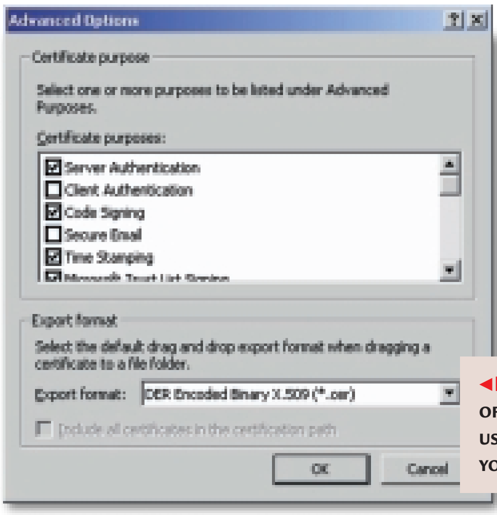
Signed, sealed and secure

Bob Walder guides you step by step through the process of digitally signing your email.

As part of our series on public key cryptography and digital signatures and certificates, last month we acquired a digital ID of our own from VeriSign and got as far as installing it in our browser.

Now the digital certificate is in your web browser, you need to know how to view it and use it to sign email and so on. To use your VeriSign digital ID, you use VeriSign-aware, security-enhanced applications. Many applications, such as secure web browsers and S/MIME-compliant email tools, support the use of digital IDs for electronic communication. Once your digital ID is installed, your web browser uses it automatically when you access sites which request a digital ID. Sites can then use your digital ID to determine what information or services to allow you to access.

For example, a site could check your ID against a list of paying members, recognise that you have paid-for access to live stock quotes, and allow you to access up-to-the-minute stock prices. You don't have to enter a member name, number, or password – your digital ID is used to verify your identity automatically. You don't have to remember a different membership ID and password for each service you access, and the services are assured that someone else isn't accessing the information using your account.



Advanced Options

Certificate purpose

Select one or more purposes to be listed under Advanced Purposes.

Certificate purposes:

☑ Server Authentication
☐ Client Authentication
☑ Code Signing
☐ Secure Email
☑ Time Stamping
☑ Microsoft Trust List Signing

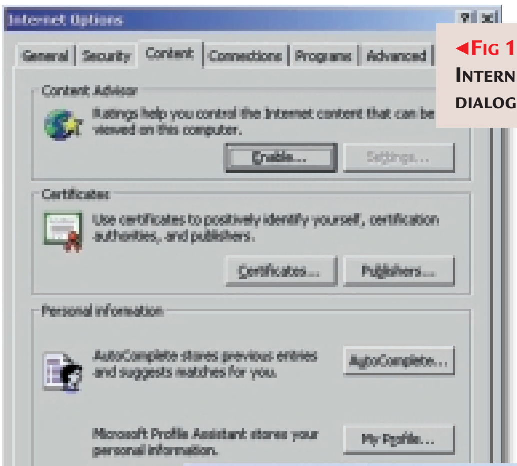
Export format

Select the default drag and drop export format when dragging a certificate to a file folder.

Export format: DER Encoded Binary X.509 (*.cer)

☐ Include all certificates in the certification path

◄Fig 3 A list of possible uses for your ID



Internet Options

Content Advisor

Ratings help you control the Internet content that can be viewed on this computer.

Certificates

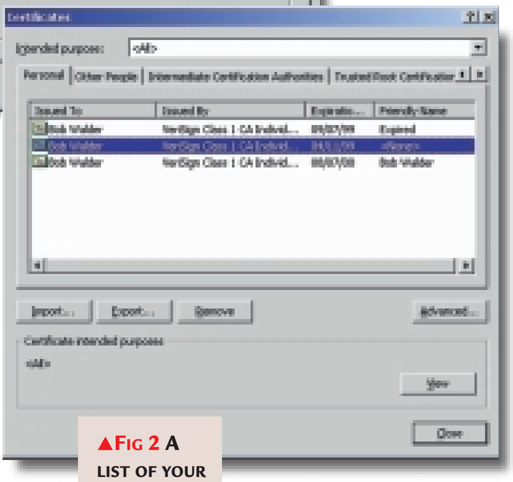
Use certificates to positively identify yourself, certification authorities, and publishers.

