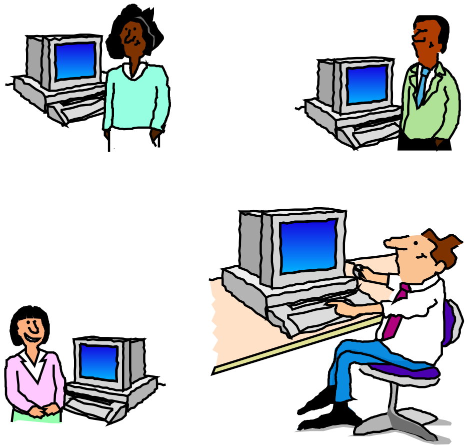
Client Authentication

in CWS/SSL with VSE/ESA 2.6.2

Helmut Hellner
VSE/ESA Development
hhellner@de.ibm.com

December 5, 2002



The Secure Sockets Layer (SSL) protocol is a common way to secure the data exchange between clients and servers in the Web. It provides data privacy and integrity as well as server and client authentication based on public key certificates.

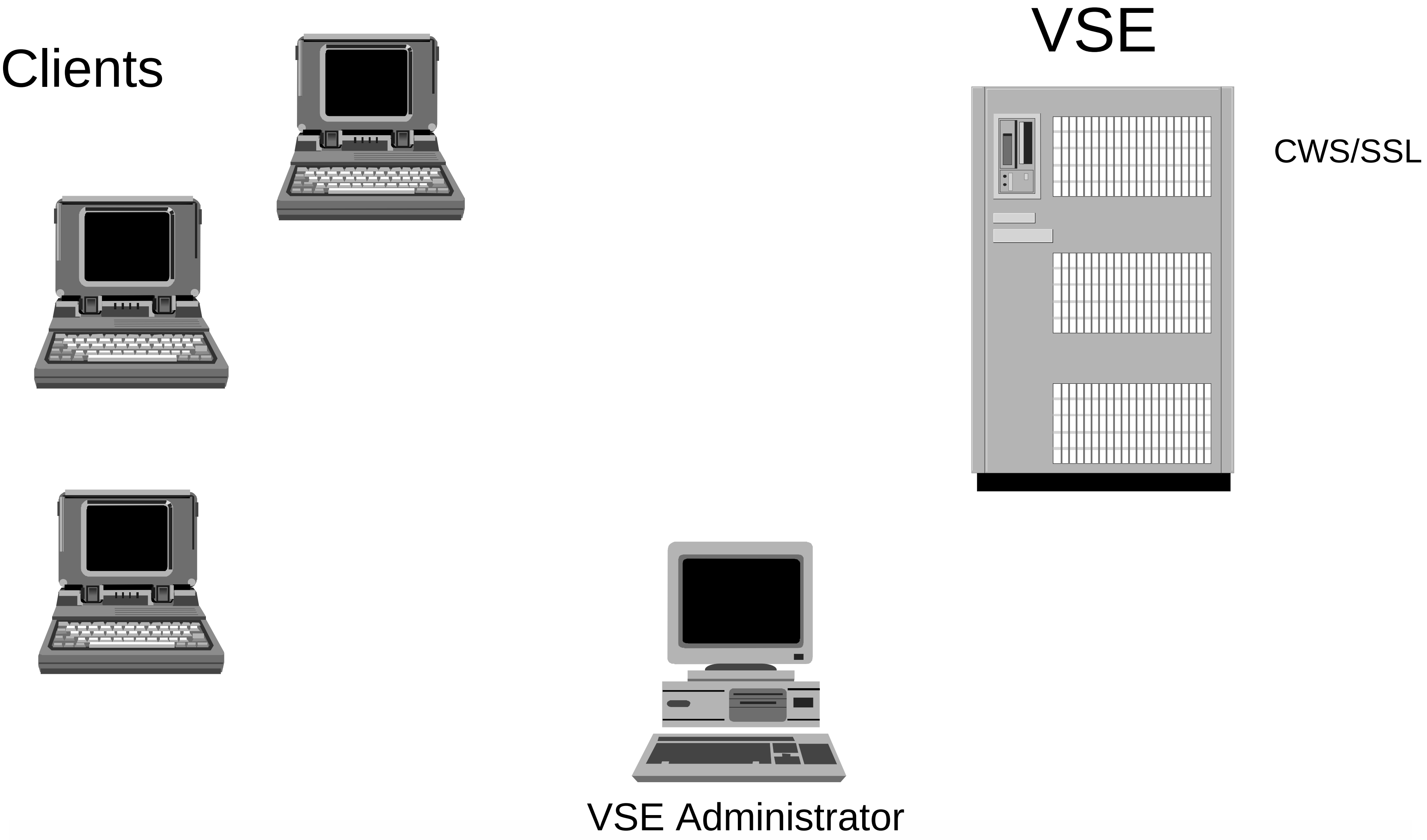
A certificate identifies the owner like a passport. It contains also the public key of the owner. Only the owner has the private key. Data encrypted with the private key can only be decrypted with the public key and vice versa.

