



Sinnott, R.O. and Bayliss, C. and Chadwick, D. W. and Doherty, T. and Harbulot, B. and Jones, M. and Martin, D. and Millar, C. and Roy, G. and Roy, S. and Stewart, G. and Su, L. and Watt, J. and Asenov, A. (2008) *Scalable, security-oriented solutions for nanoCMOS electronics*. In: UK e-Science All Hands Meeting , 8-11 Sept 2008, Edinburgh, UK.

<http://eprints.gla.ac.uk/7387/>

Deposited on: 8 September 2009

## Scalable, Security-Oriented Solutions for Nano-CMOS Electronics

**Gordon Stewart**

National e-Science Centre  
University of Glasgow

# Project Overview

- £5.3M EPSRC Pilot Project
- Provide a grid-based framework to enable scientists and engineers in the electronics field to design and simulate devices and circuits at the “nano” (i.e. sub-90 nm) scale
- 4-year project which started in November 2006



University  
of Glasgow

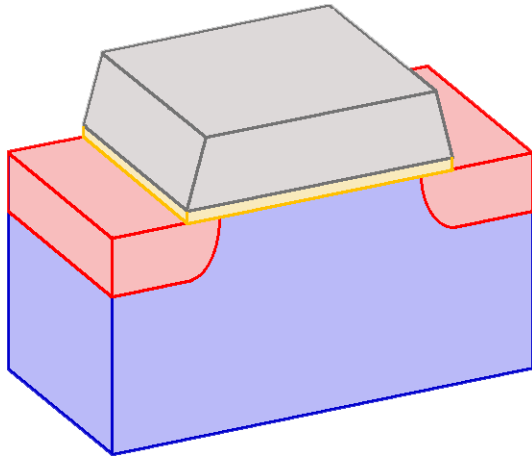


UNIVERSITY OF  
Southampton

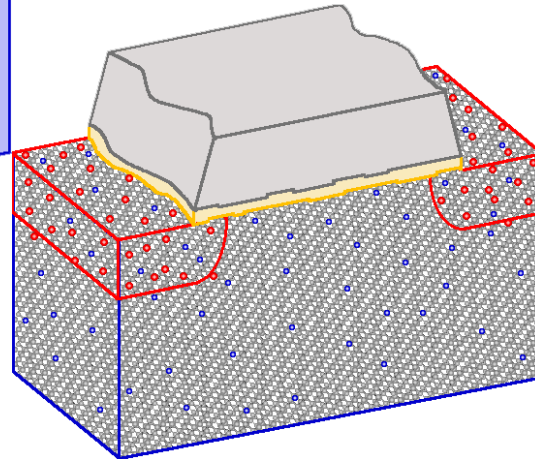
MANCHESTER  
1824

THE UNIVERSITY of York

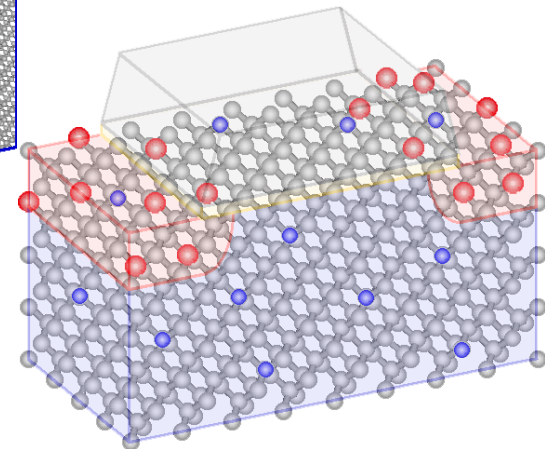
# Project Overview



The simulation  
Paradigm  
now



A 22 nm MOSFET  
In production 2009



A 4.2 nm MOSFET  
In production 2023



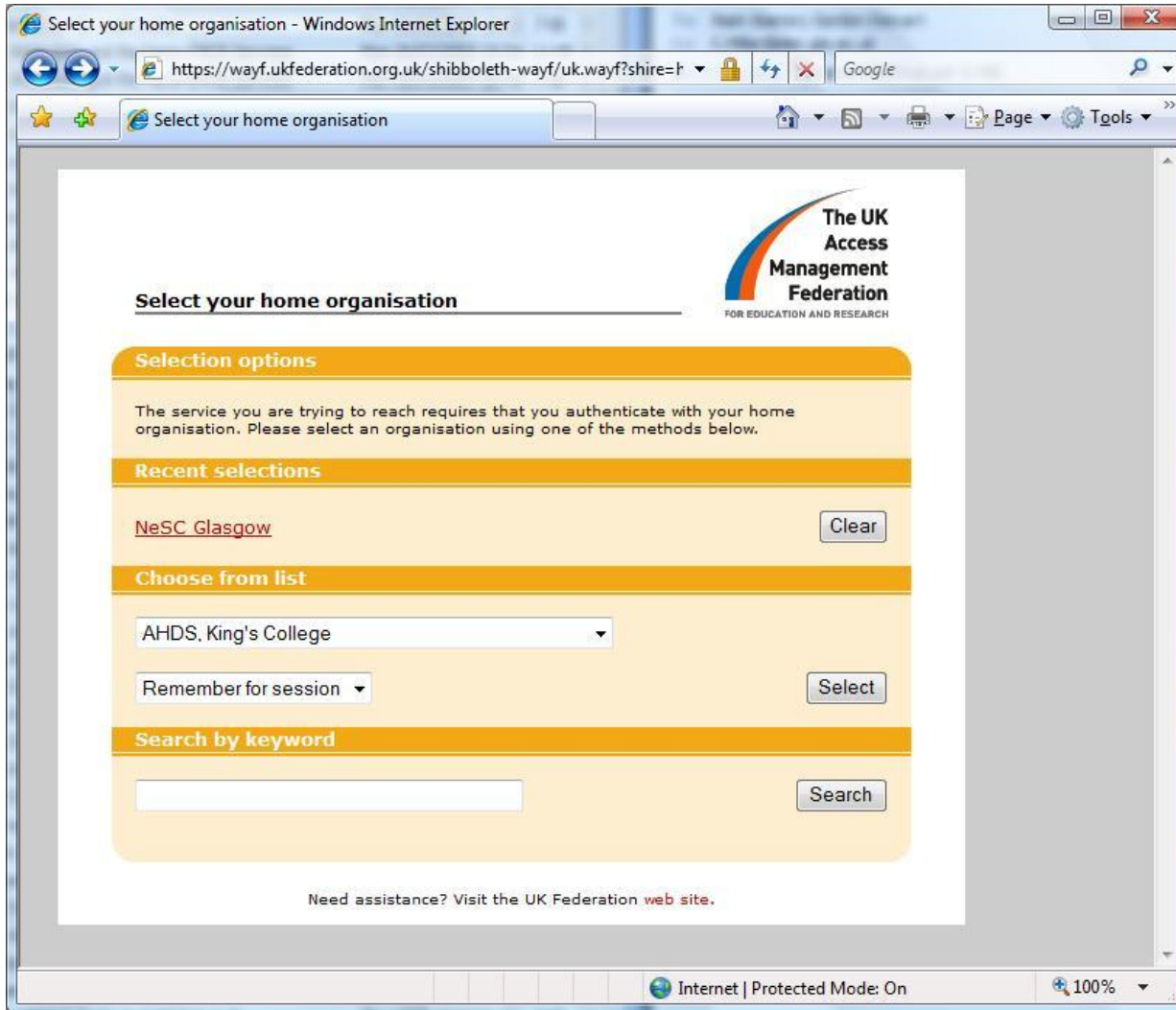
- Security framework requires integration of various technologies
  - Portal-level
    - Shibboleth, SPAM-GP
  - Service-level
    - WS-Security, GSI, VOMS
  - Data-level
    - Kerberos, GSI
  - Resource-level
    - GSI, VOMS, LCMAPS, LCAS



