National e-Science Centre

Scalable, Security-Oriented Solutions for Nano-CMOS Electronics

Gordon Stewart

National e-Science Centre

University of Glasgow

Project Overview

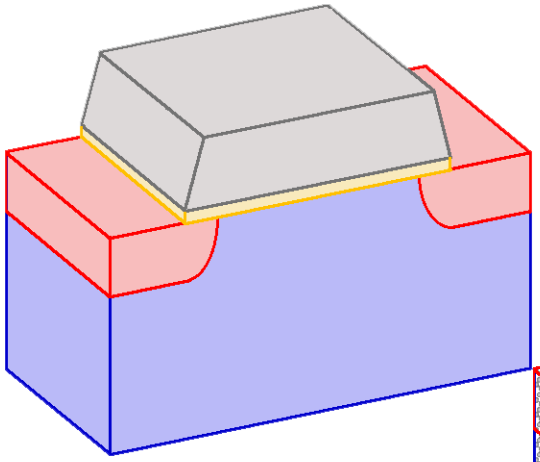
National e-Science Centre

- £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

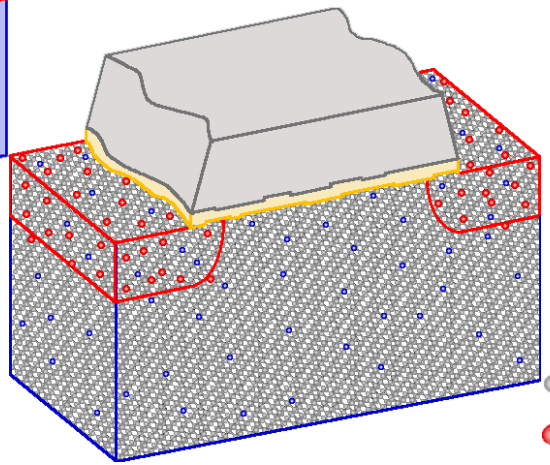
University of Glasgow · The University of Edinburgh · University of Southampton · Manchester 1824 · The University of York

Project Overview

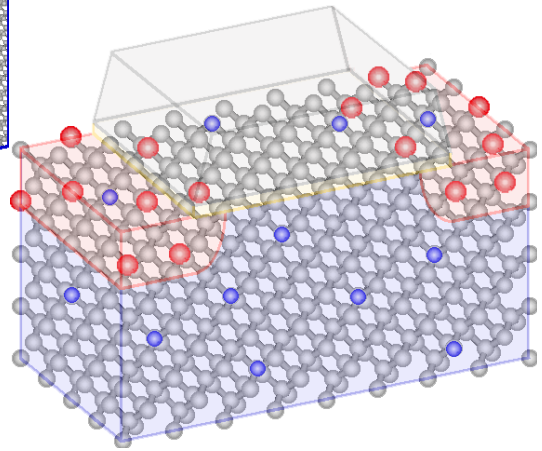
National e-Science Centre



The simulation
Paradigm now



A 22 nm MOSFET
In production 2009



A 4.2 nm MOSFET
In production 2023

University of Glasgow · The University of Edinburgh · University of Southampton · Manchester 1824 · The University of York