Personal information

AutoComplete stores previous entries and suggests matches for you.

Microsoft Profile Assistant stores your personal information.

◄Fig 1 The Internet Options dialog in IE5



Certificates

Intended purpose: <All>

Personal
Other People
Intermediate Certification Authorities
Trusted Root Certification

Issued To	Issued By	Expiratio...	Friendly Name
Bob Walder	VeriSign Class 1 CA Individ...	[illegible]	Expired
Bob Walder	VeriSign Class 1 CA Individ...	[illegible]	<None>
Bob Walder	VeriSign Class 1 CA Individ...	[illegible]	Bob Walder

Import...
Export...
Remove
Advanced...

Certificate intended purposes

<All>

▲Fig 2 A list of your viewing certificates

Every browser is slightly different, but the processes used are similar. To keep things simple, I am going to use Microsoft Internet Explorer 5 as the basis for this article.

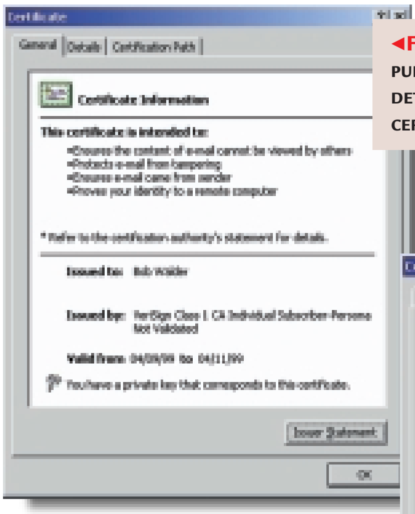
To access your digital certificate, select the Tools option on the main toolbar. Then choose Internet Options and select the Content tab. You will see a window similar to Fig 1.

Click on the Certificates button to bring up a list of the digital IDs you have installed. Under the Personal tab, you should just have the one which we acquired as part of last month's exercise. As you can see from Fig 2 I actually have three currently installed. The bottom one is my current digital ID, and the top one is a previous version of that ID, now expired (full digital IDs require renewal each year). The middle one is the temporary ID I acquired last month.

Select the Trusted Root Certification Authorities (CA) tab, and you will see a list of the Root CA certificates that have been 'hard-coded' into Internet Explorer. As you can see, at the top are the VeriSign Class 1, 2 and 3 root certificates. This allows IE5 to rapidly verify the validity of any VeriSign user (or website) certificate since it automatically trusts VeriSign as a root CA (it does not have to go back to VeriSign each time it needs to check a certificate). Note also the expiry dates. If you have earlier versions of IE or Netscape Navigator, you may notice that some of the root certificates expire in the year 2000! This is yet another Y2K issue, since once those certificates expire, it will effectively invalidate all VeriSign certificates, as it will appear to the browser that the CA root certificate has expired. If you have these older versions of IE and Netscape, you need to upgrade them as soon as possible.

Go back to the Personal tab, select your certificate and click on Advanced. Here you can see the uses to which your digital ID can be put (eg server or client authentication, secure email, virtual private network user, and so on) [Fig 3]. Make sure that you check both the Client Authentication and Secure Email boxes.

Close this window and click on the View button. You can now view the details of your digital certificate [Fig 4].



Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended to:

- •Ensures the content of e-mail cannot be viewed by others
- •Protects e-mail from tampering
- •Ensures e-mail came from sender
- •Proves your identity to a remote computer

* Refer to the certification authority's statement for details.

