“Want my autograph?”

The use and abuse of digital signatures by malware

Name: Mike Wood

Date: Sept 30, 2010

Agenda

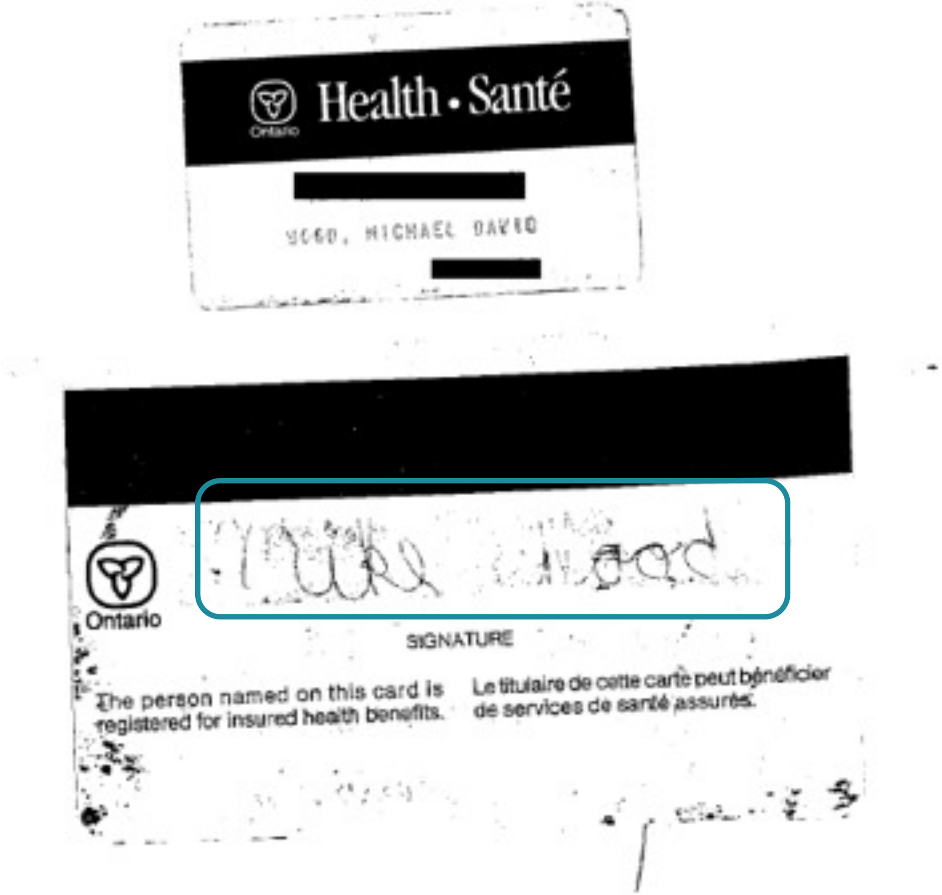
- Digital signature fundamentals
- Signed malware
- Online fraud & SSL
- Implementation issues
- Lessons learned

Digital Signature Fundamentals

Purpose

- Authentication
  - … who are you?
- Integrity
  - … has what you’ve got been tampered with?

Signatures in the physical world…



Health • Santé

Ontario

[redacted]

WOOD, MICHAEL DAVID

[redacted]

Mike Wood

SIGNATURE

The person named on this card is registered for insured health benefits.

Le titulaire de cette carte peut bénéficier de services de santé assurés.

Signatures in the digital world…

```
-----BEGIN PKCS7-----
MIIXaAYJKoZIhvcNAQcCoIIXWTCCF1UCAQExCzAJBgUrDgMCGgUAMGgGCisGAQQB
gjcCAQSgWjBYMDMGCisGAQQBgjcCAQ8wJQMBAKAgoh6AHAA8ADwAPABPAGIAcwBv
AGwAZQB0AGUAPgA+AD4wITAJBgUrDgMCGgUABBT9dwcRaU+XH04Qja1rllaVtnBG
faCCEjAwggRgMIIDTKADAgECAgouqxHcUP9cncvAMAkGBSsOAwIdBQAwcDErMCkG
A1UECxMiQ29weXJpZ2h0IChjKSAxOTk3IE1pY3Jvc29mdCBDb3JwLjEeMBwGA1UE
CxMVTWljcm9zb2Z0IENvcnBvcmF0aW9uMSEwHwYDVQQDExhNaWNyb3NvZnQgUm9v
dCBBdXRob3JpdHkwHhcNMDcwODIyMjIzMTAyWhcNMTIwODI1MDcwMDAwWjB5MQsw
CQYDVQQGEwJVUzETMBEGA1UECBMKV2FzaGluZ3RvbjEQMA4GA1UEBxMHUmVkbW9u
ZDEeMBwGA1UEChMVTWljcm9zb2Z0IENvcnBvcmF0aW9uMSMwIQYDVQQDExpNaWNy
b3NvZnQgQ29kZSBTaWduaW5nIFBDQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBALd5fdZds0U5qDSsMdr5JTVJd8D7H57HRXHv0Ubo1IzDa0xSYvSZAsNN
2EIsLyQ+Zb/OI7cLSLd/dd1FvaqPDlDFJSvyoOcNIx/RQST6YpnPGUWlk0ofmc2z
LyLDSi18b9kVHjuMORA53b0p9GY7LQEy//4nSKa1bAGHnPu6smN/gvlcoIGEhY6w
8riUo884plCFFyeHTt0w9gA99Mb5PYG+hu1sOacuNPa0Lq8KfWKReGacmHMNhq/y
……….
……….
……….
```

Digital Signature Basics – Object Signing

Digital Signature Basics – Object Signing

Signer

Private key
(secret)

Public key
(for anyone)

Digital Signature Basics – Object Signing

Signer

Private key
(secret)

Public key
(for anyone)

The Signer signs an object…

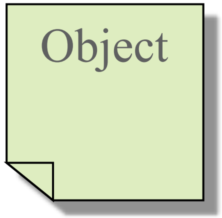
Digital Signature Basics – Object Signing

Signer

Private key
(secret)

Public key
(for anyone)

The Signer signs an object…



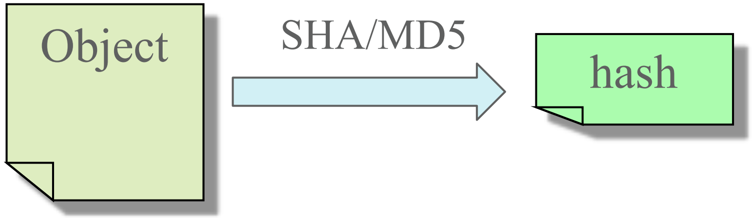
Digital Signature Basics – Object Signing

Signer

Private key
(secret)

Public key
(for anyone)

The Signer signs an object…



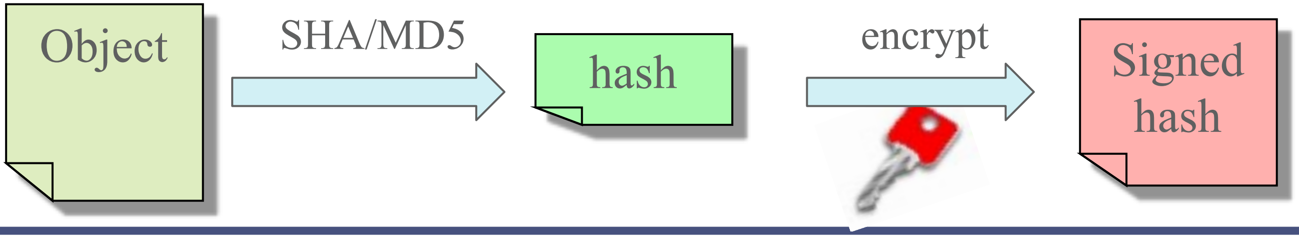
Digital Signature Basics – Object Signing

Signer

Private key (secret)

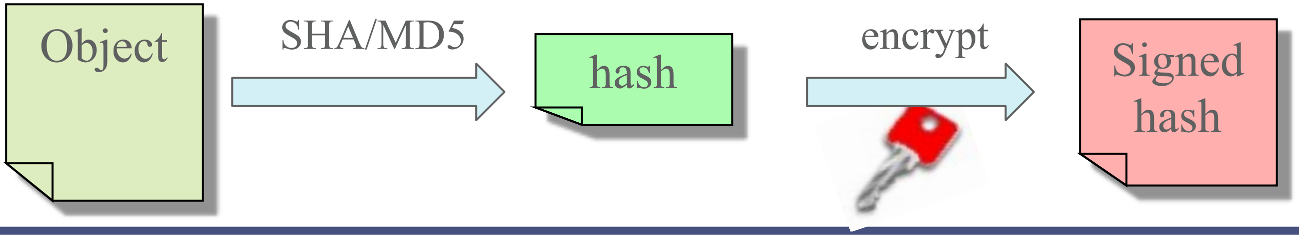
Public key (for anyone)

The Signer signs an object…



Digital Signature Basics – Object Signing

The Signer signs an object…



Anyone can verify the signature…

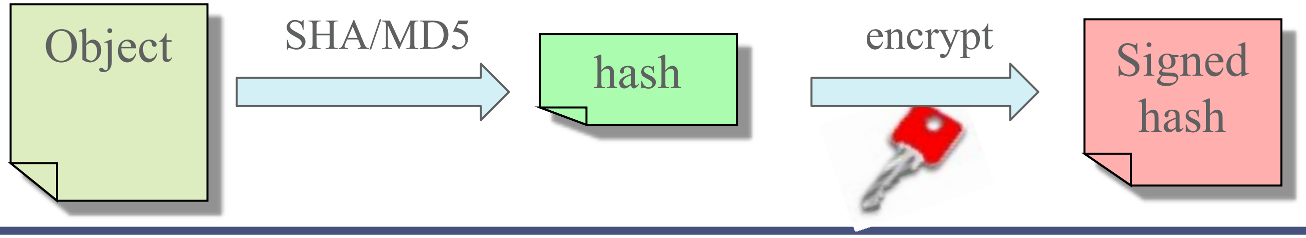
Digital Signature Basics – Object Signing

Signer

Private key
(secret)

Public key
(for anyone)

The Signer signs an object…



Object

SHA/MD5

hash

encrypt

Signed
hash

Anyone can verify the signature…

Object

Signed
hash

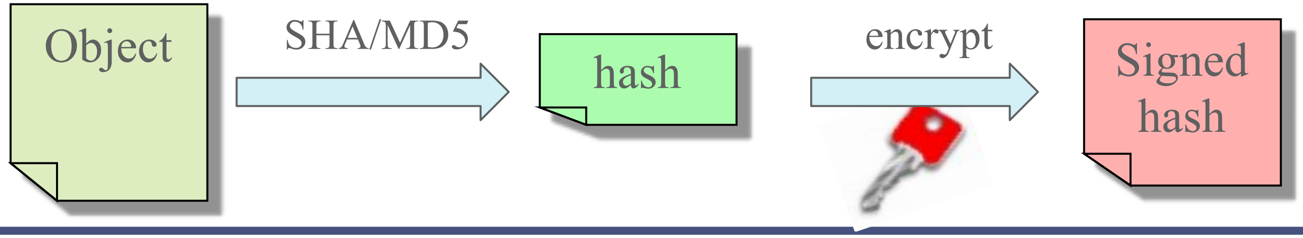
Digital Signature Basics – Object Signing