- Prototype portal developed during first year of project
- Users attempting to access restricted URLs are redirected to sign-in (“where are you from?”) page
- Following authentication, request headers include additional Shibboleth attributes
- Attributes can be used in authorization decisions

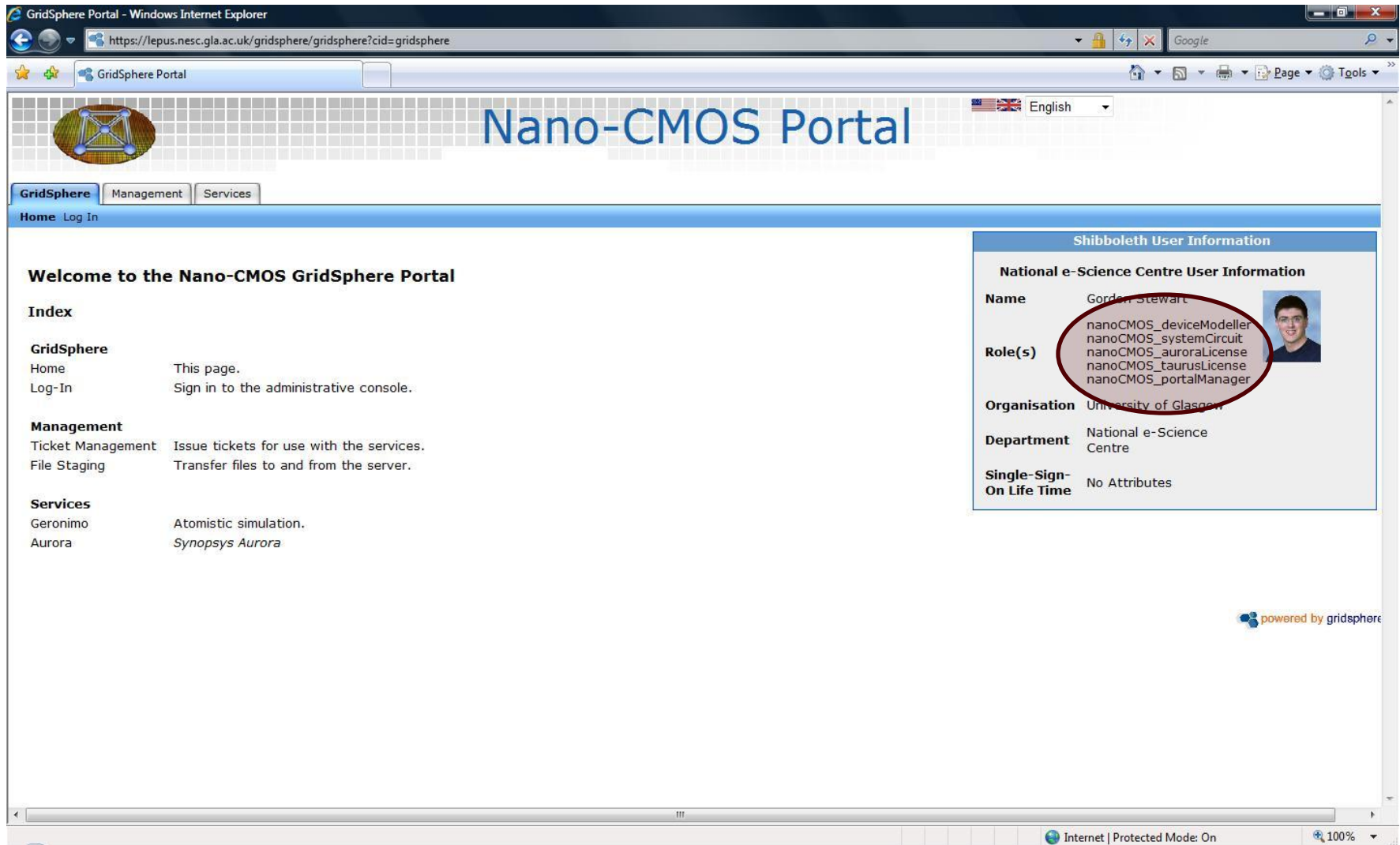


# Secure Portals – Shibboleth





# Secure Portals – Shibboleth



The screenshot shows a web browser window titled "GridSphere Portal - Windows Internet Explorer" with the URL <https://lepus.nesc.gla.ac.uk/gridsphere/gridsphere?cid=gridsphere>. The page features a "Nano-CMOS Portal" header with a logo and a language dropdown set to "English". Below the header are navigation tabs for "GridSphere", "Management", and "Services". A "Home Log In" bar is present. The main content area is titled "Welcome to the Nano-CMOS GridSphere Portal" and includes an "Index" section with links for "GridSphere", "Management", and "Services". On the right, a "Shibboleth User Information" panel displays user details for Gordon Stewart, with a red circle highlighting the "Role(s)" field. The roles listed are nanoCMOS\_deviceModeller, nanoCMOS\_systemCircuit, nanoCMOS\_auroraLicense, nanoCMOS\_taurusLicense, and nanoCMOS\_portalManager. The user's organization is the University of Glasgow, and the department is the National e-Science Centre. The page is powered by GridSphere.

Shibboleth User Information	
<b>National e-Science Centre User Information</b>	
<b>Name</b>	Gordon Stewart
<b>Role(s)</b>	nanoCMOS_deviceModeller nanoCMOS_systemCircuit nanoCMOS_auroraLicense nanoCMOS_taurusLicense nanoCMOS_portalManager
<b>Organisation</b>	University of Glasgow
<b>Department</b>	National e-Science Centre
<b>Single-Sign-On Life Time</b>	No Attributes



- Apache Rampart provides message-level security
  - Time-stamping
  - Signing: client and server authentication
  - Encryption
- Configuration policy complies with WS-SecurityPolicy standard



