

# SWITCH

The Swiss Education & Research Network

## **SCS: the new Server Certificate Service offering from SWITCH/TERENA**

Kaspar Brand  
SWITCH

# A very brief SCS project history

Discussions with other European NRENs started in 2004, within TERENA's TF-EMC2 (Task Force on European Middleware Coordination and Collaboration)


First (draft) proposal in October 2004: *“Goal: To setup a service that offers **popup-free cheap server-certificates** against a flatrate fee for educational and research organisations using their NREN as a service provider.”*

Call for Proposals issued by TERENA in August 2005; participating NRENs: ACOnet (Austria), CARNet (Croatia), CESNET (Czech Republic), CRU (France), RedIRIS (Spain), SURFnet (Netherlands), SWITCH (Switzerland), UNI•C (Denmark)

Offers from commercial CAs received in September 2005, preferred supplier (GlobalSign) announced on 19 December 2005, contract signed on 9 January 2006

Service operational by mid-March 2006

# Pop-up free?



Unable to verify the identity of aai-logon.switch.ch as a trusted site.

Possible reasons for this error:

- Your browser does not recognize the Certificate Authority that issued the site's certificate.
- The site's certificate is incomplete due to a server misconfiguration.
- You are connected to a site pretending to be aai-logon.switch.ch, possibly to obtain your confidential information.

Please notify the site's webmaster about this problem.

Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to accept this certificate for the purpose of identifying the Web site aai-logon.switch.ch?


Examine Certificate...

Accept this certificate permanently

Accept this certificate temporarily for this session

Do not accept this certificate and do not connect to this Web site

Cancel OK



Safari can't verify the identity of the website "aai-logon.switch.ch".

The certificate for this website was signed by an unknown certifying authority. You might be connecting to a website that is pretending to be "aai-logon.switch.ch" which could put your confidential information at risk. Would you like to connect to the website anyway?

Always trust these certificates

- SwissSign CA (RSA IK May 6 1999 18:00:58)
  - SwissSign Bronze CA
    - SwissSign Silver CA
      - SWITCH CA
        - SWITCH Server CA
          - aai-logon.switch.ch

SwissSign CA (RSA IK May 6 1999 18:00:58)

Root certificate authority


Expiration Date: 27 November 2031 00:00:00 UTC

Details




Trust Settings

Hide Certificate

**Security Alert**



Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

-  The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
-  The security certificate date is valid.
-  The security certificate has a valid name matching the name of the page you are trying to view.

Do you want to proceed?

Yes No View Certificate

**Certificate signer not found**

The root certificate for this server is not registered. You may install this certificate. Accept/install?

aai-logon.switch.ch

- SWITCH Server CA
- SWITCH CA
- SwissSign Silver CA

- The certificate for "aai-logon.switch.ch" is signed by the unknown Certificate Authority "SWITCH Server CA". It is not possible to verify that this is a valid certificate

- The certificate for "SWITCH Server CA" is signed by the unknown Certificate Authority "SWITCH CA". It is not possible to verify that this is a valid certificate

Help Cancel Install Accept

# SCS: enter the world of preinstalled roots SWITCH

The Swiss Education & Research Network

SCS server certificates chain up to the ubiquitous **GTE CyberTrust Global Root**, which comes preinstalled with

- all major operating systems (Windows, Mac OS 9 ff., ...)
- most Web browsers/applications (Mozilla, Opera, ...)
- many software suites (Sun JRE/JDK, IBM Websphere, Lotus Notes, Oracle Wallet Manager, KDE, OpenSSL, ...)
- many mobile devices (Palm, Blackberry; phones from Nokia, Sony Ericsson, Motorola, ...)

For issuing SCS certificates, the **Cybertrust Educational CA** intermediate cert is used (2006–2013)

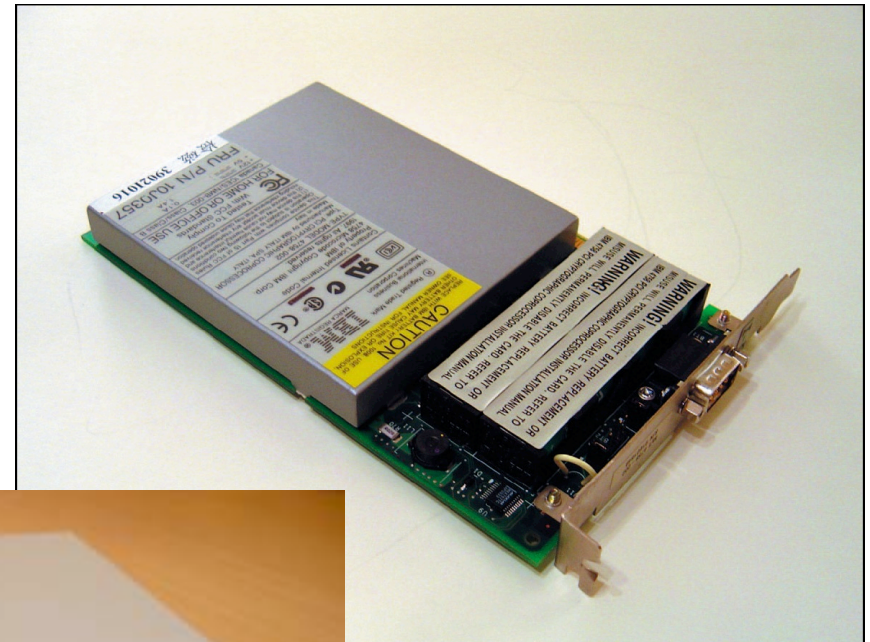
The screenshot displays a 'Certificate Hierarchy' window. At the top, it shows 'GTE CyberTrust Global Root' expanded to show 'Cybertrust Educational CA' with the URL 'www.switch.ch'. Below this is a 'Certificate Fields' section with a tree view. The 'Subject' field is highlighted in blue. Under 'Subject', there is a 'Subject Public Key Info' section containing 'Subject Public Key Algorithm', 'Subject's Public Key', 'Certificate Signature Algorithm', and 'Certificate Signature Value'. At the bottom, a 'Field Value' section lists: 'CN = GTE CyberTrust Global Root', 'OU = GTE CyberTrust Solutions, Inc.', 'O = GTE Corporation', and 'C = US'.

