of extension: 1
End cycle: ##
Level: Stream Trace



IDENTIFICATION

Resource: POS-ISO 21
Resource Id.: 211000
Wording: POS_ISO_SSL
Abbreviated wording: POS_SSL
Component category: PowerCARD Resources Interfaces & Servers
Resource type: POS

RESOURCE

Status: Sign On
Internal id: 053085423493552278125229
PID: 5308542
PPID: 1
Resource live: Live
Minimum troubles indicator: 0
Maximum troubles indicator: 0
Troubleshoot update resource id:
Troubleshoot update date:
Troubleshoot flag: ○ Yes ● No

COUNTER

Total number of threads: 50
Number of user threads: 45
Acquirer timer: 45
Delta timer between Issuer/Acquirer: 30
Frequency sending of external echo test: 0
Nbr. transaction processed simultaneously: 0
Reversal generation flag: ● Just after timeout ○ Wait for late response

6 Summary of coverage:

Customer specifications References	Requirements References

Customer specifications References	HPS proposition References

7 Acceptance of the Business Requirements

The undersigned acknowledge receipt of PowerCARD Document (referenced under brd_bsd-BMISR-POS TPDU-20150324-1.0) and its appendices. The undersigned have read and understood this document and agree with it.

For ______________________________: [CUSTOMER’S NAME HERE]	For HPS
Name:________________________________ [MUST BE AN AUTHORIZED REPRESENTATIVE]	Name:________________________________ [MUST BE AN AUTHORIZED REPRESENTATIVE]
Position:__________________________________	Position:________________________________ _
Date:__________________________________	Date:__________________________________
Signature:	Signature:

8 Acceptance of the Business Solutions

The undersigned acknowledge receipt of PowerCARD Document (referenced under brd_bsd-BMISR-POS TPDU-20150324-1.0) and its appendices. The undersigned have read and understood this document and agree with it.

For ______________________________:

[CUSTOMER'S NAME HERE]

Name:________________________________

[MUST BE AN AUTHORIZED REPRESENTATIVE]

Position:__________________________________

Date:_________________________________

Signature:

For HPS

Name:________________________________

[MUST BE AN AUTHORIZED REPRESENTATIVE]

Position:________________________________
_

Date:_________________________________

Signature: