Registration Authority at ETH Zurich

Tolga Coban Dieter Hennig Michael Koloff

ETH Zurich

18. April 2007

Introduction

No self-sign certificates visible for end user in production any more.

Motivation

- We want to change the policy as seldom as possible. SwissSign → GlobalSign?
- Roll out – only the administrators are entrusted with the responsibility to organizing the certificates.
- Approval end user are happy to have «really good certificates»

Efforts

We have run into problems by using a wildcard-certificate for our WCMS. IE 7 is interpreting **.ethz.ch* in a different way from Firefox 2.0 and Opera 9.2.

We are using Alternative Subject Names.

Our certificates can be imported by different type of equipment.

We cab search all computers on port 443 within the IT-Services.

We encountered no problems changing the root-cert, but at present it would pose a problem reverting to SwissSign, should they still be at the same stage as 2 years ago.

We have implemented a strict separation of Support and RA. This decision is final and not subject to any discussion.

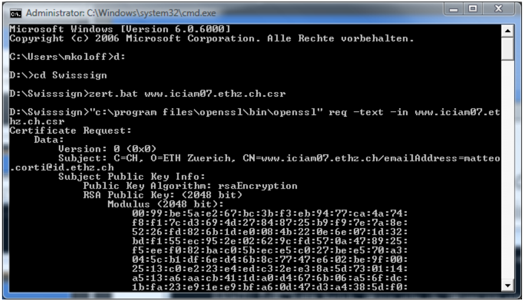
Problems

1. Colleagues from the IT-Service were definitely NOT amused.
2. Most people are so flooded by their daily work that they don't have the time to install or to ask for the right names for the certificate.
3. The multi-name certificates are hardly to check plus they maintain the disorder common in the early days.
4. Personally, I have only actually seen all SwissSign and GlobalSign forms for a few minutes.

The only problem, I recall with GlobalSign was: «who is the person who signed the contract?».
By showing the ETH Zurich website and the *who-is-who* the problem can be solved in a matter of minutes.

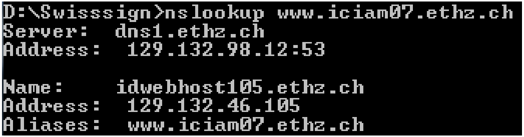
First control

First, we check the attributes and do a name server lookup for the requested domain.



```
Microsoft Windows [Version 6.0.6000]
Copyright (c) 2006 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Users\mkoloff>d:

D:\>cd Swisssign

D:\Swisssign>zert.bat www.iciam07.ethz.ch.csr

D:\Swisssign>"c:\program files\openssl\bin\openssl" req -text -in www.iciam07.et
hz.ch.csr
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=CH, O=ETH Zuerich, CN=www.iciam07.ethz.ch/emailAddress=matteo
.corti@id.ethz.ch
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:99:be:5a:e2:67:bc:3b:f3:eb:94:77:ca:4a:74:
                    f8:f1:7c:d3:69:4d:27:84:87:25:b9:f9:7e:7a:8e:
                    52:26:fd:82:6b:1d:e0:08:4b:22:0e:6e:07:1d:32:
                    bd:f1:55:ec:95:2e:02:62:9c:fd:57:0a:47:89:25:
                    f5:ee:f0:82:ba:c0:5b:ec:e5:c0:27:be:e5:70:a3:
                    04:5c:b1:df:6e:d4:6b:8c:77:47:e6:02:be:9f:00:
                    25:13:c0:e2:23:e4:ed:c3:2e:e3:8a:5d:73:01:14:
                    a5:13:a6:aa:cb:41:1d:a0:d4:67:6b:06:a5:6f:dc:
                    1b:fa:23:e9:1e:e9:bf:a6:0d:47:d3:a4:38:5d:f0:
```

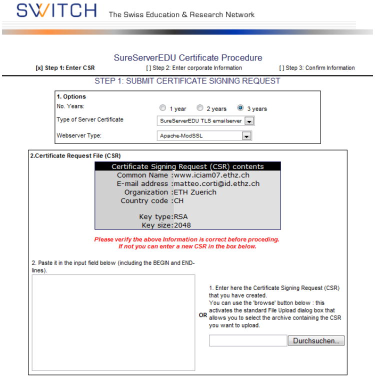
Figure: openssl req -text csr.pem



```
D:\Swisssign>nslookup www.iciam07.ethz.ch
Server:  dns1.ethz.ch
Address:  129.132.98.12:53

Name:    idwebhost105.ethz.ch
Address:  129.132.46.105
Aliases:  www.iciam07.ethz.ch
```

