



TERENA's Server Certificate Service
A short history on building a service you can't
afford by doing it together

APAN, Januari 2008, Hawaii

Jan Meijer

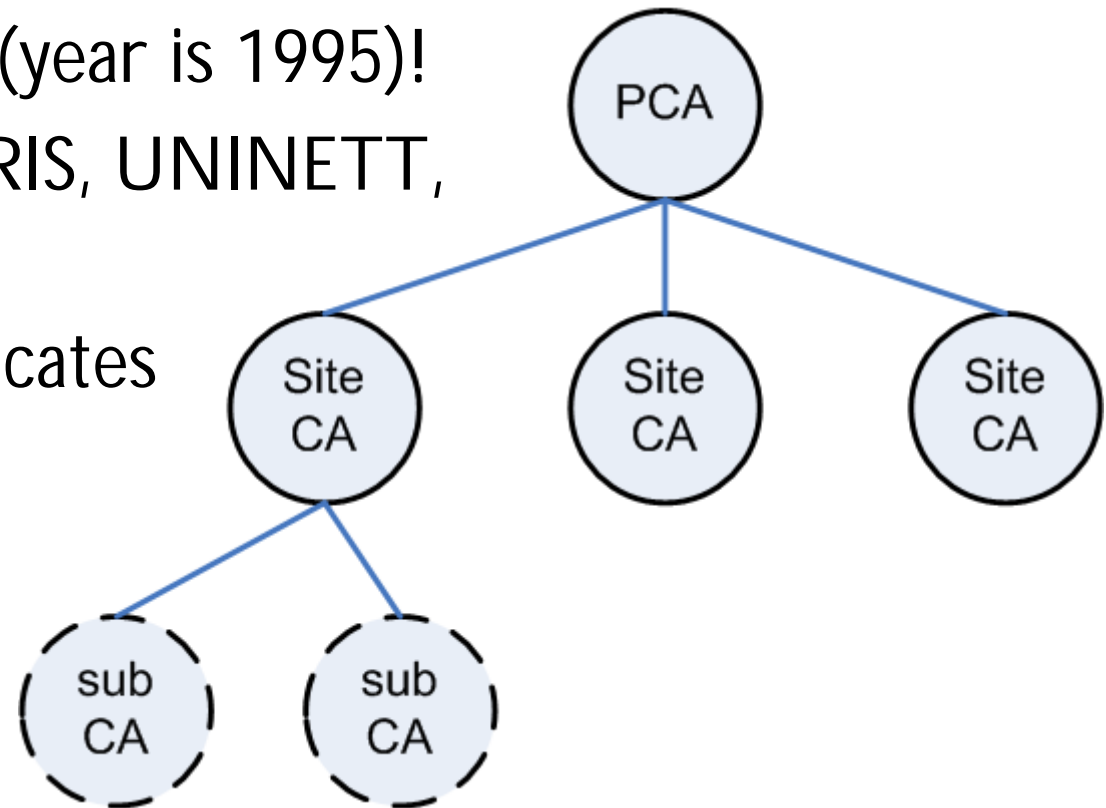
my opinions don't necessarily represent TERENA's!

< 1998: PKI promises

- < 1998
- Encrypted & Authenticated data channels
SSL
- Signed and/or encrypted emails, documents, files
PGP, S/MIME

> 1998: European NREN CAs

- PCA-CA hierarchy
- Check out RFC1875 (year is 1995)!
- DFN, SURFnet, RedIRIS, UNINETT, EuroPKI, ...
- Qualified client certificates
- One PKI fits all
- PGP PKI as well!



1998-2004, the field evolves

- Lot of focus on policy
- Where's the CA/RA separation?
- Plans to link European PKIs
- No real take up
- Qualified = expensive
- Separate Grid PKI infra (but not that scalable)
- TACAR
- Experience but not large scale deployment

1998-2004: It just didn't work out!

- Client certificate use
 - ◆ Portability
 - ◆ Us(er)ability
 - ◆ Popup
 - ◆ The problem wasn't big enough
- Server certificate use
 - ◆ Popup
- With nuances: Switch, DFN, CRU

June 2004: The SCS idea

- TERENA TNC, Rhodes
- Split the issue in manageable chunks
- There's a need for server certificates, solve that need first
- What if? You could contract a service with a commercial CA for an (for all practical purposes) unlimited amount of SSL certificates for a *flat rate per NREN*?
- How many NRENs would you need? Would there be an interested vendor?

