

# Chapter 2

## How to avoid making a pig's ear out of a king's breakfast . . .

---


**Daniel Dresner**  
**Head of Research Programmes**  
**The National Computing Centre**  
**daniel.dresner@ncc.co.uk**

### 2.1 Introduction

This chapter contains a fictitious case study of how Internet communications were made with the best intentions and disastrous results. The chapter:

- Takes us through the story
- Describes what went wrong
- Suggests what could have been done to improve things
- Explains a generic technical solution

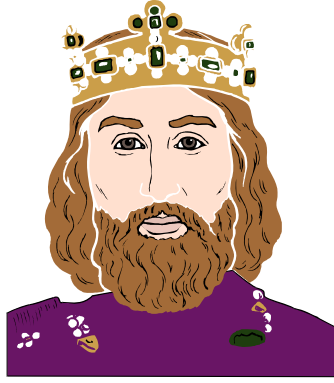
## 2.2 The story



Helping your business grow through knowledge

### 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



© The National Computing Centre Limited, 2000

### CAUTION

**Please note that any resemblance to any person living or dead, any organisation in business, liquidation, bankruptcy or chapter 11 is wholly coincidental.**

This is the story of King's Diners Inc. and how they realised the potential for getting the ingredients for their chain of restaurants using the Internet.

Now Joseph King had long since handed over the day-to-day running of the diners to Anne Keen. Anne had developed a good rapport with their immediate suppliers. As you would expect, Anne's suppliers relied on the goods and services of others, and as the chain of supply lengthened, so the potential for missing orders, incorrect orders, and late orders increased. Not only that, as the smaller suppliers to Kings Diners were not sufficiently big concerns to guarantee their livelihoods from one source, they tried to keep open as many options as possible. This meant that whilst they tried to keep up with one order they were calling around looking for new or repeat orders – they were keeping all the plates spinning so to speak.



This worked best when orders were large and plenty of lead time provided. But as Anne wanted to control the cash flow and reduce waste, she preferred a 'just in time' approach to stock management. Customer satisfaction is the key to customer relationship management and so suppliers to Kings Diners met their customer's requirements. This had knock effects in the quantities ordered throughout the supply chain. Significantly, whilst the overall quantities supplied over time may have been on the increase, the quantities in each order decreased. More orders meant more information being passed from supplier to supplier with additional purchase orders, invoices, receipts, and general information as product lines changed to meet overall changes in the requirements of the market.

Then one morning Mr King came to take breakfast at one of his diners. He enjoyed it so much that he promised to return the following day. That's when the problems started . . .

Anne checked the fridge. No butter. Well that's no problem, she thought. Just pick up the phone to Dairy Made Catering Supplies and a new box of butter will be delivered by refrigerated van in the afternoon.

However, when Anne tried to 'phone Dairy Made, all Dairy Made's lines were engaged. The fax was no better. Well Joseph King was not one to be left behind in the Internet revolution. All his diners had a PC in the back office, linked to the Internet. Jo's son had done most of the installation and set up and a pirated *wav* file announced the arrival of every e-mail message. Sadly, however, the Kings Diner website with its radio button breakfast menu had failed to encourage orders for eggs over easy from anyone. Which is just as well; fried eggs do not post well.

Anne e-mailed her order to info@dairymade.com and relaxed, when half an hour later the reply:

Certainly

from sales@dairymade.com appeared. Dairy Made forwarded the e-mail to Alderney Farm Fresh Foods (www.afff.co.uk) and within a few minutes, orders@afff.co.uk had responded, promising their best product.

Meanwhile . . . at Alderney Farm Fresh Foods, the marketing department had come up with the killer product for the breakfast table. It didn't need refrigerating, and most monarchs who expressed a preference, said that their subjects shall prefer it.

Anne looked with satisfaction, when later that day, a van with the Dairy Made livery pulled up at the back door and delivered a carton which was placed straight into the cold store.

Night fell.

Dawn broke.

Joseph King arrived to survey his estate.

The chef opened the Alderney Farm Fresh Foods carton that Dairy Made had delivered the day before . . .

. . . to find it full of marmalade, not butter.

The chef said, 'Fancy!' or at least that is what we would like to think that he said. Anne heard the commotion, saw the marmalade, understood the problem and turned a little red.

She went to tell the boss, who said 'Bother', or at least that is what we would like to think that he said.

'Oh, deary me!' said Joseph King.

Ms Keen said, 'There, there!' and immediately rang Dairy Made, who rang Alderney Farm Fresh Foods.

Alderney soon discovered that their marketing department was intercepting orders as part of their market research. One of marketing's food testers was also called Anne. Marketing had seen the name on the e-mail and had assumed it was their Anne and despatched the marmalade for which they had been waiting for a delivery address after a previous piece of correspondence. Alderney rushed round a block of butter straight to the diner, adding a complementary carton of cream as a gesture of good will.