Figure: nslookup

Enter the request



SWITCH The Swiss Education & Research Network

SureServerEDU Certificate Procedure

[x] Step 1: Enter CSR [ ] Step 2: Enter corporate Information [ ] Step 3: Confirm Information

STEP 1: SUBMIT CERTIFICATE SIGNING REQUEST

1. Options

No. Years: ○ 1 year ○ 2 years ● 3 years

Type of Server Certificate: SureServerEDU TLS emailserver

Webserver Type: Apache-ModSSL

2.Certificate Request File (CSR)

Certificate Signing Request (CSR) contents

Common Name :www.iciam07.ethz.ch
E-mail address :matteo.corti@id.ethz.ch
Organization :ETH Zuerich
Country code :CH

Key type:RSA
Key size:2048

Please verify the above Information is correct before proceding.
If not you can enter a new CSR in the box below.

2. Paste it in the input field below (including the BEGIN and END-lines).

OR

1. Enter here the Certificate Signing Request (CSR) that you have created.
You can use the 'browse' button below : this activates the standard File Upload dialog box that allows you to select the archive containing the CSR you want to upload.

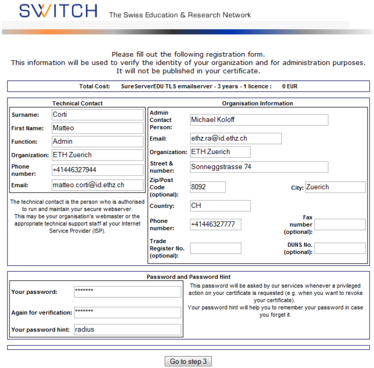
Figure: Switch-Web-Site

At the Switch submit page we use these settings:

- 3 years.
- SureServerEDUTLS emailserver.
- Webserver Type.
- Path to the request.

Enter corporate information

- The information page automatically shows the email address from the applicant.
- All other information must be entered manually.
- A password is necessary to revoke the certificate.



SWITCH The Swiss Education & Research Network

Please fill out the following registration form.
This information will be used to verify the identity of your organization and for administration purposes.
It will not be published in your certificate.

Total Cost: SureServerEDU TLS emailserver - 3 years - 1 licence : 0 EUR

Technical Contact

Surname:	Corti
First Name:	Matteo
Function:	Admin
Organization:	ETH Zuerich
Phone number:	+41446327944
Email:	matteo.corti@id.ethz.ch

The technical contact is the person who is authorised to run and maintain your secure webserver.
This may be your organisation's webmaster or the appropriate technical support staff at your Internet Service Provider (ISP).

Organisation Information

Admin Contact Person:	Michael Koloff		
Email:	ethz.ra@id.ethz.ch		
Organization:	ETH Zuerich		
Street & number:	Sonneggstrasse 74		
Zip/Post Code (optional):	8092	City:	Zuerich
Country:	CH		
Phone number:	+41446327777	Fax number (optional):	
Trade Register No. (optional):		DUNS No. (optional):	

Password and Password Hint

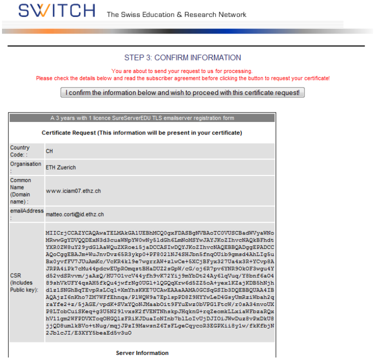
Your password:	*******
Again for verification:	*******
Your password hint:	radius

This password will be asked by our services whenever a privileged action on your certificate is requested (e.g. when you want to revoke your certificate).
Your password hint will help you to remember your password in case you forget it.

Figure: Switch-Web-Site

Terminate the request

- The page presents a summary of the entered information.
- After submit, requesting is finished.



SWITCH The Swiss Education & Research Network

STEP 3: CONFIRM INFORMATION

You are about to send your request to us for processing.
Please check the details below and read the subscriber agreement before clicking the button to request your certificate!