To ensure integrity, the certificate is digitally signed with the private key of an external authority known as a certificate authority.

In SSL, the server certificate is mandatory, but the client certificate is optional. It is up to the server (that is, CICS or VSE Java-based Connectors) to decide whether to accept a connection from a client without a certificate.

The client authentication capability in CICS Web Support (CWS) including EXTRACT CERTIFICATE is available with VSE/ESA 2.6.2. The following presentation provides an overview how client authentication with CWS works and how it can be used in a customer environment.

Customer Environment



Clients

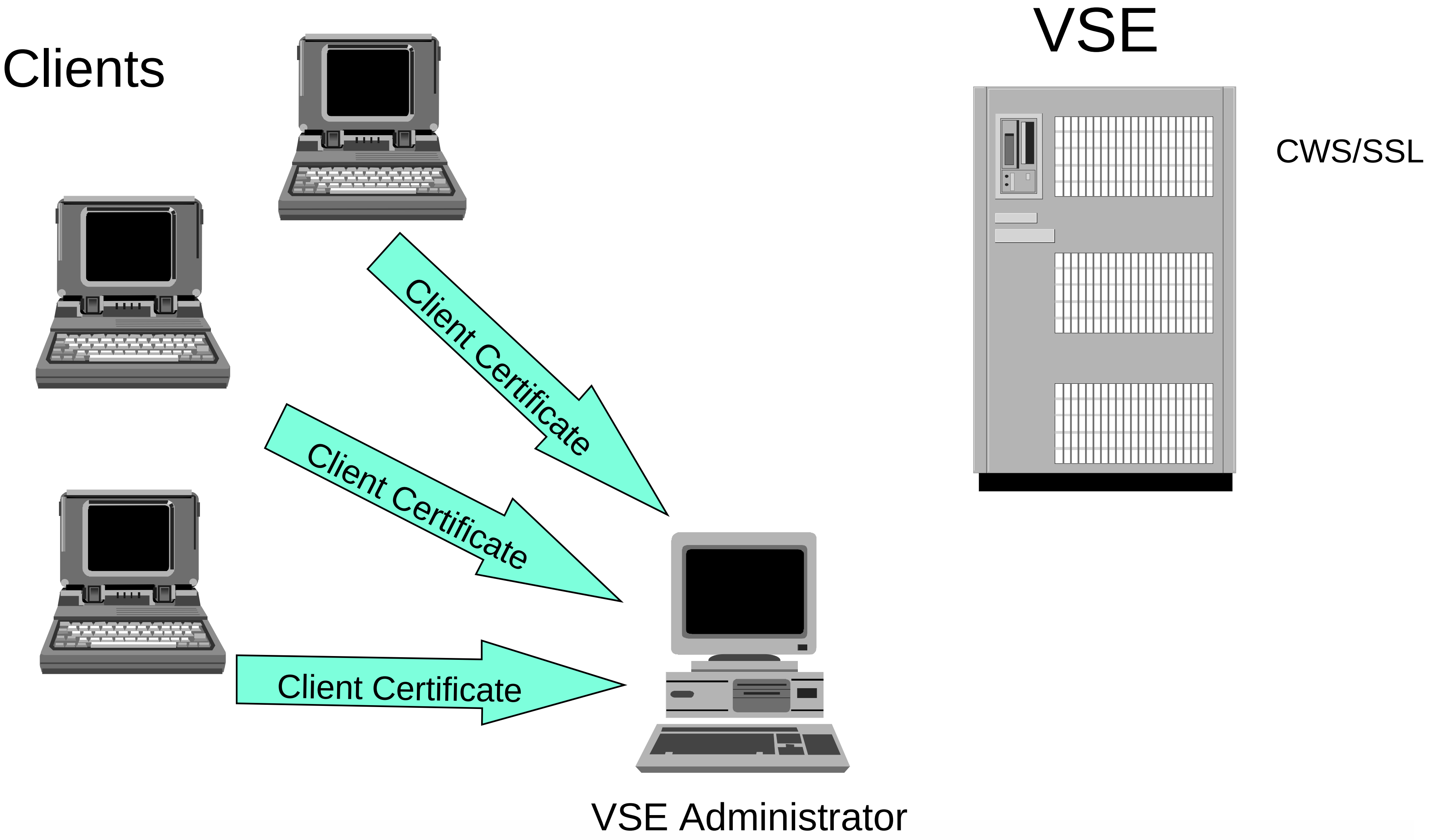
VSE

CWS/SSL

VSE Administrator

Let us assume that we have three clients which should be able to use sensitive server applications (e.g. show the daily revenue). As opposed to most Web applications, these clients must be defined to the server before they can connect to the server. Therefore they send their own certificates to the VSE administrator for registration (see next page).