Signer

Private key
(secret)

Public key
(for anyone)

The Signer signs an object…



Object

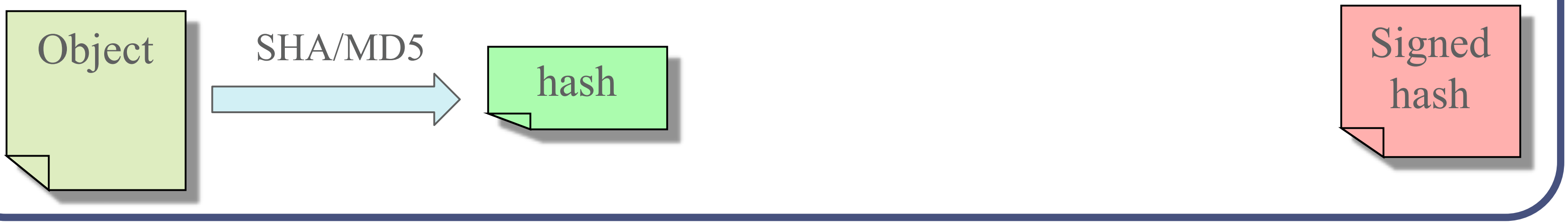
SHA/MD5

hash

encrypt

Signed hash

Anyone can verify the signature…



Object

SHA/MD5

hash

Signed hash

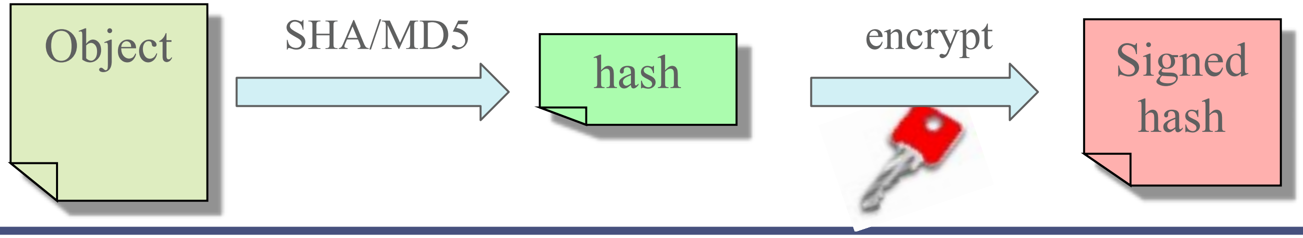
Digital Signature Basics – Object Signing

Signer

Private key
(secret)

Public key
(for anyone)

The Signer signs an object…



Object

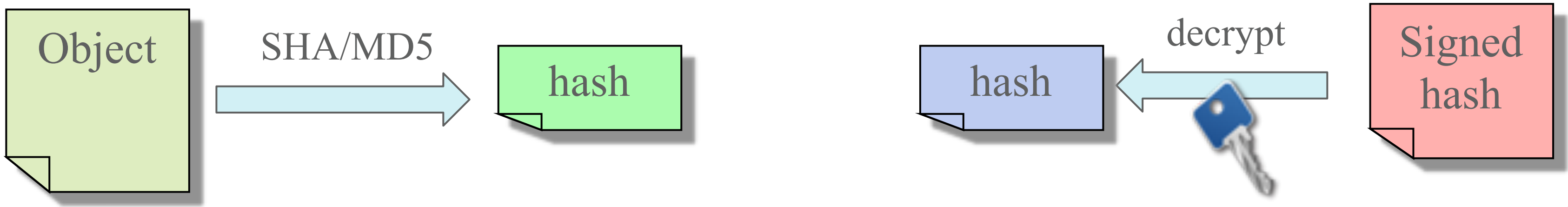
SHA/MD5

hash

encrypt

Signed hash

Anyone can verify the signature…



Object

SHA/MD5

hash

hash

decrypt

Signed hash

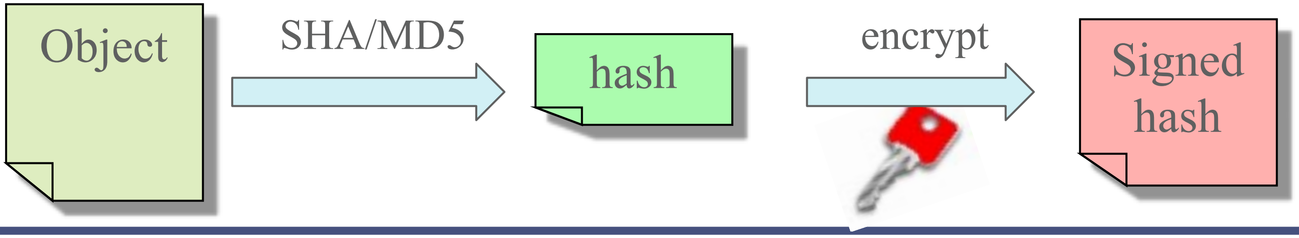
Digital Signature Basics – Object Signing

Signer

Private key
(secret)

Public key
(for anyone)

The Signer signs an object…



Object

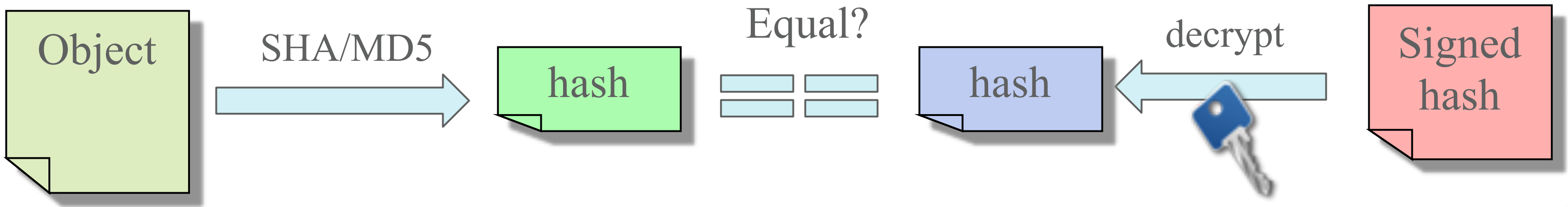
SHA/MD5

hash

encrypt

Signed hash

Anyone can verify the signature…



Object

SHA/MD5

hash

Equal?

hash

decrypt

Signed hash

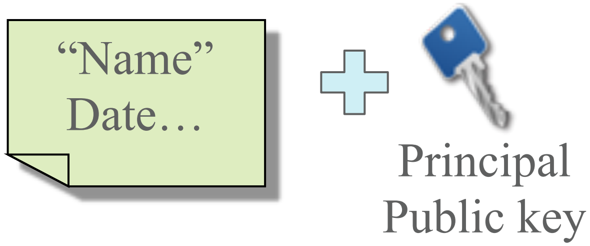
Digital Signature Basics – Certificate Creation

Digital Signature Basics – Certificate Creation

A Certificate Authority (CA) issues a certificate to a Principal

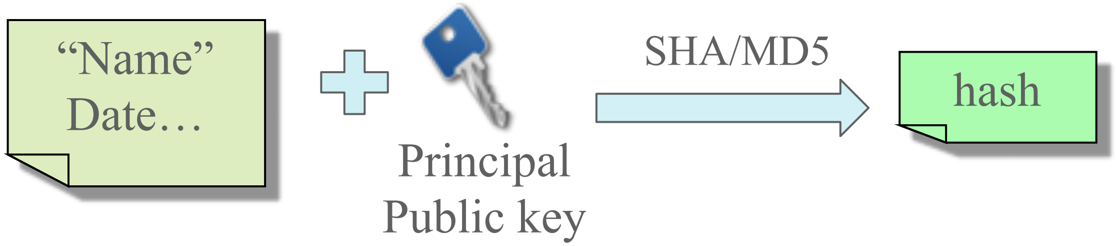
Digital Signature Basics – Certificate Creation