# And – where's the private key...?

... on an HSM (hardware security module), which come in different flavors:



Chrysalis (SafeNet) Luna CA3



IBM 4758



nCipher nShield

# GTE and GlobalSign/Ubizen/Cybertrust

1959	General Telephone & Electronics Corp. established as a merger of General Telephone (founded 1918) and Sylvania Electric Products (founded 1910)
May 1995	Ubizen founded
February 1996	“GTE CyberTrust Root” issued (valid thru 2006)
October 1996	BelSign founded
January 1998	GTE CyberTrust CA starts operations
<b>August 1998</b>	<b>“GTE CyberTrust Global Root” issued</b> (valid thru 2018)
August 1998	BelSign becomes GlobalSign
September 1998	“GlobalSign Root CA” issued (valid thru 2014)
1999	Betrusted started as PwC's e-security business
<b>March 2000</b>	<b>GTE's CyberTrust Solutions, Inc. acquired by Baltimore Technologies (\$150M)</b>
April 2000	Verizon merger (Bell Atlantic/GTE) completed
July 2002	GlobalSign acquired by Ubizen (73%)
February 2003	Betrusted acquired by One Equity Partners (Bank One)
<b>September 2003</b>	<b>Baltimore's “OmniRoot” (GTE root certificate) acquired by Betrusted (\$3.2M)</b>
December 2003	Baltimore's “UniCERT” product acquired by Betrusted (\$8M)
May 2004	Ubizen acquired by Betrusted (78.7%)
<b>September 2004</b>	<b>Cybertrust formed by a merger of Betrusted and TruSecure</b> (majority owner: One Equity Partners / Bank One)
January 2006	TERENA signs contract with GlobalSign/Ubizen/Cybertrust

# Cheap?

From the January 2006 press release of TERENA: *This solution makes the cost per certificate very low when large numbers of certificates are issued.*

External costs for SCS certificates lower than for SwissSign

SWITCH intends to offer two PKI service options:

- **SWITCHpki Basic:** for smaller organizations, basic fee includes up to ~10 certificates/year (either SwissSign or SCS)
- **SWITCHpki Extended:** for larger organizations (RA operators with direct access to CA platform), basic fee includes ~30 SwissSign certificates and an unlimited number of SCS certificates

# The SCS offering in more detail

SCS = **Server** certificate service (no user certificates currently)

Three types of server certificates available with **1, 2 or 3 years validity**

## – **SureServerEDU TLS**

- ❑ recommended default type for general-purpose servers (Web, e-mail, directory service, ...)
- ❑ mandatory attributes: *countryName (C)*, *organizationName (O)*, *commonName (CN)*
- ❑ optional attributes: *stateOrProvinceName (ST or S)*, *localityName (L)*, *organizationalUnitName (OU)*, *domainComponent (DC)*

## – **SureServerEDU TLS emailserver**

- ❑ special-purpose type for servers creating e-mail messages on their own (alerting service or similar) – not needed for standard SMTP/IMAP/POP servers
- ❑ mandatory attributes: *countryName (C)*, *organizationName (O)*, *commonName (CN)*, *emailAddress (E)*
- ❑ optional attributes: *stateOrProvinceName (ST or S)*, *localityName (L)*, *organizationalUnitName (OU)*, *domainComponent (DC)*

## – **SureServerEDU**

- ❑ standard type used by GlobalSign (includes legacy *netscape-cert-type* extension)

Not yet available with SCS (but announced for June 2006): *subjectAltName* extension with one or more *dNSNames* (support for DNS aliases)



Pre-registration of the organization with SWITCHpki using three registration forms (currently under development):

- for new participants: “**Application for SWITCHpki participation**”, signed by an official representative of the organization
- “**Proxy for SWITCHpki certificate applicants**”: appointment of contact persons/RA operators at the organization, signed by an official representative
- “**DNS domain authorization**”: authorization of SWITCHpki contact persons to authorize requests for specified list of DNS domains, signed by an official representative (unless specifically delegated to the contact persons)

TANSTAAFL: liabilities arising from the contract with GlobalSign have to be accepted by each participating organisation (e.g. when approving a possibly fraudulent certificate request by ignoring mandatory verification steps).

→ *Risk is mostly hypothetical* if procedures are properly adhered to (liability per SCS certificate capped at 0 Euro as per contract).

# Requesting an SCS certificate

- 1) Sysadmin generates key pair and creates CSR
- 2) Sysadmin submits CSR through GlobalSign's enrollment pages
- 3) Admin contact of organization receives a challenge e-mail to be replied to (with postal mail, fax, e-mail with scan of signed document, later possibly with a digitally signed e-mail)
- 4) RA administrator verifies request (identity of the applicant, organization, DNS domain in subject)
- 5) RA administrator approves (or rejects) the request
- 6) If approved: sysadmin receives certificate by mail



# SWITCH

The Swiss Education & Research Network