Security Overview

National e-Science Centre

- 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

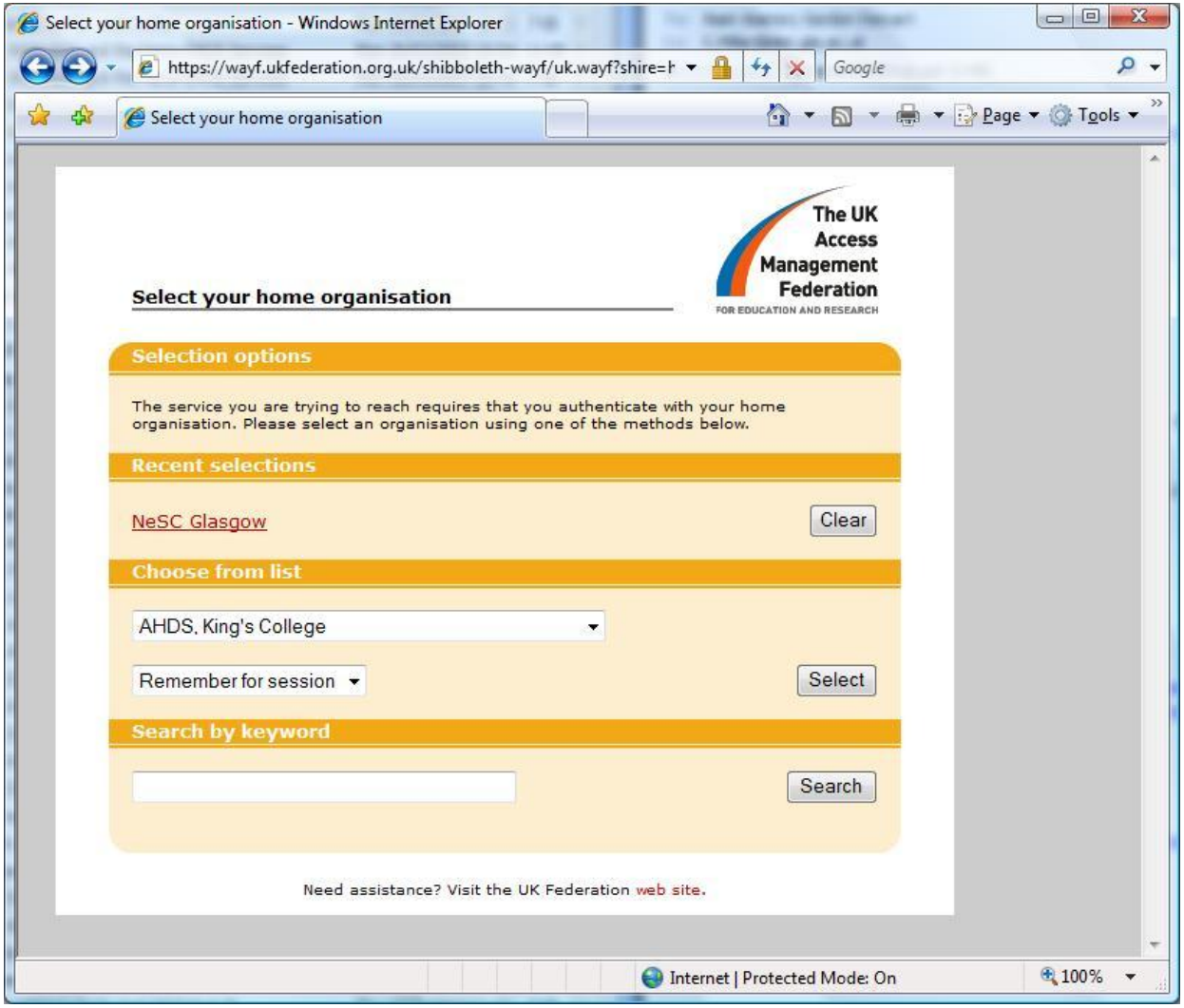
Secure Portals – Shibboleth

National e-Science Centre

- 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

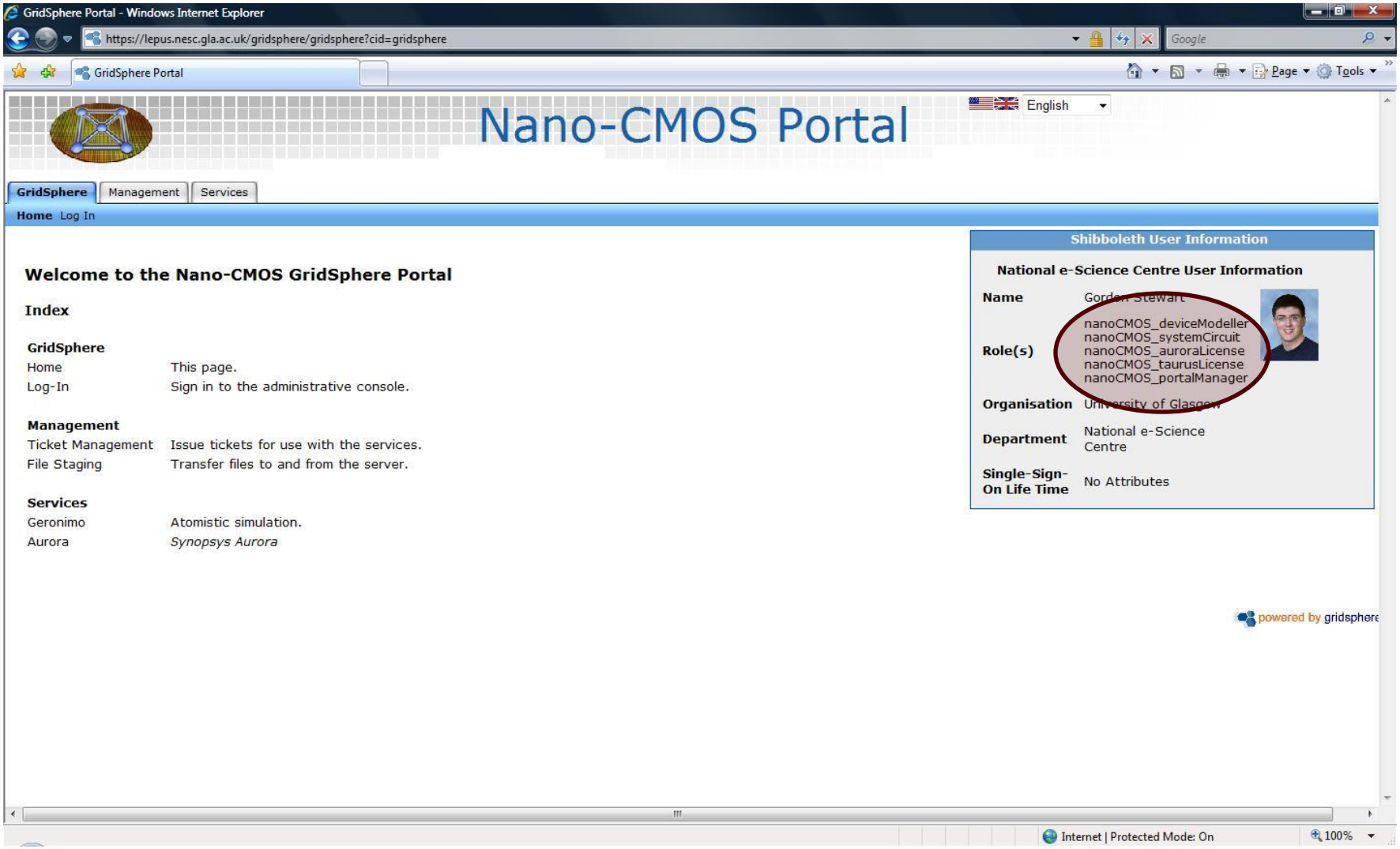
National e-Science Centre



University of Glasgow · The University of Edinburgh · University of Southampton · Manchester 1824 · The University of York

Secure Portals – Shibboleth

National e-Science Centre



University of Glasgow · The University of Edinburgh · University of Southampton · Manchester 1824 · The University of York

Service Security

National e-Science Centre

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

Service Security

National e-Science Centre

```
<?xml version="1.0" encoding="UTF-8"?>
<wsp:Policy
 wsu:Id="SigEncr"
 xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy"
 xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy"
 xmlns:wsu="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>
     <sp:RecipientToken>
      <wsp:Policy>
       <sp:X509Token sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/Never">
        <wsp:Policy>
         <sp:WssX509V3Token10/>
        </wsp:Policy>
       </sp:X509Token>
      </wsp:Policy>
     </sp:RecipientToken>
     <sp:AlgorithmSuite>
      <wsp:Policy>
       <sp:Basic256Sha256/>