A Certificate Authority (CA) issues a certificate to a Principal



Digital Signature Basics – Certificate Creation

A Certificate Authority (CA) issues a certificate to a Principal



"Name"
Date…

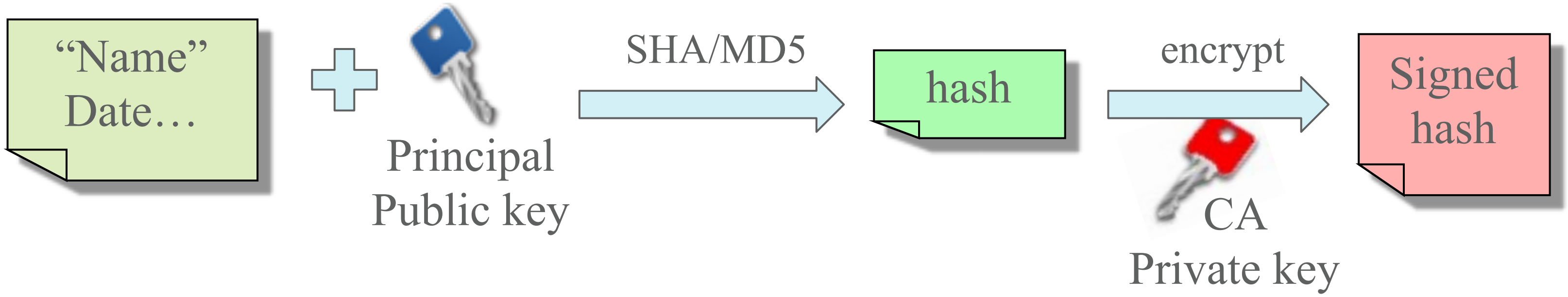
Principal
Public key

SHA/MD5

hash

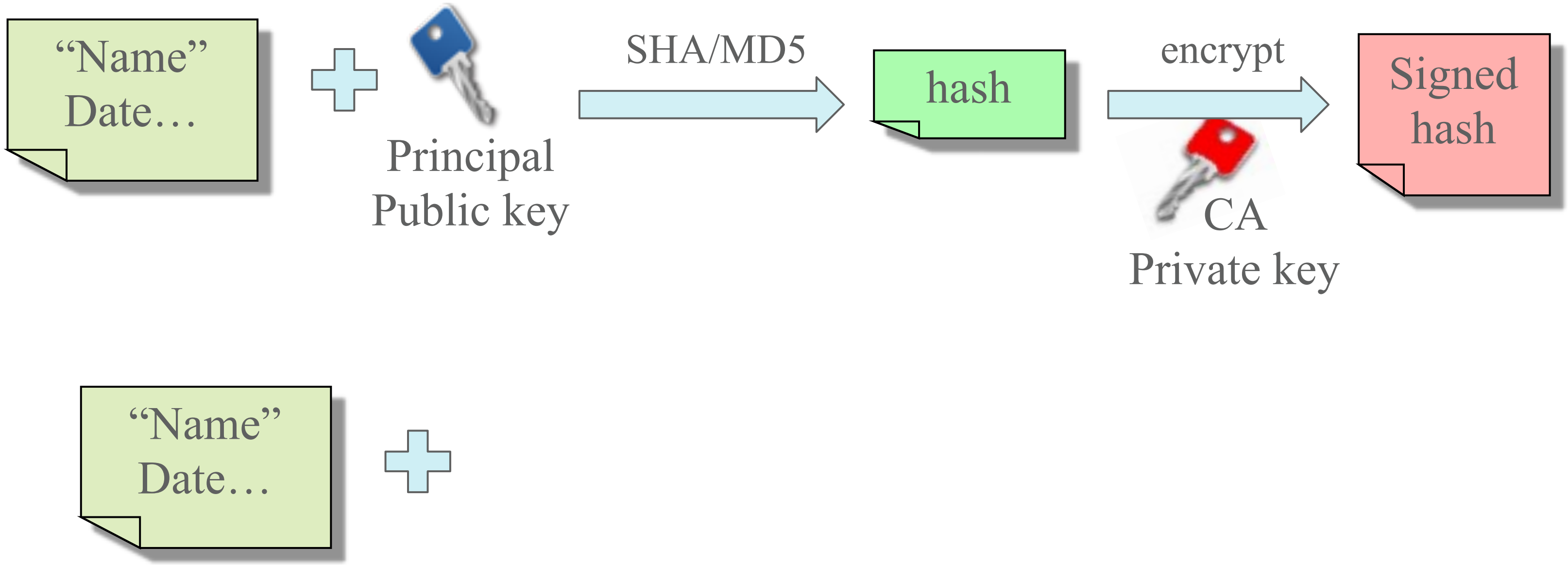
Digital Signature Basics – Certificate Creation

A Certificate Authority (CA) issues a certificate to a Principal



Digital Signature Basics – Certificate Creation

A Certificate Authority (CA) issues a certificate to a Principal



"Name"
Date…

Principal
Public key

SHA/MD5

hash

encrypt

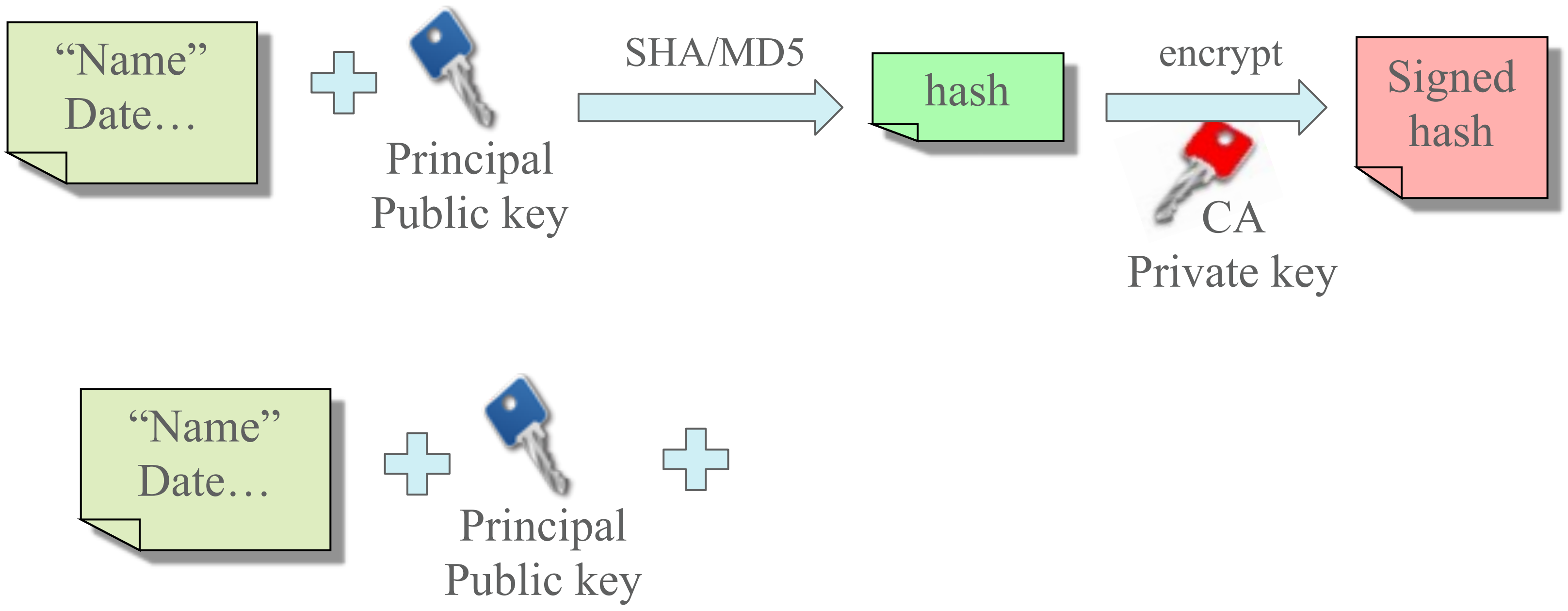
CA
Private key

Signed
hash

"Name"
Date…

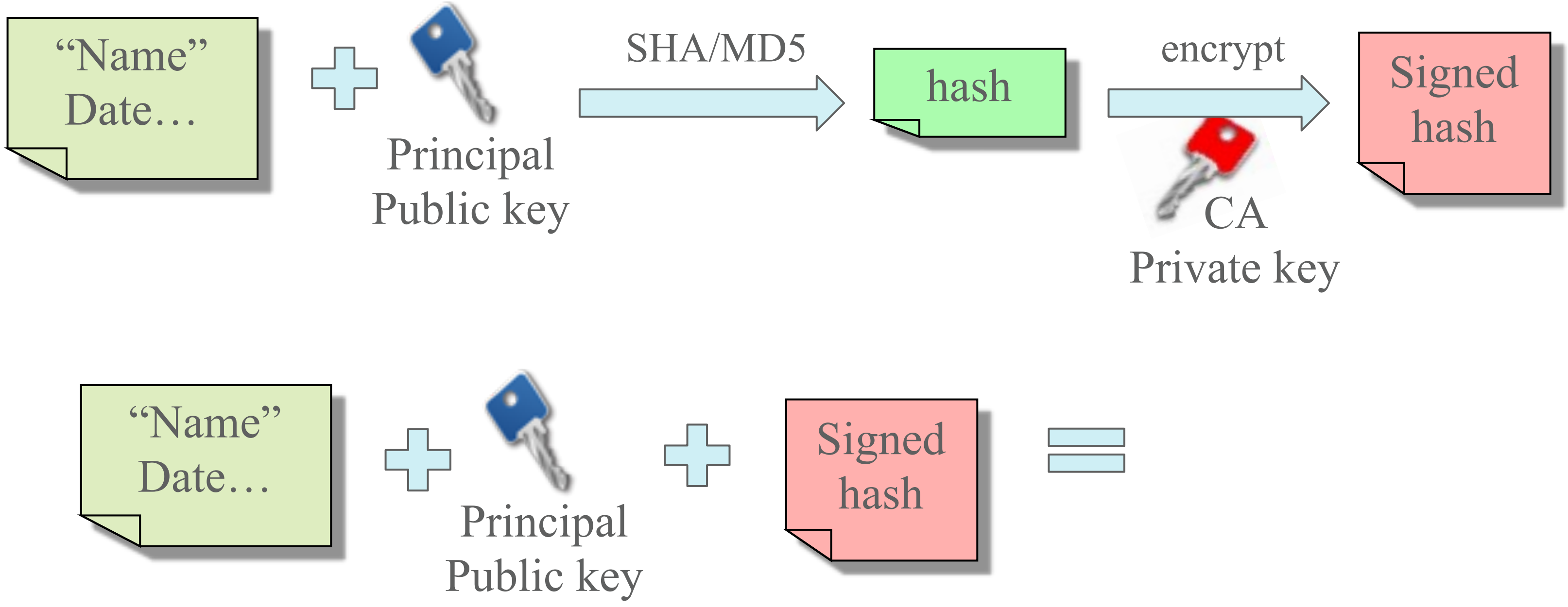
Digital Signature Basics – Certificate Creation

A Certificate Authority (CA) issues a certificate to a Principal



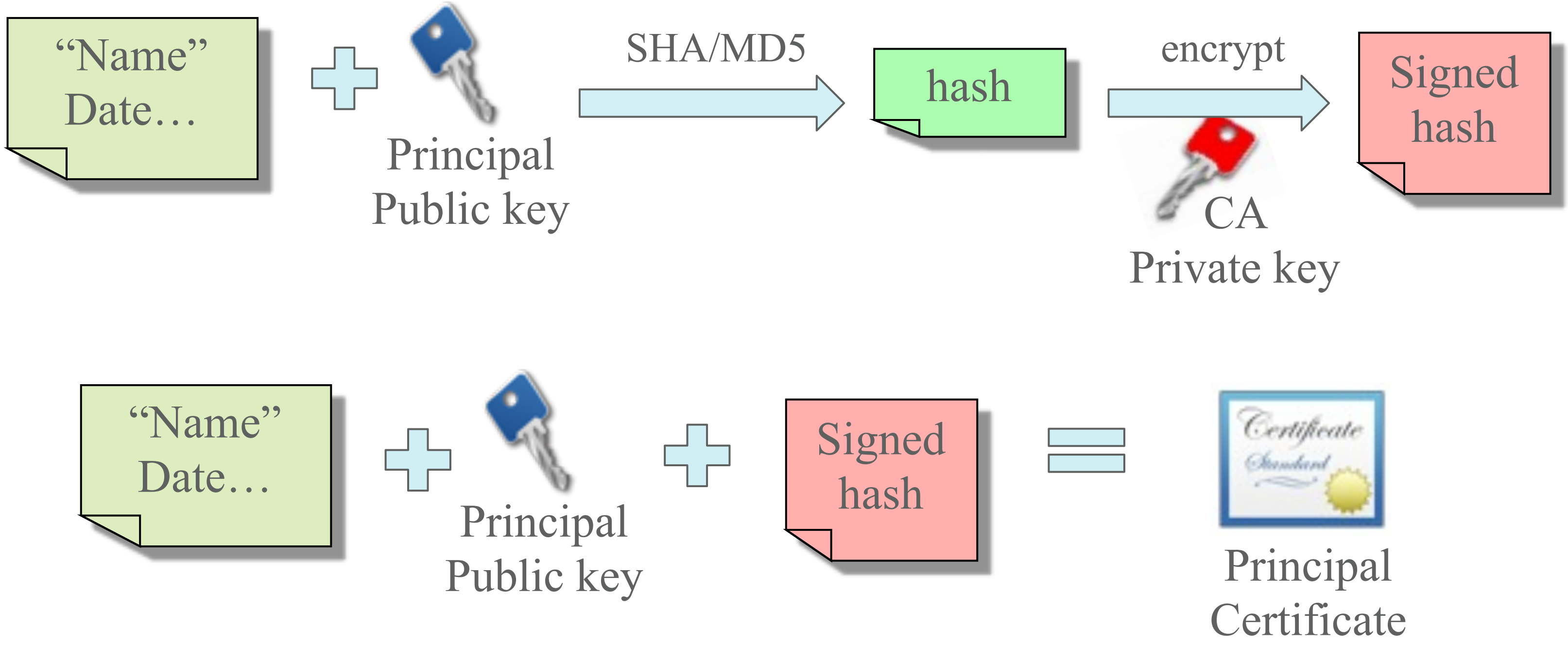
Digital Signature Basics – Certificate Creation