I confirm the information below and wish to proceed with this certificate request!

A 3 years with 1 licence SureServerEDU TLS emailserver registration form

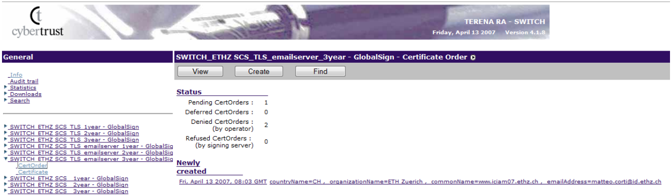
Certificate Request (This information will be present in your certificate)

Country Code: :	CH
Organisation :	ETH Zuerich
Common Name (Domain name) :	www.iciam07.ethz.ch
emailAddress :	matteo.corti@id.ethz.ch
CSR (Includes Public key):	MIICrjCCAZYCAQAwaTELMAkGA1UEBhMCQ0gxFDASBgNVBAoTC0VUSCBadWVyaWNo MRwwGgYDVQQDExN3d3cuaWNpYW0wNy5ldGh6LmNoMSYwJAYJKoZIhvcNAQkBFhdt YXR0ZW8uY29ydGlAaWQuZXRoei5jaDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC AQoCggEBAJm+WuJnvDvz65R3ykp0+PF802lNJ4SHJbn5fnqOUib9gmsd4AhLIg5u Bx0yvfFV7JUuAmKc/VcKR4kl9e7wgrrAW+zlwCe+5XCjBFyx327Ua4x3R+YCvp8A JRPA4iPk7cMu44pdcwEUpROmqstBHaDUZ2sGpW/cG/oj6R7pv6YNR9OkOF3wgu4Y d52vdSRvvm/jaAzQ/HU7O1vcV44yfh9vK72Yij9mYbDt24Ay6lqVuq/Y8bnf6aO4 89shVkUFY4qsAH5fkQu4jwfrNg0UGl+lQGQqXrw6d5ZZ5oA+yex1KZajKDB5hNjh d1z1SNGhBqTEvpRsLCq1+XmYhsKKE7UCAwEAAaAAMA0GCSqGSIb3DQEBBQUAA4IB AQAjzI6nKho7ZM7WFfEhnqa/PlWQW9a7EplspPD8Z9HYYwLeD4GsyUmRziWbah2q raYfe2+z/5jAGE/vpdK+SVxYQoNJMaabOit9FYuEwz0bVPG1FtcW/r0sA34nvoUX P8LTobCuiSKeq+g3U5N29lvxsK2fVENTNhskpJHqknG+rqZeomkLLxiaWFbzaRQx hV11gm2WFPDVXToqOHGQlzFRiKJDuaIoNInb7blLoIvUjDJIOiJWwDuz8vPxDkU8 jjQD8umlkBVo+tNug/mqjJPzI9MawsnZ6TsFLgeCqycoR3EGPXii8y1w/fkKfbjN 2JblcJI/E3XYY5beaEd5v3uO

Server Information

Issue certificate order I

- In the „CertOrder“ of the GlobalSign website you see all your requests, wich you have to process.
- This site utilizes your own personal certificate for authentication.



cybertrust

TERENA RA - SWITCH

Friday, April 13 2007 Version 4.1.8

General

- Info
- Audit trail
- ▸ Statistics
- ▸ Downloads
- ▸ Search

- ▸ SWITCH_ETHZ SCS_TLS_1year - GlobalSign
- ▸ SWITCH_ETHZ SCS_TLS_2year - GlobalSign
- ▸ SWITCH_ETHZ SCS_TLS_3year - GlobalSign
- ▸ SWITCH_ETHZ SCS_TLS_emailserver_1year - GlobalSig
- ▸ SWITCH_ETHZ SCS_TLS_emailserver_2year - GlobalSig
- ▾ SWITCH_ETHZ SCS_TLS_emailserver_3year - GlobalSig
  - CertOrder
  - Certificate
- ▸ SWITCH_ETHZ SCS_ 1year - GlobalSign
- ▸ SWITCH_ETHZ SCS_ 2year - GlobalSign
- ▸ SWITCH_ETHZ SCS_ 3year - GlobalSign

