South African e-Science CA

Bruce Becker | bbecker@csir.co.za
SANREN - Meraka Institute, CSIR
Coordinator, SAGrid

Outline

- Back to the future
- SA e-Science CA – topics of interest
  - organisational structure
  - SANREN and SAGrid
- Current CP/CPS overview
  - General CP/CPS status
  - Special topics
    - Identity vetting
    - Auditing and retention
    - Technical controls
- Proposed way forward.

Back to the Future

- We last spoke in December 2009 ! First presentation of CP/CPS to EUGridPMA in Berlin
  - Initial efforts to create a CA were concurrent with the creation of SAGrid – stifled by manpower issue
  - Work focussed on development of CP/CPS – no implementation of working CA.

Little Italy

2009 – 2012: SA was a ”province” of the INFN CA

https://security.fi.infn.it/CA/en/RA/

iThemba LABS, South Africa	Sean Hamilton Thomas Murray	ZA-ITHEMBALABS
Meraka Institute, South Africa	Bruce Becker	ZA-MERAKA
Universite' de Saint-Josef, Lebanon	Ziad Francis Edgard Seif	LB-USJ-FS
University of Cape Town, South Africa	Timothy John Carr Andrew Dale Lewis	ZA-UCT
University of the Free State, South Africa	Albertus van Eck	ZA-UFS
University of Johannesburg, South Africa	Francois Wolmarans	ZA-UJ
University of Witwatersrand, South Africa	Scott Edward Hazelhurst	ZA-Wits

A bottleneck

- From 2012 onwards, we tried to add several new sites in South Africa to the SAGrid infrastructure – unable to add new RA's and issue host certs !
- Epic fails and lots of frustration – couldn't deploy new sites and identify users
  - SAAO (Astronomy, Astrophysics) – ~20 researchers very high usage
  - SANBI – National Bioinformatics Institute – high-priority research activities
  - University of KwaZulu Natal – ATLAS member

A temporary workaround

INFN CA was not willing to assign new RA's, but the EGI Catch-All CA was :

