

# TERENA eScience Personal CA

## MICS4All

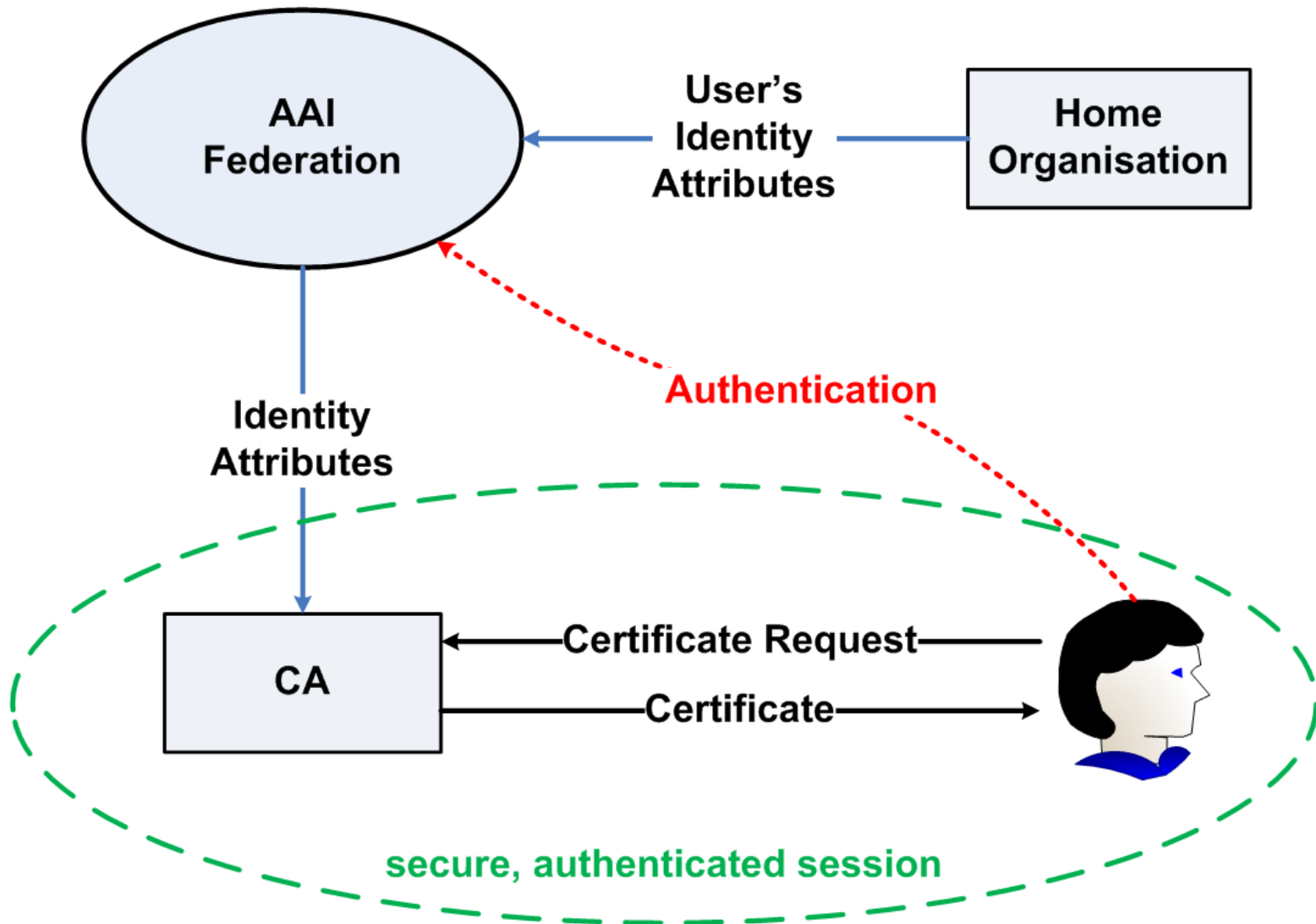
...in the TERENA constituency...