      </wsp:Policy>
     </sp:AlgorithmSuite>
     <sp:Layout>
      <wsp:Policy>
       <sp:Strict/>
      </wsp:Policy>
     </sp:Layout>
     <sp:IncludeTimestamp/>
     <sp:OnlySignEntireHeadersAndBody/>
    </wsp:Policy>
   </sp:AsymmetricBinding>
   <sp:Wss10>
    <wsp:Policy>
     <sp:MustSupportRefEmbeddedToken/>
     <sp:MustSupportRefIssuerSerial/>
    </wsp:Policy>
   </sp:Wss10>
   <sp:SignedParts>
    <sp:Body/>
   </sp:SignedParts>
   <sp:EncryptedParts>
    <sp:Body/>
   </sp:EncryptedParts>
   <ramp:RampartConfig xmlns:ramp="http://ws.apache.org/rampart/policy">
    <ramp:user>suilven.nesc.gla.ac.uk</ramp:user>
    <ramp:encryptionUser>lepus.nesc.gla.ac.uk</ramp:encryptionUser>
    <ramp:signatureCrypto>
     <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/to/keystore</ramp:property>
      <ramp:property name="org.apache.ws.security.crypto.merlin.keystore.password">PASSWORD</ramp:property>
     </ramp:crypto>
    </ramp:signatureCrypto>
    <ramp:encryptionCypto>
     <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/to/keystore</ramp:property>
      <ramp:property name="org.apache.ws.security.crypto.merlin.keystore.password">PASSWORD</ramp:property>
     </ramp:crypto>
    </ramp:encryptionCypto>
   </ramp:RampartConfig>
  </wsp:All>
 </wsp:ExactlyOne>
</wsp:Policy>
```

Security policies can be rather complicated!