Get the Client Certificates

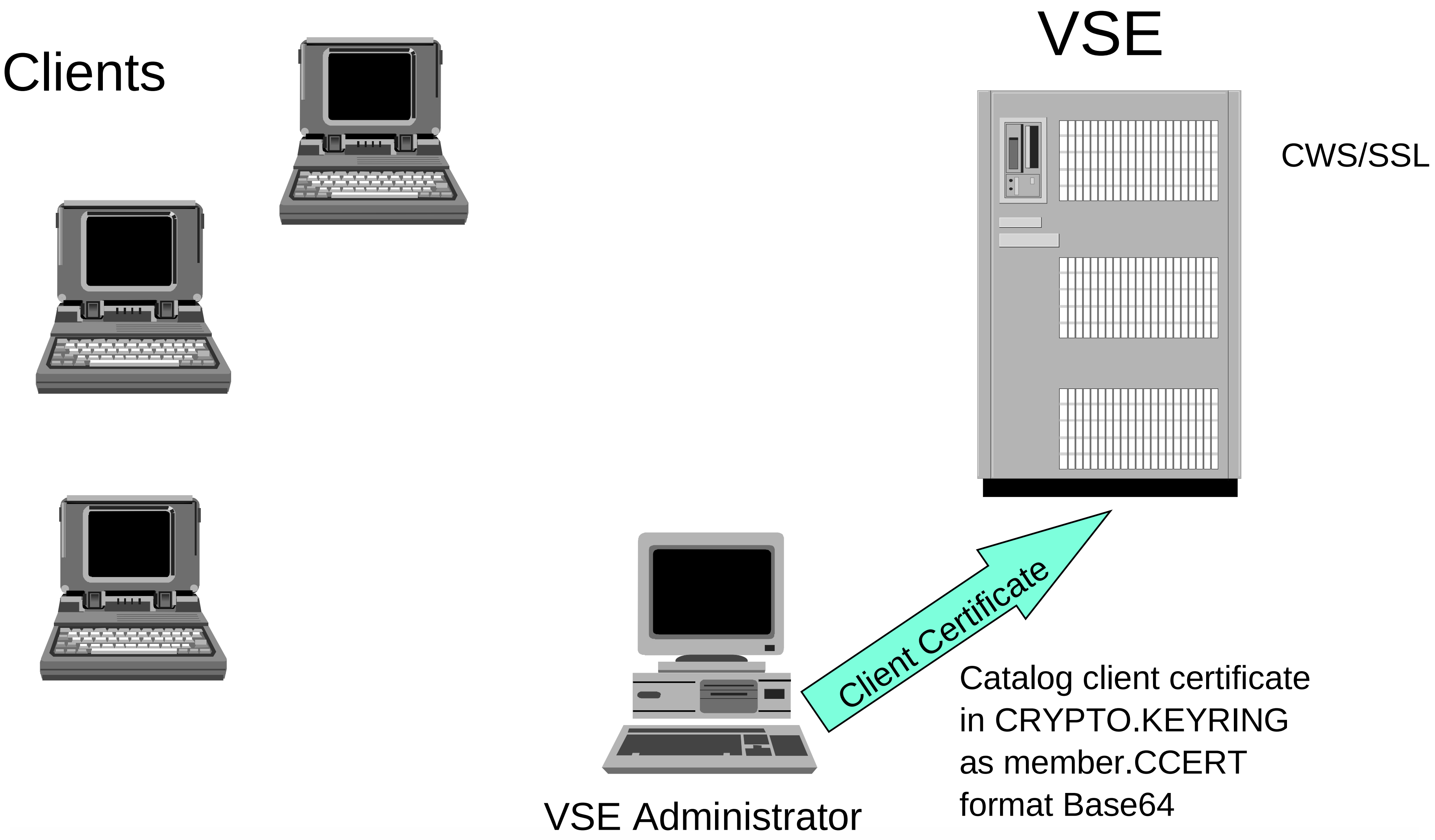


The clients have to provide their certificates in Base64 format. It looks like this:

```
-----BEGIN CERTIFICATE-----
MIICUDCCAbkCBN50nYUwDQYJKoZIhvcNAQEFBQAwcjEqMCgGA1UEAxMhSGVsbXV0
J3MgVEVTVCBST09UIENBIENlcnRpZmljYXRlMRQwEgYDVQQLEwtEZXZlbG9wbWVu
dDEMMAoGA1UEChMDSUJNMRMwEQYDVQQHEwpCb2VibGluZ2VuMQswCQYDVQQGEwJE
RTAeFw0wMjA1MTcxMjQzNTNaFw0wNTA2MTYyMjAwMDBaMGwxJDAiBgNVBAMTG0hl
bG11dCdzIENsaWVudCBDZXJ0aWZpY2F0ZTEUMBIGA1UECxMLRGV2ZWxvcG1lbnQx
DDAKBgNVBAoTA0lCTTETMBEGA1UEBxMKQm9lYmxpbmdlbjELMAkGA1UEBhMCREUw
gZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAJ2clxsQ2JlC+Rn4fE6FJFZWDNjl
/n0GO17+Pz6gVZi+PJgA0UOzuh+0nj3a3KmbNast+svNhPAWv60t6/DxnOYK65Ck
vXALI3dzAS7sGVo0+9arQyCnuZBfM2VEjKMNi2uGOWXDG7sHnW51a3K63sq7N+Kw
O9JxFQ83DL+JqFNLAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAjHTqXTsckRvUjMzU
ZCCPV48i2tquRe4aFlsOsXQ7BY8I/QpxTVEAGdwmpCzVg+RNRGdBk+VPmL+TCj07
Z/9zxOQ7AKqXeI1U/hsSQHCNKpG0udt834d+Rp9sZBPPQS3Hu0+1QDkfqw52V969
C/FB4llwBFJT+f0xofbzvfrBomA=
-----END CERTIFICATE-----
```

The VSE administrator stores each client certificate as a separate member in his VSE crypto sublibrary (default CRYPTO.KEYRING). The member type is CCERT. The contents of the certificate should not be converted to upper cases.