Jan Meijer



**EuGridPMA 17**  
14-16 Sept. 2009  
Berlin

# how things started



we wanted...

the certificates, not a CA

issue Grid certificates using our federation

scalable

for < 10 kEUR/year

the project formerly known as..

NetherNordic SLCS / TERENA GCS

**TERENA + NDGF + National Grid  
Initiatives, AAI Federations and NRENs  
of**

*Denmark*

*Finland*

*Netherlands*

*Norway*

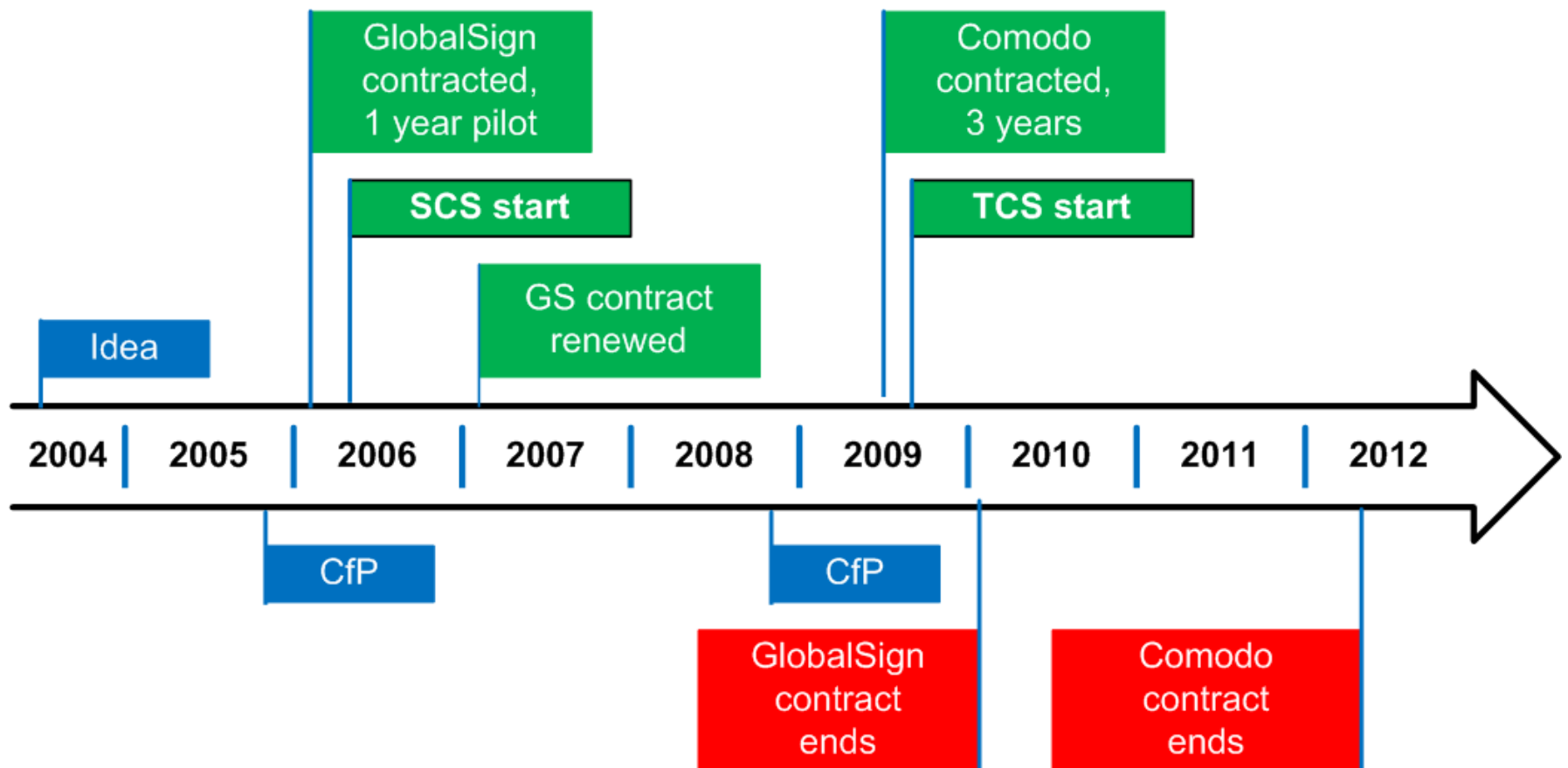
*Sweden*

# **Enter TCS**

consolidate  
into  
well established service

# TERENA Certificate Service

*by NRENs for NRENs*



# SCS Numbers

Apr 2006 – Aug 2008

Participating NRENs	<b>18 (3 recent)</b>
---------------------	----------------------

Certificates issued	<b>19,400</b>
---------------------	---------------

Participating organisations	<b>2,225</b>
--------------------------------	--------------

Proxies	<b>3,800</b>
---------	--------------

# TCS Participating NRENS

Country	Member org.	Server	Code Signing	Personal
Austria	ACOnet	X	X	X
Belgium	BELNET	X	X	X
Croatia	CARnet	X		
Czech Republic	CESNET	X		X
Denmark	UNI-C	X		
France	RENATER	X		X