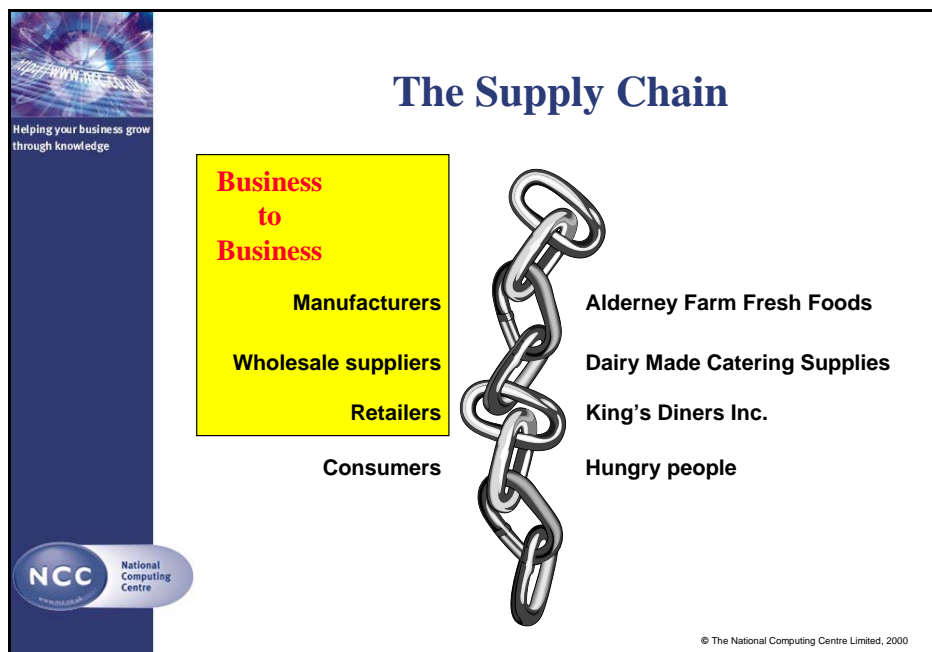
King looked at his breakfast and said, 'Can I believe it's butter?'

Anne showed him the wrapper.

Well fed, King bounded out of the door, turning only to blow a kiss to Anne and calling, 'Nobody would call me a fussy man to my face, but customers don't complain, they switch. If they'd like a bit of butter on their bread, we need a way to be sure that we get what we want. Look into to it.'

## 2.3 The supply chain

Let's look at this supply chain . . .




One of the first things to note in this story is that the Internet is only being used for basic correspondence – to create a crude purchase order. Invoices and receipts are not considered. So the potential to reduce and streamline paperwork is lost, as is the opportunity to manage lead times better because of the rework caused by poor control over the process.

Another benefit that could be reaped from this supply chain would be the opportunity to build relationships between suppliers who will have a degree of commonality created by the shared areas of automation. Also, the more transactions which are routed through a common path, the more scheduling processes can be managed more smoothly, and the expectations between links in the supply chain can be built into the system.

## 2.4 So what went wrong?

- (1) Ordering was haphazard. If e-mail is to be used for ordering then it should be part of a defined and audited procedure, not an ad hoc last resort.
- (2) Information should be sent with some structure. Rather than flat e-mails, it would be more efficient to have a workflow system that ensures that the information supplied is complete and passed on unaltered to whosoever needs it

- (3) Anyone receiving an order could process it, unaware of the standard quality checks to which regular order processing staff would be familiar.
- (4) The corollary is that anyone at the diner could have placed the order with no knowledge of correct prices, manageable quantities, approved suppliers, and so on.




