SWITCH

The Swiss Education & Research Network

SWITCHpki Service Launch

The SWITCHpki Team

pki@switch.ch

http://www.switch.ch/pki/

2004 © SWITCH

Overview

SWITCH
The Swiss Education & Research Network

- Introduction
- CA Structure
- Roles, Entities
- Service Options
- Example
- SwissSign Introduction
- Outlook: Client Certs

Overview

SWITCH
The Swiss Education & Research Network

Introduction

CA Structure

Roles, Entities

Service Options

Example

SwissSign Introduction

Outlook: Client Certs

Introduction

SWITCH
The Swiss Education & Research Network

Motivation for SWITCHpki

- Requirement of AAI Project: server certificates protecting backend communication
- Administrative hassle with commercial certificate issuers
- PKI initiatives within our community could benefit from a common service

What happened so far?

- AAI-TF-CA: Taskforce within AAI project
- Produced a CP/CPS draft, recommending SWITCH to make a service out of it
- SWITCH took this up, engaged SwissSign as consultant and potential outsourcing partner and drafted a new CP/CPS
- Result rediscussed in AAI-TF-CA and made into the service being presented today

Overview

SWITCH
The Swiss Education & Research Network

Introduction

CA Structure

Roles, Entities

Service Options

Example

SwissSign Introduction

Outlook: Client Certs

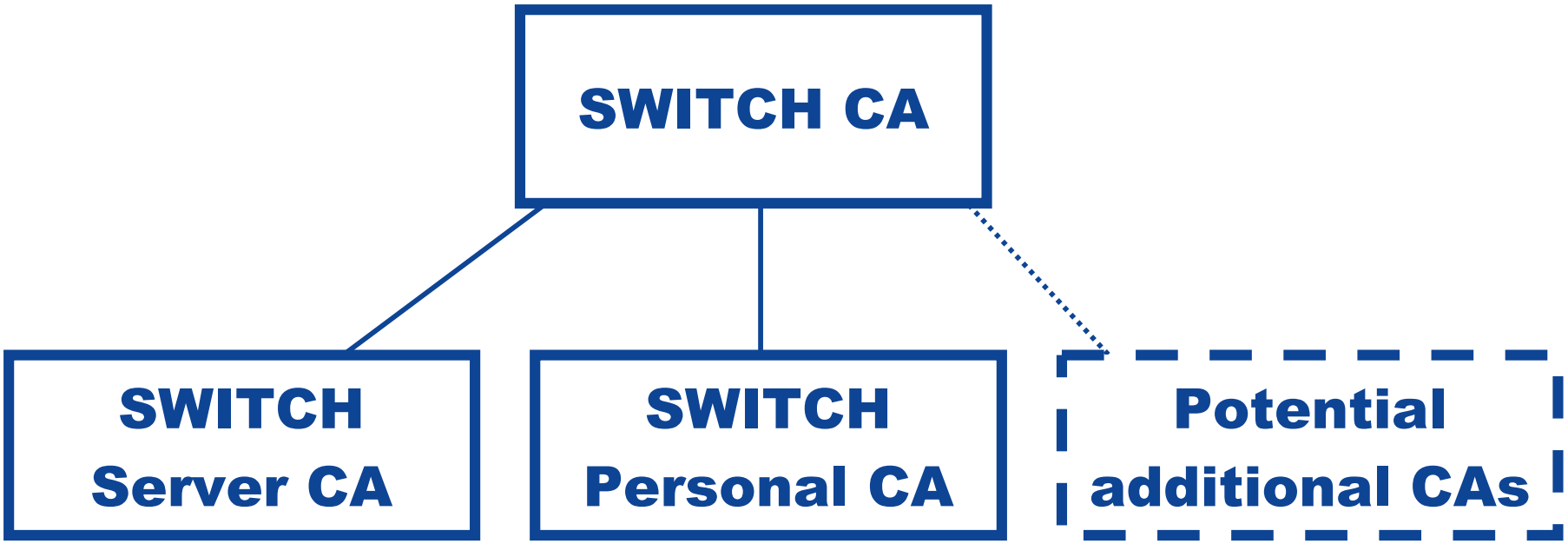
SWITCHpki - CA Structure

SWITCH
The Swiss Education & Research Network

- Different CAs for different usage (e.g server certificates, personal certificates)

  ⇨ Hierarchical approach
- Different level of trust
- Ability to set 'trust anchor' based on personal requirements
  (e.g trust everything under SWITCH Server CA)
  ⇨ Trust on certificates can not be based on what is already included in a product, but on what is known about a certificate (what are the policies, the certificate relies on)
- Open for additional CAs