Issued to: Bob Walder

Issued by: VeriSign Class 1 CA Individual Subscriber-Persona Not Validated

Valid from: 04/09/99 to 04/11/99

You have a private key that corresponds to this certificate.

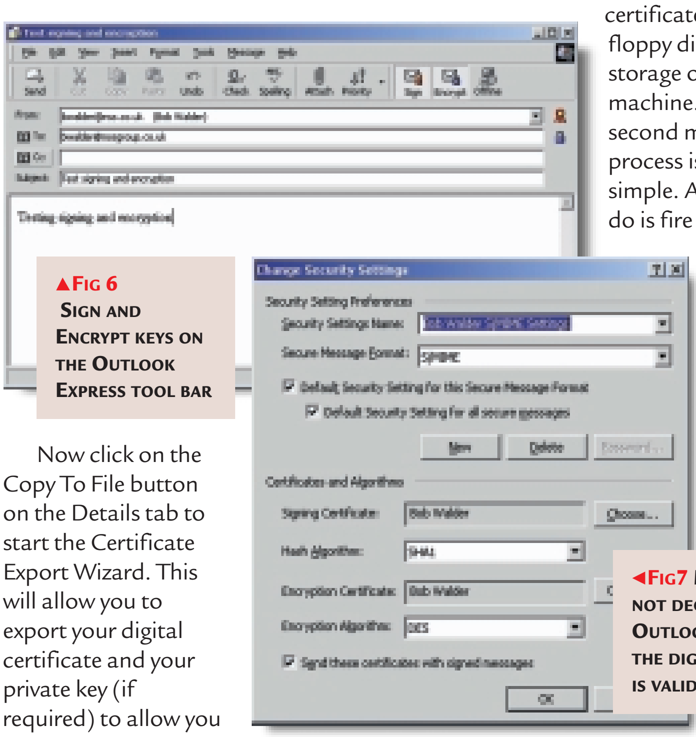
◄Fig 4 Checking public key details in the certificate

The General Information tab shows whom the certificate was issued to, who it was issued by, the expiry date, and its intended uses.

Click on the Certification Path tab and you can see the validation path from your certificate back to the root, and you can view each certificate on the path.

Click on the Details tab and you can examine each of the fields on your certificate. Click on any one of them and the extended information will appear – you can even view your public key [Fig 5].

By clicking on Edit Properties, you can change the friendly name and description for this certificate (which will appear when viewing a list of certificates).



Test signing and encryption

File Edit View Insert Format Tools Message Help
Send Cut Copy Paste Undo Check Spelling Attach Priority Sign Encrypt Offline

From: bwalder@vnu.co.uk (Bob Walder)

To: bwalder@rossgroup.co.uk

Cc:

Subject: Test signing and encryption

Testing signing and encryption

Change Security Settings

Security Setting Preferences

Security Settings Name: Bob Walder (S/MIME Settings)

Secure Message Format: S/MIME

☑ Default Security Setting for this Secure Message Format

☑ Default Security Setting for all secure messages

Certificates and Algorithms

Signing Certificate: Bob Walder

Hash Algorithm: SHA1

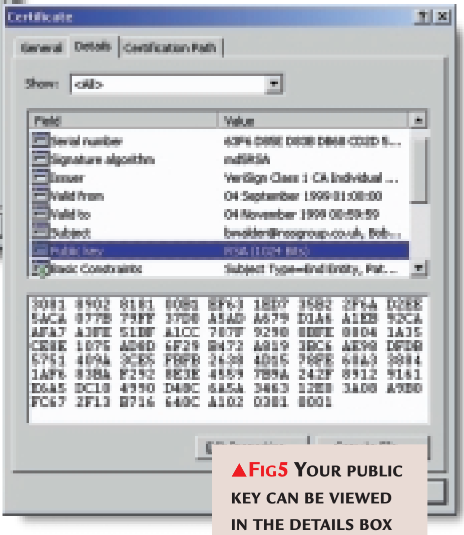
Encryption Certificate: Bob Walder

Encryption Algorithm: DES

☑ Send these certificates with signed messages

▲Fig 6 Sign and Encrypt keys on the Outlook Express tool bar

Now click on the Copy To File button on the Details tab to start the Certificate Export Wizard. This will allow you to export your digital certificate and your private key (if required) to allow you to use it on other machines, or simply to keep as a backup. Click on Next. Say 'Yes to export private key' (a password will be required to access it later). Click Next again. Then select the default options for the Export File Format and confirm it by clicking Next.