Greece	GRNET	X		X
Hungary	HUNGARNET	X		
Ireland	HEAnet	X		X
Italy	GARR	X		
Lithuania	LITNET	X		X
Malta	UoM	X		
Netherlands	SURFnet	X	X	X
Norway	UNINETT	X	X	X
Poland	PSNC	X	X	X
Portugal	FCCN	X		
Slovenia	ARNES	X		
Spain	RedIRIS	X	X	X
Sweden	SUNET	X	X	X
UK	JANET	X		
		20	7	12



# People in TCS

## **SCS**

Guido Aben, Kaspar Brandt, Licia Florio, Jan Meijer, Teun Nijssen, Milan Sova, Karel Vietsch  
and more...

## **TCS**

Kent Engstrøm, Licia Florio, Jan Meijer, Kevin Meynell, Teun Nijssen, Milan Sova, Karel Vietsch  
and more...

## **TCS Tender Committee**

Kurt Bøge, Daniel Garcia, Licia Florio, Dominique Launay, Jan Meijer, Damien Shaw, Milan Sova, Karel Vietsch

# Formal decision making process

- **Service responsible: *TERENA***  
delivers on behalf of participating NRENs
- **Important decisions: *SCS-Rep per NREN***
- **Day-to-day: *TCS PMA***

Kent Engström, Jan Meijer,  
Kevin Meynell, Teun Nijssen,  
Milan Sova

# TCS

- TERENA SSL CA: Server certificates
- TERENA eScience SSL CA
- TERENA Code Signing CA
- TERENA Personal CA
- TERENA eScience Personal CA

