



National  
Computing  
Centre

Helping your business grow  
through knowledge

# PKI for Aspiring Dummies

<http://www.ncc.co.uk>

**Danny Dresner**  
**daniel.dresner@ncc.co.uk**





Helping your business grow  
through knowledge

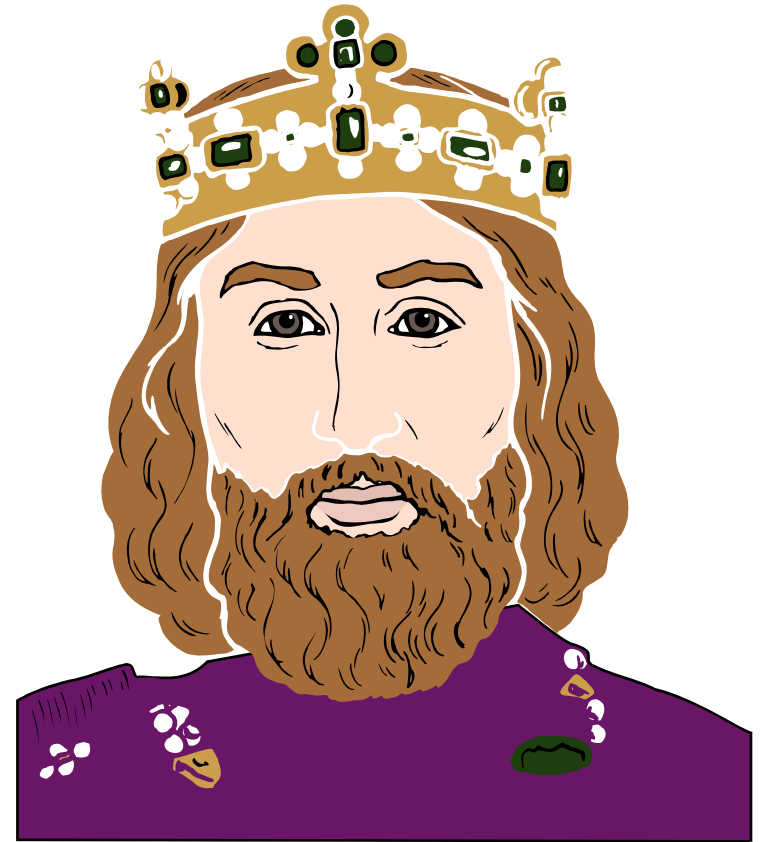
# Objectives

- A well rounded view of conducting secure transactions over the Internet
- E-commerce:
  - ‘Electronic commerce is the exchange of information across electronic networks, at any stage in the supply chain, whether within an organisation, between businesses, between businesses and consumers, or between the public and private sectors, whether paid or unpaid.’ (e-commerce@its.best.uk)



# The Story of King's Diner

- Shows potential
- Dispels myths
- Warns of dangers
- Looks familiar?
- Could be orders
- Could be payment
- Could be plans, drawings, specifications . . .
- Could be legal briefs



Helping your business grow  
through knowledge

NCC

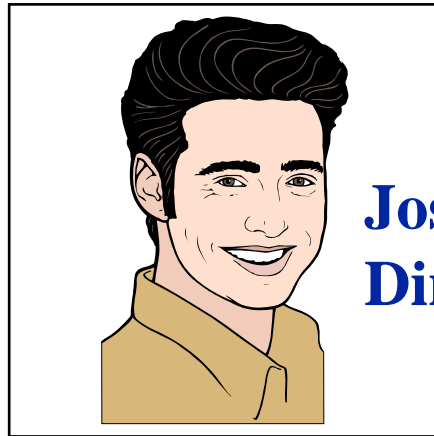
National  
Computing  
Centre

[www.ncc.co.uk](http://www.ncc.co.uk)

