The case for devolved authentication: over-centralised security doesn't work

JISC Core Middleware meeting at NeSC: Developments within Security and Access Management

Mark Norman

20 October 2005

This talk

- The DCOCE and ESP-GRID projects
- What is authentication?
- What is authorisation?
- And Shibboleth…?
- Why do we need to devolve anything?
- Over-centralised PKI vs Shibboleth, a security scenario…
  - Should Shibboleth play a role with the grid?

The DCOCE and ESP-GRID projects

- DCOCE
  - Digital Certificate Operation in a Complex Environment
  - Certificates *shouldn't* be hard to use
    - But they are…
  - Identity management should not be done centrally
    - Clashes a little with the idea of a central Certification Authority (CA)

The DCOCE and ESP-GRID projects

- ESP-GRID
  - Evaluation of Shibboleth and PKI for Grids
  - Shibboleth means devolved authentication
    - PKI-minded grid folks don't really like that
    - You must devolve authentication to stay secure and for the grid to scale!

What is authentication?

- Authentication =
  - The act of verifying that an electronic identity (username, login name etc.) is being employed by the entity, person or process to whom it was issued.
    - Strictly it should mean "establishing the validity of something, such as an identity". This procedure can be very difficult indeed.
- Initial authentication
  - is when you establish your identity with what then becomes your ‘Identity Provider’

What is authorisation?

- Associating rights or capabilities with a subject
- A network *resource* (such as a grid node or file server) needs to decide what the 'subject' can do
  - The decision is taken by the resource
  - Not by someone/something else
  - Sometimes something else may supply some information (attributes) that enables the resource to decide.

What is PKI?

- Public Key Infrastructure
  - Very clever!
  - Behind much internet security
  - Can be employed to give end users digital certificates
- Many users don't like certificates
  - They don't need to be hard to handle, but they are

What's this Shibboleth?

- It *isn't* an authentication or authorisation system
- It is a means (or methodology) whereby this kind of information may be exchanged
  - It allows for (but doesn't mandate) anonymity (or *pseudonymity*) which can be really useful
- It enables *devolved authentication*

Why do we need to devolve anything?

- If you try to manage everyone's identities in a central place, you can't keep them up to date
- If a user is used to their own institution's authentication system, that's good…
- Your own local institution knows whether you have recently turned into a fraudster

Centralised PKI vs Devolved AuthN

- Short-hand:
  - PKI = a high security, but (usually) centralised system relying on difficult-to-forge digital certificates
  - DA = Let each institution use their own system of AuthN and the central 'system' trusts the local ones

    - You are invited to Buckingham Palace for a once in a lifetime high tea with the Queen.
    - You can get a security pass by visiting the Palace itself (beforehand) or from one of 6 regional security centres (~= PKI)
    - Or you can get one from the High Street branch of your bank, as long as… (~= DA)