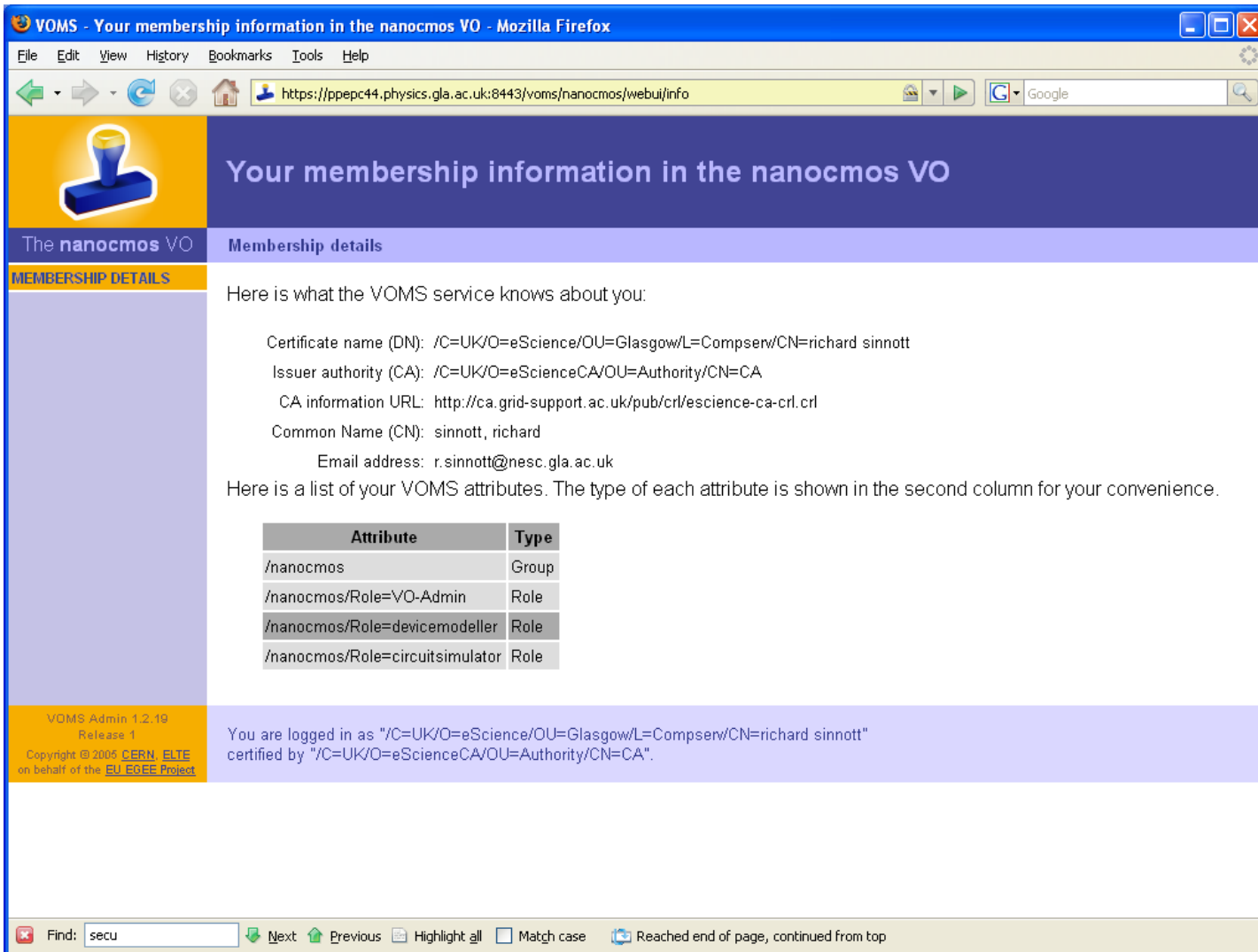
# Service Security

```
<?xml version="1.0" encoding="UTF-8"?>
<wsp:Policy
  xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy"
  xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy"
  xmlns:wssu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
  <wsp:ExactlyOne>
    <wsp:All>
      <sp:AsymmetricBinding>
        <wsp:Policy>
          <sp:InitiatorToken>
            <wsp:Policy>
              <sp:X509Token sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/AlwaysToRecipient">
                <wsp:Policy>
                  <sp:WssX509V3Token10>
                    <wsp:Policy>
                      <sp:X509Token>
                        </wsp:Policy>
                      </sp:InitiatorToken>
                    </wsp:Policy>
                  <sp:RecipientToken>
                    <wsp:Policy>
                      <sp:X509Token sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/Never">
                        <wsp:Policy>
                          <sp:WssX509V3Token0>
                            <wsp:Policy>
                              <sp:X509Token>
                                <wsp:Policy>
                                  <sp:AlgorithmSuite>
                                    <wsp:Policy>
                                      <sp:Basic256Sha256>
                                        </wsp:Policy>
                                      </sp:AlgorithmSuite>
                                    </wsp:Policy>
                                  <sp:Layout>
                                    <wsp:Policy>
                                      <sp:Strict>
                                        </wsp:Policy>
                                      </sp:Layout>
                                    </wsp:Policy>
                                  <sp:IncludeTimestamp>
                                    <sp:OnlySign/Embed/headers/AndBody/>
                                    </wsp:Policy>
                                  </sp:AsymmetricBinding>
                                </wsp:Policy>
                              </sp:Wss10>
                            </wsp:Policy>
                          <sp:MustSupportRef/EmbeddedToken>
                            <sp:MustSupportRef/IssuerSerial>
                              </wsp:Policy>
                            </sp:Wss10>