A Certificate Authority (CA) issues a certificate to a Principal



Digital Signature Basics – Certificate Creation

A Certificate Authority (CA) issues a certificate to a Principal

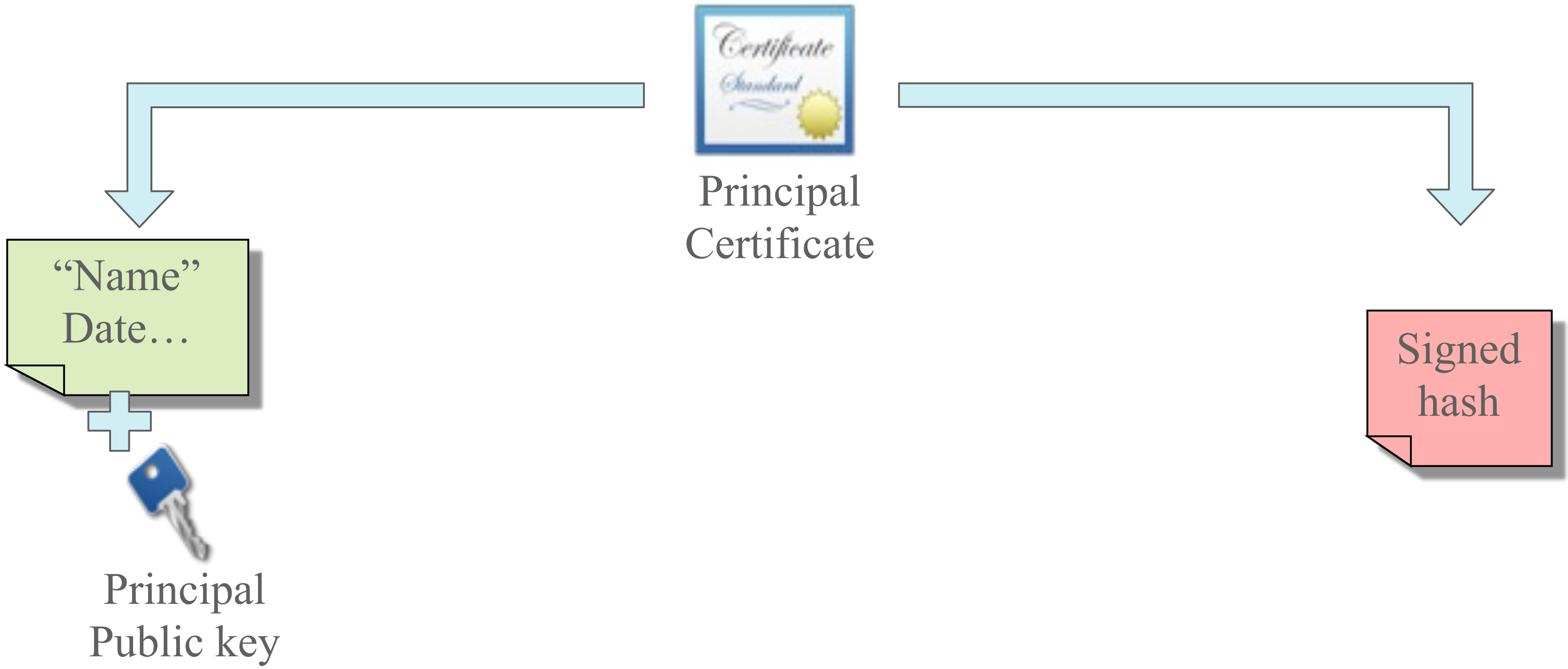


Digital Signature Basics – Cert. verification

Digital Signature Basics – Cert. verification

Principal
Certificate

Digital Signature Basics – Cert. verification



