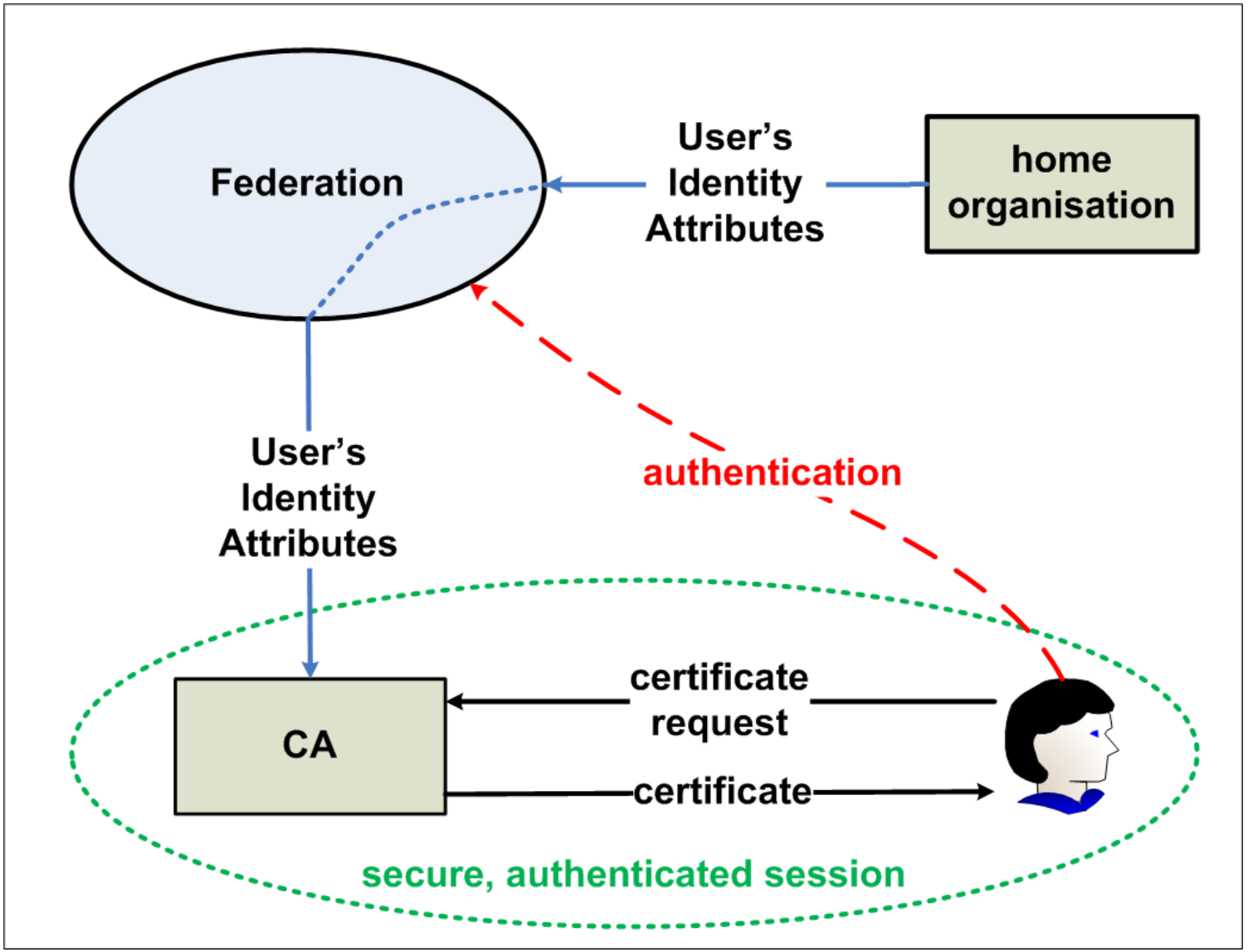
TERENA eScience Personal CA

accreditation

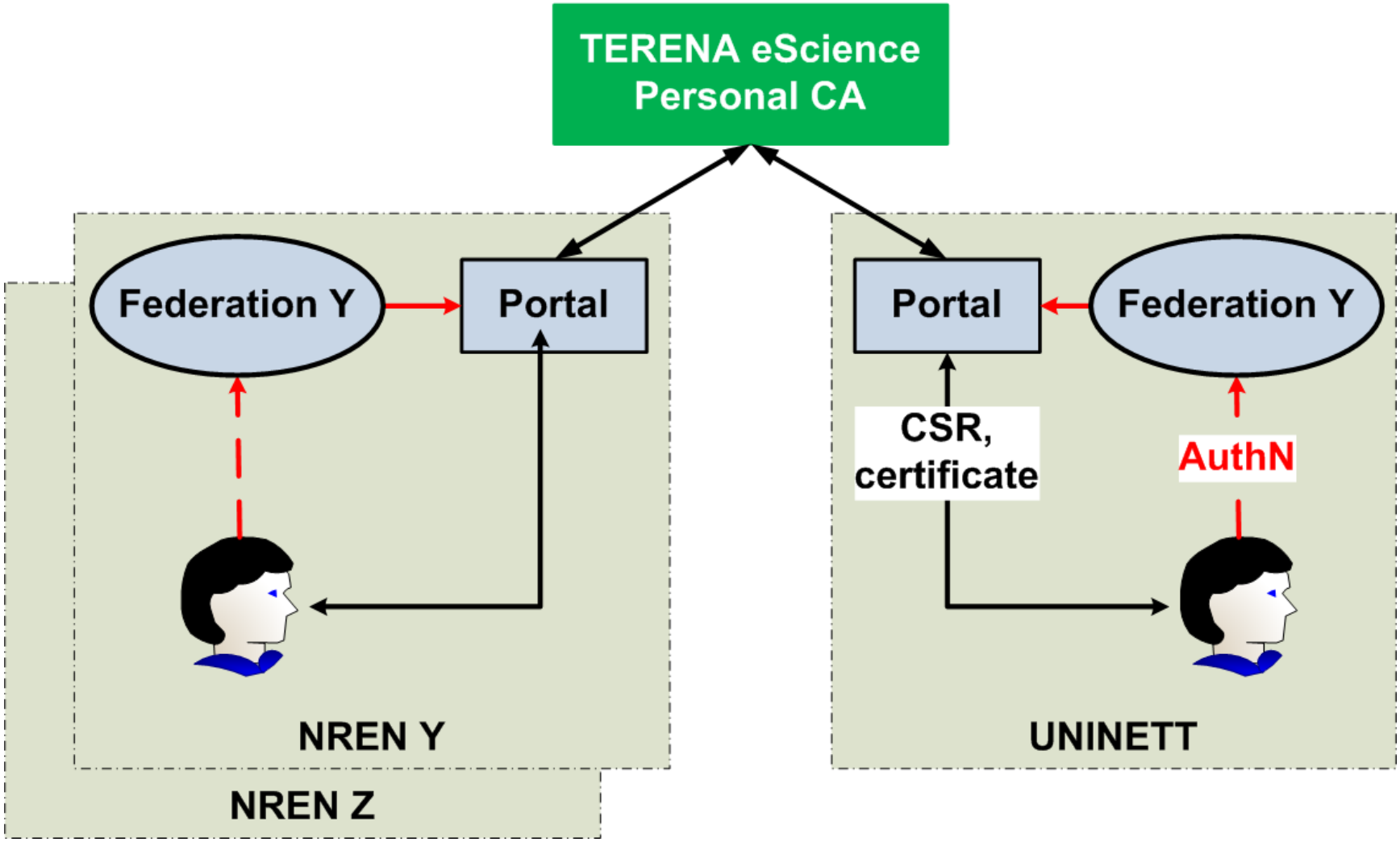
Jan Meijer, TCS PMA

EuGridPMA 18
18-20 Jan. 2010
Dublin

It's a MICS


Federation
User's
Identity
Attributes
home
organisation
User's
Identity
Attributes
authentication
CA
certificate
request
certificate
secure, authenticated session

Special MICS: shared



Project timeline so far

Jan 2009: Project public, Cyprus EuGridPMA presentation
May 2009: Zurich EuGridPMA presentation
Sep 2009: Berlin EuGridPMA presentation
CPS circulated to EuGridPMA
Sep - Oct 2009: EuGridPMA review
-Sajjad Asghar
-Reimer Karlsen-Masur
-David Kelsey
First portal operational
Nov 2009 CPS circulated to NRENs
NREN information meeting held
Dec 2009: Review comments processed
2nd review round commenced
Comodo review initiated
Jan 2010: Most 2nd review round comments processed
CPS circulated to EuGridPMA