                          </sp:SignedParts>
                        <sp:Body>
                          </sp:SignedParts>
                        <sp:EncryptedParts>
                          <sp:Body>
                            </sp:EncryptedParts>
                          </wsp:Policy>
                        </wsp:Policy>
                      </sp:RampantConfig xmlns:ramp="http://ws.apache.org/rampant/policy">
                        <ramp:user/su/hen.nesc.gla.ac.uk/ramp:user>
                          <ramp:encryptionUser/opus.nesc.gla.ac.uk/ramp:encryptionUser>
                            <ramp:signature/Cyptio>
                              <ramp:crypto provider="org.apache.ws.security.components.crypto.Merlin">
                                <ramp:property name="org.apache.ws.security.crypto.merlin.keystore.type">JKS</ramp:property>
                                <ramp:property name="org.apache.ws.security.crypto.merlin.file">{path}/keystore</ramp:property>
                                <ramp:property name="org.apache.ws.security.crypto.merlin.keystore.password">PASSWORD</ramp:property>
                              </ramp:crypto>
                              <ramp:signature/Crypto>
                                <ramp:encryption/Cyptio>
                                  <ramp:crypto provider="org.apache.ws.security.components.crypto.Merlin">
                                    <ramp:property name="org.apache.ws.security.crypto.merlin.keystore.type">JKS</ramp:property>
                                    <ramp:property name="org.apache.ws.security.crypto.merlin.file">{path}/keystore</ramp:property>
                                    <ramp:property name="org.apache.ws.security.crypto.merlin.keystore.password">PASSWORD</ramp:property>
                                  </ramp:crypto>
                                </ramp:encryption/Cyptio>
                              </ramp:RampantConfig>
                            </wsp:All>
                          </wsp:ExactlyOne>
                        </wsp:Policy>
                      </wsp:Policy>
                    </wsp:Policy>
                  </wsp:Policy>
                </wsp:Policy>
              </wsp:Policy>
            </wsp:Policy>
          </wsp:Policy>
        </wsp:Policy>
      </sp:AsymmetricBinding>
    </wsp:ExactlyOne>
  </wsp:Policy>
</wsp:Policy>
```