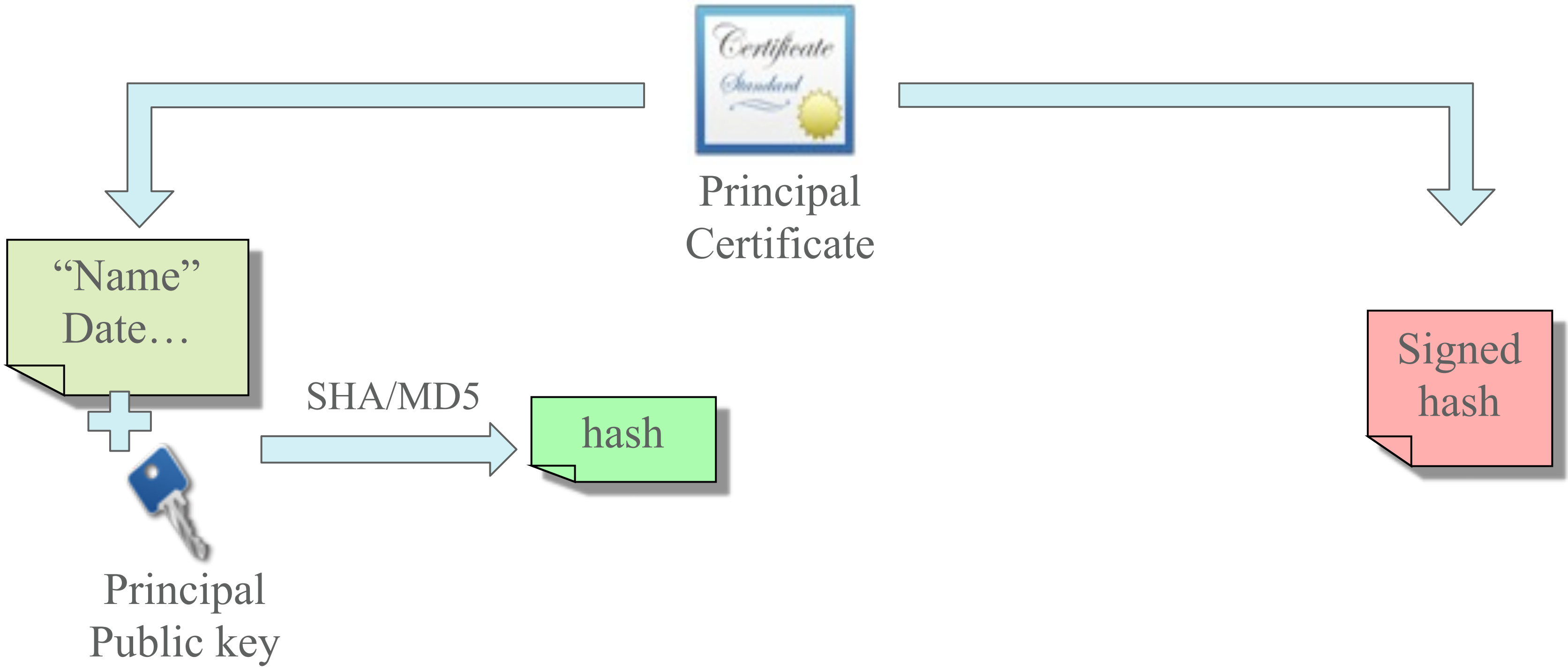
Principal Certificate

“Name” Date…

Principal Public key

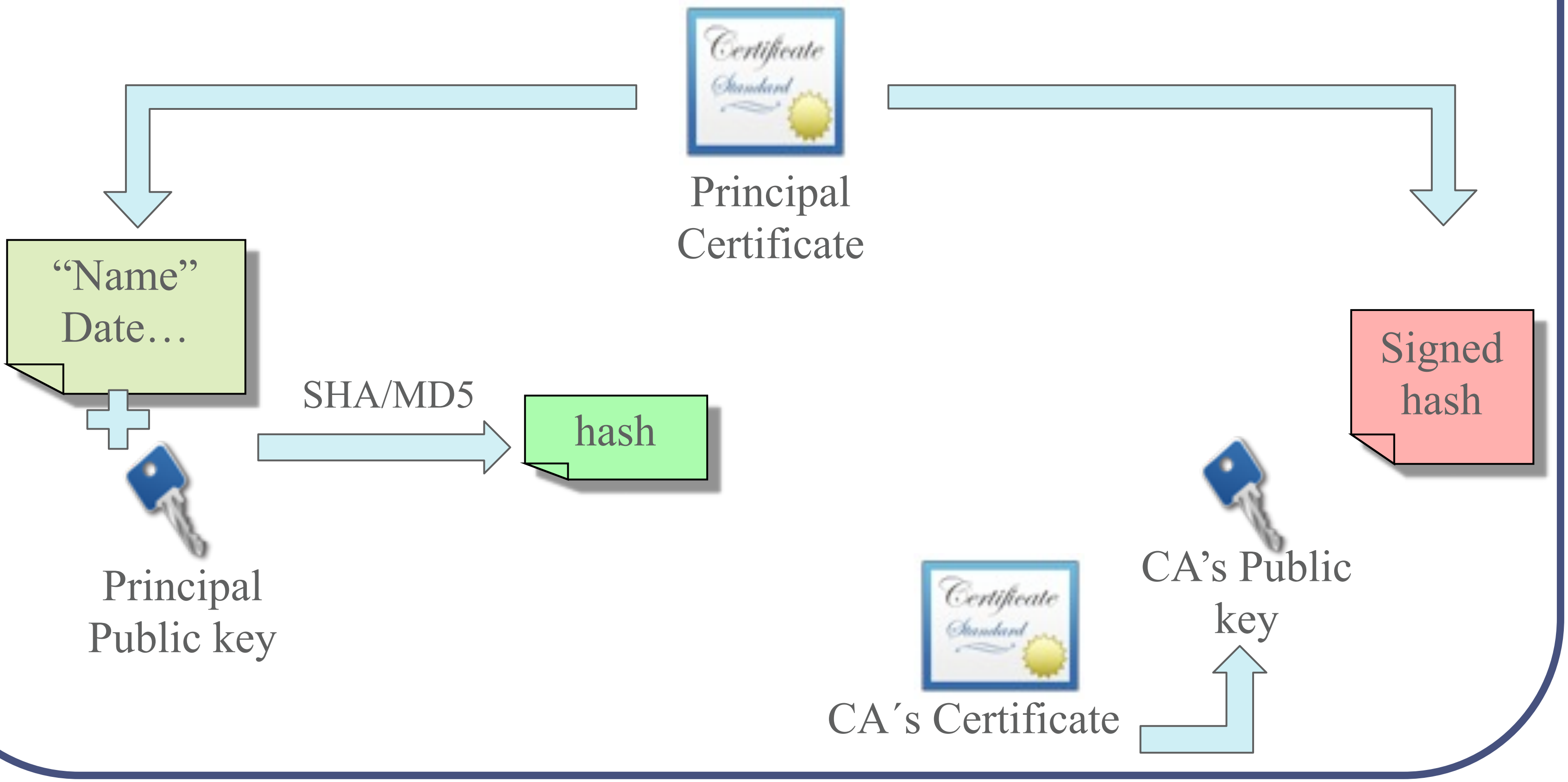
Signed hash

Digital Signature Basics – Cert. verification



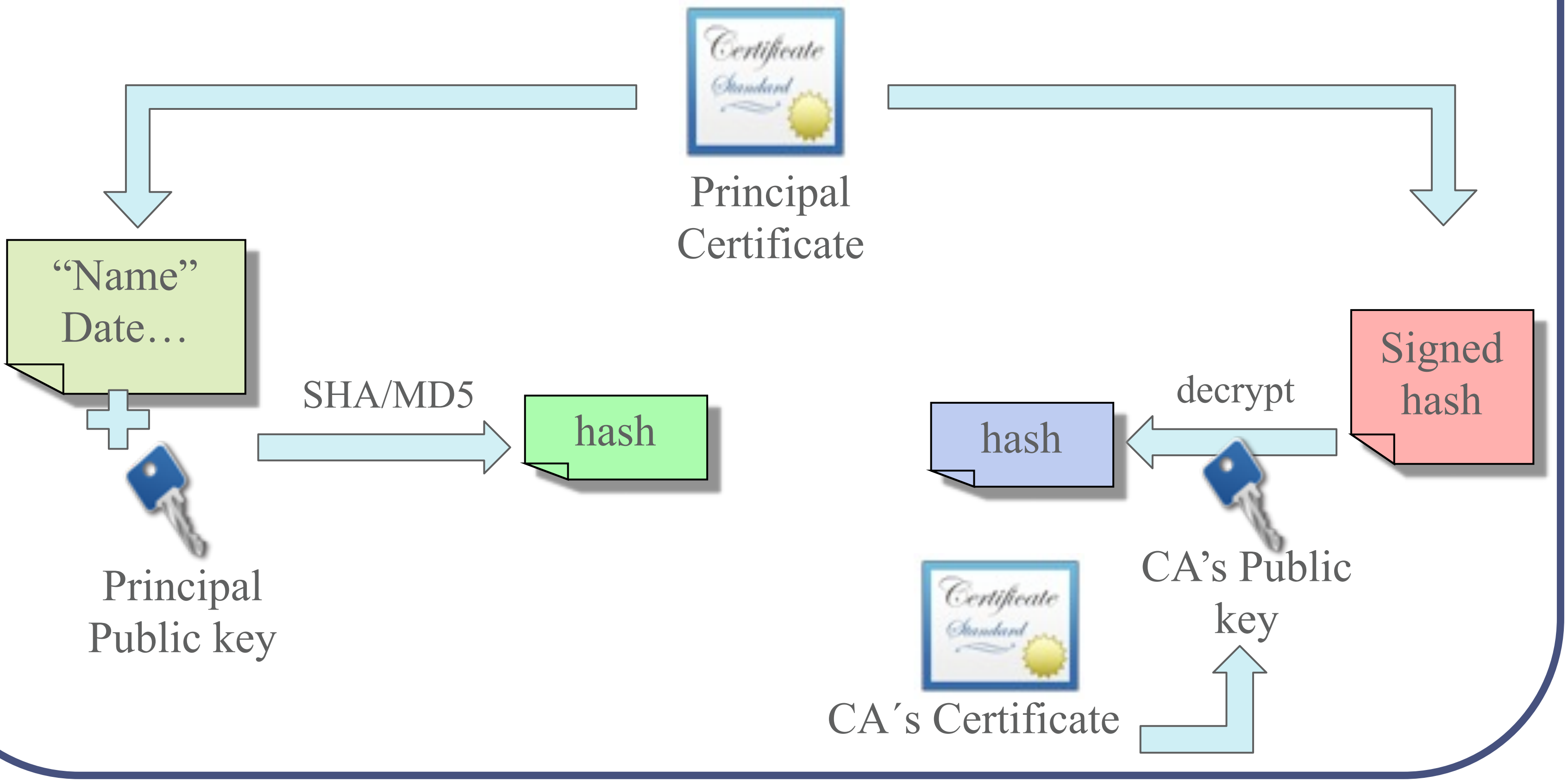
Digital Signature Basics – Cert. verification

The CA’s public key bootstraps the chain of trust…



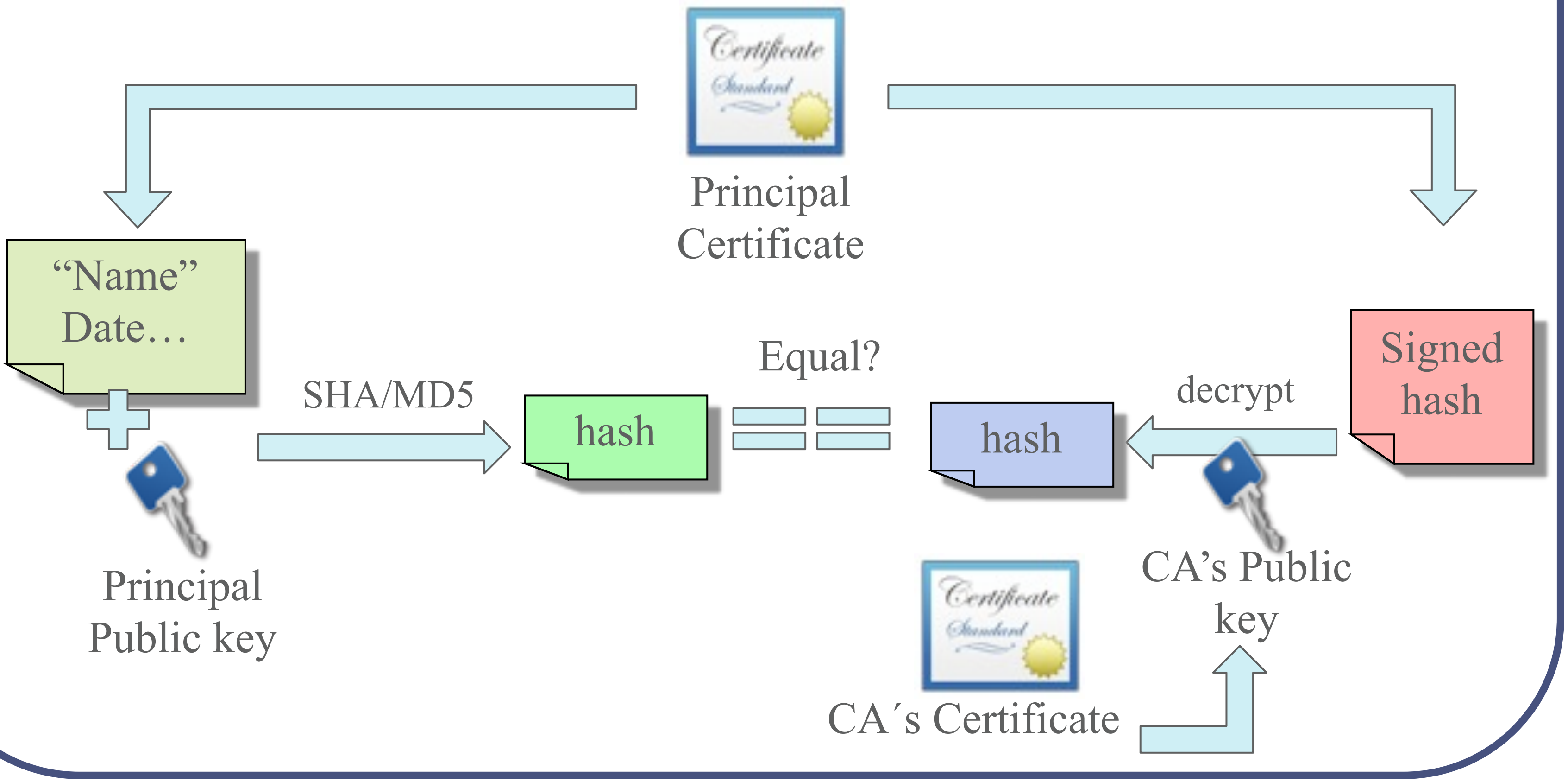
Digital Signature Basics – Cert. verification