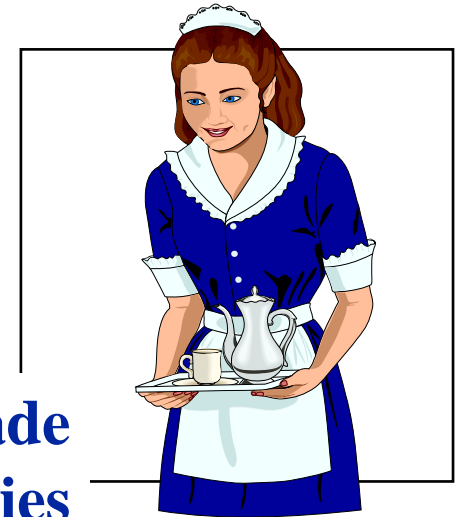


Helping your business grow  
through knowledge

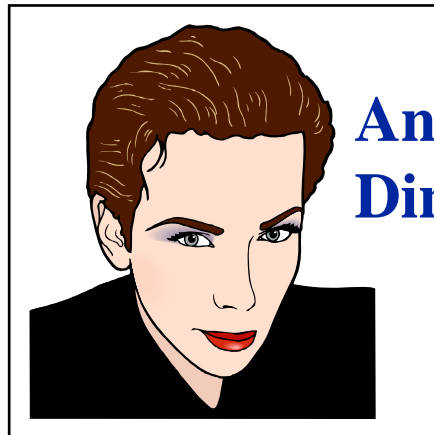
# The Players



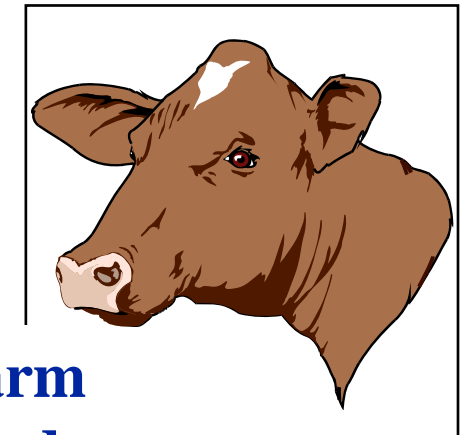
**Joseph King**  
**Diner Owner**



**Dairy Made**  
**Catering Supplies**



**Anne Kean**  
**Diner Manageress**



**Alderney Farm**  
**Fresh Foods**





Helping your business grow through knowledge

# The Supply Chain

**Business  
to  
Business**

**Manufacturers**

**Wholesale suppliers**

**Retailers**

**Consumers**



**Alderney Farm Fresh Foods**

**Dairy Made Catering Supplies**

**King's Diners Inc.**

**Hungry people**





Helping your business grow  
through knowledge

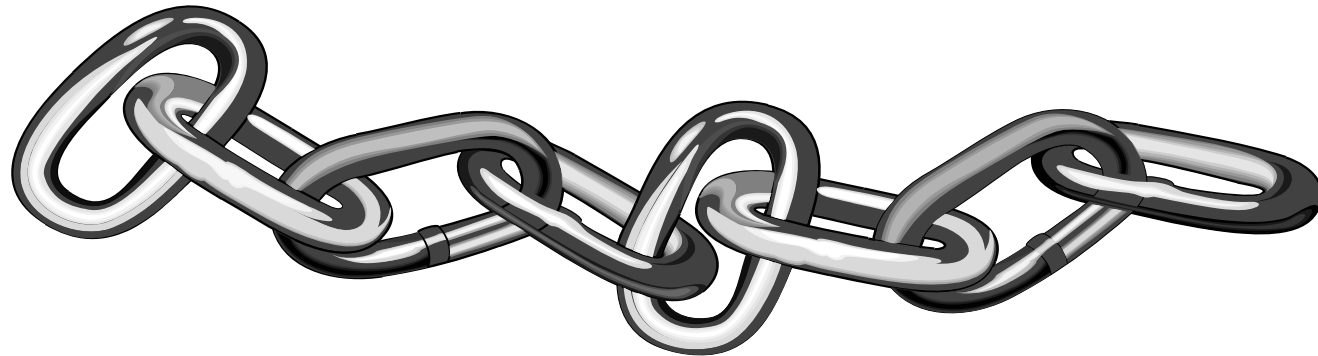
# The Story . . .

- Joseph King asked Miss Kean
- Miss Kean ordered from Dairy Made
- Dairy Made ordered from Alderney Farm Fresh Foods
- Alderney Farm Fresh Foods delivered to King's Diners
- Mr King wanted butter but got marmalade
- Why?



# Organisational Issues

- Who made the order?
- Who received the order?
- Who despatched the order?



- Goods and information – the problems are the same . . .