SWITCH_ETHZ SCS_TLS_emailserver_3year - GlobalSign - Certificate Order

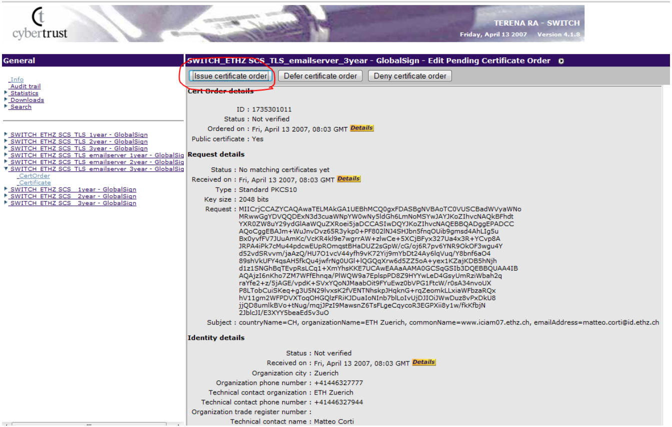
Status

Pending CertOrders :	1
Deferred CertOrders :	0
Denied CertOrders : (by operator)	2
Refused CertOrders : (by signing server)	0

Newly created

Fri, April 13 2007, 08:03 GMT countryName=CH , organizationName=ETH Zuerich , commonName=www.iciam07.ethz.ch , emailAddress=matteo.corti@id.ethz.ch

Issue certificate order II



TERENA RA - SWITCH
Friday, April 13 2007 Version 4.1.8

General

- Info
- Audit trail
- Statistics
- Downloads
- Search

- SWITCH_ETHZ SCS_TLS_1year - GlobalSign
- SWITCH_ETHZ SCS_TLS_2year - GlobalSign
- SWITCH_ETHZ SCS_TLS_3year - GlobalSign
- SWITCH_ETHZ SCS_TLS_emailserver_1year - GlobalSig
- SWITCH_ETHZ SCS_TLS_emailserver_2year - GlobalSig
- SWITCH_ETHZ SCS_TLS_emailserver_3year - GlobalSig
  - CertOrder
  - Certificate
- SWITCH_ETHZ SCS__1year - GlobalSign
- SWITCH_ETHZ SCS__2year - GlobalSign
- SWITCH_ETHZ SCS__3year - GlobalSign

SWITCH_ETHZ SCS_TLS_emailserver_3year - GlobalSign - Edit Pending Certificate Order

Cert Order details

```
               ID : 1735301011
           Status : Not verified
       Ordered on : Fri, April 13 2007, 08:03 GMT Details
Public certificate : Yes
```

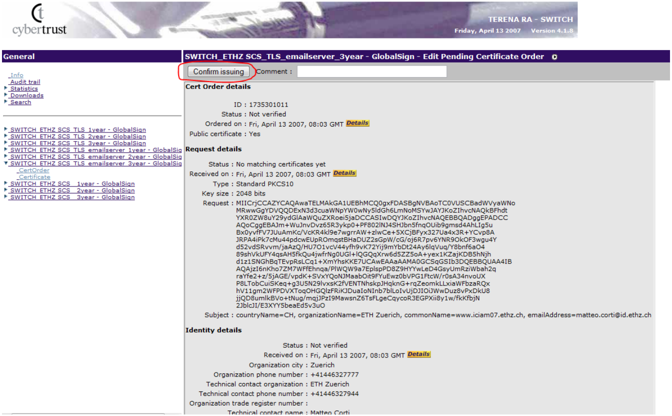
Request details

```
     Status : No matching certificates yet
Received on : Fri, April 13 2007, 08:03 GMT Details
       Type : Standard PKCS10
   Key size : 2048 bits
    Request : MIICrjCCAZYCAQAwaTELMAkGA1UEBhMCQ0gxFDASBgNVBAoTC0VUSCBadWVyaWNo
              MRwwGgYDVQQDExN3d3cuaWNpYW0wNy5ldGh6LmNoMSYwJAYJKoZIhvcNAQkBFhdt
              YXR0ZW8uY29ydGlAaWQuZXRoei5jaDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
              AQoCggEBAJm+WuJnvDvz65R3ykp0+PF802lNJ4SHJbn5fnqOUib9gmsd4AhLIg5u
              Bx0yvfFV7JUuAmKc/VcKR4kl9e7wgrrAW+zlwCe+5XCjBFyx327Ua4x3R+YCvp8A
              JRPA4iPk7cMu44pdcwEUpROmqstBHaDUZ2sGpW/cG/oj6R7pv6YNR9OkOF3wgu4Y
              d52vdSRvvm/jaAzQ/HU7O1vcV44yfh9vK72Yij9mYbDt24Ay6lqVuq/Y8bnf6aO4
              89shVkUFY4qsAH5fkQu4jwfrNg0UGl+lQGQqXrw6d5ZZ5oA+yex1KZajKDB5hNjh
              d1z1SNGhBqTEvpRsLCq1+XmYhsKKE7UCAwEAAaAAMA0GCSqGSIb3DQEBBQUAA4IB
              AQAjzI6nKho7ZM7WFfEhnqa/PlWQW9a7EplspPD8Z9HYYwLeD4GsyUmRziWbah2q
              raYfe2+z/5jAGE/vpdK+SVxYQoNJMaabOit9FYuEwz0bVPG1FtcW/r0sA34nvoUX
              P8LTobCuiSKeq+g3U5N29lvxsK2fVENTNhskpJHqknG+rqZeomkLLxiaWFbzaRQx
              hV11gm2WFPDVXToqOHGQlzFRiKJDuaIoNInb7blLoIvUjDJIOiJWwDuz8vPxDkU8
              jjQD8umlkBVo+tNug/mqjJPzI9MawsnZ6TsFLgeCqycoR3EGPXii8y1w/fkKfbjN
              2JblcJI/E3XYY5beaEd5v3uO
    Subject : countryName=CH, organizationName=ETH Zuerich, commonName=www.iciam07.ethz.ch, emailAddress=matteo.corti@id.ethz.ch
```