The CA’s public key bootstraps the chain of trust…



Digital Signature Basics – Cert. verification

The CA's public key bootstraps the chain of trust…

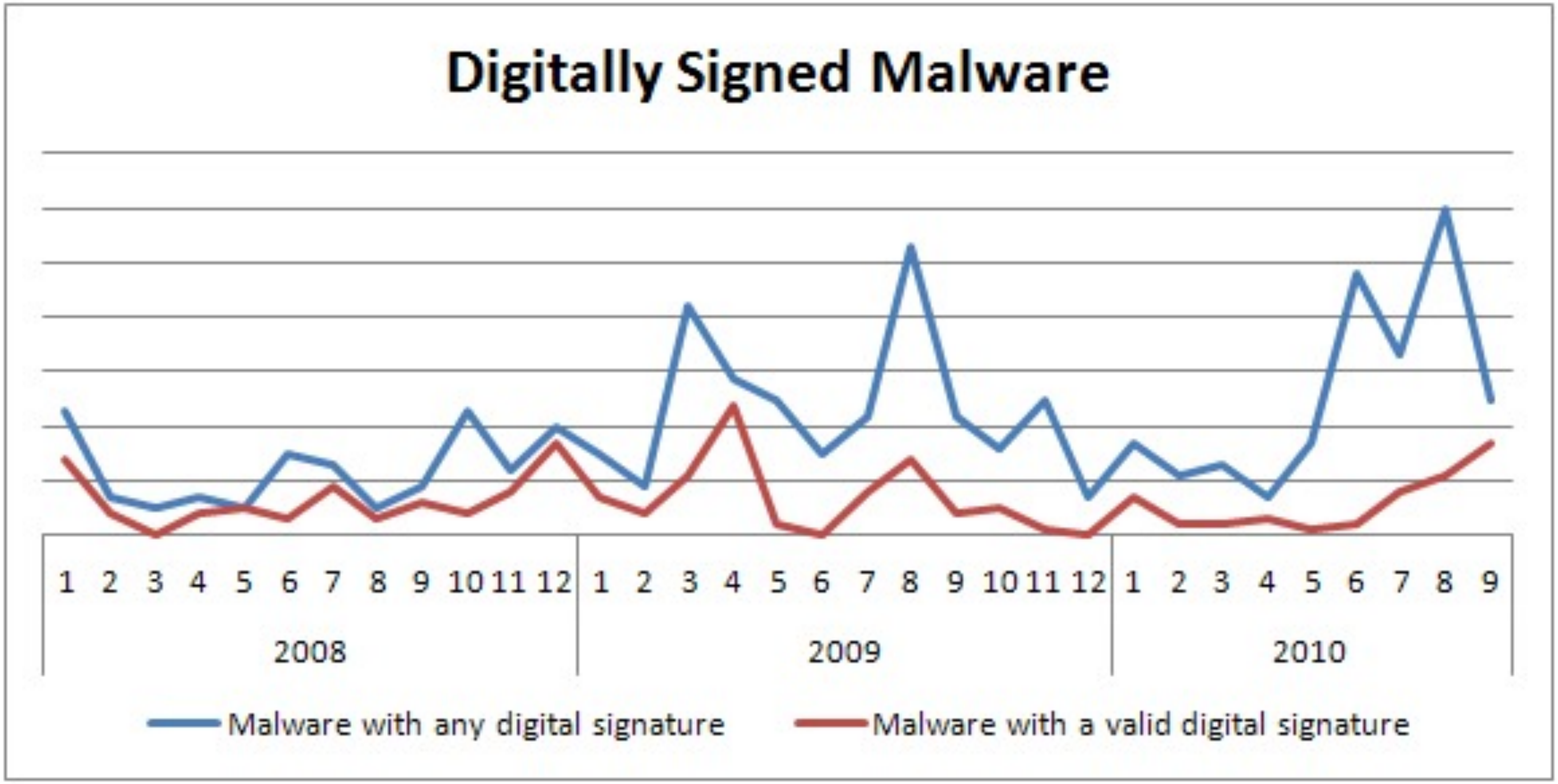


Digitally Signed Malware

Microsoft Authenticode Signature Basics

- Public-Key Cryptography Standards
  - PKCS #7 , x509, etc.
- Ensures authenticity / integrity of the EXE
  - … for the most part
- A few references…
  - “Windows Authenticode Portable Executable Signature Format” (ms docx)
  - WinVerifyTrust function (MSDN)

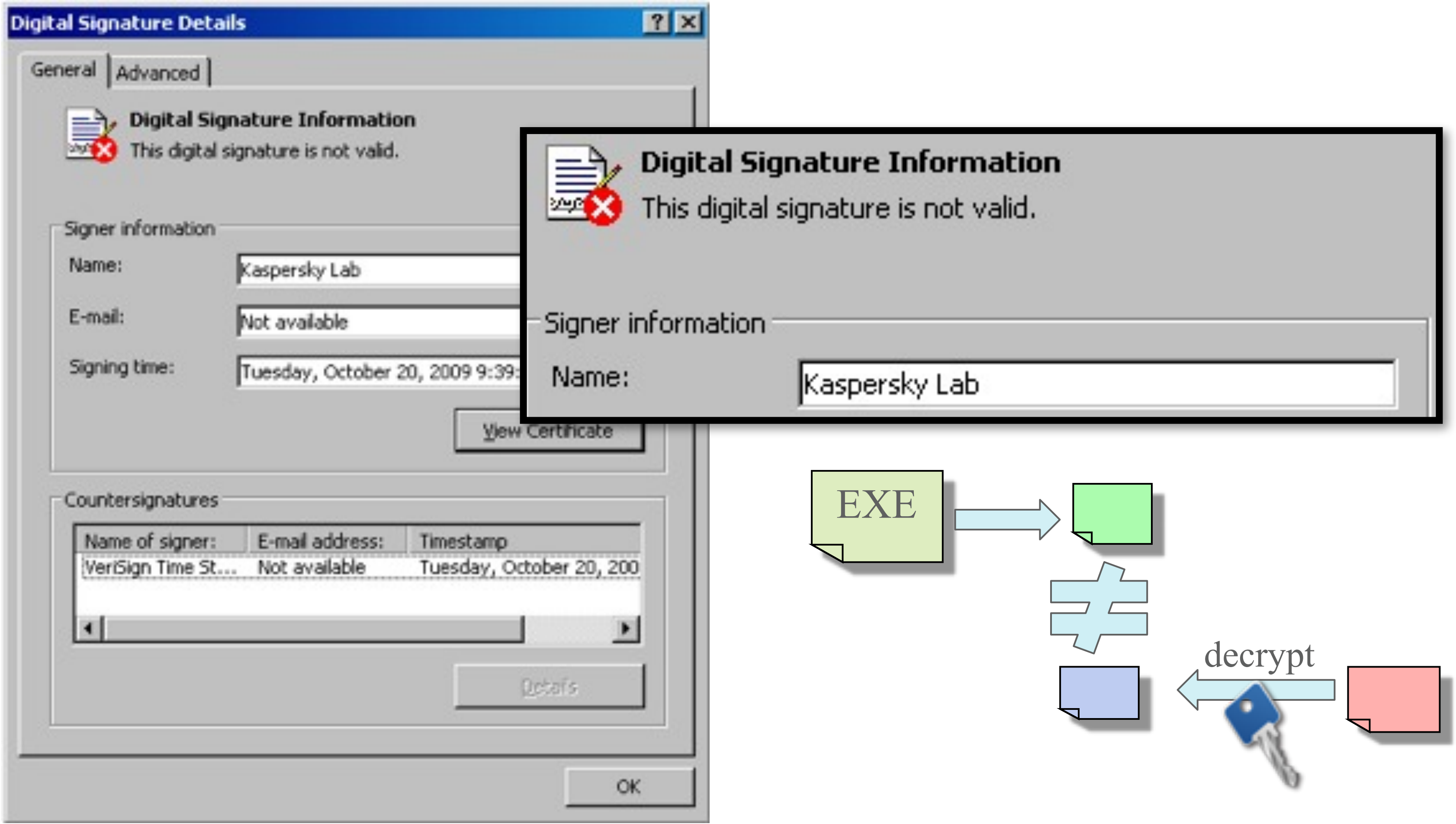
Malware samples with digital signatures



* NB: 2010/09 only up to Sept 15

Malware Digital Signature – FAIL!

- Copy / Paste -- invalid hash



Digital Signature Details

General | Advanced

Digital Signature Information
This digital signature is not valid.

Signer information

Name: Kaspersky Lab

E-mail: Not available

Signing time: Tuesday, October 20, 2009 9:39:

Countersignatures

Name of signer:	E-mail address:	Timestamp
VeriSign Time St...	Not available	Tuesday, October 20, 200

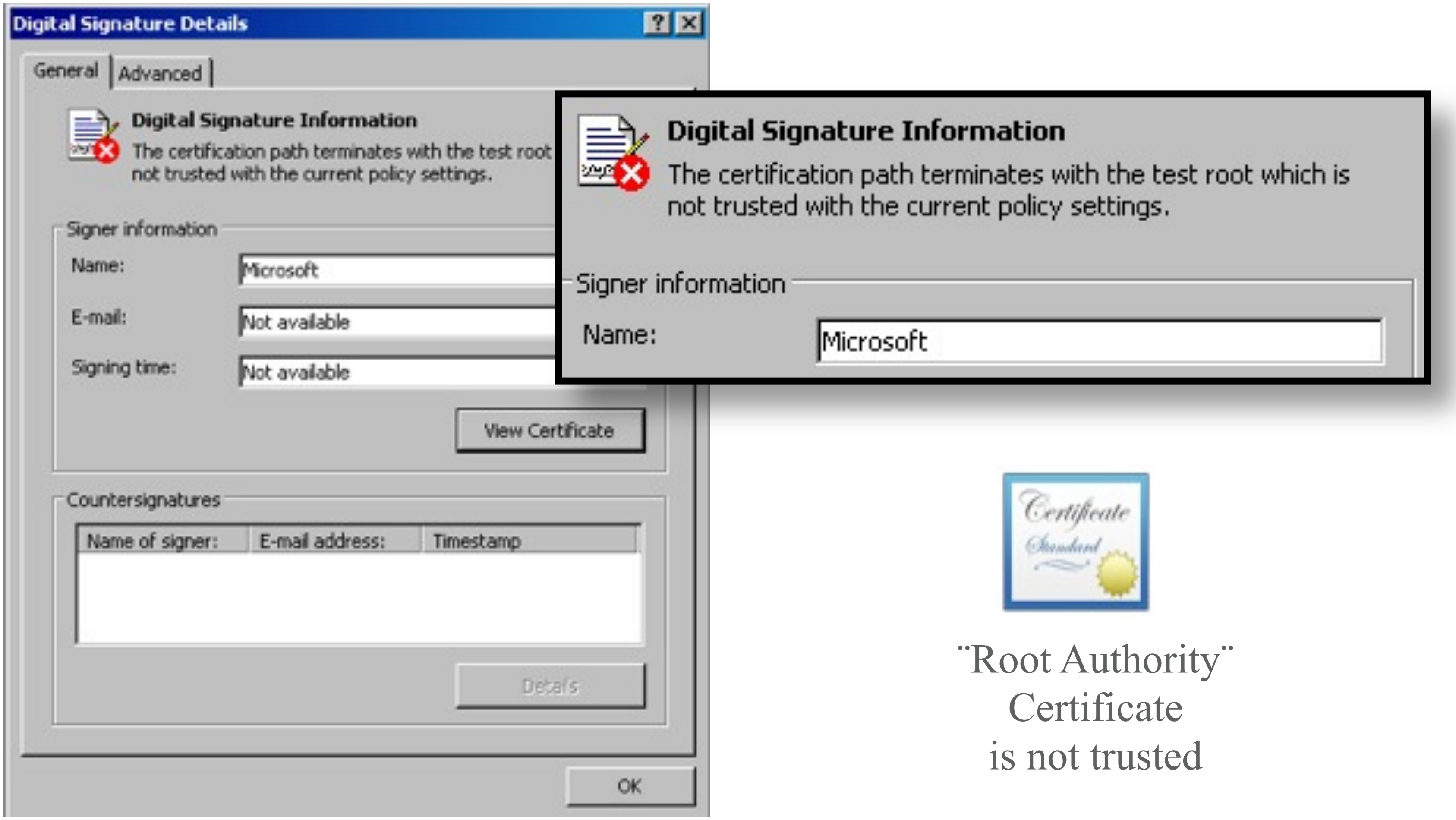
Digital Signature Information
This digital signature is not valid.

Signer information

Name: Kaspersky Lab

Malware Digital Signature – FAIL!

- MakeCert.exe – generated test certificates



Digital Signature Details

Digital Signature Information

The certification path terminates with the test root which is not trusted with the current policy settings.