Helping your business grow  
through knowledge





Helping your business grow through knowledge

# Behind the Scenes



**Joseph King**  
Diner Owner

Orders  
breakfast →



**Anne Kean**  
Diner Manageress

Orders  
butter ↓



**Alderney Farm**  
Fresh Foods

← Forwards  
order

**Dairy Made**  
Catering Supplies



Delivers  
order ↘

**Jo's Diner**

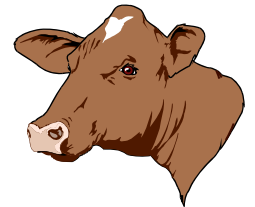




Helping your business grow  
through knowledge

# Down at the Farm

- Message received by the wrong person
- Message thought to be from someone else
- Wrong action taken with good intentions
- Not to mention lost potential
  - Crude method of creating purchase orders
  - Receipts, invoices etc. not considered





Helping your business grow  
through knowledge

# Potential

- Potential to reduce and streamline paperwork lost
- Relationships built through common processes
- Can create the framework for additional process improvement
  - Improved delivery
  - Can speed up payment





Helping your business grow  
through knowledge

## But . . .

- . . .with all that information, how can you safeguard reliability and security





Helping your business grow  
through knowledge

## So . . .

- Know with whom you deal
- Agree the information you both require
- Standardise the processes with all your suppliers
- Protect the information from tampering





# Managing Risk

Organisation 'Infrastructure' + Defined Responsibilities + Procedures + Technology = **Managed Risk**

## Management System





Helping your business grow  
through knowledge

## How about . . .

- Making sure that orders can only be sent by certain individuals
- Being sure that the individual making the order is who they claim to be
- Allowing a wider group of people to follow the progress of an order
- Being sure that a confidential message can only be read by the recipient



# Too good to be true?

- ‘If it’s easy, you’re not doing it right.’
- Why not . . . ?
- Installed by experts
- Smartcard and password/PIN
- Some extra processing time
- Can be learnt in minutes