SWITCHpki - CA Structure



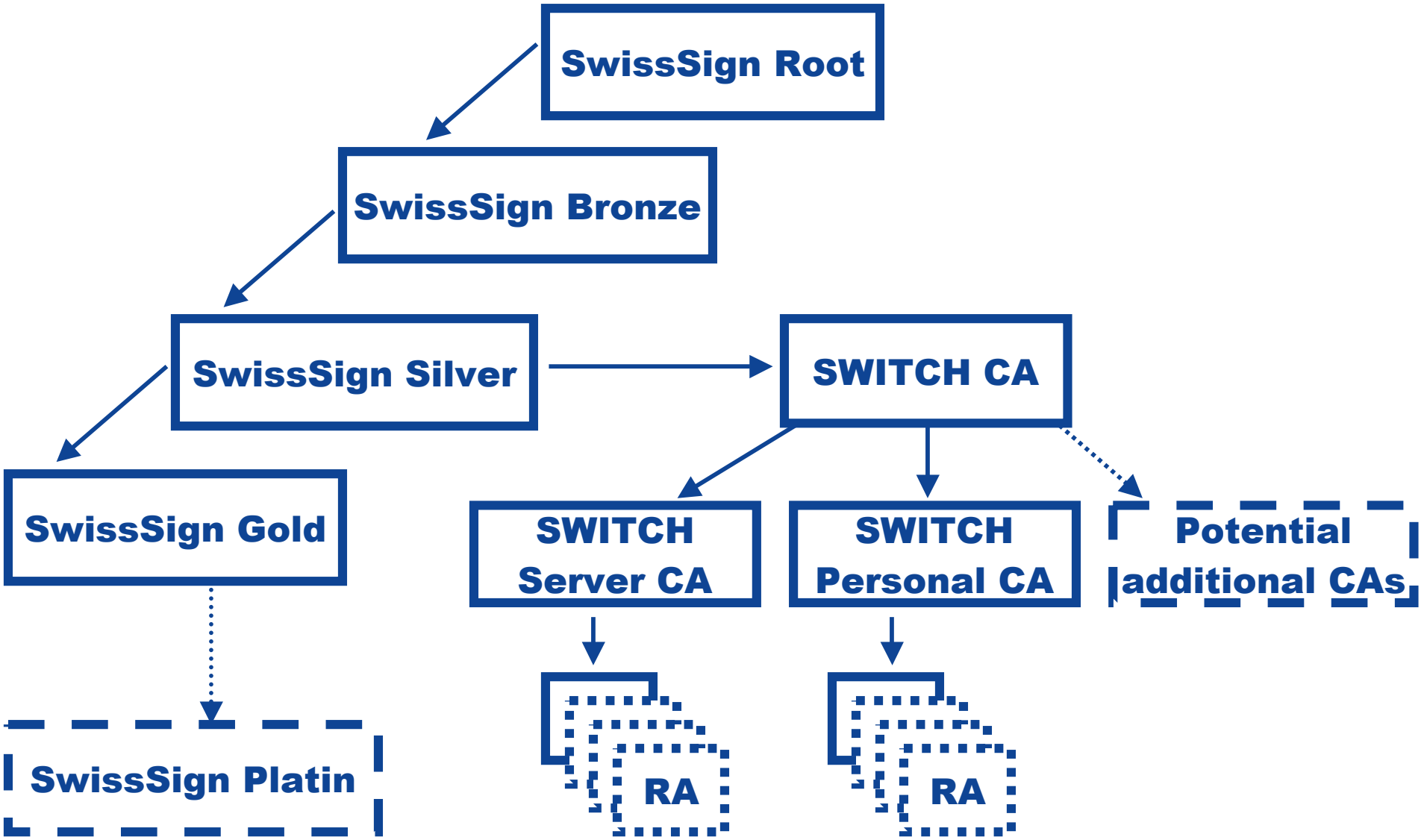
SWITCHpki - CA Structure

SWITCH
The Swiss Education & Research Network

- If the SWITCH CA would stand for its own, the structure presented would be fine & sufficient, but
- Benefits if being integrated in SwissSign structure:
  - Usage from existing X.509 know-how from SwissSign
  - Existing framework to rely on
  - Use of existing SwissSign service possible
  - Certification of SwissSign CA positively influence SWITCH CA (Certification 'automatically' included)
  - If SwissSign Root CA will be integrated in clients (usability issue, not a trust issue and mostly contrary to that), SWITCH CA will be recognised by the clients as well (based on certificate chain)

CA Structure SwissSign & SWITCHpki

SWITCH
The Swiss Education & Research Network



CA Structure “Who is signing Whom ?”

SWITCH
The Swiss Education & Research Network

At a first glance it’s not logic why a SwissSign Bronze CA signs a SwissSign Silver CA; shouldn’t it be vice versa ?

with that hierarchical model, you’re able to set the trust e.g on SwissSign Silver CA & no certificates signed by SwissSign Bronze will be accepted, but a certificate signed by SwissSign Gold would be fine, because it even has a stronger policy

a CA couldn’t sign a different CA, which has a weaker policy, therefore a ‘less trustworthy CA’ can only sign a ‘more trustworthy’ one

⇨ a root CA is the weakest CA in a CA chain

SWITCHpki - CA Structure

SWITCH
The Swiss Education & Research Network

SWITCH CA

- signed by ‘SwissSign Silver’
- off-line
- stored in a bank safe
- only used to sign sub-CAs (SWITCH Personal CA & SWITCH Server CA at the moment)
- once in a while used to issue CRL for SWITCH Server CA & SWITCH Personal CA