TERENA Certificate Service

TCS

NREN collaboration

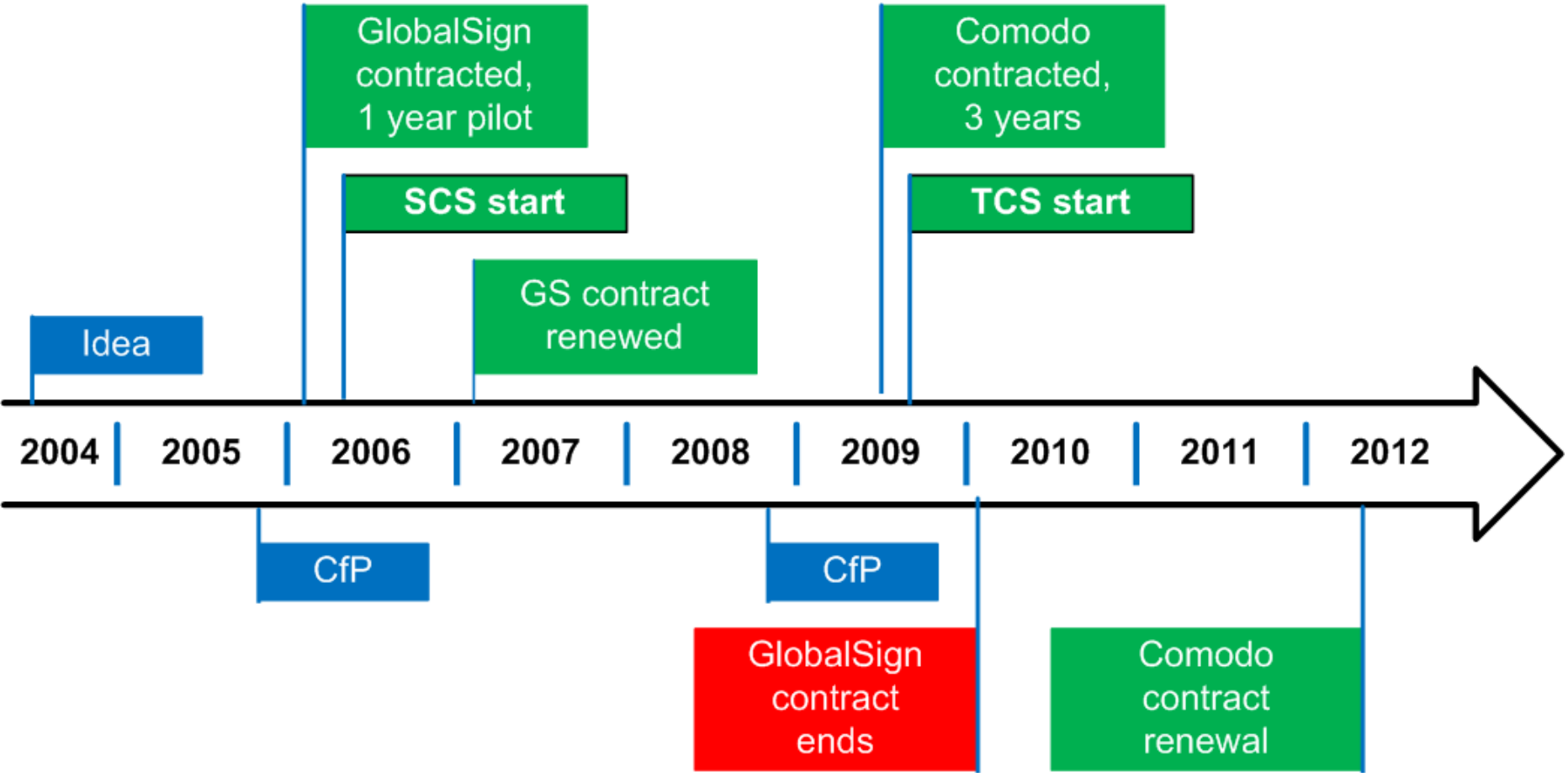
joint procurement & operation

of

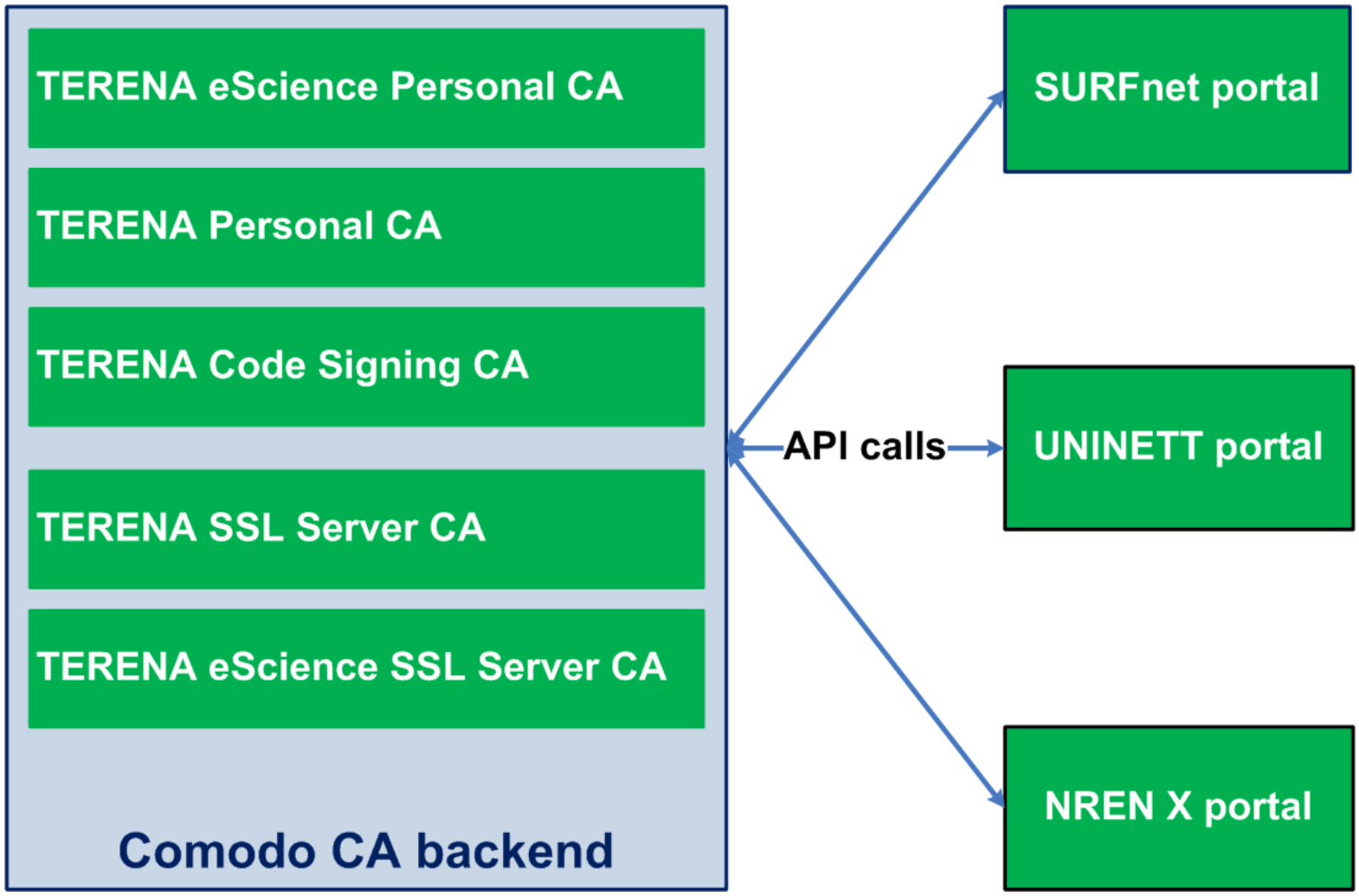
x.509 certificate service

Comodo current service provider

TERENA Certificate Service



TERENA Certificate Service



TCS organisation

- **TERENA**

  contractual party, financial clearinghouse, contact conduit to Comodo
- **TCS Representatives**