Helping your business grow  
through knowledge

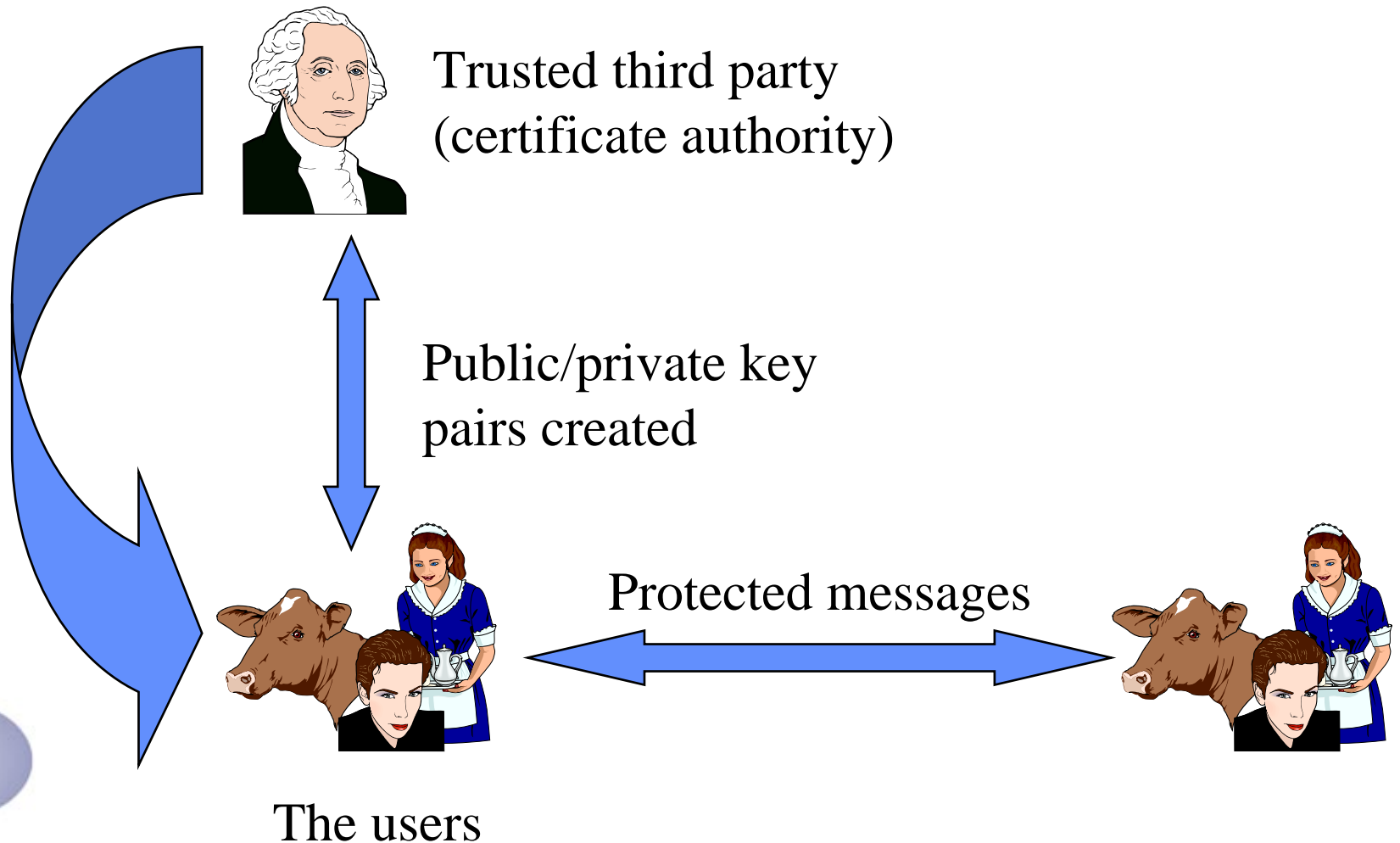




Helping your business grow through knowledge

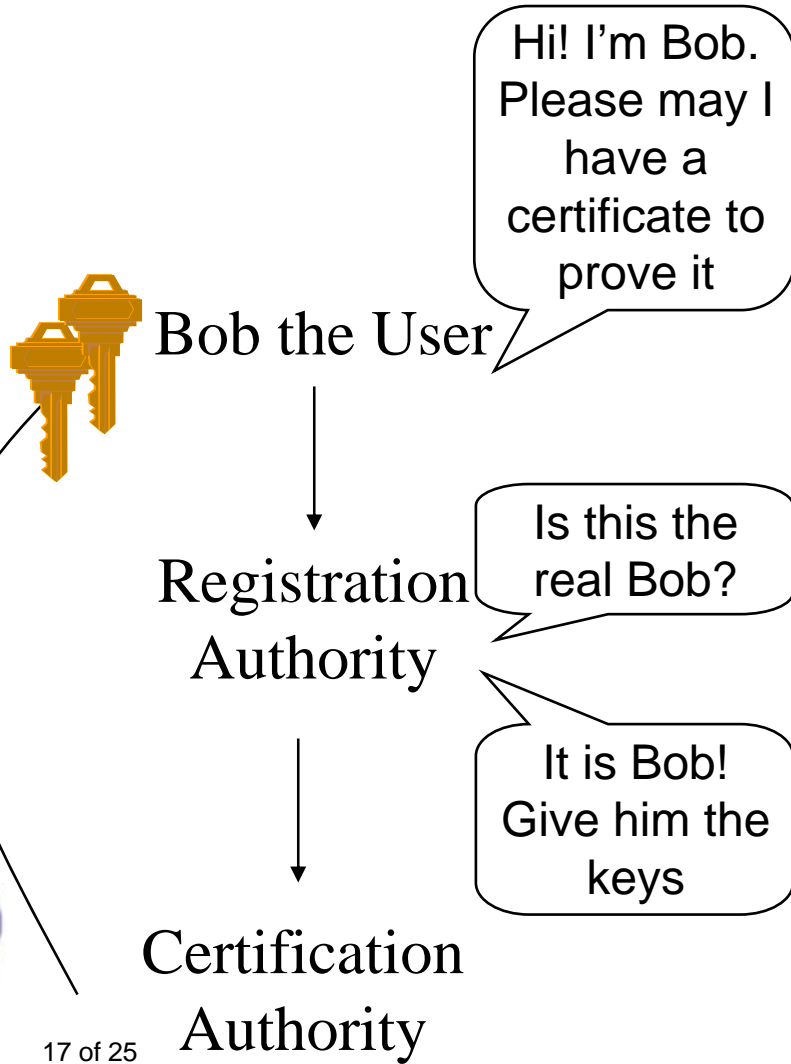


# As simple as possible . . .





Helping your business grow through knowledge





Helping your business grow through knowledge



Private Key  
Bob the User



Registration Authority



Certification Authority