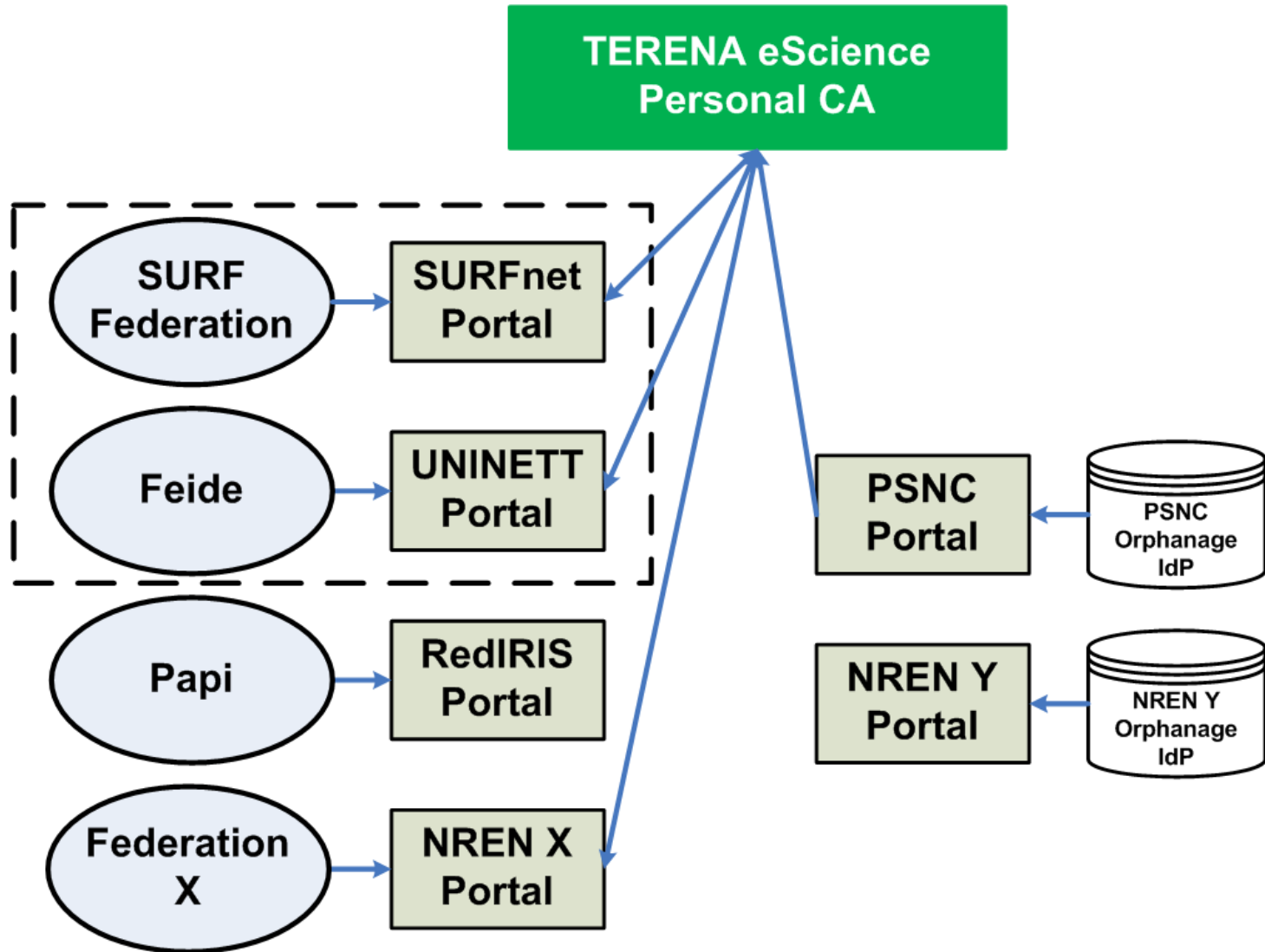
# Why *TWO* Personal CAs?

- (centralised) bulk generation of tokens
- machine-generated DNs
- use case beyond eScience Grid context