Identity details

```
                            Status : Not verified
                       Received on : Fri, April 13 2007, 08:03 GMT Details
                 Organization city : Zuerich
         Organization phone number : +41446327777
    Technical contact organization : ETH Zuerich
    Technical contact phone number : +41446327944
Organization trade register number :
            Technical contact name : Matteo Corti
```

Issue certificate order III



General

- Info
- Audit trail
- Statistics
- Downloads
- Search

- SWITCH_ETHZ SCS_TLS_1year - GlobalSign
- SWITCH_ETHZ SCS_TLS_2year - GlobalSign
- SWITCH_ETHZ SCS_TLS_3year - GlobalSign
- SWITCH_ETHZ SCS_TLS_emailserver_1year - GlobalSig
- SWITCH_ETHZ SCS_TLS_emailserver_2year - GlobalSig
- SWITCH_ETHZ SCS_TLS_emailserver_3year - GlobalSig
  - CertOrder
  - Certificate
- SWITCH_ETHZ SCS_ 1year - GlobalSign
- SWITCH_ETHZ SCS_ 2year - GlobalSign
- SWITCH_ETHZ SCS_ 3year - GlobalSign

SWITCH_ETHZ SCS_TLS_emailserver_3year - GlobalSign - Edit Pending Certificate Order

Cert Order details

```
                ID : 1735301011
            Status : Not verified
        Ordered on : Fri, April 13 2007, 08:03 GMT Details
Public certificate : Yes
```