Public Key



Directory

Public Key Public Key Public Key Public Key



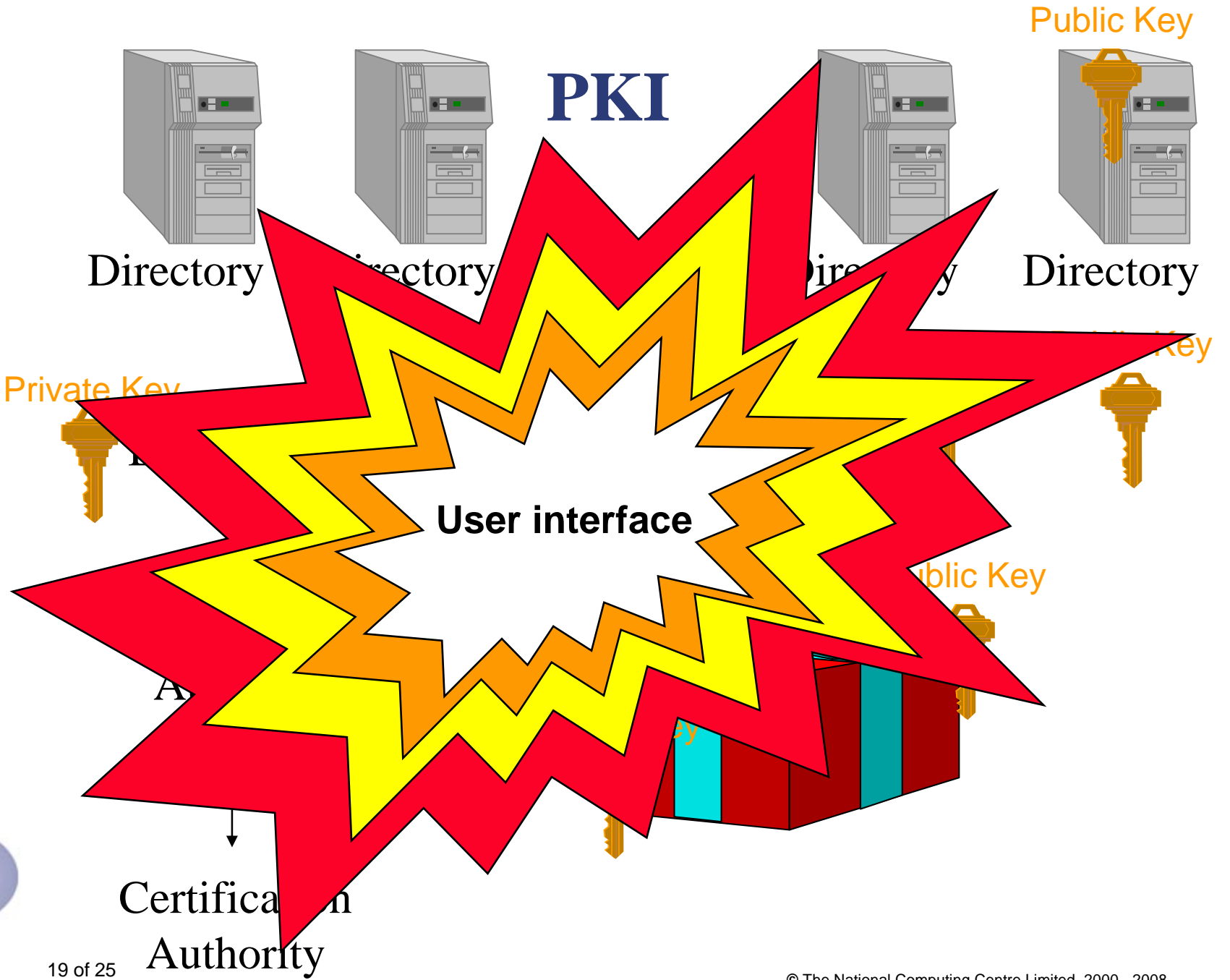
Public Key

Private Key





Helping your business grow through knowledge





Helping your business grow through knowledge

# Standards

- An interest in doing something about 'risk'?
- Risk treatment
  - ISO/IEC 17799 (now ISO/IEC 27002)
  - Cataloguing
  - Gap analysis