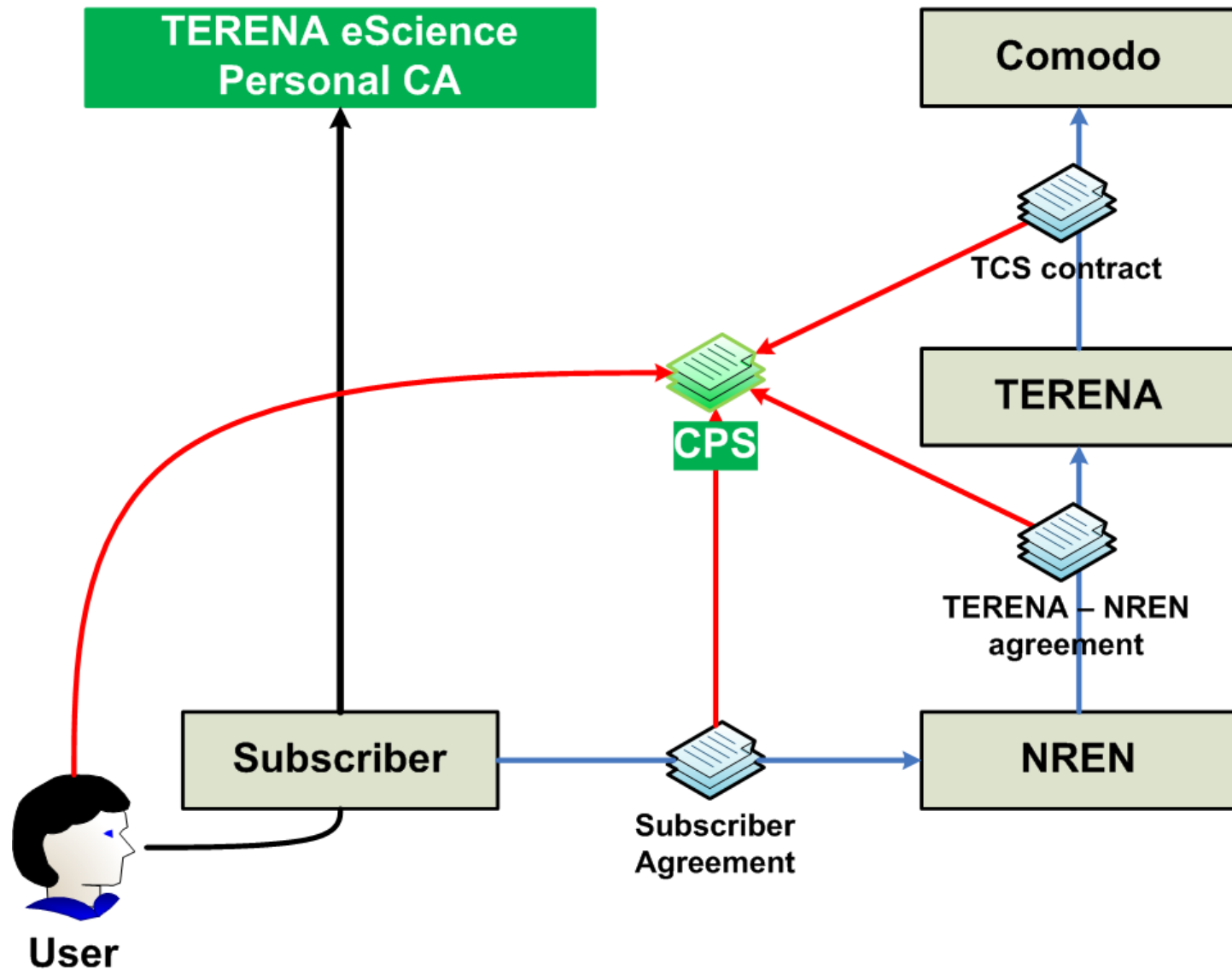
# TCS eScience Personal CA

- Comodo CA backend
- TERENA formulates own CPS
- 12 NRENs participate (a.t.m.)
- Seeking EuGridPMA MICS accreditation
- Effort carried by NRENS, NGIs, AAI Federations, TERENA, NDGF