SWITCH Server CA

- implemented on the SwissSign infrastructure
- online, stored in HSM (Hardware Security Module)

SWITCH Personal CA

- implemented on the SwissSign infrastructure
- online, stored in HSM

SWITCHpki - SWITCH CA

SWITCH
The Swiss Education & Research Network

Overview

SWITCH
The Swiss Education & Research Network

Introduction

CA Structure

Roles, Entities

Service Options

Example

SwissSign Introduction

Outlook: Client Certs

Roles, Entities: Underlying Principles

SWITCH
The Swiss Education & Research Network

Correctness of information

- Included information must be correct
- E.g. no nicknames, pseudonyms need to be marked as such

Verifiability of information

- Included information must be verifiable and meaningful
- E.g. organisation names must be registered somewhere

Auditability

- All contents of signed information in certificates must be supported with some form of documentation attainable in reasonable time (e.g. during an audit)

Roles, Entities: The Players

SWITCH
The Swiss Education & Research Network

The issuer

- Signs certificate requests issued by the subject
- Registration Authority (RA): entitiy doing all the checks and paperwork
- Certification Authority (CA): dumb signing engine, following the orders given by its RA

The subject

- Issues certificate signing requests
- Holds the issued certificate

The relying party

- The ones relying on (accepting) a given certificate
- Wants to understand the elements in the cert

Roles, Entities: Signed Information

SWITCH
The Swiss Education & Research Network

Organisation names

- Correctness and verifiability: we require evidence of the correctness of organisation names from a trustworthy, official source
- Auditability: we want it on paper

Domain names

- Correctness and verifiability: we require evidence from the domain name holder, that the domain names are correct
- Auditability: we want it on paper

Subject information

- Correctness and verifiability: we require some evidence about the subject from a trustworthy, official source
- Auditability: we want it on paper

Roles, Entities: Who is doing what? (1)

SWITCH
The Swiss Education & Research Network

Site/Organisation contact:

- Gets clearance from the represented organisation and relevant domain name holders to issue certificates linking each other and lets SWITCH-RA know about it
- Acts as primary contact to SWITCH regarding SWITCHpki services
- Checks the correctness of presented personal identification (e.g. student/staff card), takes copies and checks whether they link to the certificate requestor
- Checks whether the requestor is entitled to get a certificate for the service or server in question (assuming local procedures exist, probably linked to DNS maintenance)
- Decides whether the represented organisation wants to grant this certificate request (cost issues, other local policies)
- Discard the request or forward it to SWITCH-RA with supporting documentation

⇨ primarily checks the correctness of the documentation

Roles, Entities: Who is doing what? (2)

SWITCH
The Swiss Education & Research Network

SWITCH-RA

- Checks authenticity of incoming certificate request from site contacts
- Checks whether the elements fit together (site contact - organisation name - domain name)
- Checks completeness of provided information
- Approves or denies certificate requests

➪ primarily checks the completeness of the documentation

Overview

SWITCH
The Swiss Education & Research Network

Introduction

CA Structure

Roles, Entities

Service Options

Example

SwissSign Introduction

Outlook: Client Certs

Service Option: RAstartup

SWITCH
The Swiss Education & Research Network

Participating organisation:

- Assigned contact person(s)
- Documentation regarding organisation name and relevant domain names
- own internal website for PKI topics recommended

SWITCH:

- documentation for issued certificates archived @ SWITCH

Status: available now

Cost:

- not individually billed (included in foundation component) for a low number of certificates (approx. 10) per organisation
- Above that number, move to other service options required

Service Option: RAlight

SWITCH
The Swiss Education & Research Network

Participating organisation:

- Assigned contact person(s)
- Documentation regarding organisation name and relevant domain names
- Own internal website for PKI topics recommended
- Documentation for issued certificates archived @ site

SWITCH:

- Contract with organisation as RA operator for organisation

Status: available soon, awaiting pilot sites

Cost:

- tba, will be made part of the official price sheet of SWITCH

Service Option: RA

SWITCH
The Swiss Education & Research Network

Participating organisation:

- Assigned contact person(s)
- Documentation regarding organisation name and relevant domain names
- Own internal website for PKI topics
- Own registration website for certificate issuance
- Documentation for issued certificates archived @ site

SWITCH:

- Contract with organisation as RA operator for organisation

Status: available soon, awaiting pilot sites

Cost:

- tba, will be made part of the official price sheet of SWITCH

Overview

SWITCH
The Swiss Education & Research Network

Introduction

CA Structure

Roles, Entities

Service Options

Example

SwissSign Introduction

Outlook: Client Certs

Requirements

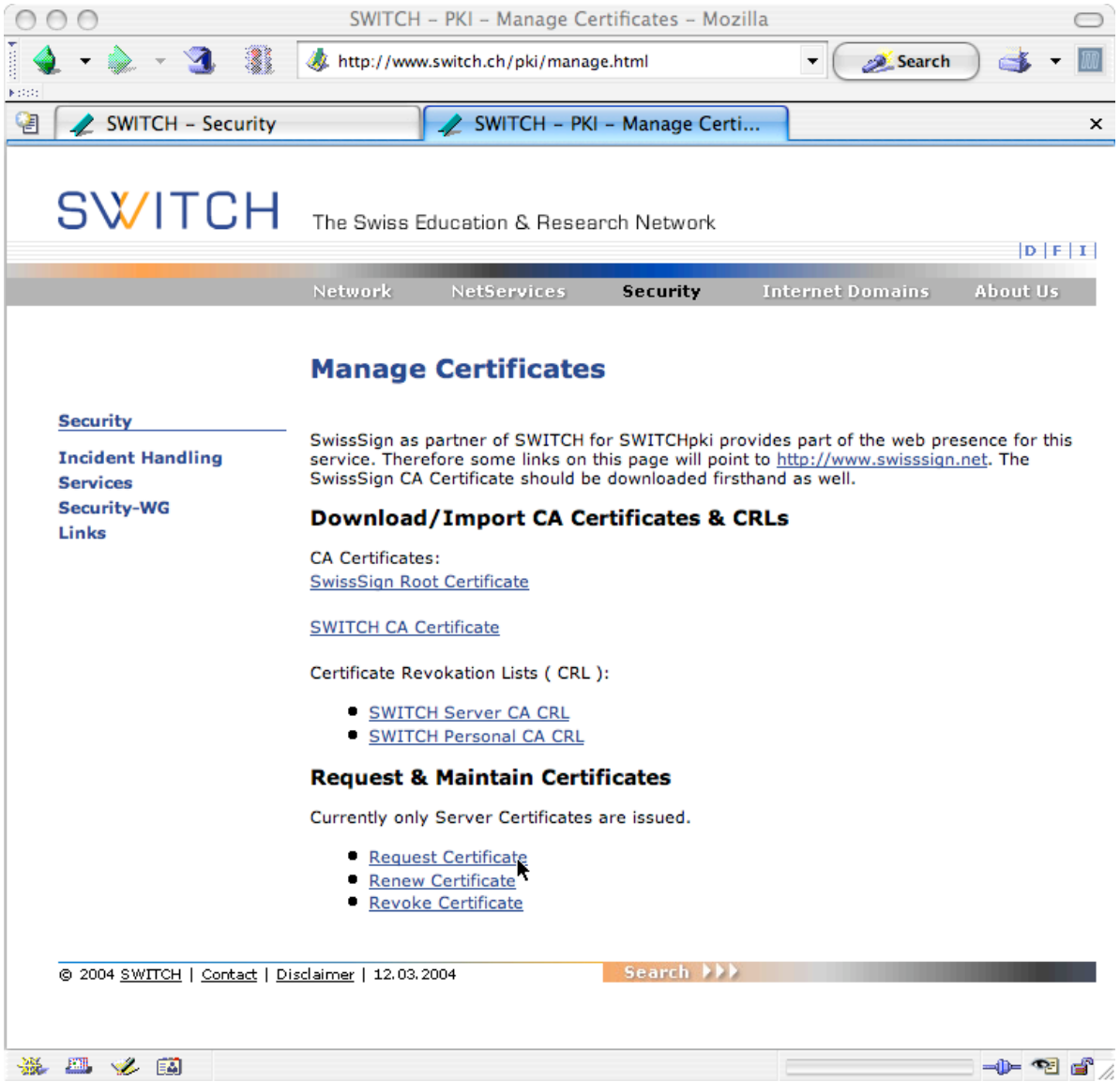
SWITCH
The Swiss Education & Research Network

Let's assume Organisation 'My Own University' is interested in a small amount of server certificates signed by SWITCH Server CA:

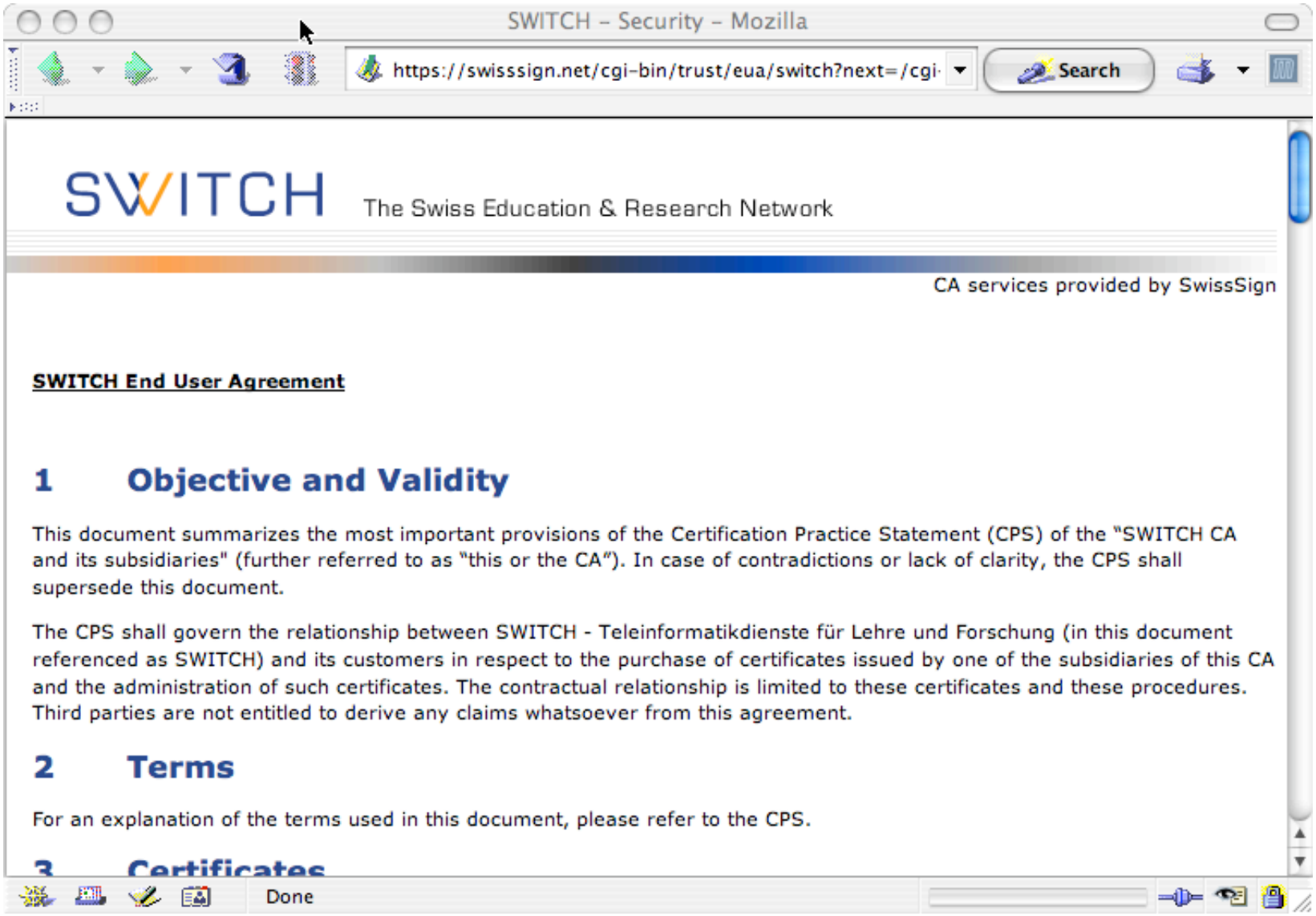
Requirements:

- **initially:**
  - **Contact person for PKI topics at 'My Own University'**
  - **copy of picture ID of contact person**
  - **Legal document which verify that organisation 'My Own University' really is 'My Own University' (e.g commercial register, cantonal university law, foundation document ...)**
- **per second level domain:**
  - **signed Whois entry (signed by representative of domain owner)**
  - **copy of picture ID of signatory**
- **per certificate:**
  - **signed request form (by requestor & contact person)**
  - **copy of picture ID of requestor**