Catalog the Client Certificates



Clients

VSE

CWS/SSL

Client Certificate

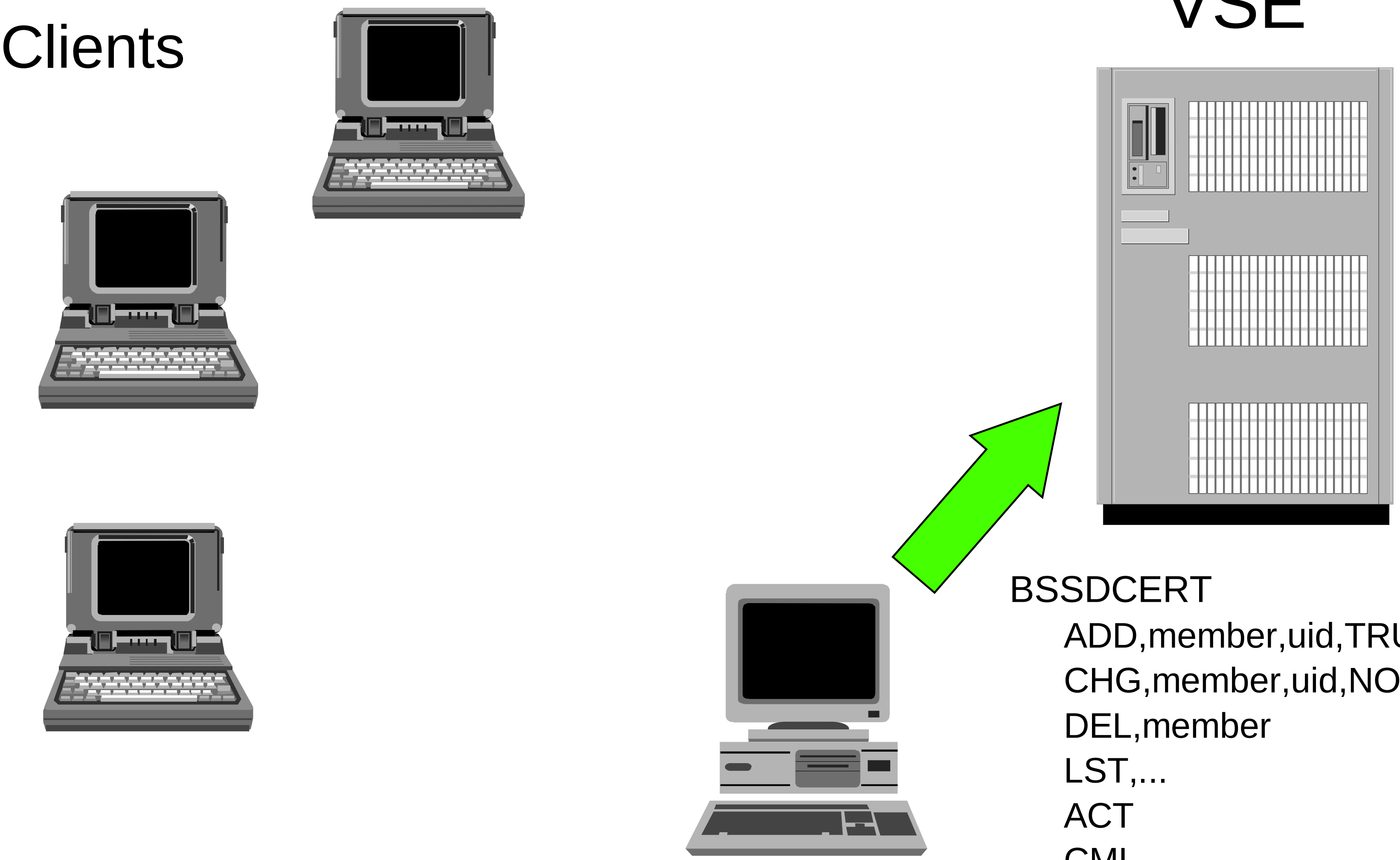
Catalog client certificate
in CRYPTO.KEYRING
as member.CCERT
format Base64

VSE Administrator

Now we have the client certificates on the VSE systems but the access control functions of VSE can only handle user IDs and not certificates. Therefore the VSE administrator has to register the client and assign a VSE user ID to each client certificate. This information will be store in an external mapping list.

For this administration work the new service BSSDCERT was introduced (see next page).

Client Certificate Administration



Clients

VSE

CWS/SSL

VSE Administrator

```
BSSDCERT
    ADD,member,uid,TRUST
    CHG,member,uid,NOTRUST
    DEL,member
    LST,...
    ACT
    CML,...
    STA,...
```