University of Glasgow · The University of Edinburgh · University of Southampton · Manchester 1824 · The University of York

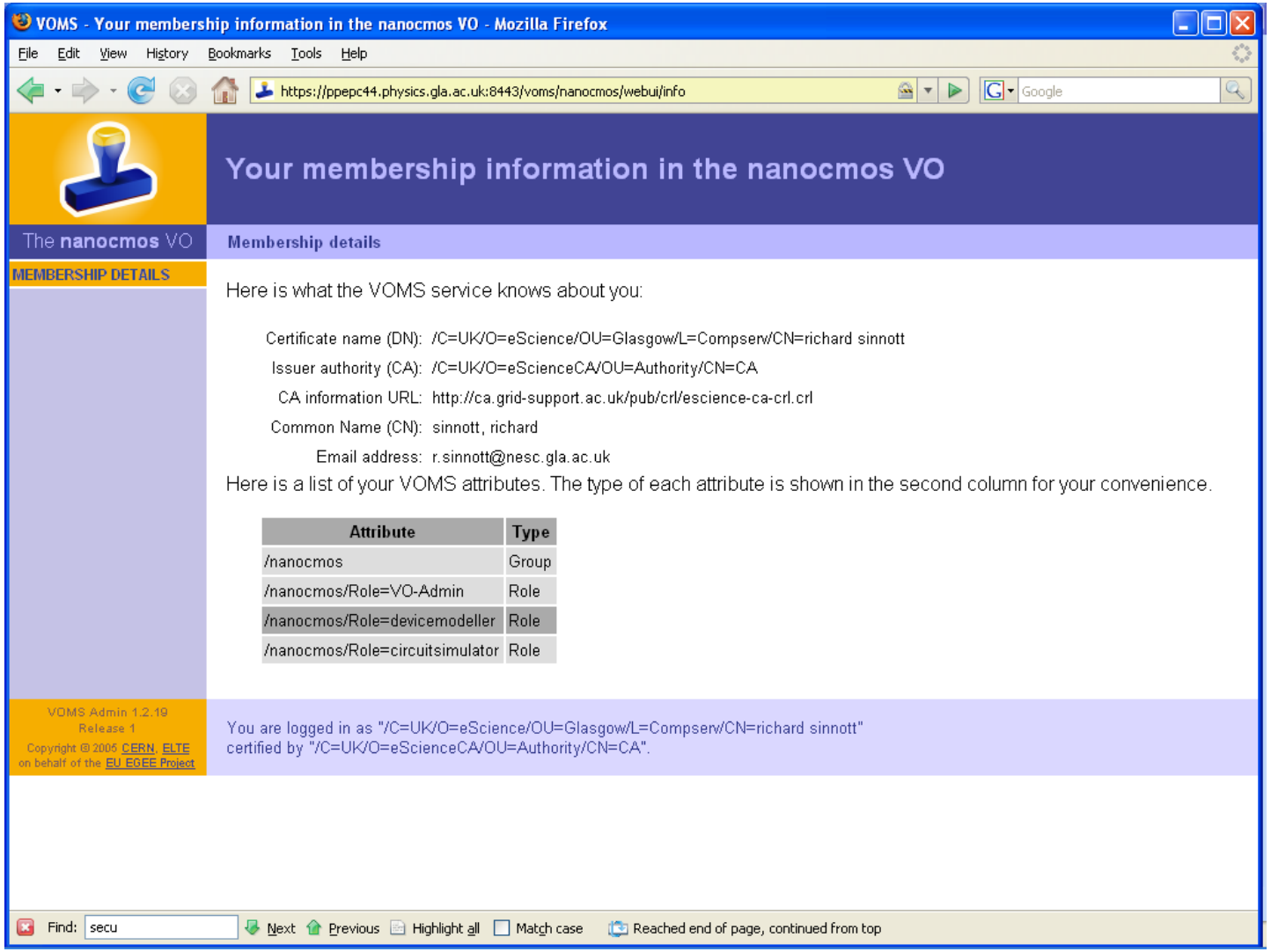
Securing Resources

National e-Science Centre

- 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

National e-Science Centre



University of Glasgow · The University of Edinburgh · University of Southampton · Manchester 1824 · The University of York