Signer information

Name: Microsoft

E-mail: Not available

Signing time: Not available

Countersignatures

Name of signer:	E-mail address:	Timestamp

Digital Signature Information

The certification path terminates with the test root which is not trusted with the current policy settings.

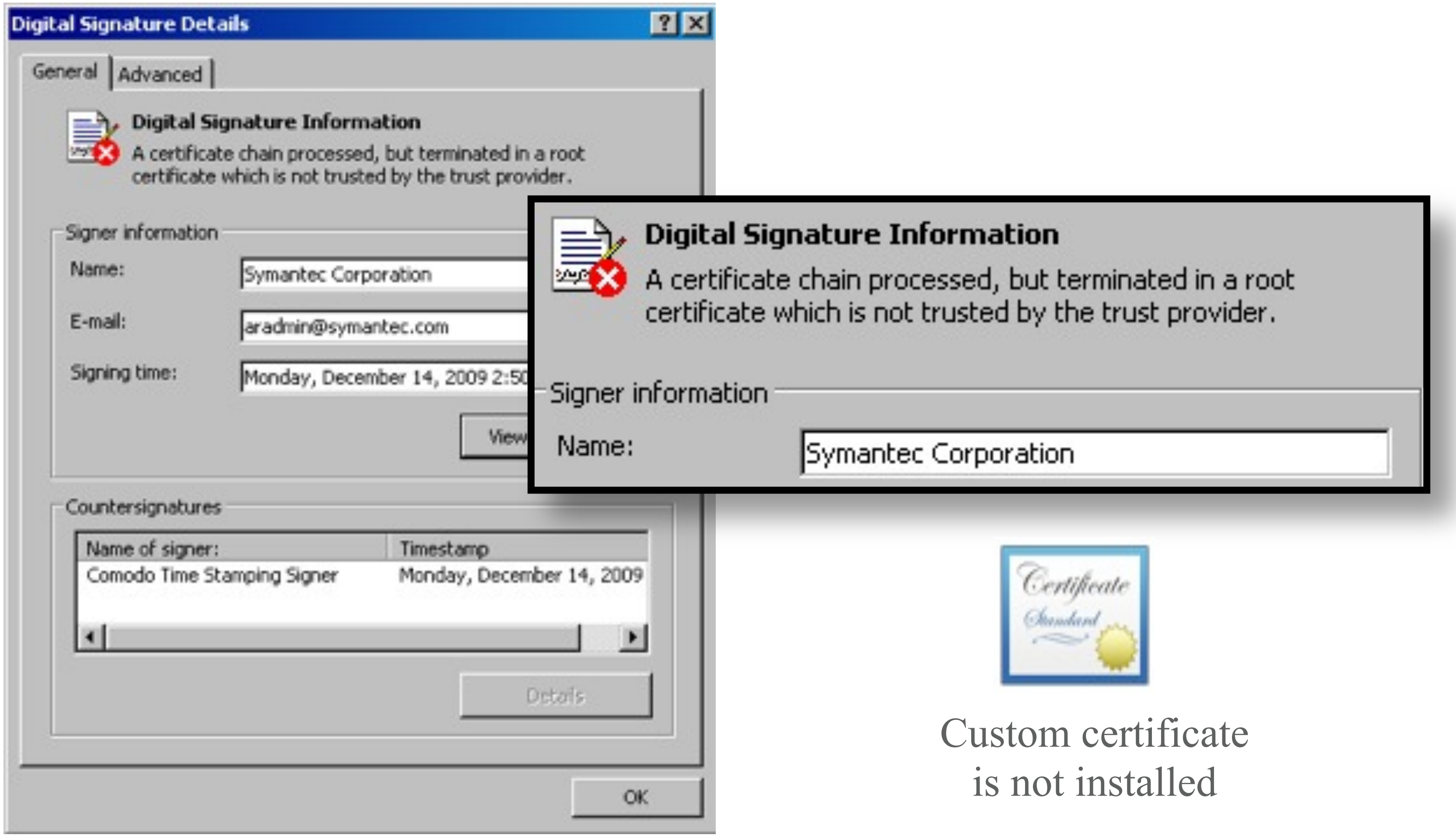
Signer information

Name: Microsoft

¨Root Authority¨
Certificate
is not trusted

Malware Digital Signature – FAIL!

- Rogue custom generated certificates



Digital Signature Details

Digital Signature Information

A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider.

Signer information

Name: Symantec Corporation

E-mail: aradmin@symantec.com

Signing time: Monday, December 14, 2009 2:50

Countersignatures

Name of signer:	Timestamp
Comodo Time Stamping Signer	Monday, December 14, 2009

Digital Signature Information

A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider.

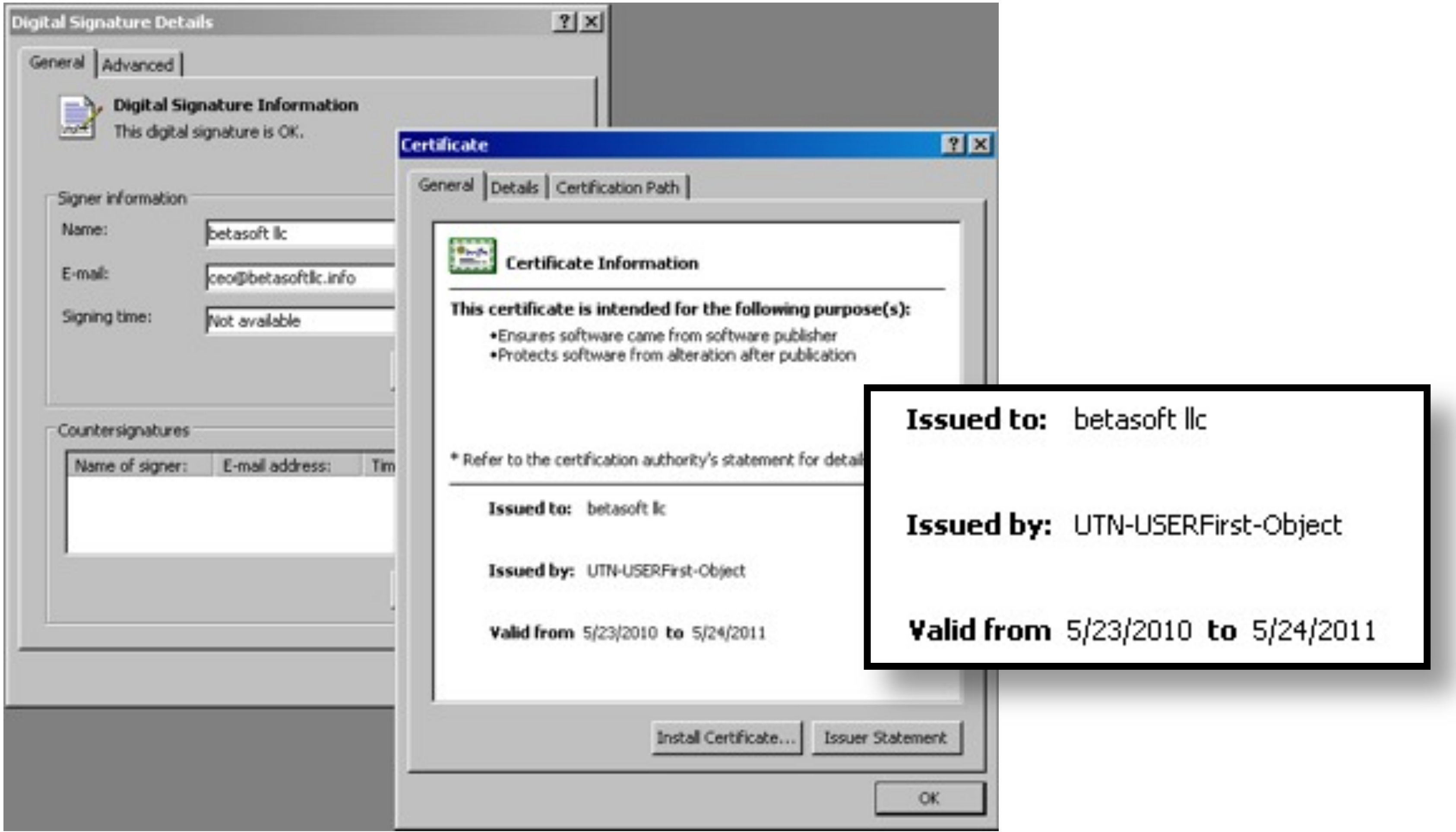
Signer information

Name: Symantec Corporation

Custom certificate
is not installed

Malware Digital Signature – OK

- Illegitimate company registration



Digital Signature Details

General | Advanced

Digital Signature Information

This digital signature is OK.

Signer information

Name: betasoft llc

E-mail: ceo@betasoftllc.info

Signing time: Not available

Countersignatures

Name of signer:	E-mail address:	Tim

Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

•Ensures software came from software publisher
•Protects software from alteration after publication