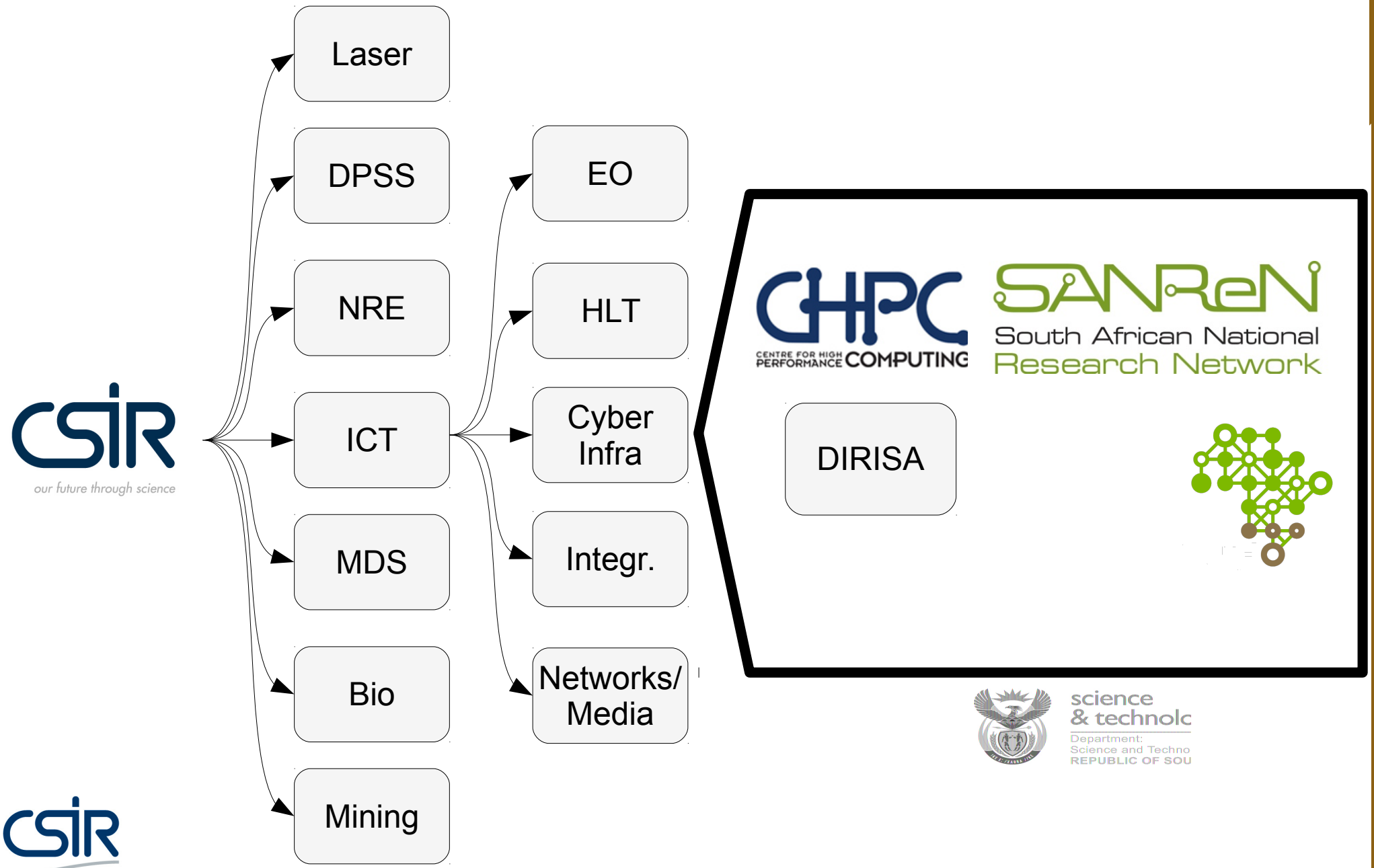
http://see-grid-ca.hellasgrid.gr/

Country	Institute
South Africa	SANBI
Nigeria	Nsukka University
Senegal	UCAD
Tanzania	TERNET

Stop-gap measures aren't enough

- Many institutes, projects and researchers don't have access to the collaboration...
- Clearly the lack of an accredited e-Science CA is impeding collaboration
- ”Where” should the CA be ?
  - The natural place for the CA to sit is with the grid initiative
  - The natural place for the grid initiative is close to the NREN, which provides many other services