  1 per NREN, Formal decisions
- **TCS RAs**

  day to day operations
- **TCS PMA**

  responsible for policy

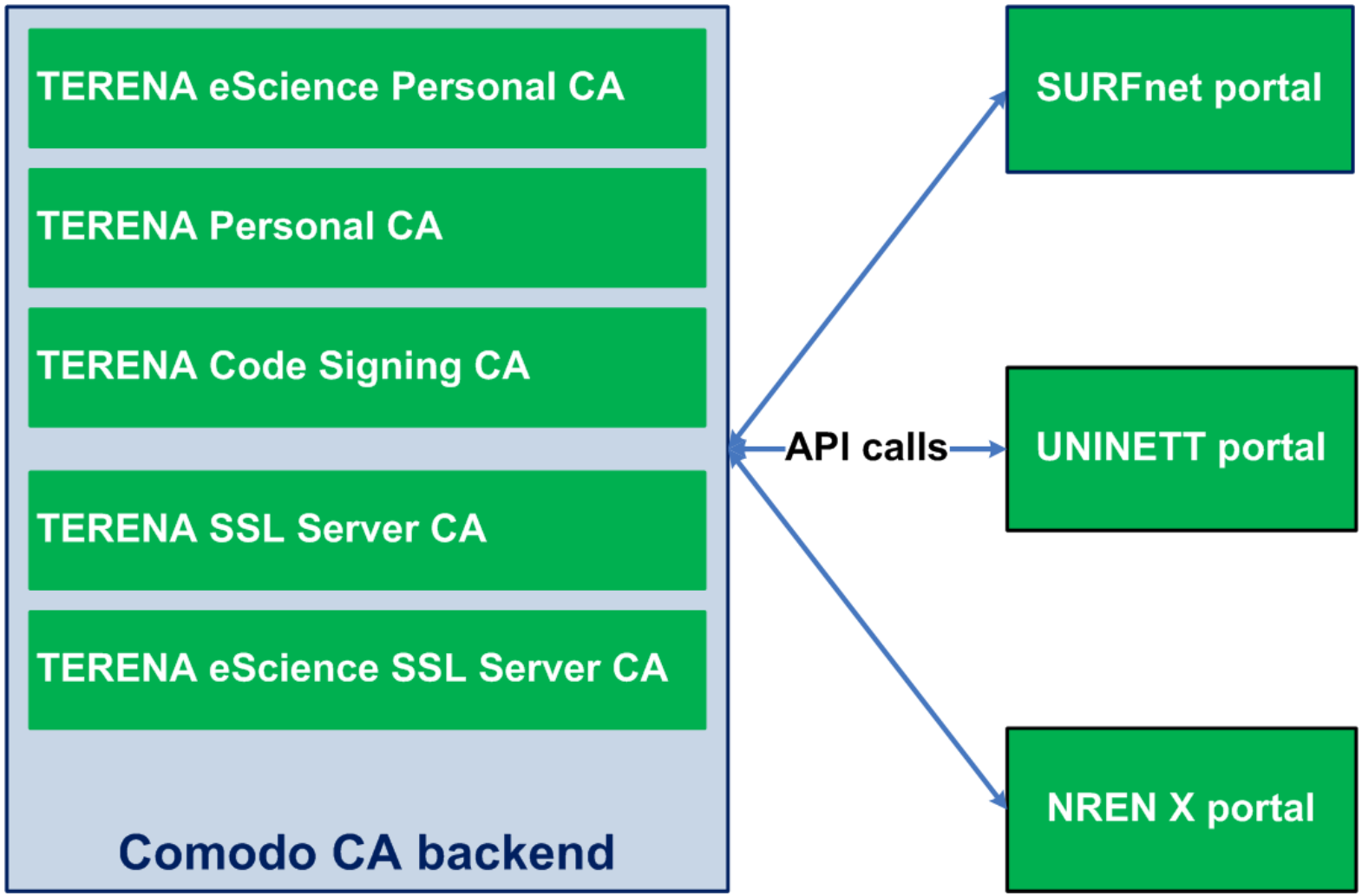
  Kent Engstrom, Jan Meijer, Kevin Meynell,, Teun Nijssen, Milan Sova
- **NREN community**

  various other tasks (portal software, etc.)