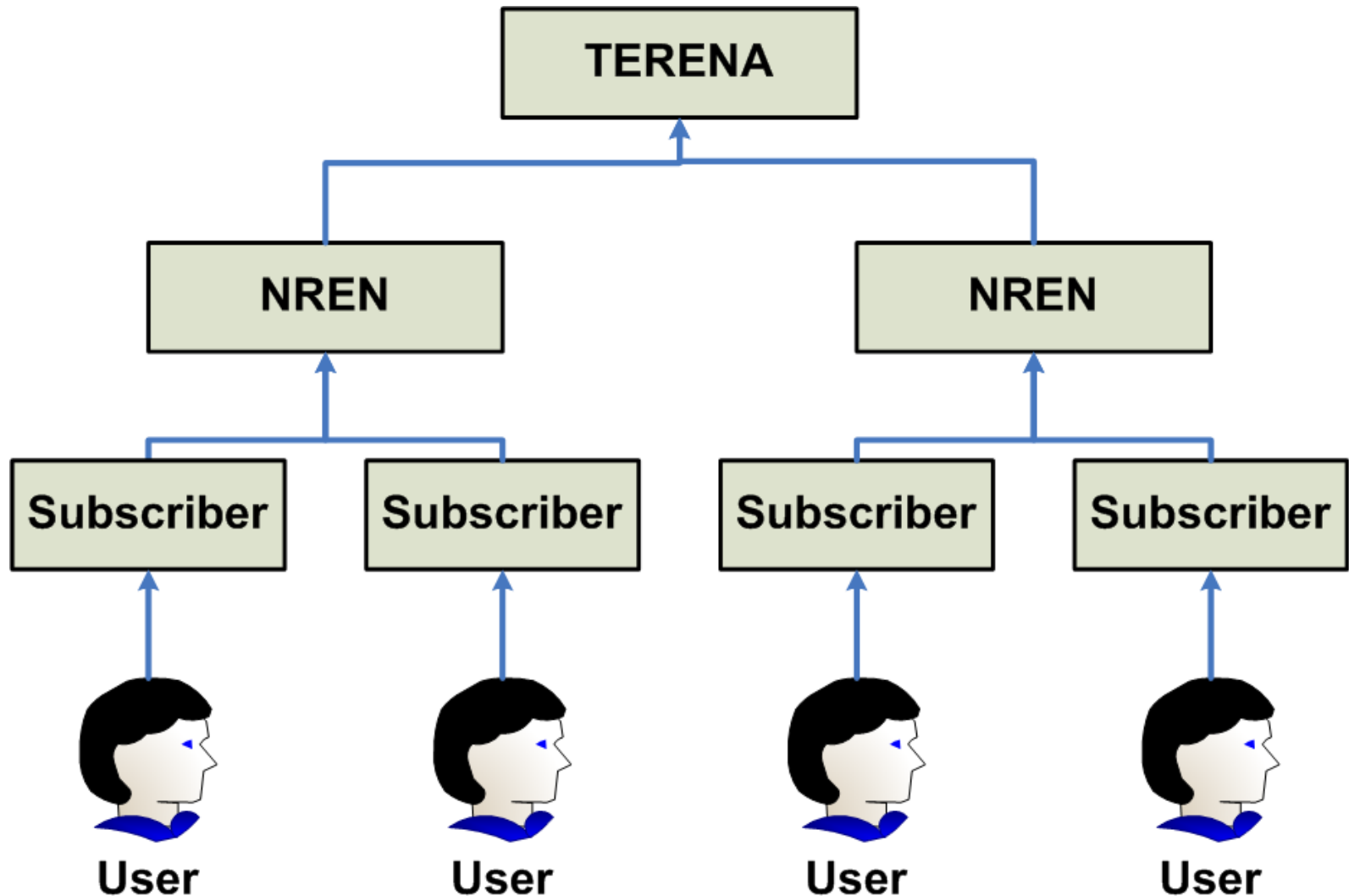
# What will you accredit?



# Contractual relationships



# Delegated Responsibilities





# summing up

## Delegated responsibility

- **NREN** responsible for **Subscribers**
  - Agreement TERENA - NREN
- **Subscriber** responsible for **Users**
  - Agreement NREN – Subscriber