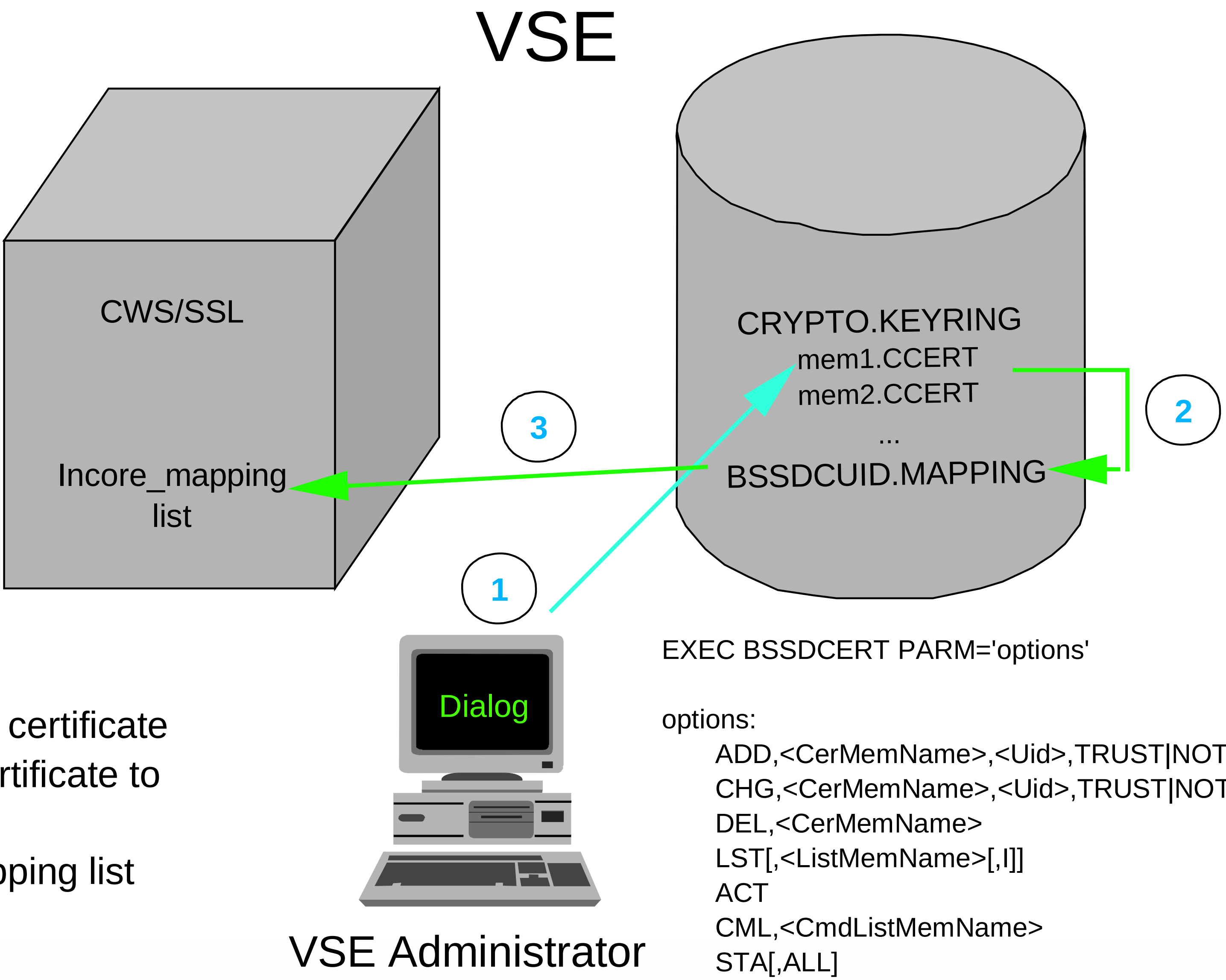
The different functions of BSSDCERT can be specified as option of parameter PARM=. With the function ADD, CHG, and DEL the VSE administrator creates and modifies the assignments of client certificates and user IDs in the member BSSDCUID.MAPPING. This member is called an external mapping list.

The function ACT extracts information from the external mapping list and creates an incore mapping and activates it. Only the incore mapping list will be used by the applications for certificate verification.

An II dialog is available to support this administration work (fastpath 29).

All these administration steps are shown on the next page.