Helping your business grow through knowledge

**NCC** National Computing Centre

## Organisational Issues

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

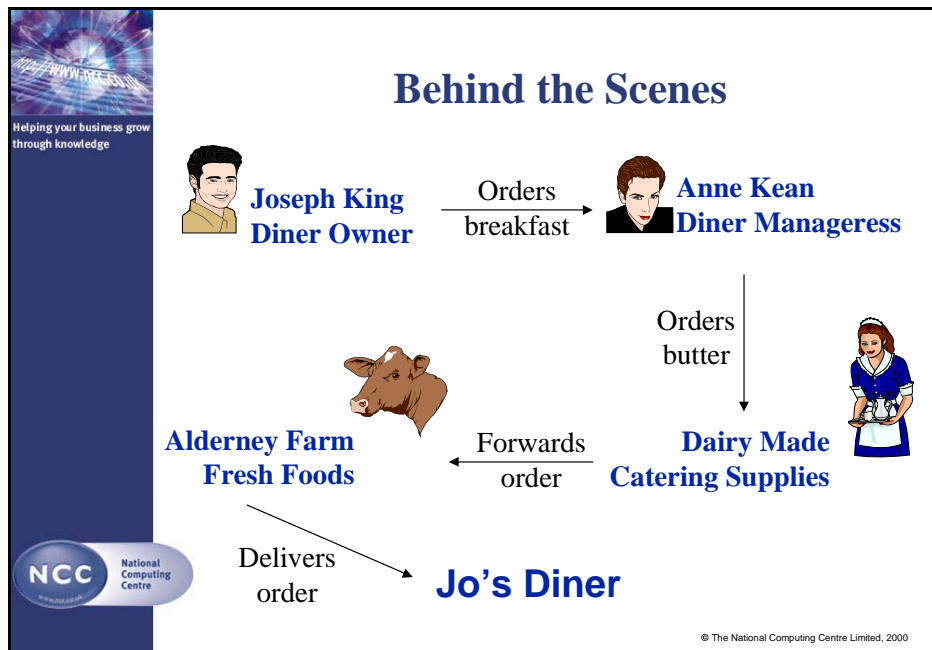


- Goods and information – the problems are the same . . .

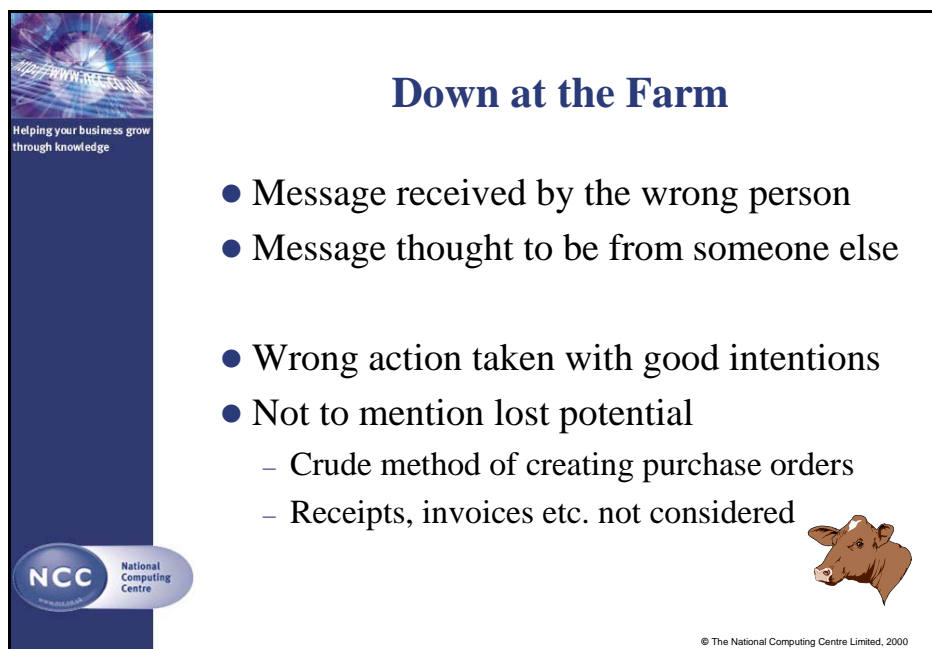
© The National Computing Centre Limited, 2000

Hold on to this idea: clever technology will not eliminate human error. Risk can only be managed when you deal with the following . . .

Let's focus for a moment on the transactions between the suppliers.



There is plenty of scope for misinformation and overkeen employees, not to mention the possibility of someone somewhere with an axe to grind, so . . . Dairy Made should verify who sent the order.



Competitors could be interested in the quantities used by the Diner, new products coming out of Alderney Farm and so on. Hold on to another idea: how do we prevent the wrong person getting the information?

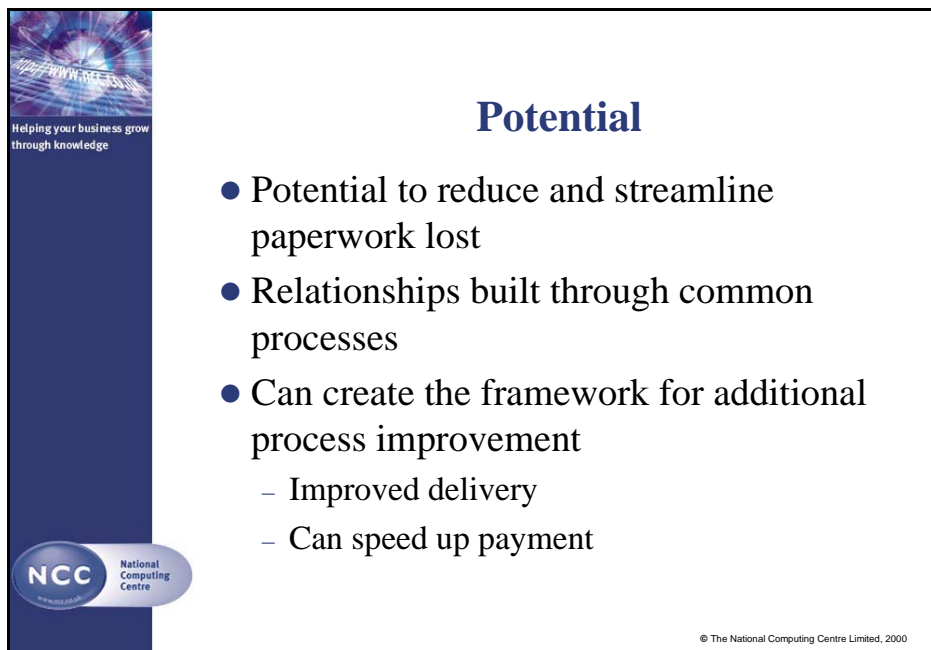
Remember if standards are met – probably implemented in a proprietary system – the order information will contain:

- Automatically generated purchase order numbers (this could be version control if we looked at an example of transferring design documents)
- Stock taking information
- Invoice/billing information

Then there's more added extras: being sure when an order was made (a potential for scheduling) and by whom, VAT records and on and on and on. Here we have the potential to link a strong, cooperative supply chain and we can lock the links together with keys.

## 2.5 Whose keys?

A plain description of the use of keys – a Public Key Infrastructure (PKI) – is contained below (*see What is PKI? on page 15*). Here is how it may be applied to our story.



The slide features a dark blue vertical sidebar on the left with a network graphic at the top and the text "Helping your business grow through knowledge". The NCC logo is at the bottom of the sidebar. The main content area has a white background with a blue title "Potential" and a bulleted list of three main points, each with sub-points. A small copyright notice is at the bottom right of the slide.

**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

© The National Computing Centre Limited, 2000

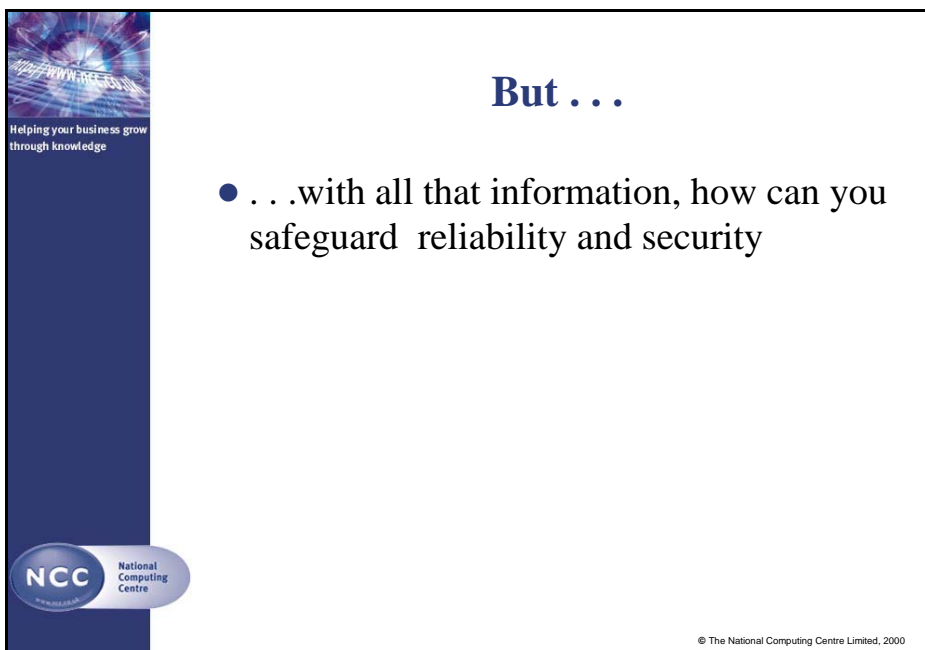
Electronic communications between the Diner, Dairy Made, and Alderney Farm would be improved if they are part of a Public Key Infrastructure. The important word here is infrastructure (*see Chapter 6*). This is how it works . . .

The Diner Chain authorises limited members of staff to make orders. This is down to good, old-fashioned levels of authority handed out throughout the organisation if not big and small then at least big and medium. In practice, in the PKI, authority is tied to digital certificates, just in the same way that a paper certificate from the British Dental Association licences a

dentist to work. Depending on the organisational requirements, certificates may be set to different levels. For example, perhaps only management get the top level, let's call it a high assurance certificate, and only holders of high assurance certificates may make orders. (This is an example of Certificate Policy.) Imagine Anne holds a high assurance certificate. She has a user name and password which invokes the software which releases the certificate for use. Note that Anne is responsible for taking care with these user details in the same way you protect your cash card and PIN number. PKI systems can only be as secure as their users. If Anne passes on her details to her friend Eve, Eve can pose as Anne.

When Anne runs the ordering system on the PC at the Diner, she logs on with her username and password, fills in the forms, and sends them to Dairy Made. The order, now an electronic message is wrapped up with Anne's electronic identity and locked by Anne's *private key* (remember that she had to use a name and password) – the message has been encrypted. Should the message be intercepted it can't be deciphered without access (again in client-end software) to Anne's *public key* which is under the control of the authority which hands out these *digital certificates*. The message arrives at Dairy Made where complementary software uses a *public key* to authenticate who sent the message, and that it hasn't been altered since Anne sent it. Dairy Made's staff could use Anne's public key to lock up a message that can only be opened with Anne's private key, so the system works both ways. A users private key and public key are called the *key pair*. The same software is used by Dairy Made to pass on the Order to Alderney Farm.