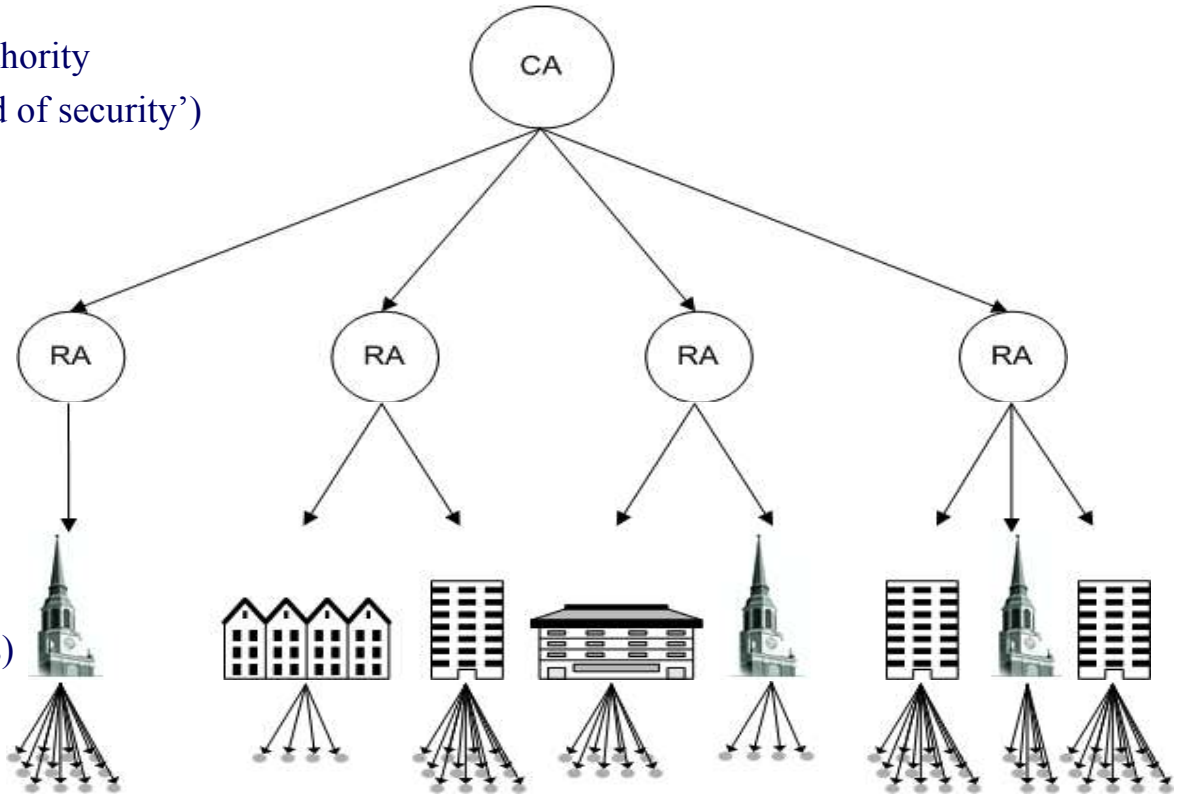
Centralised Security with the UK Grid

Certification Authority
(A national 'head of security')

(Regional)
Registration
Authorities

Organisations
(e.g. Universities)

Personnel
Officers etc.
(people at the end of the chain of trust!)



The parable of Oldman, Newman, Rita and Devla

The cast

- Oldman
  - An old and wise university researcher
- Newman
  - A new and keen researcher
- Rita
  - The e-Science Registration Authority (RitA)
- Devla
  - The departmental personnel officer (Devolved authenticator)
- With thanks to…
  - Alun Edwards, James AJ Wilson, Jackie Hewitt and Wendy Simmonds

A great new resource for researchers

Newman: What's that? It looks great!
Oldman: That's our new e-Science building. It's got lots of cool stuff and any researcher can use it!
Newman: Oooh, I can't wait! I think I'll go there now!
Oldman: Ah, erm… You need a special security pass.
Newman: Eh?

Newman: But I've got my University swipe card!

Oldman: That isn't good enough! You need a *high* security card to get in – like this one. Chip and pin, you know!

Newman: OK, where do I get one of those?

Oldman: Because it's such high security, these babies are issued nationally, via regional centres! As we work at *Cotswolds University*, we don't have a centre here – you need to go to Oxford e-Science Centre.

Newman: Blinking heck! I'm only an ordinary biologist. Maybe I don't need to use the building after all…

Oldman: No really – it's fantastic in there. Free coffee too!

Newman: Oh… alright then.

Rita: Welcome to Oxford e-Science Centre. My name is Rita and I'm your Registration Authority!

Newman: Hello Rita. It's taken me hours to get here. Traffic was awful!

Rita : Sorry to hear about that. Ah, I see you're from Cotswolds University. Your University Card looks fine to me and that is certainly your picture on it. I shall authorise a gold pass for you right away.

Newman: Great. Thanks!