Request details

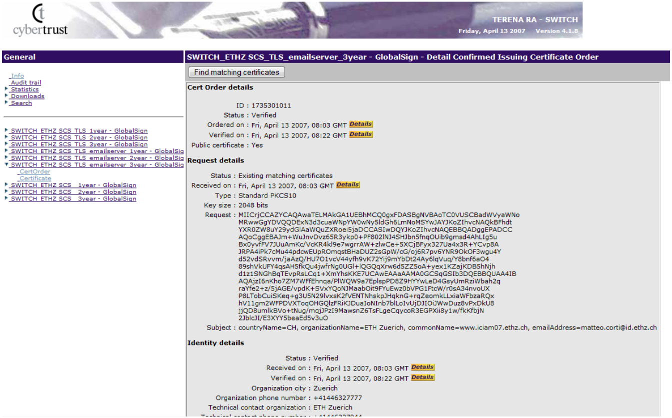
```
     Status : No matching certificates yet
Received on : Fri, April 13 2007, 08:03 GMT Details
       Type : Standard PKCS10
   Key size : 2048 bits
    Request : MIICrjCCAZYCAQAwaTELMAkGA1UEBhMCQ0gxFDASBgNVBAoTC0VUSCBadWVyaWNo
              MRwwGgYDVQQDExN3d3cuaWNpYW0wNy5ldGh6LmNoMSYwJAYJKoZIhvcNAQkBFhdt
              YXR0ZW8uY29ydGlAaWQuZXRoei5jaDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
              AQoCggEBAJm+WuJnvDvz65R3ykp0+PF802lNJ4SHJbn5fnqOUib9gmsd4AhLIg5u
              Bx0yvfFV7JUuAmKc/VcKR4kl9e7wgrrAW+zlwCe+5XCjBFyx327Ua4x3R+YCvp8A
              JRPA4iPk7cMu44pdcwEUpROmqstBHaDUZ2sGpW/cG/oj6R7pv6YNR9OkOF3wgu4Y
              d52vdSRvvm/jaAzQ/HU7O1vcV44yfh9vK72Yij9mYbDt24Ay6lqVuq/Y8bnf6aO4
              89shVkUFY4qsAH5fkQu4jwfrNg0UGl+lQGQqXrw6d5ZZ5oA+yex1KZajKDB5hNjh
              d1z1SNGhBqTEvpRsLCq1+XmYhsKKE7UCAwEAAaAAMA0GCSqGSIb3DQEBBQUAA4IB
              AQAjzI6nKho7ZM7WFfEhnqa/PlWQW9a7EplspPD8Z9HYYwLeD4GsyUmRziWbah2q
              raYfe2+z/5jAGE/vpdK+SVxYQoNJMaabOit9FYuEwz0bVPG1FtcW/r0sA34nvoUX
              P8LTobCuiSKeq+g3U5N29lvxsK2fVENTNhskpJHqknG+rqZeomkLLxiaWFbzaRQx
              hV11gm2WFPDVXToqOHGQlzFRiKJDuaIoNInb7blLoIvUjDJIOiJWwDuz8vPxDkU8
              jjQD8umlkBVo+tNug/mqjJPzI9MawsnZ6TsFLgeCqycoR3EGPXii8y1w/fkKfbjN
              2JblcJI/E3XYY5beaEd5v3uO
    Subject : countryName=CH, organizationName=ETH Zuerich, commonName=www.iciam07.ethz.ch, emailAddress=matteo.corti@id.ethz.ch
```

Identity details

```
                          Status : Not verified
                     Received on : Fri, April 13 2007, 08:03 GMT Details
               Organization city : Zuerich
       Organization phone number : +41446327777
  Technical contact organization : ETH Zuerich
  Technical contact phone number : +41446327944
Organization trade register number :
          Technical contact name : Matteo Corti
```

Figure: Check again and confirm procedure

Issue certificate order IV



General

- Info
- Audit trail
- Statistics
- Downloads
- Search

- SWITCH ETHZ SCS TLS 1year - GlobalSign
- SWITCH ETHZ SCS TLS 2year - GlobalSign
- SWITCH ETHZ SCS TLS 3year - GlobalSign
- SWITCH ETHZ SCS TLS emailserver 1year - GlobalSig
- SWITCH ETHZ SCS TLS emailserver 2year - GlobalSig
- SWITCH ETHZ SCS TLS emailserver 3year - GlobalSig
  - CertOrder
  - Certificate
- SWITCH ETHZ SCS 1year - GlobalSign
- SWITCH ETHZ SCS 2year - GlobalSign
- SWITCH ETHZ SCS 3year - GlobalSign

SWITCH_ETHZ SCS_TLS_emailserver_3year - GlobalSign - Detail Confirmed Issuing Certificate Order

Find matching certificates

Cert Order details

ID : 1735301011
Status : Verified
Ordered on : Fri, April 13 2007, 08:03 GMT Details
Verified on : Fri, April 13 2007, 08:22 GMT Details
Public certificate : Yes

Request details

Status : Existing matching certificates
Received on : Fri, April 13 2007, 08:03 GMT Details
Type : Standard PKCS10
Key size : 2048 bits
Request :