The Marketing department (in this scenario) only have a medium level assurance certificate so that they cannot open the orders (which are created with a high assurance certificate) so their market testing does not interfere with the day to day fulfilment of orders.



Helping your business grow through knowledge

**But . . .**

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

NCC National Computing Centre

© The National Computing Centre Limited, 2000

But say that they were allowed access, would that lead to the same confusion of the two Annes? No. It wouldn't and there are two reasons for this:

- If Anne the market tester was passing results and requests through to the marketing department – who would certainly want to keep them secret from competitors – she would have her own identifying certificate
- This is a PKI – it is an infrastructure. Marketing (with its departmental key) would be bound by the same on-line procedures that manage the identifying keys, as well as the organisational procedures

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

NCC National Computing Centre

© The National Computing Centre Limited, 2000

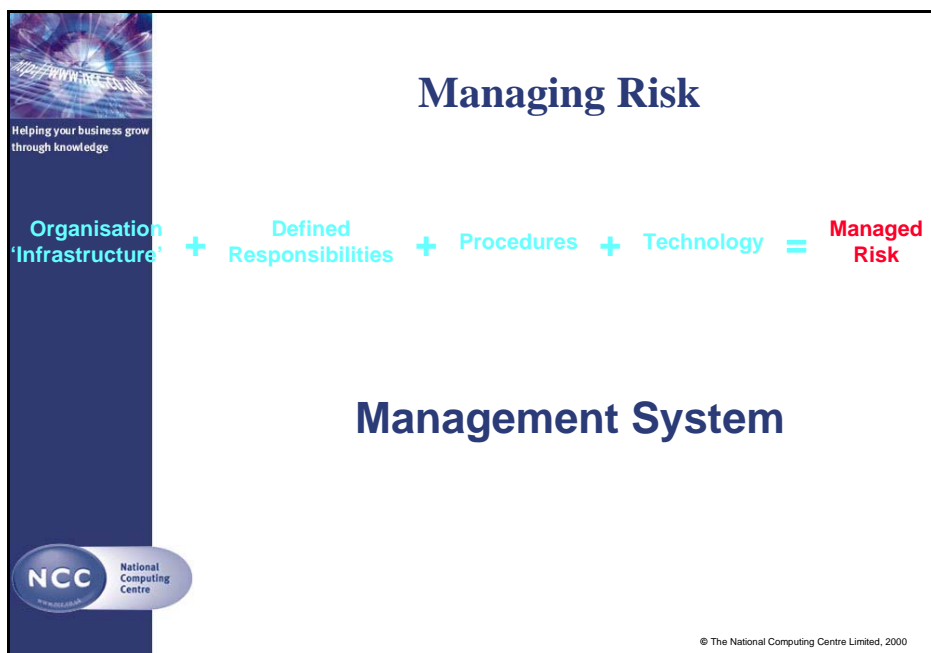
A PKI is only as good as the effort put into its establishment and running.

In this example, we've only looked at part of the picture – look at the more detailed description below – and remember the government definition:

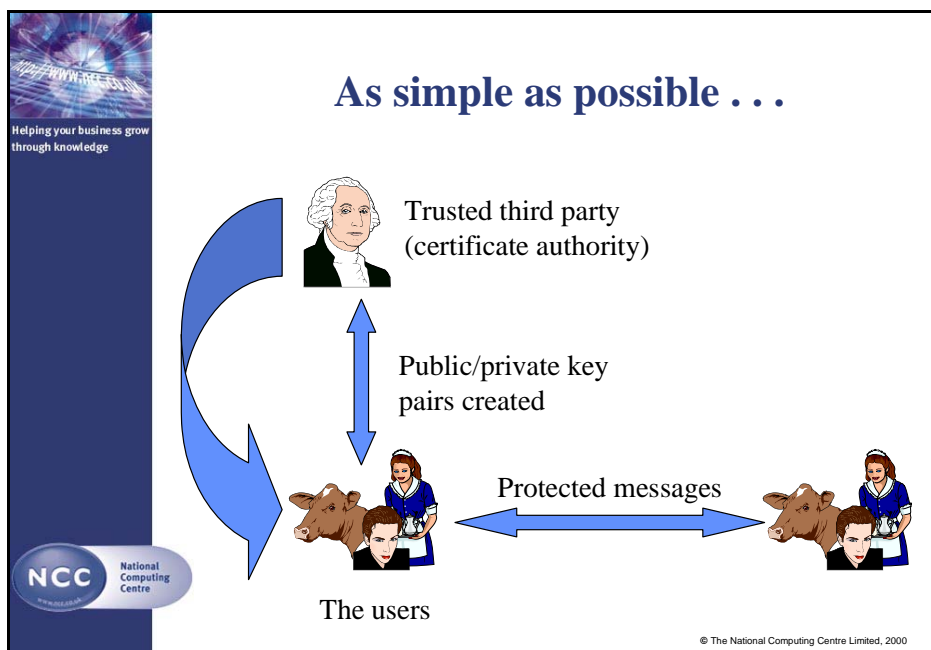
'Electronic commerce is the exchange of information across electronic networks, at any stage in the supply chain, whether within an organisation, between businesses, between businesses and consumers, or between the public and private sectors, whether paid or unpaid.'