Sep 2004: Making it happen

- September 2004, TF-CSIRT, Malta: Jan Meijer & Christoph Graf meet up and write up proposal with a *security twist*!
- Create massive deployment of encrypted channels
- Popup-free SSL certificates for a flat rate
- Nice to have: certificate profile flexibility
- Leverage existing NREN PKI RAs, where in place
- TERENA as contracting party

2005: Ball starts rolling

- November 2004, 1st TF-EMC2, Amsterdam, Jan presents proposal, asks NRENs to join the gamble for EUR 20K each
- Also approaching TF-CSIRT folks into PKI and EUGridPMA folks in Jan 2006
- Februari 2006, 2nd TF-EMC2, Amsterdam, update, etc., etc.

March 2005-Sep 2005: answer questions

- Vendor interested?
- Enough NRENs (enough money)?
- Able to line up diversity of wishes without compromising ultimate goal?
- Need to do official EU tender (legal)?
 - ◆ service, 235KEUR/4 years
 - ◆ risk for TERENA?

Sep 2005: Call for Tender!

- ACOnet (.at), CARnet (.hr), CESnet (.cz), CRU (.fr), UNI-C (.dk), RedIRIS (.es), SURFnet (.nl), SWITCH (.cz) start
- Conservative estimate: ~2800 certificates/yr
- Asking for multiple profiles (would add Grid community!)
- Open process but NOT EU guidelines
- Not mentioned budget
- One clarification round

December 2005: we had a winner!

- 1 year contract signed with GlobalSign, then a Cybertrust company
- CyberTrust root
- Multiple profiles
- RA per NREN
- Optimal price scaling: very cheap for large numbers

Jan – Mar 2006: service setup

- Agree on TERENA specific RA procedures: pre-registering organizations, pre-reg of domains possible, fax or signed email
- First (mandatory) RA training

16 March 2006: Go!



13

Popular service

- @SURFnet: ~30 clients within 2 months without effort
- takeup numbers?
- Beginning: approx 5 minute handling time / certificate
- Halved by dedicated printer on desk chief RA.....
- Further optimization by dig sig

SCS numbers: TERENA

<i>NRENs</i>	<i># issued</i>	<i># SCS users</i>
ACONet	979	26
ARNES*	23	
BELNET	673	57
CARNet	166	n/a
CESNET	452	20
CRU/RENATER	1446	134
GARR**	100	20
JANET (UK)	2300	212
RedIRIS	1077	86
SUNET***	487	17
SURFnet	1934	91
SWITCH	1200	n/a
UNI-C****	1366	n/a
UNINETT	348	24

- * Service started in Sep 07
- ** Service started in Apr 07
- *** Service started in Jul 07
- **** Service started in Oct 07



SCS numbers: UNINETT

Month	Certificates				Subscribers	
	requests	issued	denied	revocations	new	total
2006-10	21	16	4	1	4	4
2006-11	22	20	2		3	7
2006-12	9	8	1		1	8
2007-01	4	3	1		1	9
2007-02	25	16	8	1	2	11
2007-03	20	13	7		0	11
2007-04	16	14	2		4	15
2007-05	27	24	3		2	17
2007-06	28	24	4		0	17
2007-07	25	18	7		2	19
2007-08	33	30	3		2	21
2007-09	55	53	2		2	23
2007-10	35	31	4		0	23
2007-11	60	49	11		0	23
2007-12	31	29	2		1	24
Total	411	348	61	2		

16



Mar 2006 – now: so far so good

- Contract renewed: Jan 2007- Jan 2010
- Core functions, vendor has been taken over twice though
- Some performance issues
- Scaling works well for *server* certificates!
- One certificate profile dominates, 3 year validity