**Review of Publicly Available Information Assurance Guidance**

Publication Number	CSIA 001
Document Number	Information Assurance Guidance
Issue	1
Date	11 January 2007
Author	John Grogan
Technical Approval	See CSIA 001
Final Approval	Debbie Judd NCC

**8. People Treatments**

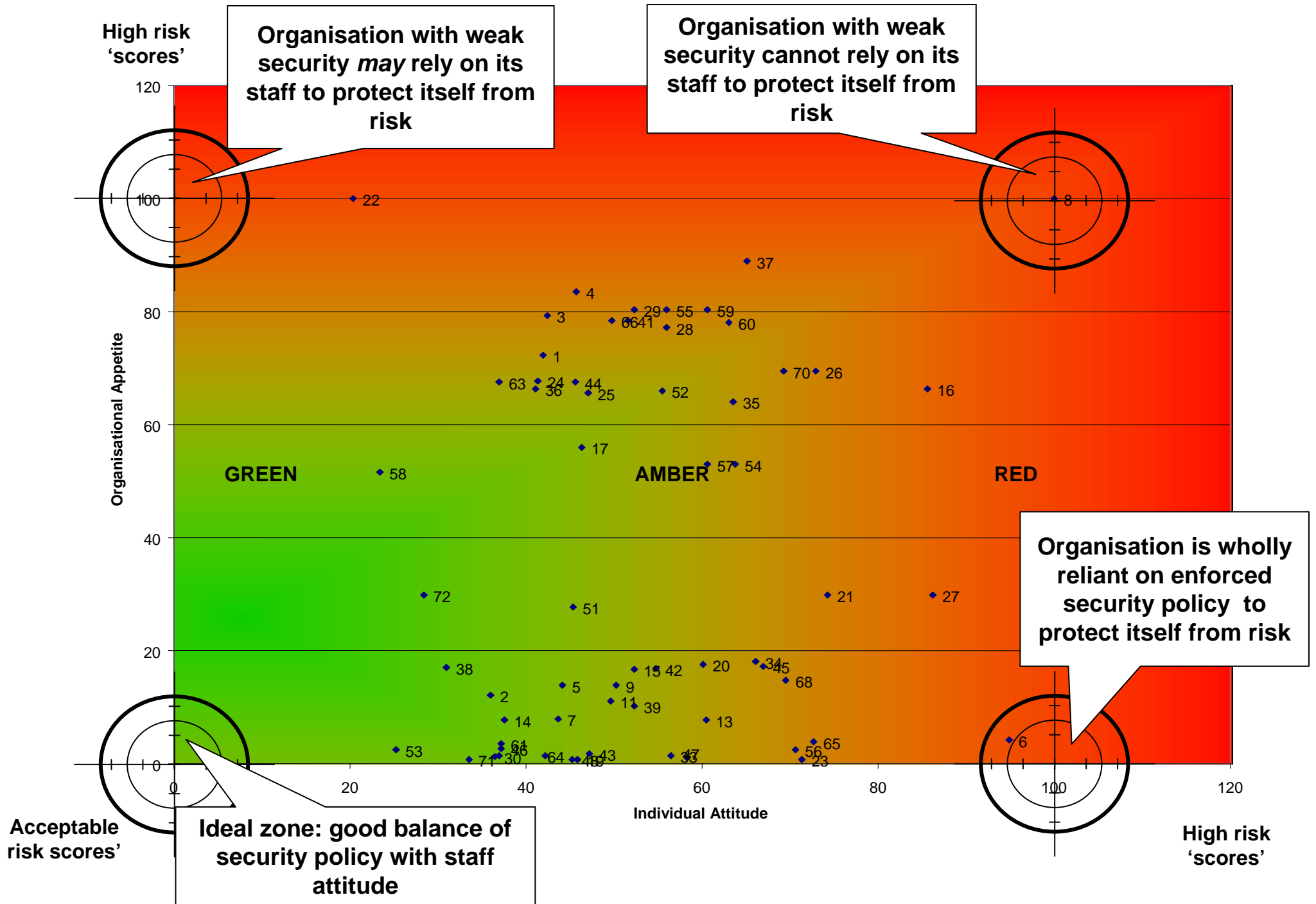
Table 3: Risk Treatments Supporting ISO/IEC 17799 clause 6 Security policy