Org. Structure



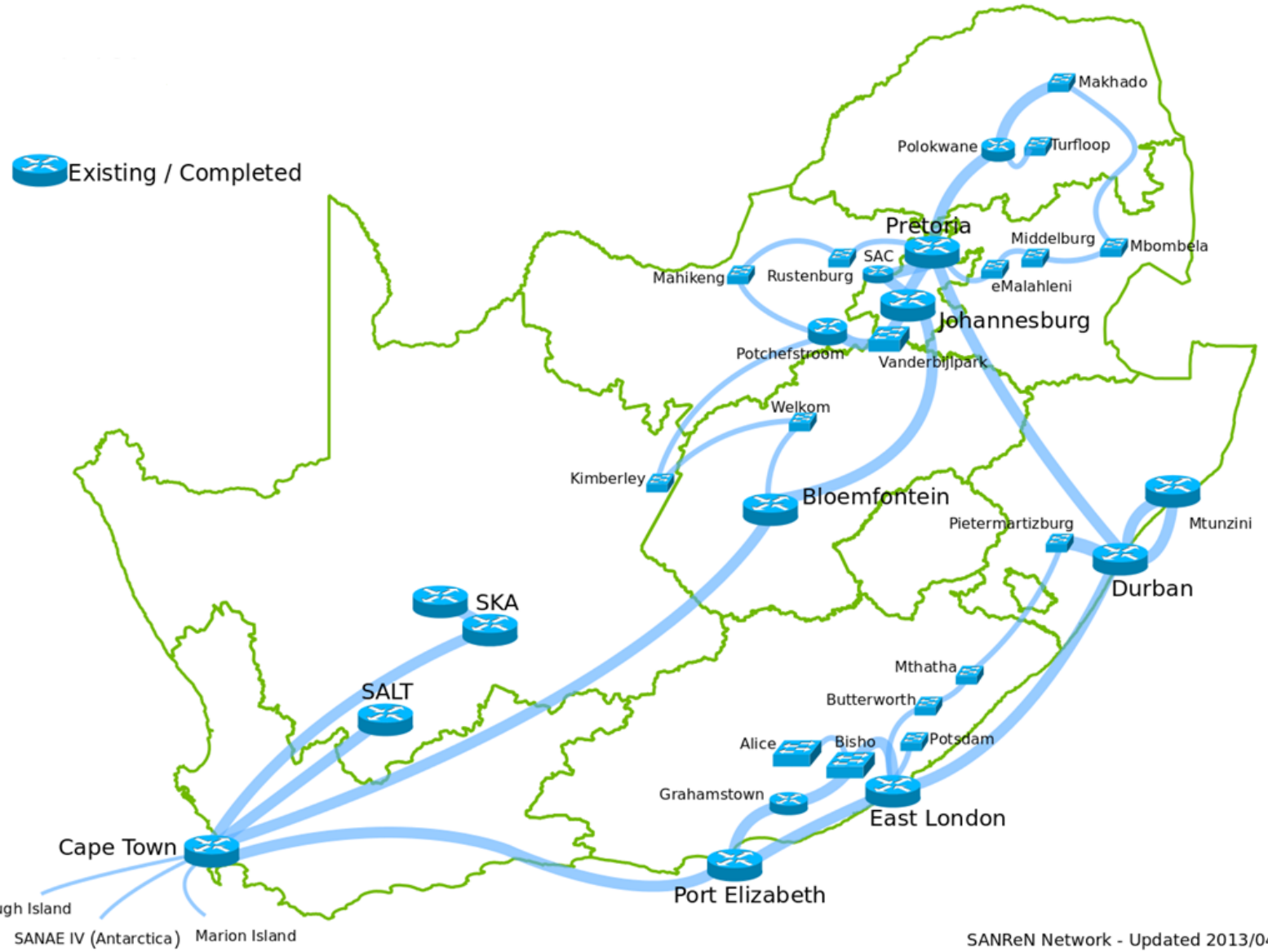
SANReN
South African National Research Network

SANReN and TENET: The SA NREN

- SANReN's mandate:
  - Roll-out fully CAPEX funded broadband connectivity to all publicly funded universities, sciences councils and science projects of national interest
  - HCD and research in broadband technologies
  - **Develop advanced services (e.g. eduroam, LightPaths, Science DMZs, perfSONAR, CSIRT iDF)**
  - **Custodian for the SAGrid initiative**
- SANReN and TENET relationship:
  - Both not-for-profit organisations together form the South African NREN (SANREN)
  - SANReN designs, plans and manages the roll-out of the NREN
  - SANReN develops experimental services and hands over to TENET when mature
  - TENET manages the network and its services on a day-to-day basis
  - TENET handles all contracting with beneficiaries, as well as cost recovery
  - SANReN + TENET = SA NREN