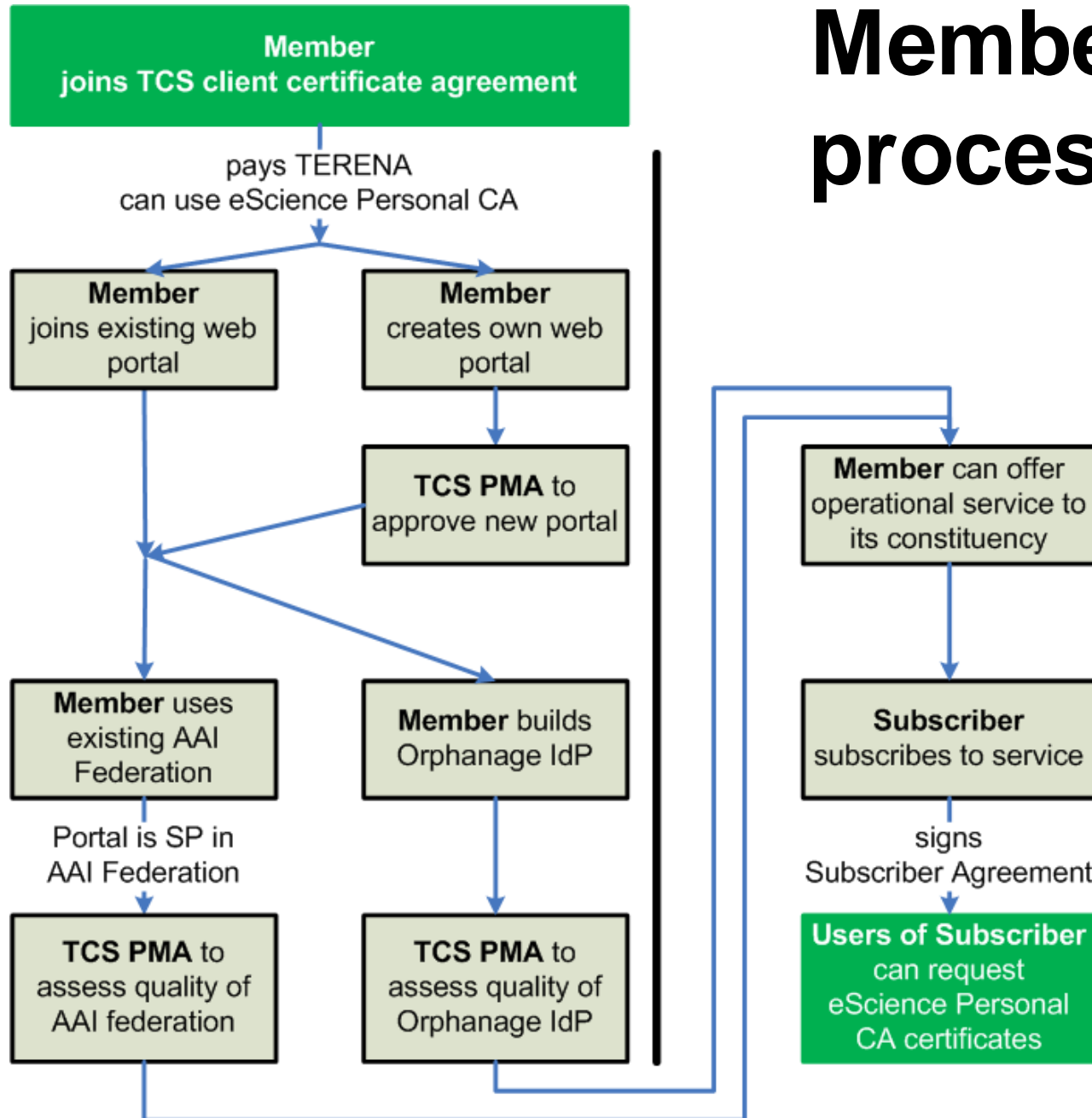
In all agreements:

**adhere to CPS**

# Repository

<http://www.terena.org/activities/tcs/repository>

# Membership process flow



# CA Hierarchy

**UTN-USERFirst-Client Authentication and e-mail**  
(expiry = 09/07/2019)



**TERENA eScience Personal CA**  
(expiry = 31/12/2028)



**End Entity**

(expiry = 14 or 395 days from issuance)

*Cross signed -for visibility in Netscape compatible software- with:*

**AAA Certificate Services**  
(expiry = 31/12/2028)

# Identity Vetting

## 3.2.3 Authentication of Individual Identity

The identity of a Requester in a Subscriber's IdP has been validated by the Subscriber. During the validation process or during processes supporting that validation process the identity of the requester was confirmed with a **face-to-face meeting and valid photo identification** and/or similar official documents.