Request a Certificate

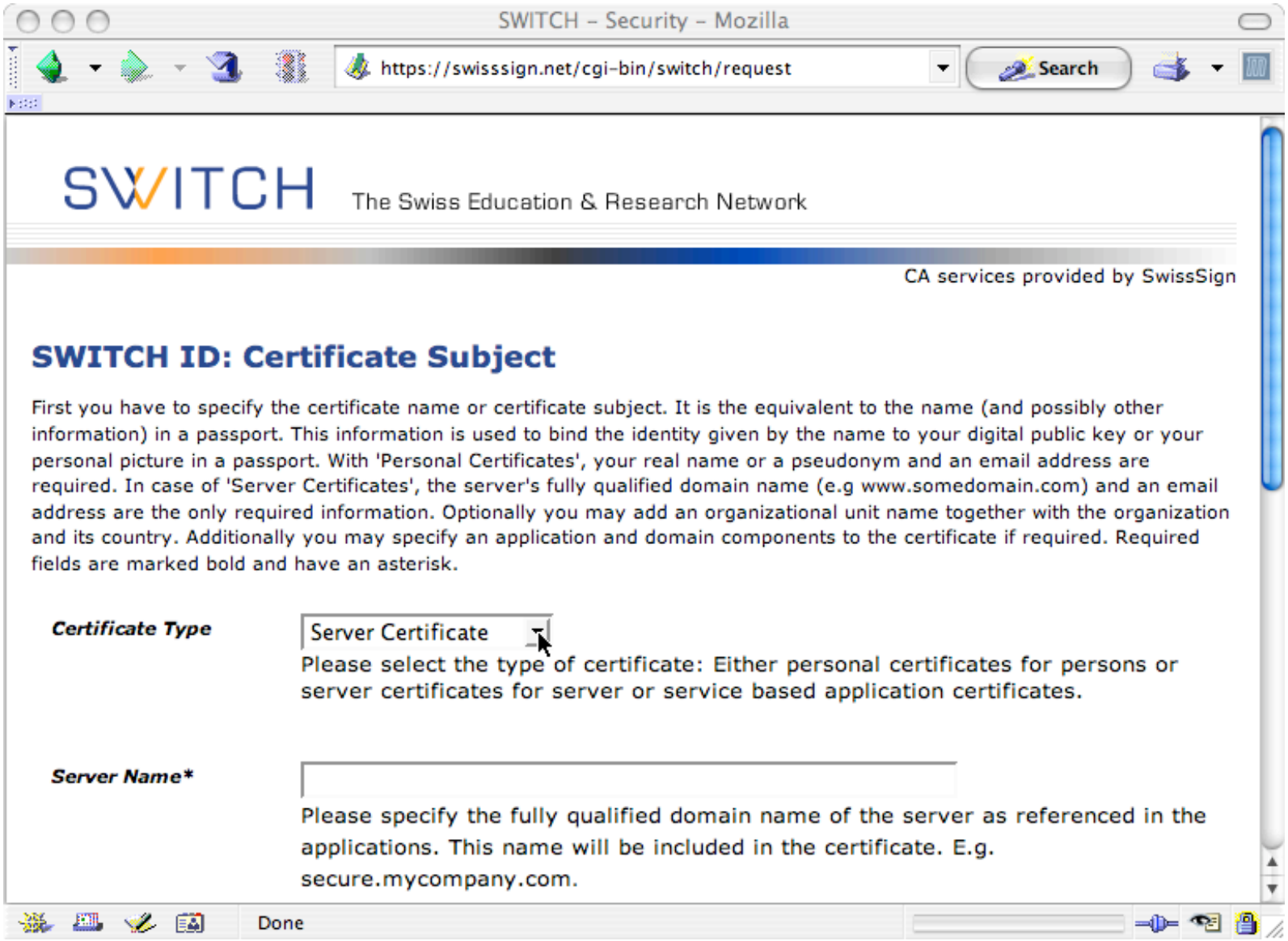


End User Agreement

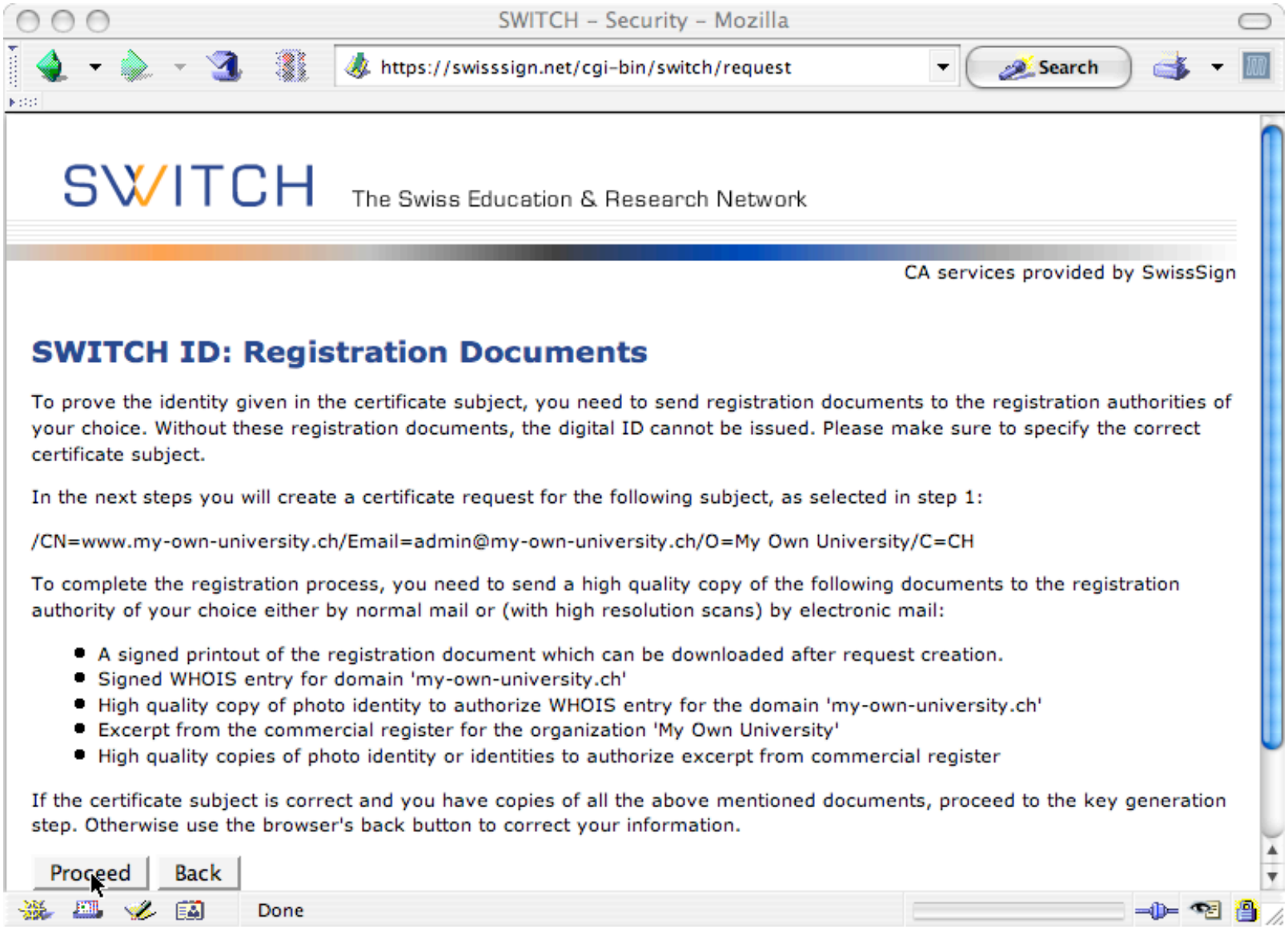


Certificate Fields

SWITCH
The Swiss Education & Research Network



Registration Documents



E-mail Correspondance

SWITCH
The Swiss Education & Research Network

Dear Customer

You have submitted a new SWITCH ID request with subject

'/CN=www.my-own-university.ch/Email=admin@my-own-university.ch/O=My Own University/C=CH'

for approval. To complete the registration process you need to send a signed copy of the following documents to one of the registration authorities:

- A signed copy of the registration document. Click here to download the registration document.
- Signed WHOIS entry for domain 'my-own-university.ch'
- High quality copy of photo identity to authorize WHOIS entry for the domain 'my-own-university.ch'
- Excerpt from the commercial register for the organization 'My Own University'
- High quality copies of photo identity or identities to authorize excerpt from commercial register

Choose one of the registration authorities below to submit your documents and have your request approved.
.....

E-mail Correspondance

SWITCH
The Swiss Education & Research Network

Dear Customer

Your new SWITCH ID Request 41306305B18143E3 with subject /CN=www.my-own-university.ch/Email=admin@my-own-university.ch/O=My Own University/C=CH has been approved. To download and install the new SWITCH ID click here.

Regards,

Your SWITCH Team

.....