Client Certificate Administration



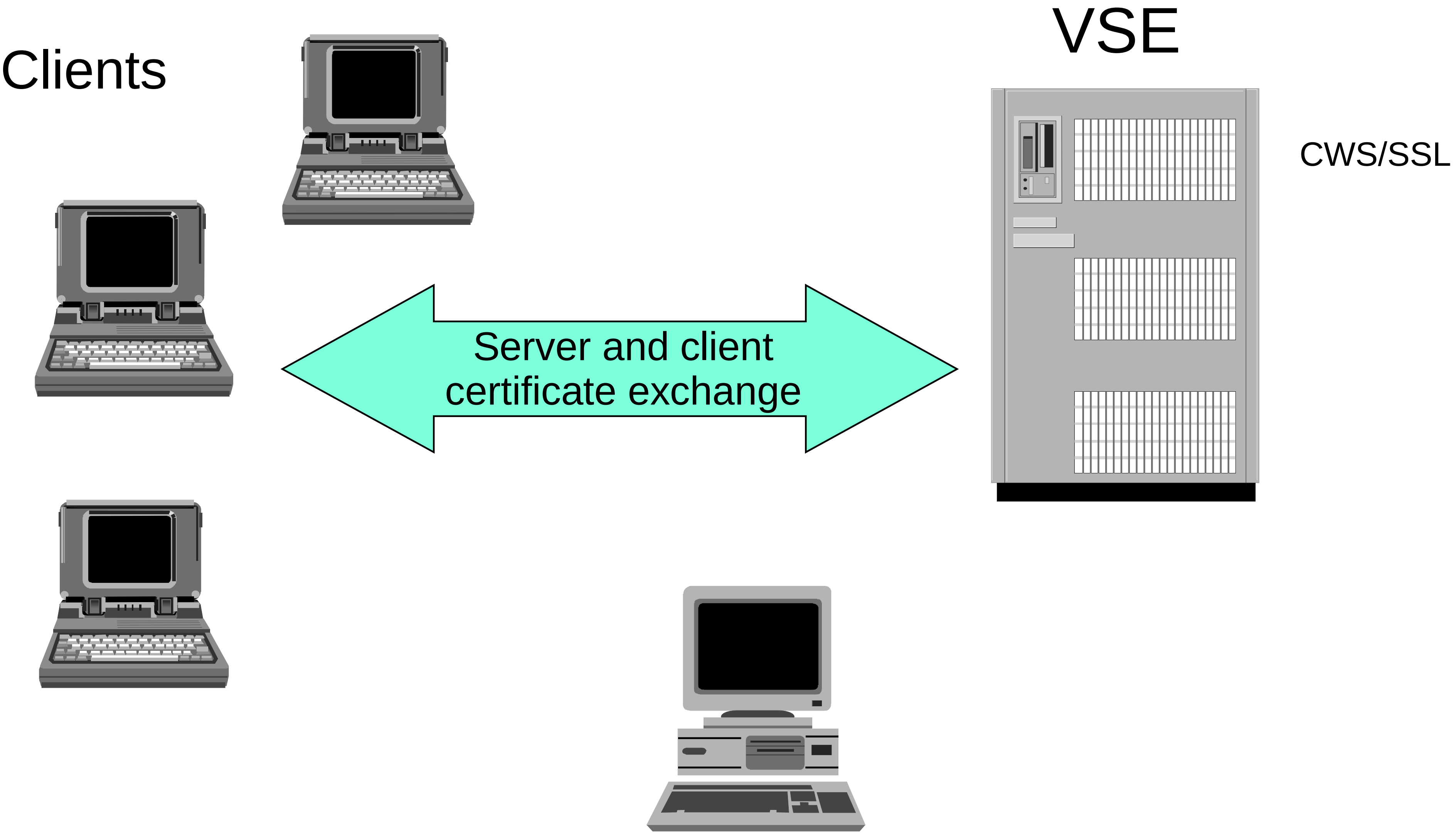
1 Catalog client certificate
2 ADD client certificate to mapping list
3 ACTivate mapping list

```
EXEC BSSDCERT PARM='options'

options:
      ADD,<CerMemName>,<Uid>,TRUST|NOTRUST
      CHG,<CerMemName>,<Uid>,TRUST|NOTRUST
      DEL,<CerMemName>
      LST[,<ListMemName>[,l]]
      ACT
      CML,<CmdListMemName>
      STA[,ALL]
```

Now, the incore mapping list is ready to be used by an application which requires client authentication when a client connects.