A PKI could be used to manage the distribution of architects drawings between architect, other architects and surveyors. You can control who sends items and who opens them. Many of the permission concepts will be familiar to network administrators but this 'network administration' can have its running costs reduced to the price of a local phone call because all

the PKI does is provide the security; the Internet provides the network connections.



## 2.6 What is PKI?<sup>1</sup>



PKI combines authentication software, encryption technologies, and services designed to help enterprises protect the security of

1. This description of PKI is extracted from *NCC Guideline 248 – PKI and the Security of E-business*, available to NCC Members.

communications across the Internet. The key to PKI is the digital certificate, which is often compared to a passport. Like a passport, the digital certificate identifies its bearer and makes certain guarantees about the bearer's status. In any secure transaction, an exchange of such certificates must precede the business itself if all the parties concerned are to be assured of the identity and status of the others.

This is how it works, according to one leading PKI vendor<sup>1</sup>:

- (1) Before sending a secret message, ask to see the other party's certificate to get their public key
- (2) When signing a document encrypt using your private key and send encrypted document plus *your* certificate
- (3) Before trusting a document verify signature using the sender's certificate
- (4) Before doing anything with a certificate, be sure you trust the Certificate Authority who issued it'



**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

© The National Computing Centre Limited, 2000

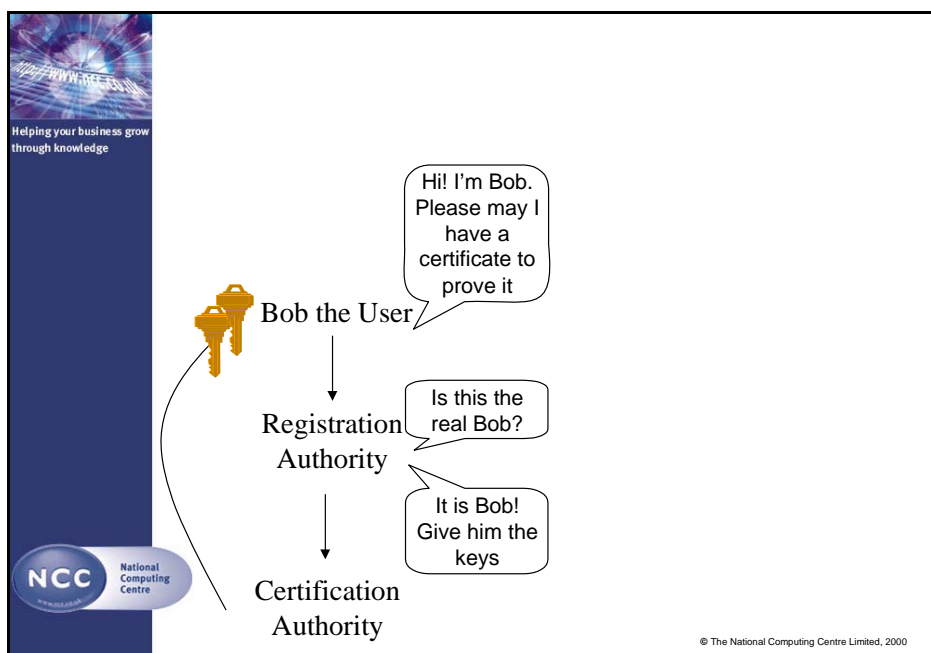
PKI is intended to protect data and secure transactions at every stage in the process:

- (1) **Identification**  
Digital certificates can replace user names and passwords with their attendant weaknesses (they are easily breakable and frequently lost). This makes intranet and Internet log-in procedures faster, more efficient and more secure, and reduces demands on the IS department.

---

1. Excluding the use of a centralised certificate authority.

- (2) **Authorisation**  
PKI allows IS departments to control access privileges for specific on-line transactions, whether commercial or not.
- (3) **Authentication**  
Digital certificates allow individuals, organizations, and web sites to validate the identity of all parties to an on-line transaction.
- (4) **Verification**  
PKI guarantees that data signed with a digital certificate has not been altered or corrupted in the course of transmission – in other words, that the data received is the same as the data transmitted. *(This function is sometimes considered to be optional.)*
- (5) **Privacy**  
Encryption protects data from interception during transmission.
- (6) **Non-repudiation**  
A digital certificate identifies its user and supports (although it doesn't guarantee) the non-repudiation of transactions – in other words, it is harder to deny making a transaction if digital certificates provide a record of the parties involved.