MIICrjCCAZYCAQAwaTELMAkGA1UEBhMCQ0gxFDASBgNVBAoTC0VUSCBadWVyaWNo
MRwwGgYDVQQDExN3d3cuaWNpYW0wNy5ldGh6LmNoMSYwJAYJKoZIhvcNAQkBFhdt
YXR0ZW8uY29ydGlAaWQuZXRoei5jaDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBAJm+WuJnvDvz65R3ykp0+PF802lNJ4SHJbn5fnqOUib9gmsd4AhLIg5u
Bx0yvfFV7JUuAmKc/VcKR4kl9e7wgrrAW+zlwCe+5XCjBFyx327Ua4x3R+YCvp8A
JRPA4iPk7cMu44pdcwEUpROmqstBHaDUZ2sGpW/cG/oj6R7pv6YNR9OkOF3wgu4Y
d52vdSRvvm/jaAzQ/HU7O1vcV44yfh9vK72Yij9mYbDt24Ay6lqVuq/Y8bnf6aO4
89shVkUFY4qsAH5fkQu4jwfrNg0UGl+lQGQqXrw6d5ZZ5oA+yex1KZajKDB5hNjh
d1z1SNGhBqTEvpRsLCq1+XmYhsKKE7UCAwEAAaAAMA0GCSqGSIb3DQEBBQUAA4IB
AQAjzI6nKho7ZM7WFfEhnqa/PlWQW9a7EplspPD8Z9HYYwLeD4GsyUmRziWbah2q
raYfe2+z/5jAGE/vpdK+SVxYQoNJMaabOit9FYuEwz0bVPG1FtcW/r0sA34nvoUX
P8LTobCuiSKeq+g3U5N29lvxsK2fVENTNhskpJHqknG+rqZeomkLLxiaWFbzaRQx
hV11gm2WFPDVXToqOHGQlzFRiKJDuaIoNInb7blLoIvUjDJIOiJWwDuz8vPxDkU8
jjQD8umlkBVo+tNug/mqjJPzI9MawsnZ6TsFLgeCqycoR3EGPXii8y1w/fkKfbjN
2JblcJI/E3XYY5beaEd5v3uO

Subject : countryName=CH, organizationName=ETH Zuerich, commonName=www.iciam07.ethz.ch, emailAddress=matteo.corti@id.ethz.ch

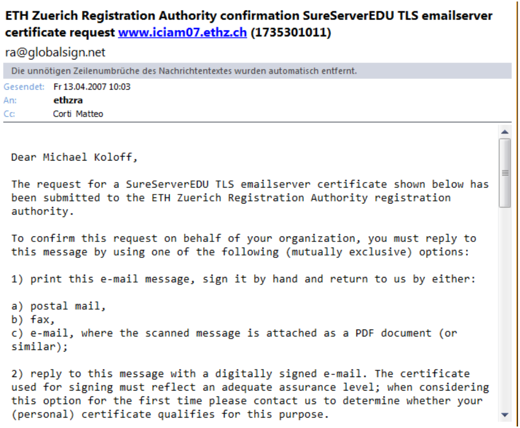
Identity details

Status : Verified
Received on : Fri, April 13 2007, 08:03 GMT Details
Verified on : Fri, April 13 2007, 08:22 GMT Details
Organization city : Zuerich
Organization phone number : +41446327777
Technical contact organization : ETH Zuerich
Technical contact phone number : +41446327944

Figure: This page presents a summary again

Paperwork

- Print out the email.
- Sign it.
- Keep it safe.



ETH Zuerich Registration Authority confirmation SureServerEDU TLS emailserver certificate request www.iciam07.ethz.ch (1735301011)

ra@globalsign.net

Die unnötigen Zeilenumbrüche des Nachrichtentextes wurden automatisch entfernt.

Gesendet:	Fr 13.04.2007 10:03
An:	**ethzra**
Cc:	Corti Matteo

```
Dear Michael Koloff,

The request for a SureServerEDU TLS emailserver certificate shown below has
been submitted to the ETH Zuerich Registration Authority registration
authority.

To confirm this request on behalf of your organization, you must reply to
this message by using one of the following (mutually exclusive) options:

1) print this e-mail message, sign it by hand and return to us by either:

a) postal mail,
b) fax,
c) e-mail, where the scanned message is attached as a PDF document (or
similar);

2) reply to this message with a digitally signed e-mail. The certificate
used for signing must reflect an adequate assurance level; when considering
this option for the first time please contact us to determine whether your
(personal) certificate qualifies for this purpose.
```