Security policies can be rather complicated!

- Different resources protected by different security technologies
  - GSI (Grid Security Infrastructure)
  - LCAS (Local Centre Authorization Service)
  - LCMAPS (Local Credential MAPping Service)
  - VOMS (Virtual Organization Membership Service)
- “nanocmos” VO exists on ScotGrid

# Securing Resources



VOMS - Your membership information in the nanocmos VO - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://ppepc44.physics.gla.ac.uk:8443/voms/nanocmos/webui/info

## Your membership information in the nanocmos VO

The nanocmos VO

### MEMBERSHIP DETAILS

#### Membership details

Here is what the VOMS service knows about you:

Certificate name (DN): /C=UK/O=eScience/OU=Glasgow/L=Compserw/CN=richard sinnott  
Issuer authority (CA): /C=UK/O=eScienceCA/OU=Authority/CN=CA  
CA information URL: http://ca.grid-support.ac.uk/pub/crl/escience-ca-crl.crl  
Common Name (CN): sinnott, richard  
Email address: r.sinnott@nesc.gla.ac.uk

Here is a list of your VOMS attributes. The type of each attribute is shown in the second column for your convenience.

Attribute	Type
/nanocmos	Group
/nanocmos/Role=VO-Admin	Role
/nanocmos/Role=devicemodeller	Role
/nanocmos/Role=circuitsimulator	Role

VOMS Admin 1.2.19  
Release 1  
Copyright © 2005 CERN, ELTE  
on behalf of the EU EGEE Project

You are logged in as "/C=UK/O=eScience/OU=Glasgow/L=Compserw/CN=richard sinnott"  
certified by "/C=UK/O=eScienceCA/OU=Authority/CN=CA".

Find: secu    Next    Previous    Highlight all    Match case    Reached end of page, continued from top



- Andrew File System
  - Distributed file system
  - Client-server architecture
  - Authentication based on Kerberos
  - Stable(-ish)
  - Clients available for many platforms
  - Connection can be encrypted

- Distribution of files across multiple volumes and file servers transparent to end-users
  - Locate read-write volumes close to resources
  - Provide multiple read-only copies of archive volumes to improve performance
  - Duplicate and relocate volumes easily for back-up and maintenance purposes





## Cell

(nesc.gla.ac.uk)