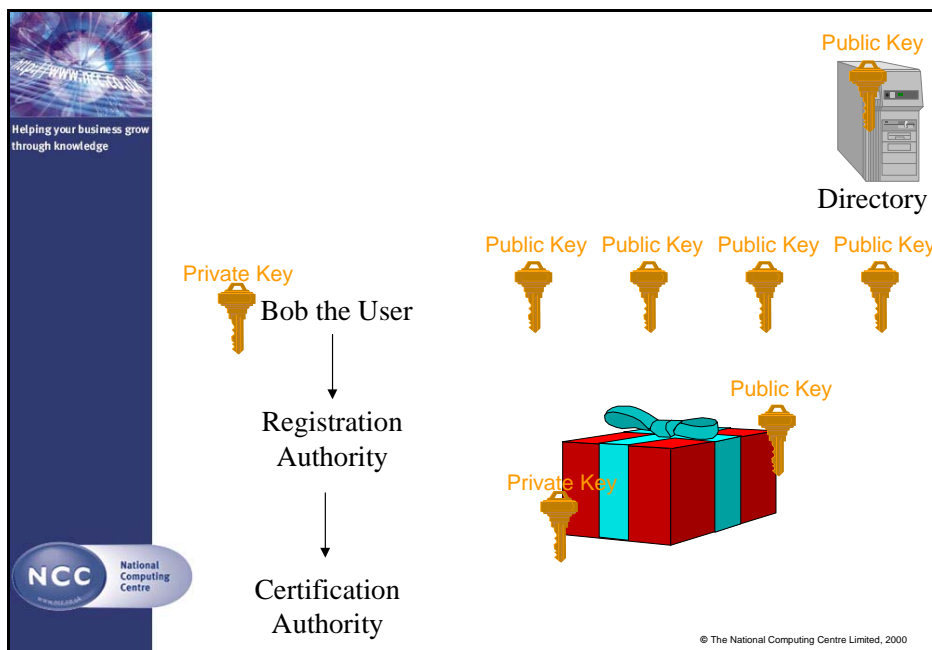


The concept of the digital certificate (or digital ID) is derived from Public Key Encryption (PKE), a cryptographic technique relying on the use of two distinct 'keys' (referred to as 'a key pair') – one to lock (or encrypt) a message and the other to unlock (or decrypt) the message. PKE avoids one of the main problems of private or secret key encryption – that keys must be shared across possibly insecure media for the encryption to work. With PKE, messages encrypted using a public key (which can be openly shared) can only be decrypted using its corresponding private key, while messages encrypted using the private key can only be decrypted using the public

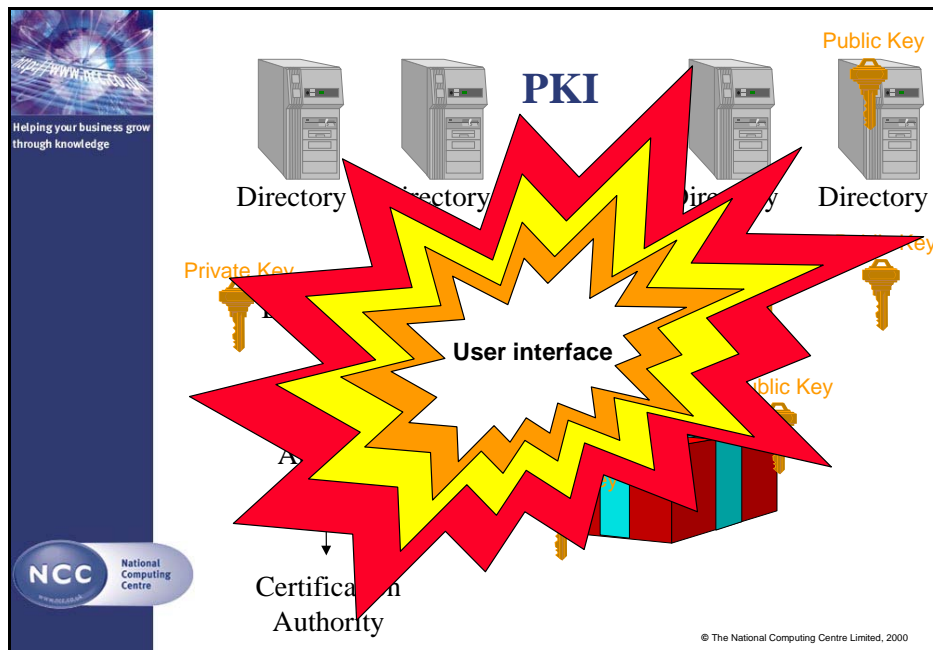
key, and there is no known method for deriving the private key from the public one. A digital certificate is essentially a record of the public key assigned to an individual, organization or network device. The certificate identifies its owner and incorporates information about such things as the owner's security level and the expiry date of the certificate itself. It is authenticated by a Certification Authority (CA) using the CA's private key – a process described as signing.