Reference	Standard	Relevant Clauses	Sub-clause
E.3.3 Information security policy documents	BS ISO/IEC 27002	6.1.1.1	6.1.1.1
		6.1.1.2	6.1.1.2
		6.1.1.3	6.1.1.3
		6.1.1.4	6.1.1.4
		6.1.1.5	6.1.1.5
		6.1.1.6	6.1.1.6
		6.1.1.7	6.1.1.7

Table 4: Risk Treatments Supporting ISO/IEC 17799 clause 8 Operations of information security

Reference	Standard	Relevant Clauses	Sub-clause
E.3.3 Information security policy documents	BS ISO/IEC 27002	8.1.1	8.1.1
		8.1.2	8.1.2
		8.1.3	8.1.3







## On the menu?

- **Passing off**
- **Flood**
- **Cyber-squatters**
- **Spoofs**
- **Firewall attacks**
- **Infiltration**
- **E-mail/spam**
- **Weather**
- **Identify theft**
- **Fire**
- **Theft**
- **Denial of service**
- **Sabotage/terrorism**
- **Industrial disputes**
- **Password interception**
- **Reputational slur**
- **Human error**
- **Usability issues**
- **Regulation**
- **Response times**
- **Fraud**
- **Transport reliability**
- **Regime change**
- **Malicious code attacks**





Helping your business grow through knowledge



# IT WEEKNEWS

25 Feb '08

## Whitehall laptops vanish

ROSALIE MARSHALL

The need for data security improvements was again highlighted last week, after it was revealed that 234 laptops have gone missing from government departments since 2001, along with more than 200 other hand-held devices including mobile phones and PDAs.

The figures were released in response to a request from a Liberal Democrat MP.

Morse consultant Simon Forster advised public sector departments to put processes in place

to ensure this scale of loss does not occur again. "When a disc, document or anything else containing data comes into an organisation it needs to be logged and then properly managed," he added.

The Ministry of Justice (MoJ) emerged as the worst culprit, with 135 laptops stolen and 34 lost, while 56 mobile phones were stolen and a further 116 went missing.

To aid firms concerned about data breaches, security company Virtuuity last week announced new software that remotely destroys information contained on a lost laptop. Backstopp uses wireless communications to identify if a laptop is moved out of its authorised areas, and automatically destroys the data if this occurs.

Also last week, Credant Technologies launched Full Data Encryption2, which limits data access for each individual in an organisation to their own set of information.

→ [End this Whitehall data farce, Leader, p6](#)

### Devices going Awol since 2001



(\*The last figure is for missing devices since 2002, when the department was created with its original name of Office of the Deputy Prime Minister)



Helping your business grow through knowledge

# Oops!



Researchers: Disk Encryption Not Secure | Threat Level from Wired.com - Microsoft Internet Explorer provi...

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Recycle Bin Mail Print TV RSS Feeds

Address <http://blog.wired.com/27bstroke6/2008/02/researchers-dis.html> Go Links >>

Google G Go 0 blocked Check Settings

**WIRED** BLOG NETWORK **D-Link** **media lounge**™ Entertainment Network

**THREAT LEVEL** PRIVACY, SECURITY, POLITICS AND CRIME ONLINE

HOME | SUBSCRIBE >> | SECTIONS >> | BLOGS >> | READ MAGAZINE

« [Hans Reiser's Father Warns of 'Techno-Geek S&M Crowd'](#) -- UPDATE II | [Main](#) | [Story on McCain's Relationship with Telecom Lobbyist Sets Bloggers Abuzz](#) »

## Researchers: Disk Encryption Not Secure

By [Kim Zetter](#) February 21, 2008 | 12:13:48 PM Categories: [Glitches And Bugs](#)

Researchers with Princeton University and the Electronic Frontier Foundation have found a flaw that renders disk encryption systems useless if an intruder has physical access to your computer -- say in the case of a stolen laptop or when a computer is left unattended on a desktop in sleep mode or while displaying a password prompt screen.

The attack takes only a few minutes to conduct and uses the disk encryption key that's stored in the computer's RAM.

The attack works because content as well as encryption keys stored in RAM linger in the system, even after the machine is powered off, enabling an attacker to use the key to collect any content still in RAM after reapplying power to the machine.