Rita : Of course, I'm kind of trusting Cotswolds University that they checked you out before giving you this card!

Newman: Hmm. I see. Devla, our departmental personnel assistant issued me my Cotswolds Card. If you rely on that, why couldn't Devla issue the gold card too?

Rita : Well, it's very high security, you see. Devla won't have been on a training course.

Newman: That seems a bit illogical to me as you're already trusting Devla to have done her job properly.
But hey, I'm only a biologist: I don't really understand this security stuff like you IT people.

Rita : Hmm…
Yes, that must be it.
Anyway, have a good journey back. Hope the traffic is better.

Newman: Thanks. Bye!

High security?

- People equate high security with ‘difficult’
  - And correlate HS with difficulty to obtain
    - (This is about as wrong as you can get!)
- Shibboleth allows the right people to manage your on-line identity
  - The people who know you
  - Your identity is managed in one place and is managed accurately
- It’s no use trusting the highly-trained Rita to carry out things she isn’t really able to do

And sometimes, bad things happen…

Caught on CCTV…

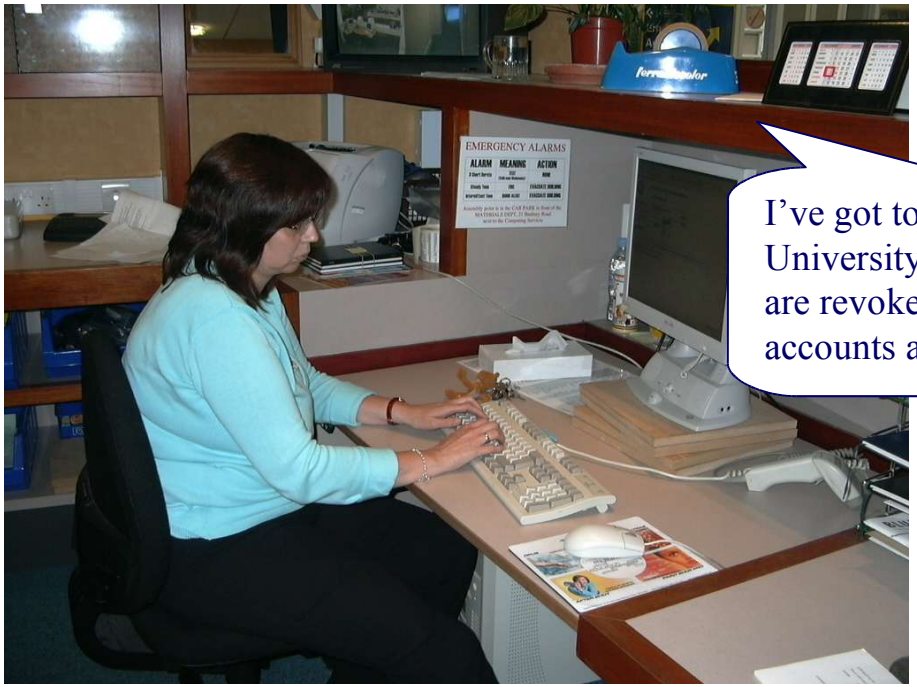
Oldman: I can't believe it – it looks like Newman!

Devla: This is terrible. We've never had a thief in this department before!

Devla: I need your building keys, your University Card, your department swipe card…
I can't even look at you, I'm so ashamed!

Oldman: And never darken our door again…

The conscientious Devla finishes the job…



But meanwhile, back in the Oxford e-Science Centre, things are more pleasant for Rita…

Ha ha! They took everything away from me, apart from the highest security pass I had!

And it might be a year before anyone checks Newman's security credentials!

To centralise or to devolve?

- Devolved authentication should be more secure
  - As long as Devla is trustworthy
  - But when it comes down to it, we were going to have to trust Devla, anyway!
- More information at:
  - http://wiki.oucs.ox.ac.uk/esp-grid/ShibEvaluation
- Send your angry emails to
  - mark.norman@oucs.ox.ac.uk !!