# User authorisation

## 3.2.3 Authentication of Individual Identity

The Subscriber expresses that an identity has been properly validated by setting a specific value in the *eduPersonEntitlement* attribute of the Requester's identity in the Subscriber's IdP.

# Persistently unique DNs

## 3.1.1 Types of Names

CN: A reasonable representation of the name of the Requester appended with an Identifier that uniquely and persistently represents the Requester in the Subscriber's IdP as described in section 3.1.5

Uniqueness of Names

## 3.1.5 Uniqueness of Names

The Subject Distinguished Name of a TERENA eScience Personal CA-issued Certificate is unique for each Requester by including an Identifier that uniquely and persistently represents the Requester in the IdP of its Subscriber. A Subscriber will ensure the persistence and uniqueness of the aforementioned Identifier that its IdP releases to the TERENA eScience Personal CA. The Identifier must be traceable to a Requester for at least as long as the certificate issued to the Requester is valid.

# Revocation

## **4.9.2 Who can Request Revocation**

- a Member can request the revocation of any certificate within its constituency of Subscribers;
- a Subscriber can request the revocation of any certificate within its constituency of Requesters;
- a Requester can request the revocation of its own certificate.
- A revocation request can be initiated by other entities. Such a revocation request has to be properly and convincingly documented.

## **4.9.1 Circumstances for Revocation**

- The Requester's IdP account is compromised, revoked or its password is compromised;
- There has been a modification of the information pertaining to the Requester that is contained within the certificate;



# Revocation (2)

## **4.9.4 Revocation Request Grace Period**

Any of the parties defined in Section 4.9.2  
“Who can request revocation that becomes aware of circumstances that require revocation of a certificate is obliged to initiate a revocation request as soon as possible.

**Manual and automated revocation with  
Confusa portal software**

# IdP data quality

## 9.6.3 Subscriber Representations and Warranties

Upon signing and accepting the Subscriber Agreement, the Subscriber represents to TCS and to relying parties that at the time of acceptance and until further notice:

- All representations made by the Subscriber to TCS regarding the information contained in the certificate of its Requesters are accurate and true.
- The Subscriber agrees with the terms and conditions of this CPS and other agreements and policy statements of TCS.
- The Subscriber abides by the laws applicable in its country or territory including those related to intellectual property protection, viruses, accessing computer systems etc.
- The Subscriber complies with all export laws and regulations for dual usage goods as may be applicable.
- The Subscriber agrees to on request provide full documentation to Member and/or TERENA about the procedures used to populate and maintain the identity related information in its IdP

# NREN disqualification grounds

## 9.6.2 RA Representations and Warranties

To the extent specified in the relevant sections of the CPS, TCS eScience Personal Certificates Members promise to:

- Comply with this CPS.
- Ensure that the TCS web enrollment application used by the Member complies with this CPS.
- Ensure that only authorized Subscribers can access the Member's TCS web enrollment application.
- Make reasonable efforts to ensure Subscriber's IdPs are adequately maintained.

# Audits

- Comodo audits CA operational environment
- TERENA to organise self-audit of each NREN

# Steps to production

- CPS/EuGridPMA accreditation
  - Jan, Kevin, Milan, Teun
- CPS Reviews
  - TERENA, Comodo, 12 NRENs, AAI Federation folk
- Confusa portal software
  - Thomas (NDGF), Henrik (UNINETT Sigma)
- Deployment
  - NREN + local Grid community

# Timeline 2009

Sept: portal software production release

Oct: CPS through TERENA reviews

Oct: Formal start EuGridPMA accreditation

Oct: Centralised portal production ready

Nov: Production