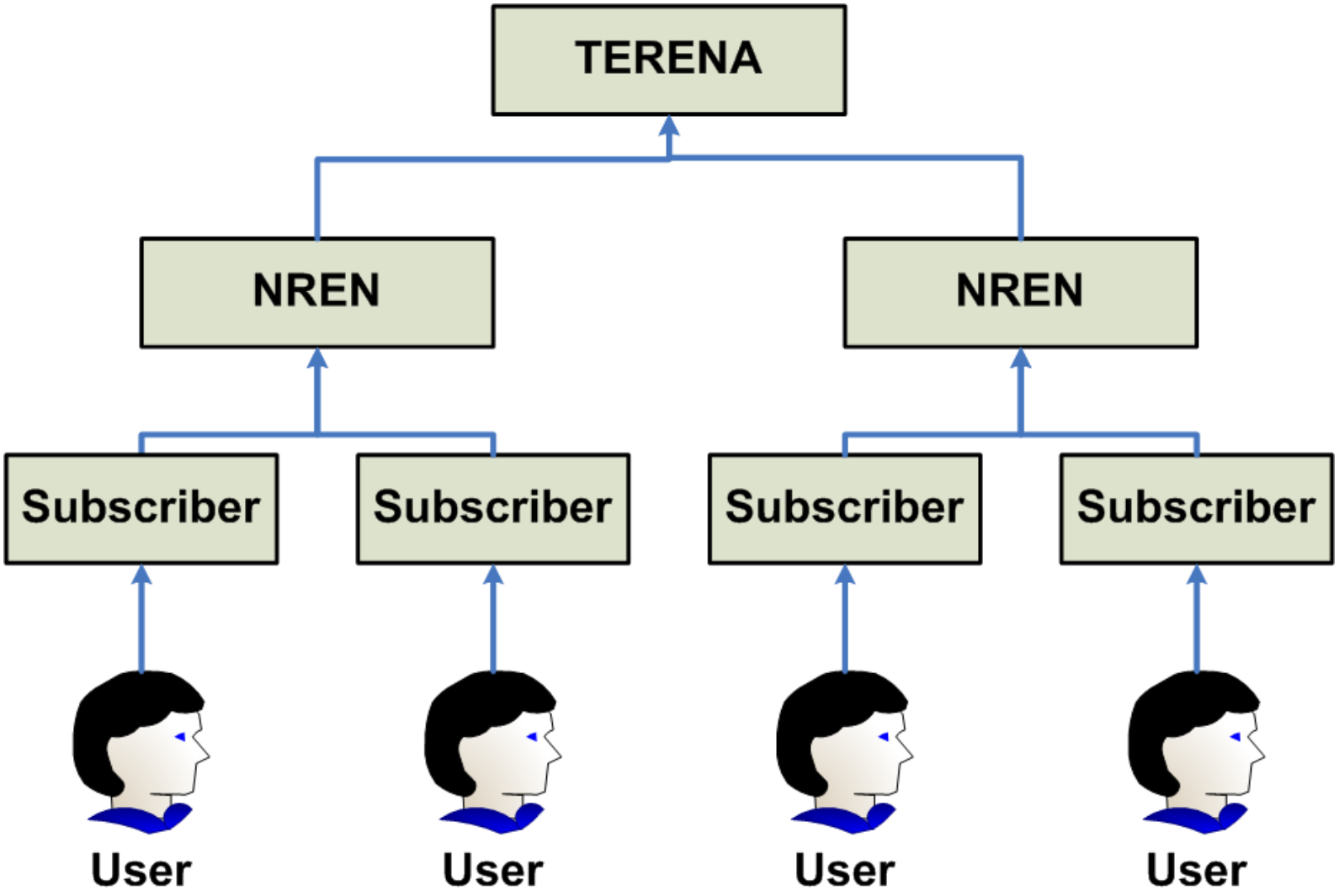
Participating NRENs

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		
Finland	CSC	X		**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		
Serbia	AMRES	X		**X**
Slovenia	ARNES	X		
Spain	RedIRIS	X	X	**X**
Sweden	SUNET	X	X	**X**
UK	JANET	X		