SSL Client Authentication



Clients

VSE

CWS/SSL

Server and client certificate exchange

VSE Administrator

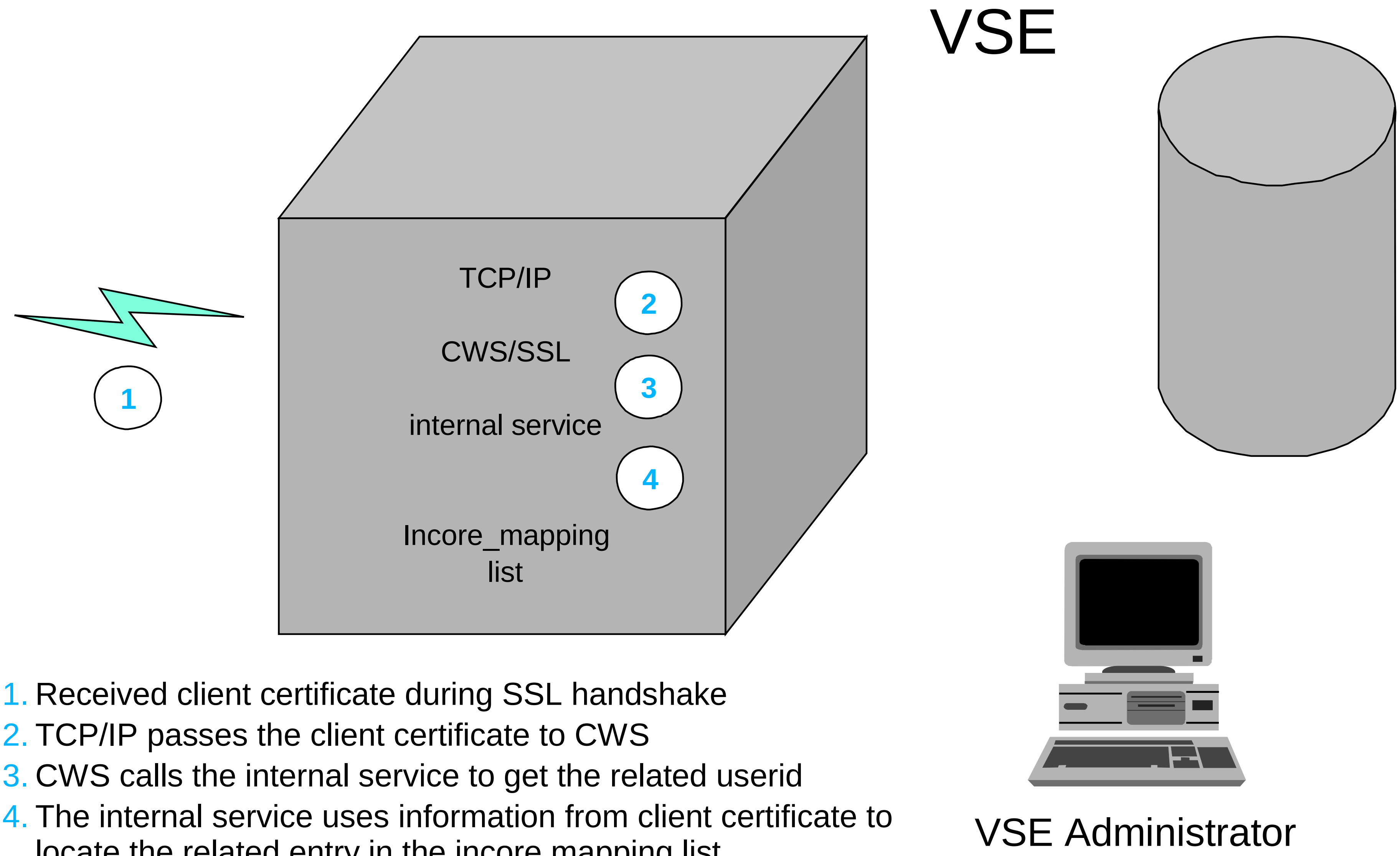
The client connects to the server and provides its certificate during the SSL handshaking.

The application (here CICS CWS) receives this client certificate and uses an internal service to check whether this client certificate is in the incore mapping list, whether it can be trusted, and which user ID was assigned to it.

CICS CWS uses this user ID for authorization checks.

These steps are shown on the next page.

Get Userid for Client Certificate



1. Received client certificate during SSL handshake
2. TCP/IP passes the client certificate to CWS
3. CWS calls the internal service to get the related userid
4. The internal service uses information from client certificate to locate the related entry in the incore mapping list

With VSE/ESA 2.6.2 EXEC CICS EXTRACT CERTIFICATE is supported. It allows a CICS application to obtain information from the X.509 client certificate. This information identifies the owner and the Certificate Authority that issued the certificate.

To exploit SSL with client authentication from CICS CWS the following settings are involved.

SIT parameters:

- ENCRYPTION
- KEYFILE
- SSLDELAY
- TCPIP

TCPIPSERVICE resource definition parameters:

- PORTNUMBER
- CERTIFICATE
- SSL

These CICS parameters and the related TCP/IP definition are described in details at:

- CICS Transaction Server for VSE/ESA Enhancement Guide (GC34-5763)
- VSE/ESA e-business Connectors User's Guide (SC33-6719)