The certification authority holds all the public keys (under its authority) and are accessible to all.

*Note: Private key encryption only guarantees the sender. To guarantee the sender and the recipient, the message must be encrypted using the sender's private key and the recipient's public key.*



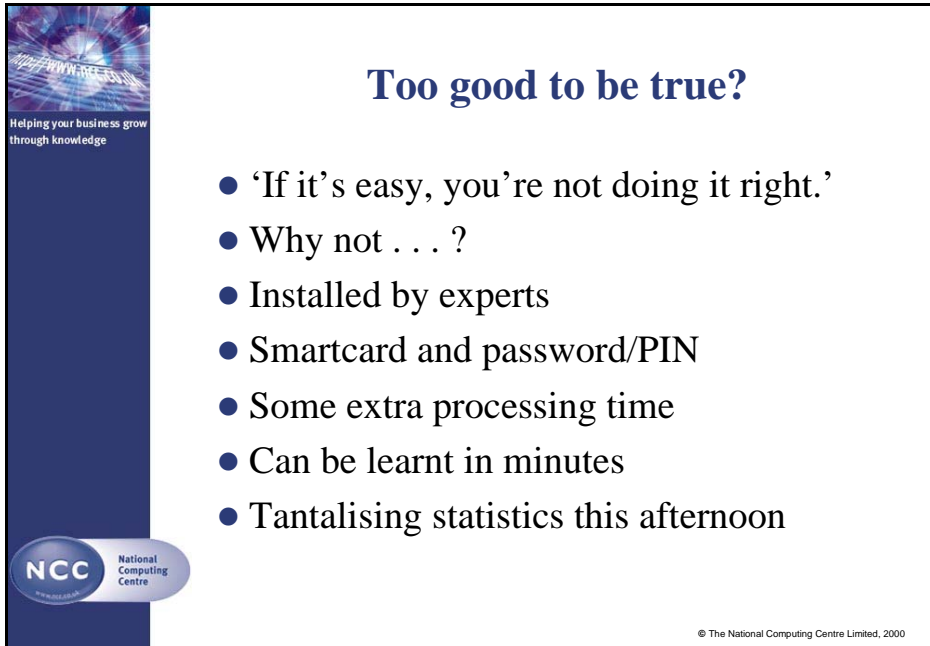
One 'standard' that has emerged in the discussion of PKI (except in embellishments like the Diner-Farm saga) is the description of a basic PKI. There are always Alice and Bob exchanging messages, and Carole as the certification authority. Occasionally, Eve may try to listen in on the exchange.



Thus Alice may be issued with a digital certificate by Carole, the certification authority. Bob can use Alice's public key – which is contained in her digital certificate – to encrypt a confidential message which can only be read by Alice (assuming no one else has access to her private key).

Before Bob commits himself to sending the message, he can confirm that the certificate he is using is indeed Alice's by decrypting the 'signature' with Carole's public key.

Carole's public key is available on her own digital certificate, which is called 'the root certificate' when it belongs, as in this case, to a CA. The root certificate is used to prove that Carole issued Alice's certificate in the first place, and demonstrates that the certificate belongs to the person identified therein – as long, that is, as Carole herself can be trusted. This, of course, is PKI's weak point.



The slide features a dark blue vertical sidebar on the left. At the top of the sidebar is a graphic with the text 'WWW.NCC.CO.UK' and 'Helping your business grow through knowledge'. Below this is the NCC logo, which consists of a blue circle with 'NCC' in white, followed by the text 'National Computing Centre'. At the bottom right of the slide, there is a small copyright notice: '© The National Computing Centre Limited, 2000'.

## 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
- Tantalising statistics this afternoon

In practice, PKIs make use of a number of more-or-less familiar security protocols to ensure the confidentiality, integrity and authenticity of any on-line communication:

- **S/MIME**  
The Secure, Multipurpose Internet Mail Extension protocol supports the sending of signed and encrypted e-mail
- **SSL**  
The Secure Sockets Layer protocol supports the encryption and authentication of communication between web browsers and web servers, or between different servers
- **IPSEC**  
The IP Security Protocol is a developing protocol which supports the encryption and authentication of communication among routers and firewalls

The diagram is titled "Standards" and lists several key standards in various colors: LDAP (green), BS 7799 (purple), ANSI (yellow), CEN (red), RSA (black), ITU (cyan), X.500 (maroon), and ISO 9000 (grey). On the left side, there is a vertical blue bar with the NCC logo and the text "National Computing Centre" and "Helping your business grow through knowledge". At the bottom right, there is a small copyright notice: "© The National Computing Centre Limited, 2000".

**Standards**

LDAP      BS 7799

ANSI      CEN      RSA

ITU      X.500

ISO 9000

**NCC** National Computing Centre  
Helping your business grow through knowledge

© The National Computing Centre Limited, 2000