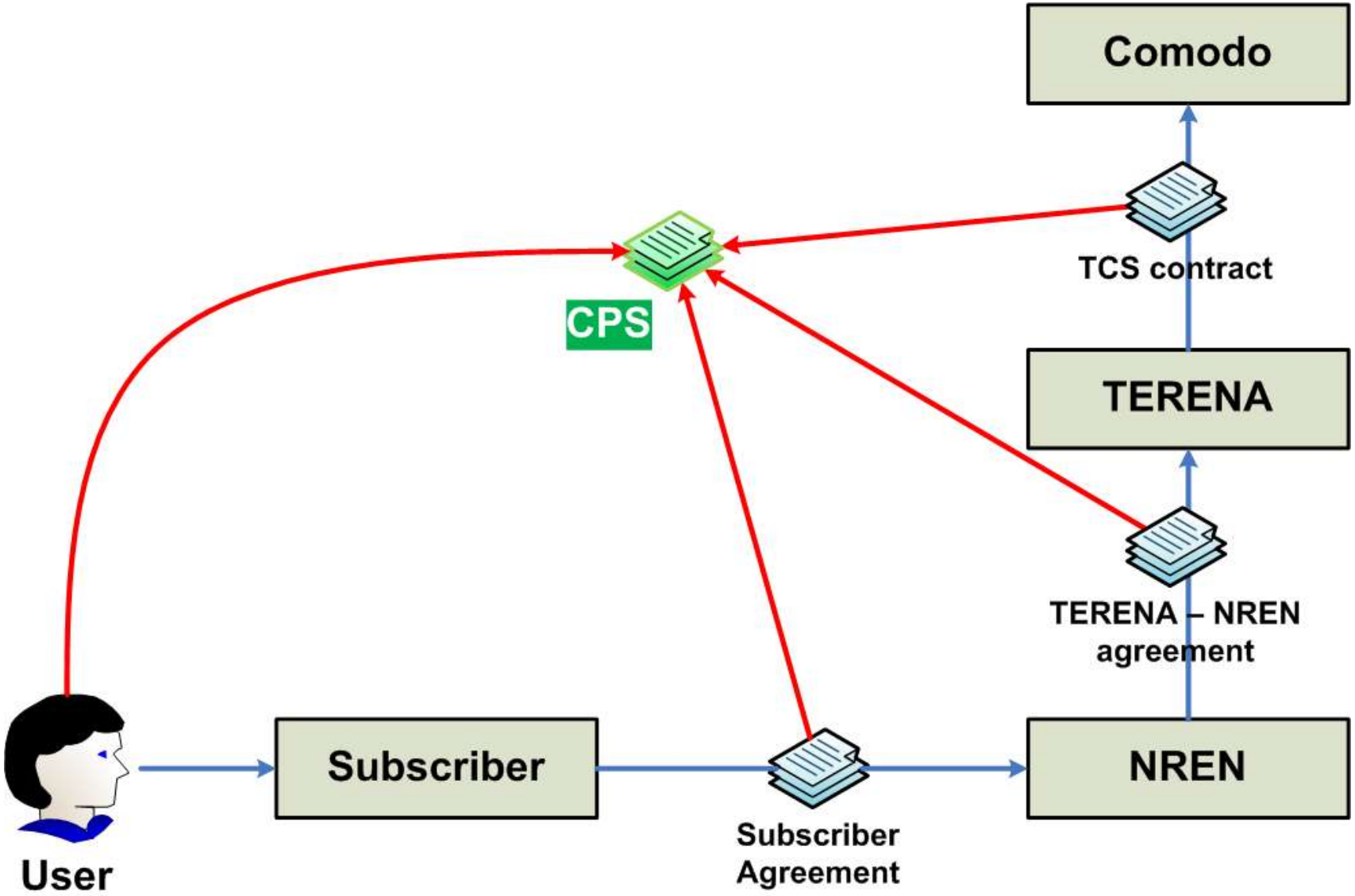
TCS technical components



Delegated Responsibilities



Built using contracts



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

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

summary

- PhotoId requirement
  eduPersonEntitlement
- Persistent unique Id requirement
  ePPN
- Revocation requirement *NREN, Subscriber, user*
- IdP data quality requirements 9.6.3 Subscriber Representations and Warranties

Audits

- No self audit
- CA backend audit part of WebTrust audit
- Asked Comodo to do audit of issuing process similar to WebTrust
- Confusa software will be security audited

Open issue: IDM management & securing (deze dus nog beter)

Profile says:

In the CP/CPS that covers the MICS, the following processes must be described, and must be compliant with this:

- How the primary identity management system is managed and secured
- We do: 9.6.x
- Not de
- Dave K.

Deployment: centralised portal

- Czech Republic, Denmark, *France*, Netherlands, Norway, Sweden, Finland

- TERENA: financial clearing house
- UNINETT: project coordination
- SURFnet: portal operations

- Uses ‘Confusa’ software

- Portal up and running since October

Steps to production

- CPS/EuGridPMA accreditation
  - Finish reviews, 2 week comment period
- CPS Reviews
  - *Comodo, NRENs final comment period*
- Confusa portal software
  - *Done.*
- Deployment
  - *Centralised portal up and running*

post accreditation

- TCS PMA representative to attend EUGridPMA meetings
- TCS eScience Personal: **Teun Nijssen**

takk for meg

http://www.terena.org/activities/tcs/