SANReN
South African National Research Network

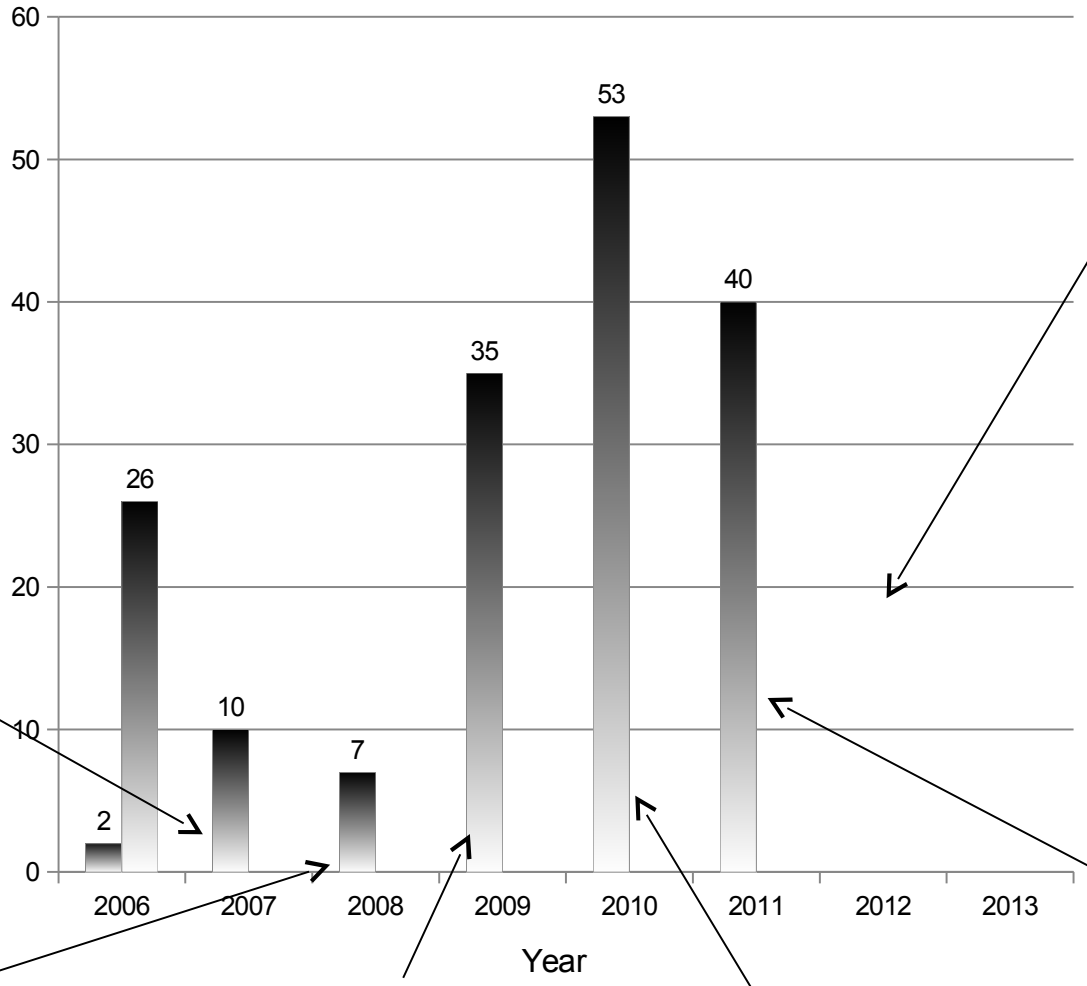
SANReN Network Roll-out: Current Backbone



science & technol
Department: Science and Techn
REPUBLIC OF SO

SANReN Network - Updated 2013/04/08

SANReN Sites Connected



Backbone extensions come online (19 sites), RCCP (7 sites) and numerous internal/other projects (14 sites)

Links to Hartebeeshoek Radio Astronomy and CSIR Satellite Applications Centre constructed. Equipment specification and procurement the focus of work in 2007.

Cape Town network completion and numerous backbone extensions mean the number of new sites connected was the largest yet

SANReN Johannesburg network implemented causing surge in number of connected institutions.

Resources and finances utilised to build the national backbone network. Few sites were connected, but the network now had a far reach and caused major price reductions.

Tshwane and Ethekwini metropolitan areas come online, causing a large increase in number of sites connected

”Sister” projects

- SANREN is a community enabler – two other projects coordinated by SANREN which support the CA mandate:
- National Identity Federation (FID)
  - Users will likely be identified mainly by their institutional credentials.
  - SAML/x.509 interoperability important
  - Science gateways will use robot certs, users hardly see x.509
- CSIRT
  - CSIRT developed and currently operated by SANREN
  - Community CSIRC model- http://www.sanren.ac.za/2013/05/csirc-model/
  - Already proved worth during heartbleed...
- There are real people ;)

General Accreditation Readiness

- SAGrid team has a long history of dealing with EUGridPMA-accredited CA.
  - CP/CPS has been prepared in 2008, updated in 2013
  - Several certificates already issued and renewed to SA entities
  - Procedures and guidelines well understood by the community
- CA is operational thanks to CHAIN-REDS and ei4Africa support
  - Hosted by SANREN at the CSIR data centre
  - Currently operational in alpha, getting feedback from selected entities
  - Needs to be informed by CP/CPS and accreditation reviewer feedback
- Generally good position.