Managing Files – AFS

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

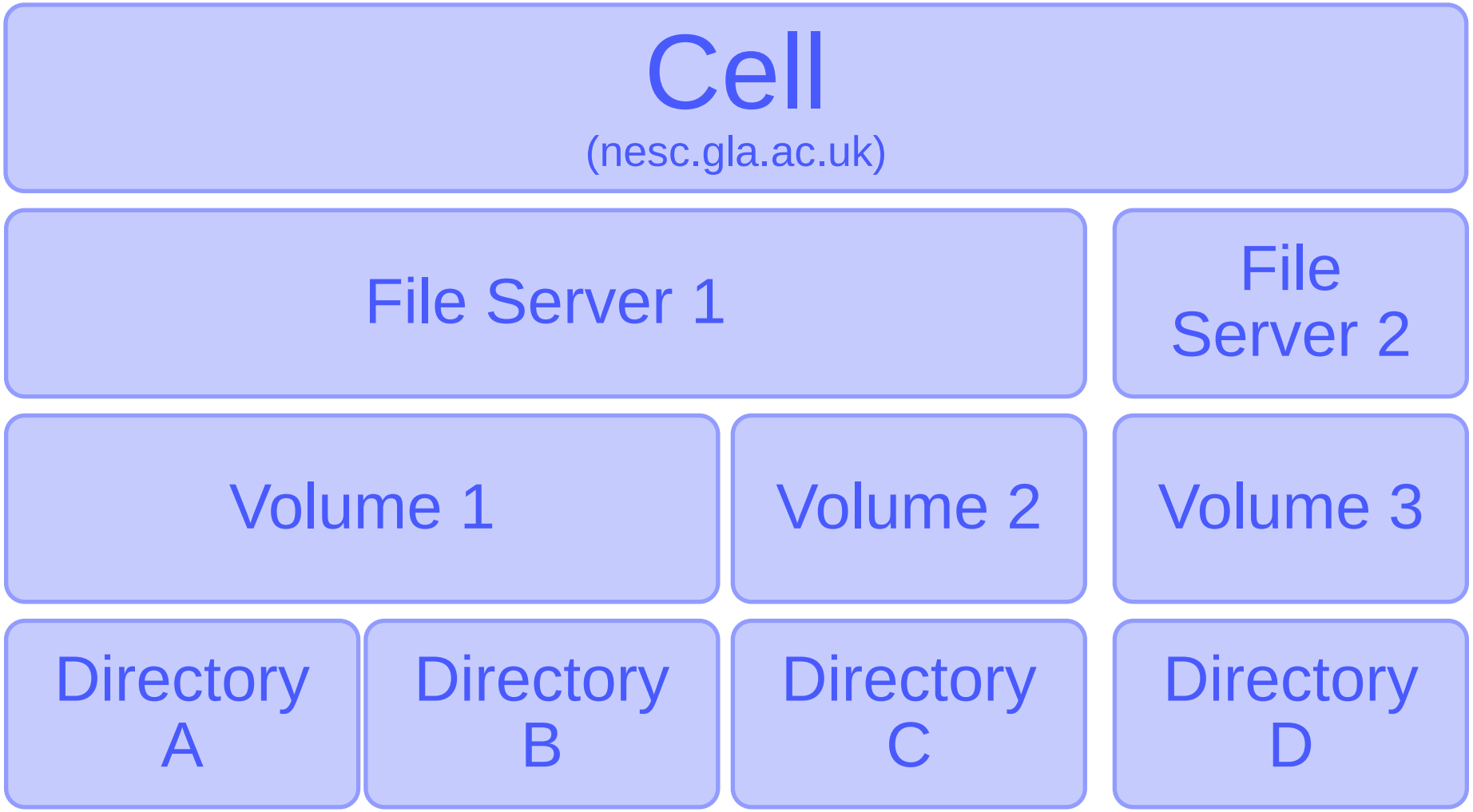
Managing Files – AFS

National e-Science Centre

- 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

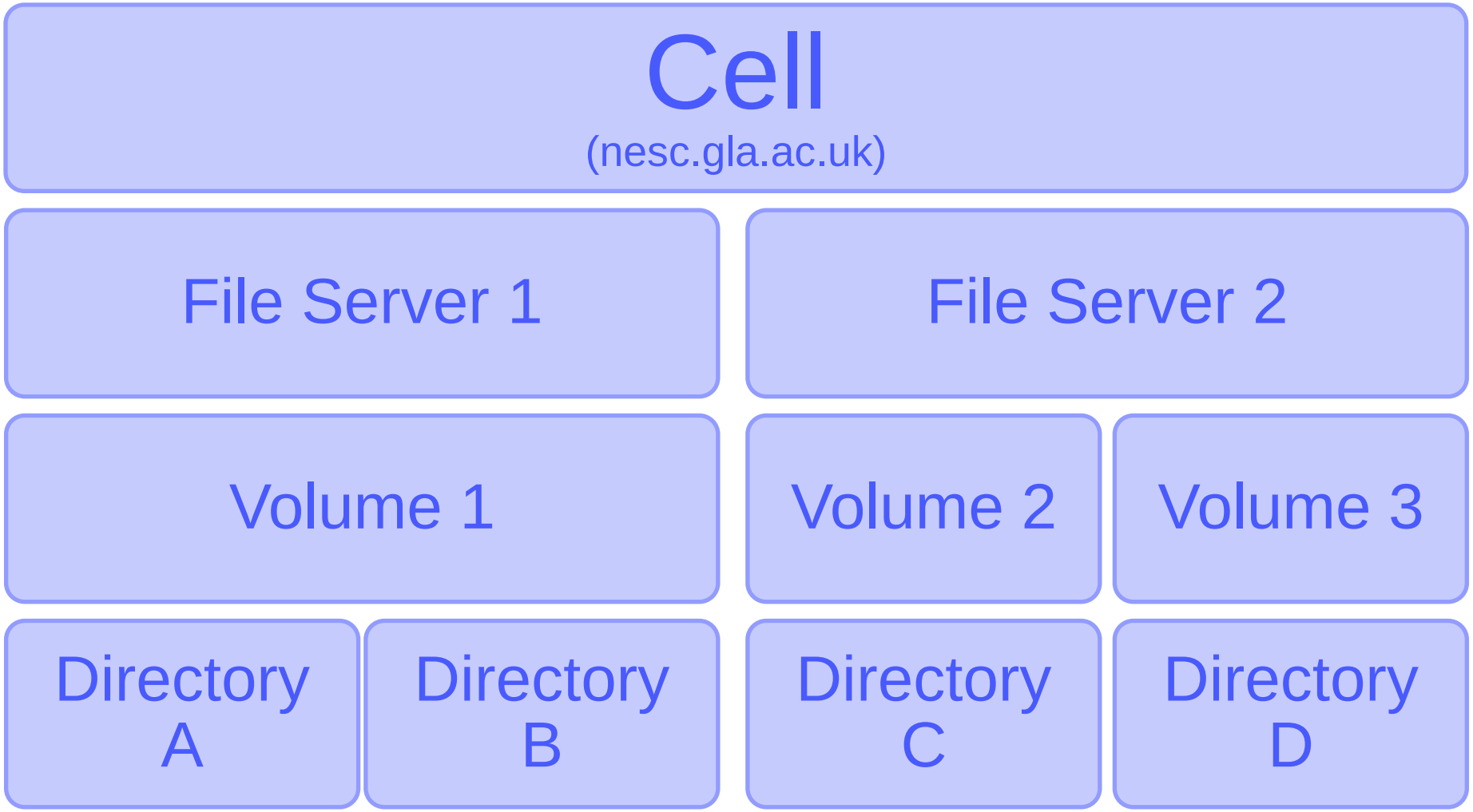
Managing Files – AFS

National e-Science Centre



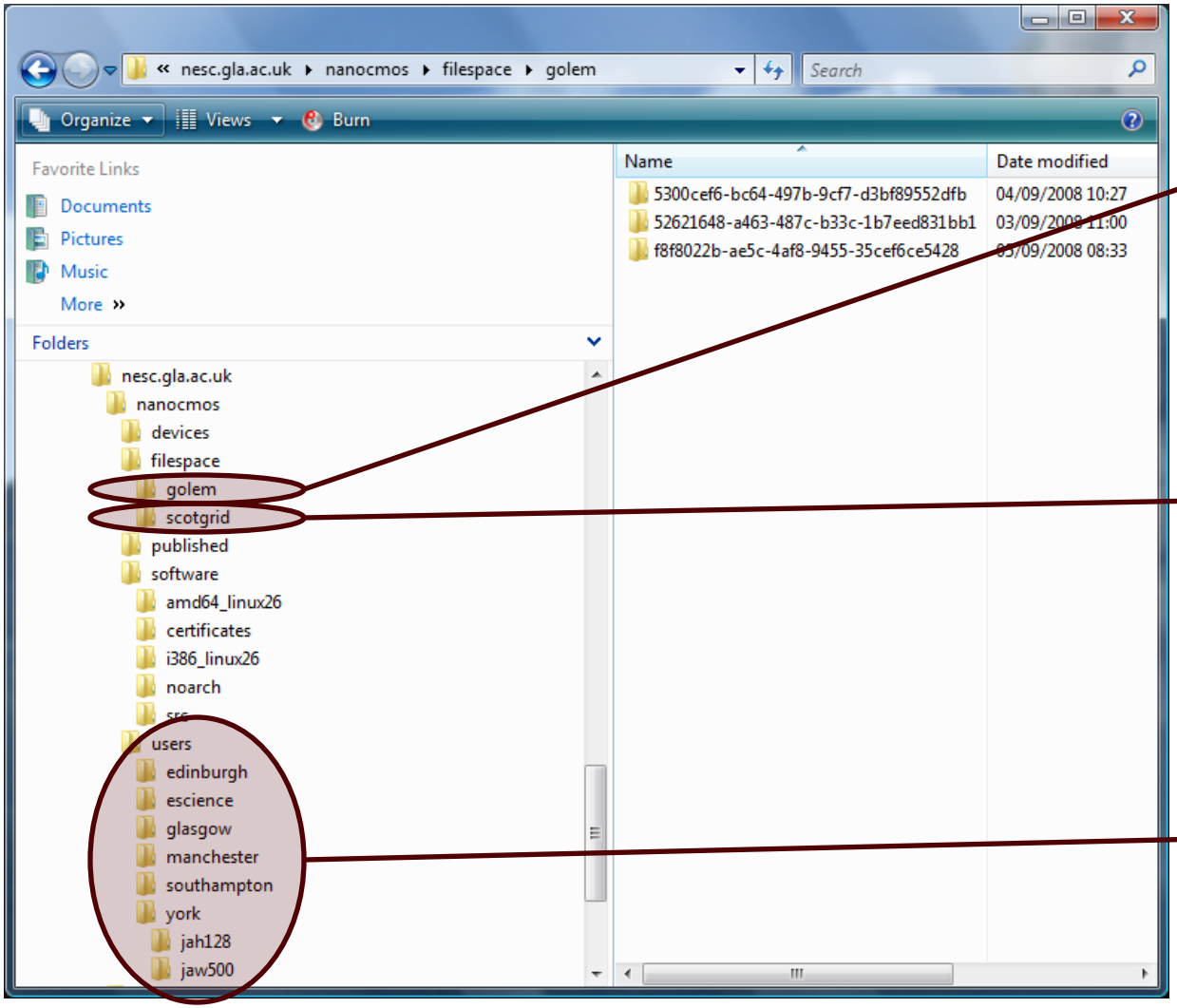
University of Glasgow · The University of Edinburgh · University of Southampton · Manchester 1824 · The University of York

Managing Files – AFS



Managing Files – AFS

National e-Science Centre



nanocmos.
fs.golem

nanocmos.
fs.scotgrid

nanocmos.
users

University of Glasgow
The University of Edinburgh
University of Southampton
Manchester 1824
The University of York

Managing Files – AFS

National e-Science Centre

- 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 (lidarwk)
    - Lookup, Insert, Delete, Administer, Read, Write and Lock
  - Negative permissions also supported

Managing Files – AFS

National e-Science Centre

- 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

Managing Files – AFS

National e-Science Centre

- 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

Challenges

National e-Science Centre

- 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

Next Steps

National e-Science Centre

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

Any Questions?

National e-Science Centre

www.nanocmos.ac.uk

University of Glasgow · The University of Edinburgh · University of Southampton · Manchester 1824 · The University of York