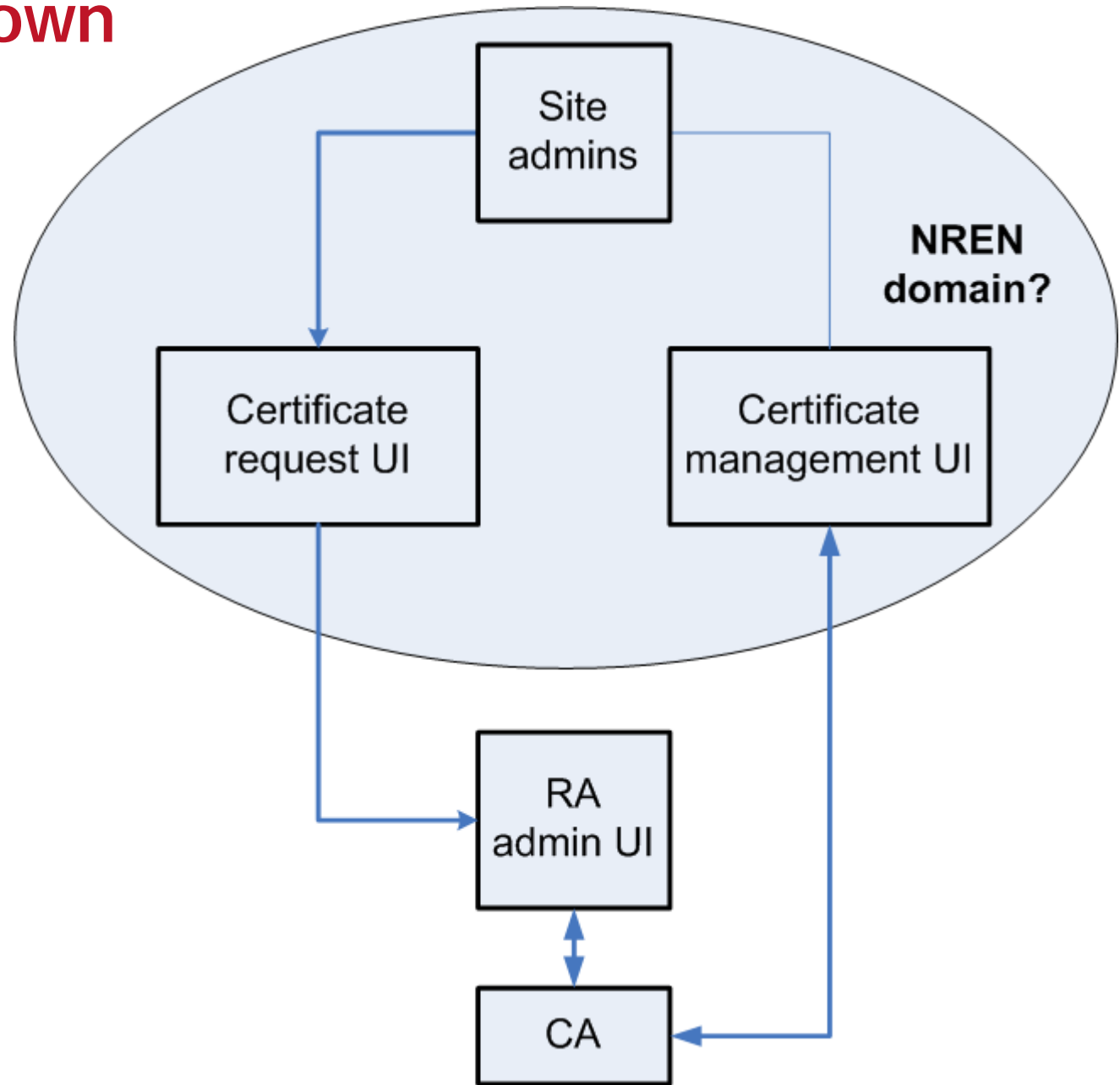
Lessons learned

- Rolling out took longer than GS anticipated
- Vested interests, existing services, individual strong opinions, the policy devil, freedom to act innovative
- Individual contacts crucial
- Organizing services together in Europe makes sense

Future

- OCSP responders
- HTTP POST interface
- What will we do after 2010?
- Client certificates?

Future: create own
PKI platform
(again)?



Interesting side effect

- Candy was too tempting
- Policy issues disappeared, magic!
- Now one RA policy for all SCS participants!

- One big purchase combination for PKI services in Europe 😊
- Massive rollout of SSL server certificates
- Massive use of encrypted channels

Mission accomplished

<http://www.terena.org/activities/scs>

23

now it's really lame not to use
encrypted channels in academic
Europe

Thanks, enjoy lunch 😊