File Server 1

File  
Server 2

Volume 1

Volume 2

Volume 3

Directory  
A

Directory  
B

Directory  
C

Directory  
D



University  
of Glasgow



UNIVERSITY OF  
Southampton

MANCHESTER  
1824

THE UNIVERSITY of York

## Cell

(nesc.gla.ac.uk)

File Server 1

File Server 2

Volume 1

Volume 2

Volume 3

Directory  
A

Directory  
B

Directory  
C

Directory  
D



University  
of Glasgow

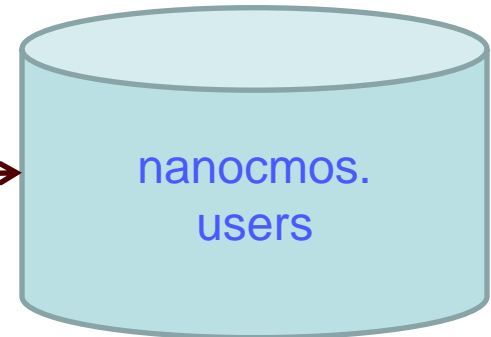
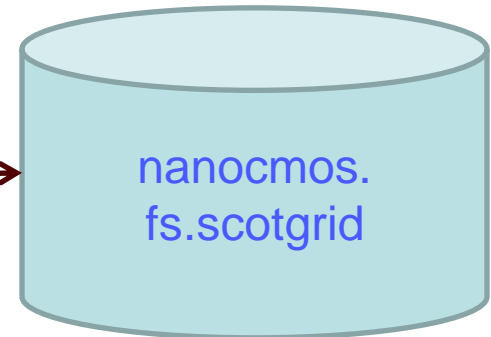
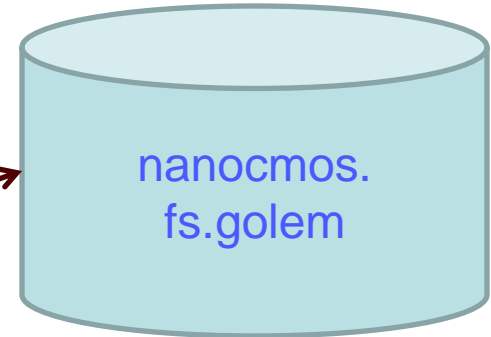
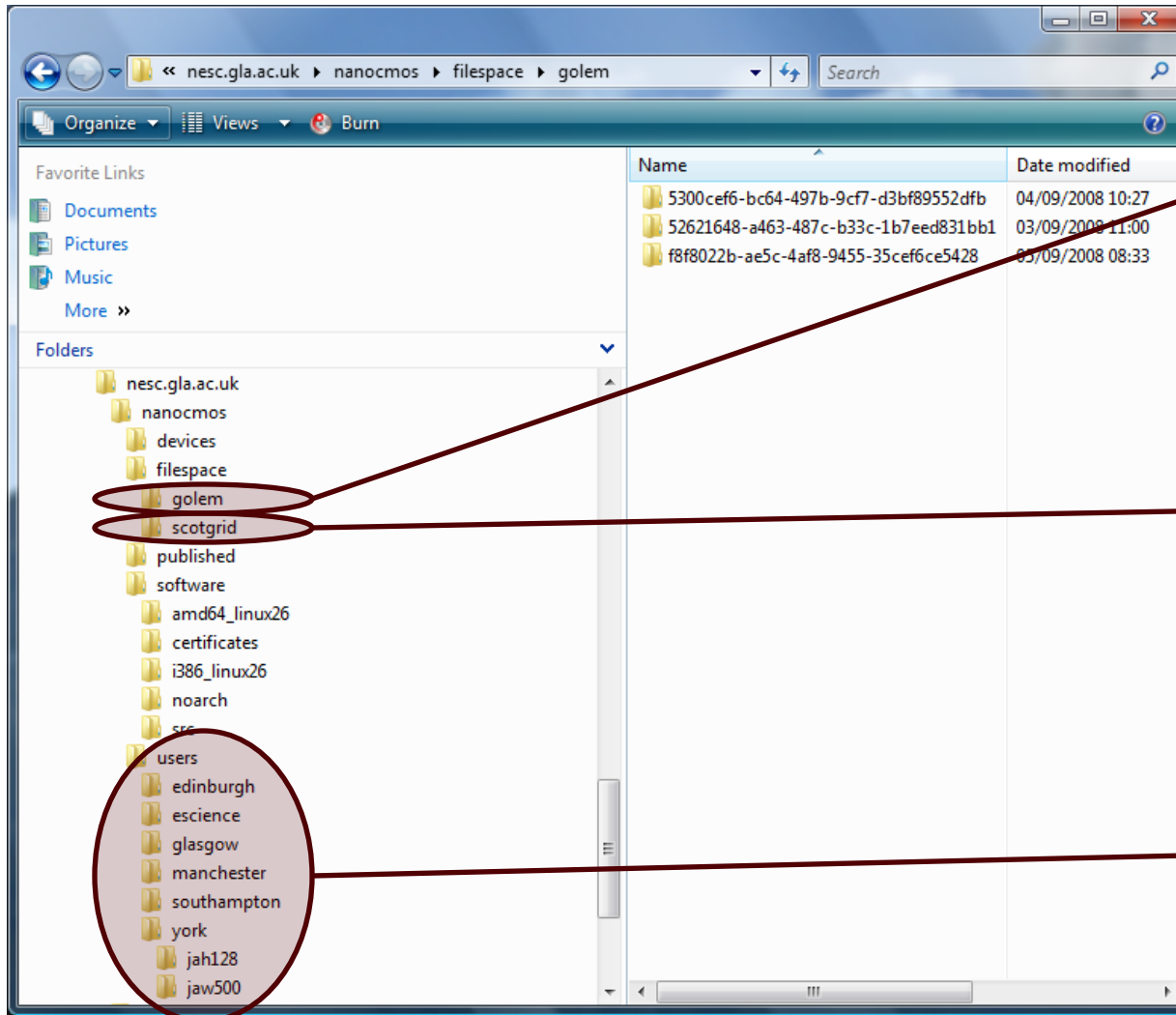