Certificate

General | Details | Certification Path

Show: <All>

Field	Value
Serial number	43F6 D85E D83B DB48 CD2D 5...
Signature algorithm	md5RSA
Issuer	VeriSign Class 1 CA Individual ...
Valid from	04 September 1999 01:00:00
Valid to	04 November 1999 00:59:59
Subject	bwalder@rossgroup.co.uk, Bob...
Public key	RSA (1024 Bits)
Basic Constraints	Subject Type=End Entity, Pat...

```
3081 8902 8181 00B1 EF63 1EDD 3582 2F6A D2EE
5ACA 077B 79FF 37D0 A5AD A679 D1A6 A1EB 92CA
AFA7 A3FE 51DF A1CC 707F 9250 8DFE 0804 1A35
CE8E 1075 AD8D 6F29 B472 A819 3BC6 AE90 DFD8
5751 409A 3CE5 FBFB 2638 4D15 79FE 6843 3984
1AF6 838A F292 8E3E 4559 7B9A 242F 8912 9161
E6A5 DC10 4990 D48C 6A5A 3463 12EB 3A08 A9B0
FC67 2F13 B716 640C A102 0301 0001
```

▲Fig5 Your public key can be viewed in the details box

Enter a password to protect the private key (this is only required if you are exporting your private key with the certificate). Click Next. Then enter the File Name and click Next again. Confirm the details and click Finish.

You can now copy the exported certificate file to a floppy disk for safe storage or to another machine. On the second machine, the process is a lot more simple. All you need to do is fire up Internet Explorer, select Tools, then Internet Options and select the Content Tab.

Next choose Certificates and click on the Import button to fire up the Certificate Import Wizard.

◄Fig7 Messages are not decrypted in Outlook 2000 until the digital signature is validated

Follow the prompts, selecting the file you exported from the source browser and entering the password you used to protect your private key.

Once you have confirmed the details and clicked on Finish, the private key and digital certificate are installed on the new machine.

Next, you need to associate your digital ID with your email account. This is the procedure for Outlook 2000, but it is similar for other clients:

In the Tools menu select Options, then the Security tab. Click on Import/Export Digital ID and then select Import Digital ID from file. Choose the file you exported from IE and enter the password for your private key (if this is applicable).

Under the Secure email section, you can specify if you always want to encrypt or sign messages, although these settings can be overridden at the time of sending.

The next step is to click on Change Settings – you will see a screen as in Fig 6. Create new security settings and make them the default for all secure messages. Then choose the signing certificate, and use the SHA-1 signing algorithm. Select the encryption certificate, and use the DES algorithm. Then click on 'Send these certificates with signed messages' to ensure recipients always have copies of your certificates and public keys.

From then on, when composing new email messages, click on View, Options or Properties, and Security in order to select the Sign and Encrypt check boxes. If you want to encrypt, Outlook Express will expect you to have a digital certificate available for the receiving party to provide it with the appropriate public key. If it cannot locate this, it will only allow you to sign the message.

When you receive a message that has been signed or encrypted, you will notice that it will not auto-preview – you need to open the message explicitly. Decryption will then occur automatically, and a small 'seal' icon will appear on the toolbar allowing you to validate the signature [Fig 7]. That's all there is to it.

PCW CONTACTS

Bob Walder is a journalist and networking consultant based in Bedfordshire. He can be contacted at the usual address or on:
networks@pcw.co.uk