General Status

- CP/CPS status – v.0.0.3 Document Object Identifier:1.2.840.113612.5.4.2.8.0.1
- Already undegone significant internal review
  - *Likely* complies with SA law
  - Updated recently (2014)
- Operational Status
  - Online machine functional – https://security.sanren.ac.za/CA
  - Online services mostly respect the CP/CPS (internal audit necessary)
  - Online machine also contains signing key (in a secure location, but still online)
  - Offline machine containing key to be deployed, secured
  - Lots of documentation and procedures missing
- CSIRT awaress
  - also hosted by SANREN
  - Aware of the project

Certificate and CRL profiles Section 7

- Cert x.509 v3 profile, CRL v1
- Name forms
  - Issuer: C=RSA,O=CSIR,CN=South African e-Science CA
- Issue certificates for
  - Natural persons
  - Hosts and services
  - robots

Insitutional Identity Vetting - Section 3.1.8

- Authentication of Organization Identity is part of the procedure for the appointment of an RA (see Section), and only the Organizations for which an RA has been appointed appear the certificates.
- SANREN connects every site that can have an RA - very good vetting of organisations
- RA identities published on website
- Central store of appointment letters

Individual Identity Vetting – Section 3.1.9

- **Natural Person**: the subscriber is authenticated by meeting the the RA face to face* and producing the following documents:
  - a valid national Identity booklet or a valid passport of a legal resident in South Africa
  - a valid official letter conforming the affiliation with the indicated organization

  The RA carefully validates the documents and confirms the photo image and then makes photocopies and scanned images of the documents.
  The original letter of affiliation is retained by the RA.
  The RA will communicate to the CA in a secure on-line transaction or in person the name and surname of the requester and the details of his ID document.
  Another set of photocopies of the subscribers documents is securely sent to the CA.
  No such photocopies will be accepted from the subscriber.
- **Digital Processing Entity** and **Service:** the requester must send the request to the RA by a signed e-mail. The RA verifies the correctness of the request and sends it – including the requester's signature – to the CA by a signed e-mail.
- **Robot**: as for a Natural Person. In addition the certificate request must be generated in the RA's presence using a secure hardware token, as described in Section .

Identity Vetting via Videoconf

- Physical face-to-face identity vetting is a problem
  - Hugely unpopular, seen as a time waste by users
  - Simply prohibitive in some cases.
- South Africa is a big country, with many institutes far and wide
  - Many remote campuses
  - Sparsely populated (scientifically speaking)
- But...
  - SANREN connects them all !
  - Videoconferencing in wide use in SA – Adobe Connect
  - Want to have the ability to Vet Identity remotely and privately over videoconf
- Want to have this in the CP/CPS.

Auditing and retention Section 4.5

- Currently keep log of :
  - authentications of natural person;
  - certification requests;
  - issued certificates;
  - revocation requests;
  - issued CRLs;
  - all correspondence sent and received by the CA;
  - Changes in signing machine state (reboot/etc)
- Full machine data (logs of everything) in a secure location to be maintained for at least 3 years
- Audit done by SANREN personnell

Technical Controls

- Key pair generation :
  - Keys for the SAGrid CA are generated by CA staff on a dedicated machine, not connected to any type of network
    - Currently generated on the online machine
    - Keyphrase for CA key kept remotely only by CA operator
  - The software package is OpenSSL
    - 1.0.1e-16
  - Each entity must generate its own key pair.
    - True
- Key delivery :
  - No private key delivery
  - CA key delivery via website
  - Entity key delivery via email and published on website

Proposed way forward

- Goal : accreditation in September
- Three phases to accreditation
  1. June/July 2014 : supervised operation
     1. CA existence is publicised
     2. Initial review comments and suggestions implemented
     3. Feedback from community about web interface adopted
     4. Finalise documentation
  2. August 2014 : service and security challenge
     1. Run a ”dress-rehearsal” of the CA
     2. Publicise execution and results of all procedures
     3. Simulate disaster ?
  3. First week of September 2014 : Accreditation preparation