UNIVERSITY OF  
Southampton

MANCHESTER  
1824

THE UNIVERSITY of York

# Managing Files – AFS



- AFS security based on Access Control Lists (ACLs)
  - ACLs are supported at the directory level
  - Users and groups can be added to ACLs
  - Various permissions can be assigned (lida<sup>r</sup>wk)
    - Lookup, Insert, Delete, Administer, Read, Write and Lock
  - Negative permissions also supported



- AFS security built around Kerberos
- Two methods of authentication
  - Traditional Kerberos-based
    - `kinit <user>`
    - `aklog`
  - X.509-based
    - `gssklog`
  - `kinit` involves user-interaction
  - `gssklog` authenticates using an X.509 credential, so is ideal for use on clusters



- Job submission becomes more complicated
  - Job submitted to resource's job manager (e.g. Sun Grid Engine) is AFS wrapper, executing within a PAG
    - PAG (Process Authentication Group) ensures AFS tokens are tied to a process and its children, as opposed to a UID
  - Wrapper obtains X.509 proxy credential from MyProxy server
  - Proxy credential used to obtain AFS token via `gssklog`
  - Wrapper starts application, which now has access to AFS





- Security framework is complex
- To what extent can we integrate the various security technologies?
  - Ensure security provision is sufficient
  - Simplify administration
  - Must tie low-level aspects (e.g. AFS permissions) to high-level security infrastructure
- Turn working prototypes into hardened, “user-proof” software



- Extend work into other areas of electronics design
  - Devices → Circuits → Systems
- Consider other aspects
  - Computational steering
  - Resource brokering: reservation and allocation
  - Scheduling



# Any Questions?

# [www.nanocmos.ac.uk](http://www.nanocmos.ac.uk)



University  
of Glasgow



UNIVERSITY OF  
Southampton

MANCHESTER  
1824

THE UNIVERSITY *of York*