Certificate Download

Overview

SWITCH
The Swiss Education & Research Network

Introduction

CA Structure

Roles, Entities

Service Options

Example

SwissSign Introduction

Outlook: Client Certs

SwissSign Introduction

SWITCH
The Swiss Education & Research Network

➪ **http://swisssign.com**

Overview

SWITCH
The Swiss Education & Research Network

Introduction

CA Structure

Roles, Entities

Service Options

Example

SwissSign Introduction

Outlook: Client Certs

Outlook Client Certificates: Comparison

SWITCH
The Swiss Education & Research Network

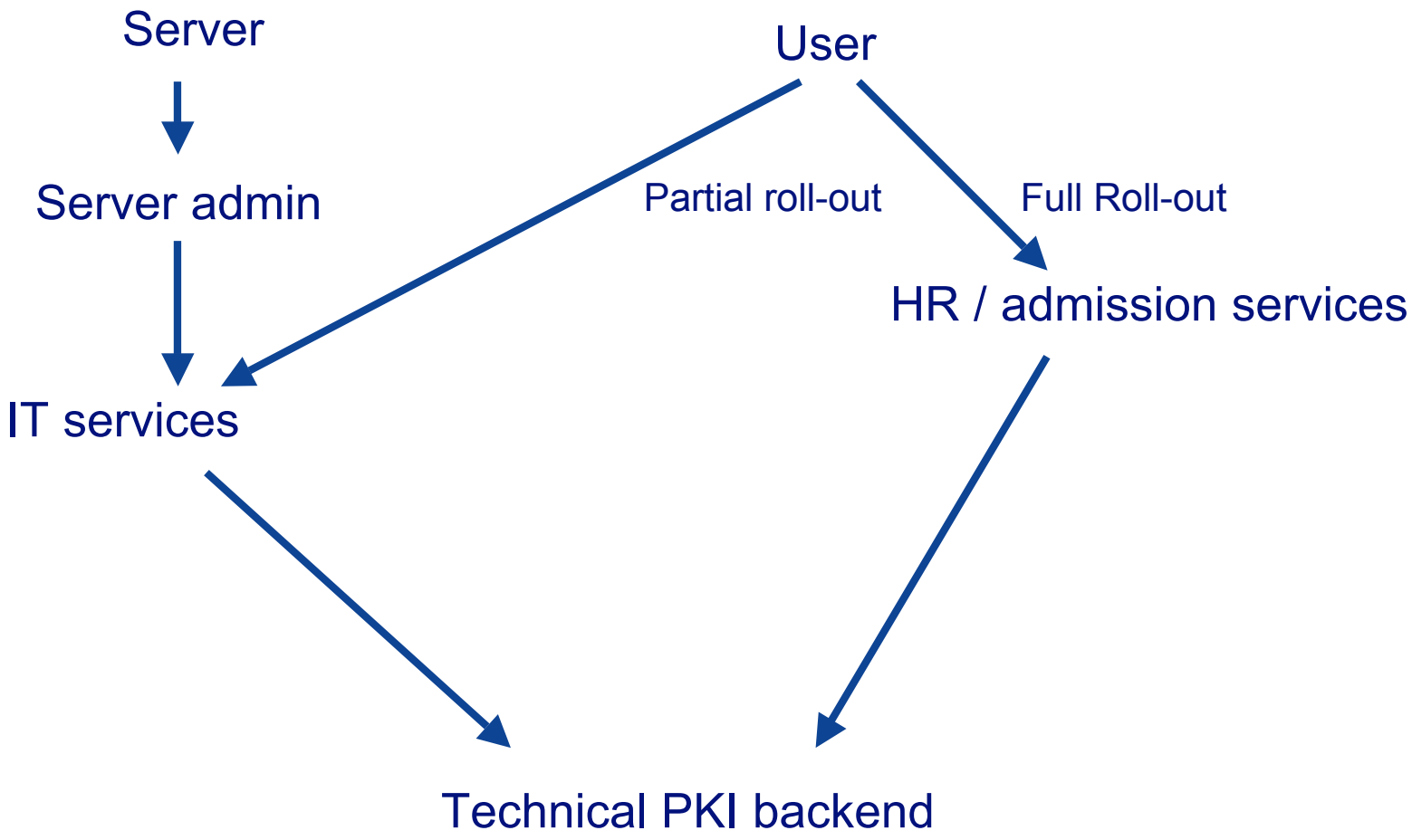
Server certificates

- Usage well understood
- 1st Goal: Network traffic encryption
- 2nd Goal: Enhanced server authentication (compared with DNS only)
- To put it simple: A technical solution to a technical problem

User certificates

- Which processes are to be secured?
- What level of security is required?
- To put it simple: mainly policies, not much techie stuff

Outlook Client Certificates: New Parties



Outlook Client Certificates: Next Steps

SWITCH
The Swiss Education & Research Network

Phase 1: Requirements (before mid 2004)

- Clarify intended usage and goals (learn about existing projects)
- Clarify quality requirements (application area, data protection, non-repudiation, liability etc.)
- Define required quality levels (as few as possible)

Phase 2: Design + Implementation (starting mid 2004)

- New task force (Techies)

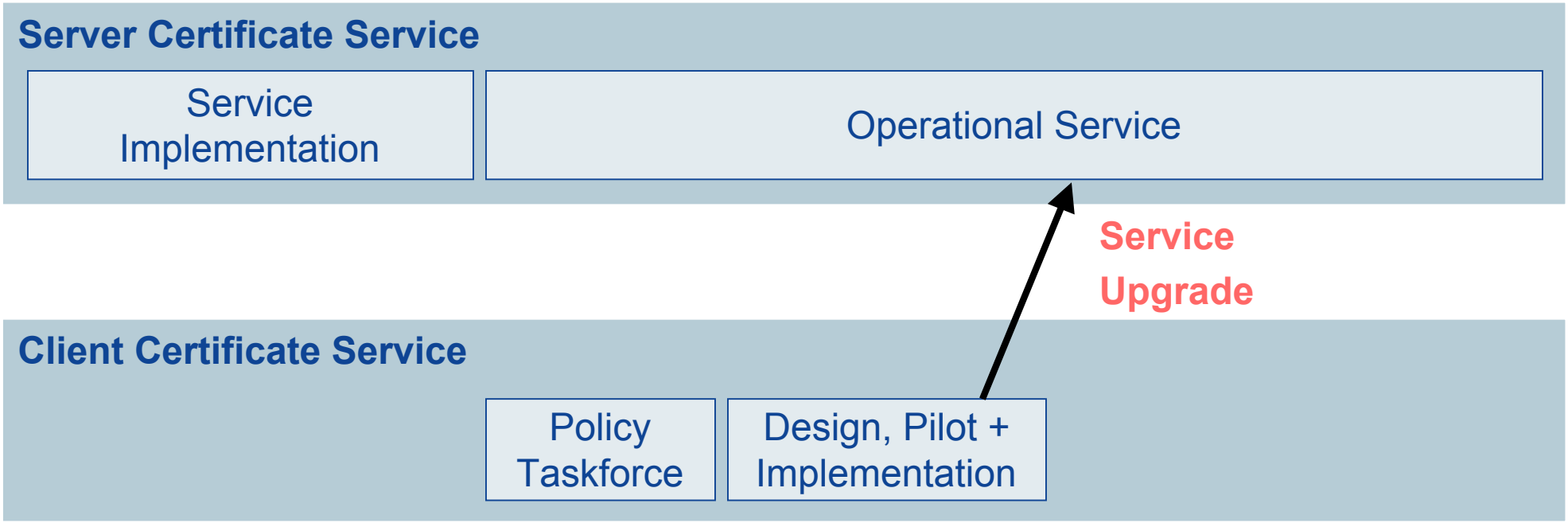
Call for participation in TF “Client Certs”

- To be issued in April 04
- We are looking for:
  - » People involved in internal PKI project definitions and projects
  - » People specialized in digital signatures (applications/user side)

Outlook Client Certificates: Roadmap

SWITCH
The Swiss Education & Research Network

2003	2004	2005	2006++



Questions & Comments

SWITCH
The Swiss Education & Research Network

➪ http://www.switch.ch/pki