


Digital Identity Forum 2001 1

PKI & Security

London,
October 2001



Neil McEvoy
neil@consult.hyperion.co.uk

consult hyperion <http://www.consult.hyperion.co.uk>

Digital Identity Forum 2001 2



consult hyperion

Digital Identity Forum 2001 3

Agenda

- PKI
- Security
- PKI's role in security

consult hyperion

Digital Identity Forum 2001 4

Explaining PKI

- Alice & Bob
- Pen & ink
- PKI for dummies...

consult hyperion

Digital Identity Forum 2001 5

PKI for dummies (1)

- Getting a certificate

Cryptographic Service Provider Name	
Microsoft Enhanced C	Microsoft Enhanced C
Microsoft Base Crypt	Microsoft Base Crypt
Gemplus GemSAFE C	Gemplus GemSAFE C
Microsoft Base Crypt	Microsoft Base Crypt
Microsoft Enhanced C	Microsoft Enhanced C
Microsoft Strong Crypt	Microsoft Strong Crypt
Schlumberger Crypt	Schlumberger Crypt

Additional Security for Your Private Key
We recommend that you protect the private key information below will provide you with security options for your private key. [Click here for more information.](#)

What Do You Do Next?
You've successfully installed your Digital ID into Microsoft Internet Explorer and are now ready to start securing your e-mail through Outlook Express or Outlook 2000. To help you get started quickly, follow the instructions below:

Associate a Digital ID With Your E-mail Account

Microsoft Outlook Express:

1. Select Accounts from the Tools menu, then the Mail tab.
2. Select your Mail account, click the Properties button, select the Security tab.
3. Check the box "Use a digital ID when sending secure messages from", then click the Digital ID button.
4. Select the certificate you want to use to digitally sign your e-mail.

Outlook 98 and 2000:

1. In the Tools menu select Options, then the Security tab
2. click "Add digital signature to outgoing messages", click the "Change Settings" button
3. On the next screen click the "Choose..." button. Select the Digital ID you want to use for signing e-mail in Outlook.

Consult our User Manual and Tutorials

1. Visit our [Learning Center](#) to view our tutorials, user manual and other useful information.
2. Visit our [Code Signing ID Center](#) to find out more about Code Signing IDs and Code Signing ID services.

consult hyperion

Digital Identity Forum 2001 6

PKI for dummies (2)

- Using certificates

Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

The security cert not chosen to trust you want to trust

The security cert is trusted

The security cert of the page you are viewing is trusted

Do you want to proceed?

Yes No

Certificate Information

This certificate cannot be verified up to a trusted certification authority.

Issued to: hermes.hyperion.co.uk

Issued by: Consult Hyperion CA

Valid from: 05/07/2001 to 05/07/2002

Install Certificate... Issue Statement

The page requires a valid client certificate - Microsoft Internet Explorer

The page you are trying to view requires the use of a valid client certificate. Your client certificate is untrusted or invalid. The client certificate is used for authenticating you as a valid user of the resource.

Please try the following:

- Click the **Refresh** button to try again, if you have changed your client certificate.
- Contact the Web server's administrator to obtain a valid client certificate.
- If you believe you should be able to view this directory or page, please contact the Web site administrator by using the e-mail address or phone number listed on the hermes.hyperion.co.uk home page.

HTTP 403.16 - Forbidden: Client certificate untrusted or invalid
Internet Information Services

Technical Information (for support personnel)

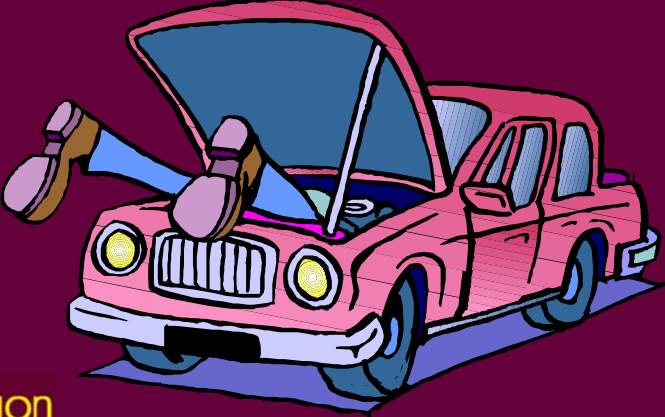
- More information: [Microsoft Support](#)

consult hyperion

Digital Identity Forum 2001 7

Interim Conclusions

- PKI isn't for dummies
- If it has a role, keep it "under the hood"

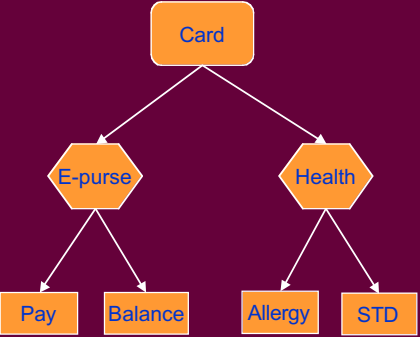


consult hyperion

Digital Identity Forum 2001 8

Multi-application cards

- Convenient for users
- Difficult to manage
- Privacy concerns
- Can be made "secure"



```
graph TD; Card[Card] --> E-purse{{E-purse}}; Card --> Health{{Health}}; E-purse --> Pay[Pay]; E-purse --> Balance[Balance]; Health --> Allergy[Allergy]; Health --> STD[STD];
```

consult hyperion

Digital Identity Forum 2001 9

Life is made of 2 x 2 s


F1 Terminal	F2 Terminal
F1 Card	F2 Card

consult hyperion

Digital Identity Forum 2001 10

Can this function happen?

- **CARD**
 - ✓ What do I know about:
 - my 'holder'
 - the terminal
 - its operator?
- **TERMINAL**
 - ✓ What do I know about:
 - my operator
 - the card
 - its holder?



consult hyperion

Digital Identity Forum 2001 11

Ahead of their time...






Knowing me, knowing you...

consult hyperion

Digital Identity Forum 2001 12

3-factor authentication

- Something you have
- Something you know
- Something you are




consult hyperion

Digital Identity Forum 2001 13

Biometrics

- **Need a degree of supervision**
- **Relatively expensive equipment**
- **Good for authentication**
- **Less good for identification**

If you're seeking 1 person per 100,000, a 99% accurate biometric will produce produce 1000 false positives for every true positive



consult hyperion

Digital Identity Forum 2001 14

Secure Access Module

- **All security critical terminal functionality implemented once**
 - ✓ Less work
 - ✓ More control
- **Implement in smart card**

consult hyperion

Digital Identity Forum 2001 15

Mutual authentication

```
graph TD; CM[Card management] -- Crypto keys --> Card; CM -- Crypto keys --> SAM; Card <--> |Context| SAM;
```

- **PKI one option for key distribution, secure messaging**

consult hyperion

Digital Identity Forum 2001 16

Ancillary crypto services

- **Given mutual authentication infrastructure, can do:**
 - ✓ Encryption
 - ✓ Digital signature

consult hyperion

Digital Identity Forum 2001 17

Conclusion

- General public will never understand PKI
- Confusion = insecurity
- PKI is a technical solution to a technical problem

The most important letter in PKI is 'I'

The least important is 'P'

consult hyperion