* Refer to the certification authority's statement for detail

Issued to: betasoft llc

Issued by: UTN-USERFirst-Object

Valid from 5/23/2010 **to** 5/24/2011

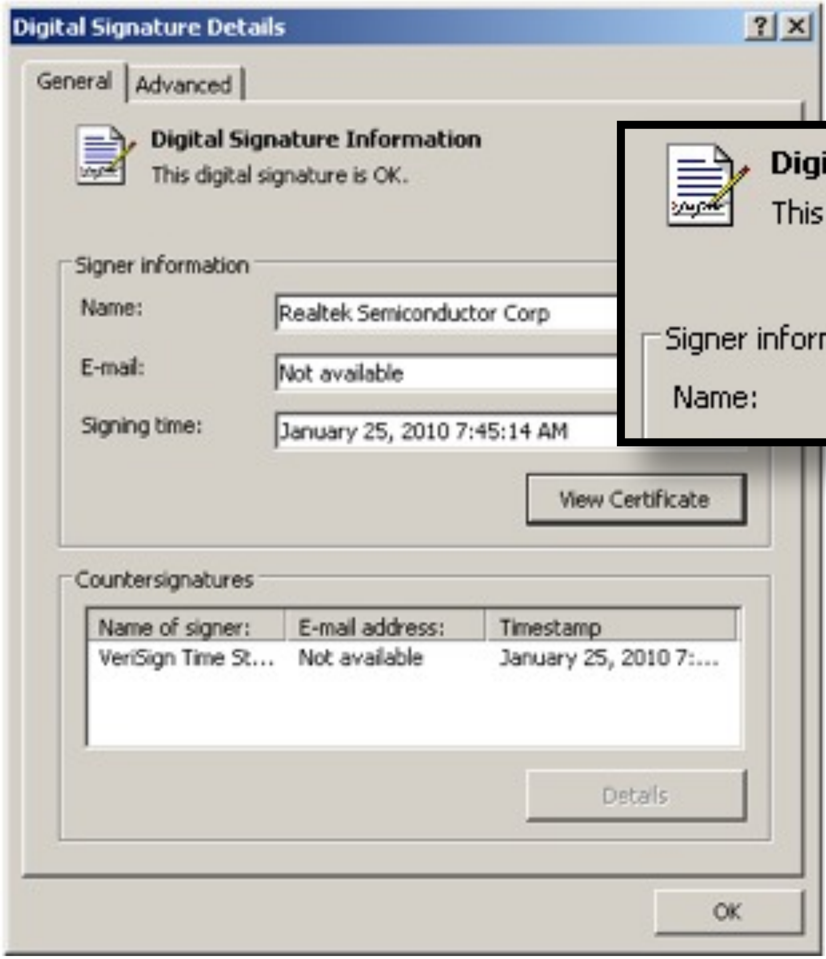
Issued to: betasoft llc

Issued by: UTN-USERFirst-Object

Valid from 5/23/2010 **to** 5/24/2011

Malware Digital Signature – OK

- Stolen/compromised certificates



Digital Signature Details

Digital Signature Information

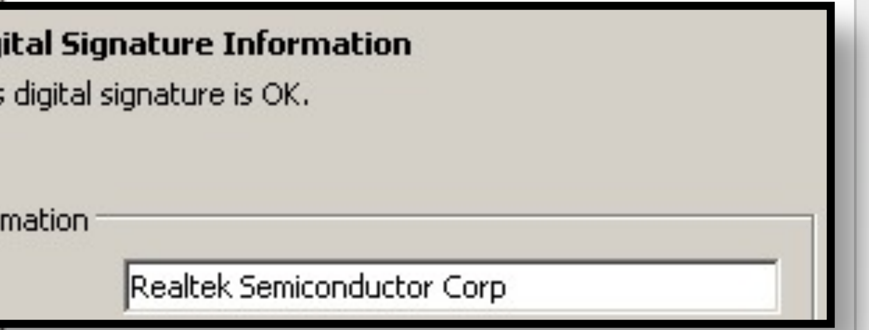
This digital signature is OK.

Signer information

Name:	Realtek Semiconductor Corp
E-mail:	Not available
Signing time:	January 25, 2010 7:45:14 AM

Countersignatures

Name of signer:	E-mail address:	Timestamp
VeriSign Time St...	Not available	January 25, 2010 7:...



Digital Signature Information

This digital signature is OK.

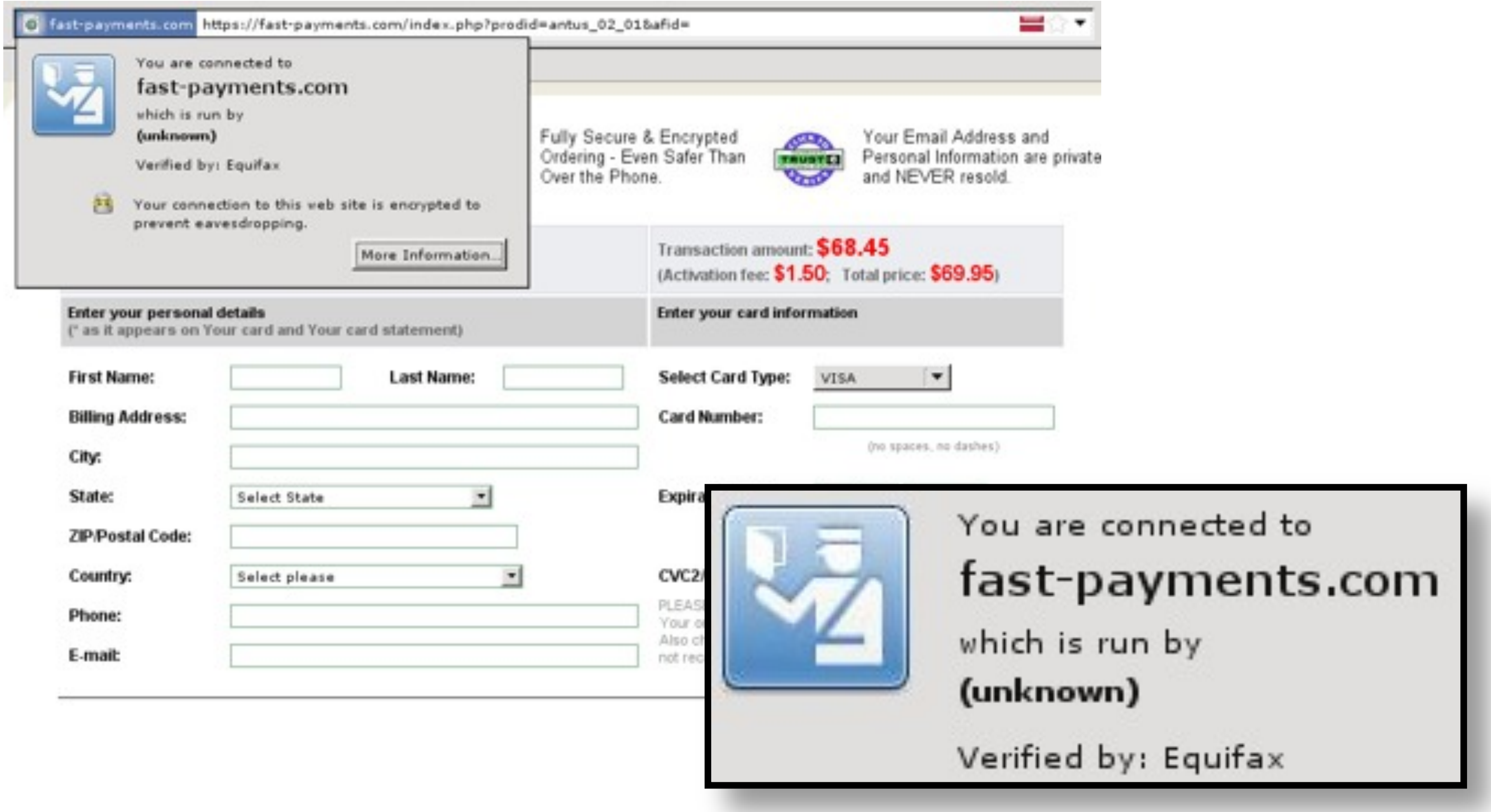
Signer information

Name: Realtek Semiconductor Corp

Principal´s Private key stolen

Online Fraud with Digital Certificates

FakeAV Payment Sites



fast-payments.com https://fast-payments.com/index.php?prodid=antus_02_01&afid=

You are connected to

fast-payments.com

which is run by

(unknown)

Verified by: Equifax

Your connection to this web site is encrypted to prevent eavesdropping.

Fully Secure & Encrypted Ordering - Even Safer Than Over the Phone.

Your Email Address and Personal Information are private and NEVER resold.

Transaction amount: $68.45

(Activation fee: $1.50; Total price: $69.95)

Enter your personal details
(* as it appears on Your card and Your card statement)

Enter your card information

First Name:		Last Name:	
Billing Address:			
City:			
State:	Select State		
ZIP/Postal Code:			
Country:	Select please		
Phone:			
E-mail:			

Select Card Type:	VISA
Card Number:	(no spaces, no dashes)
Expira	
CVC2/	

PLEAS
Your c
Also ch
not rec

You are connected to

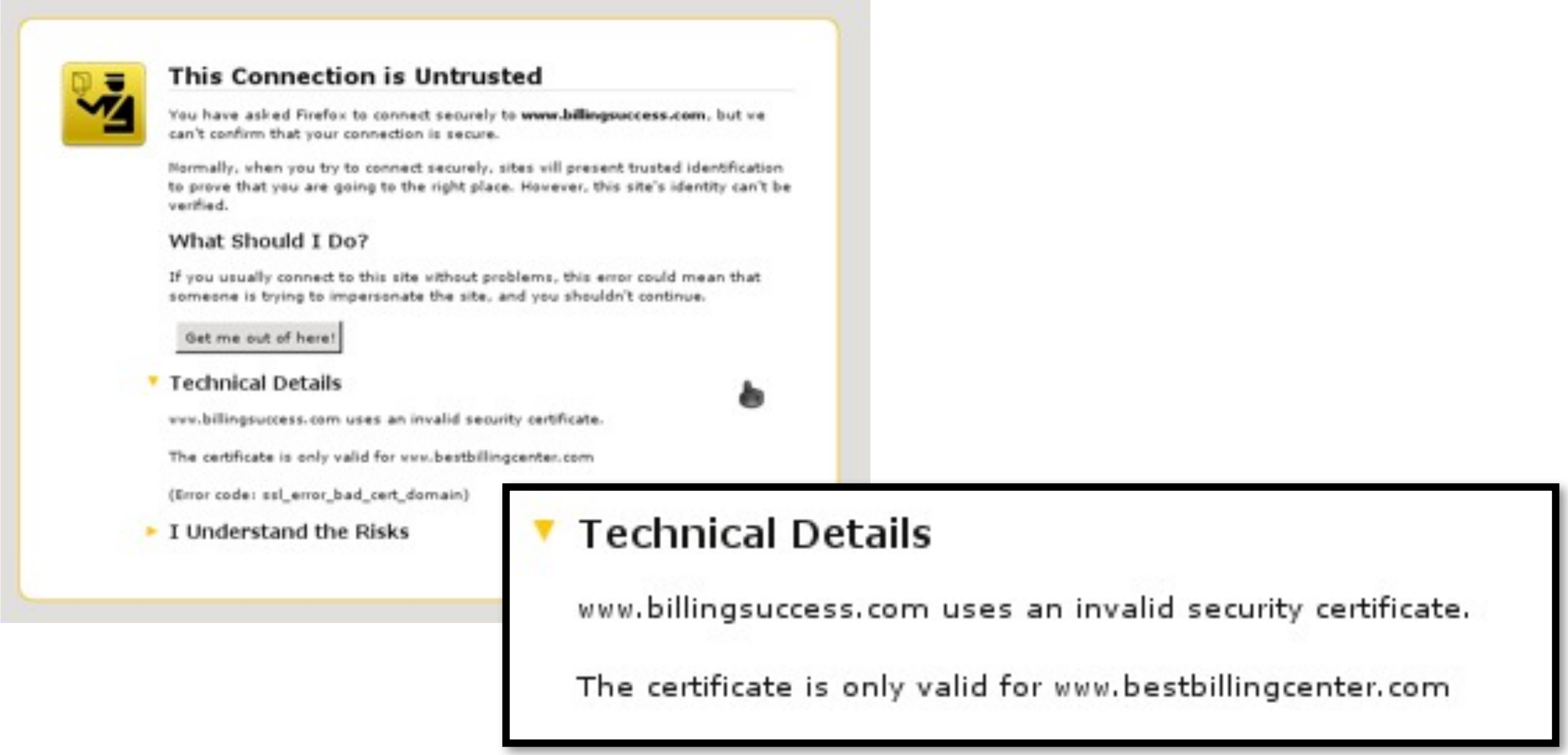
fast-payments.com

which is run by

(unknown)

Verified by: Equifax

SSL Certificate Re-use – FAIL!



This Connection is Untrusted

You have asked Firefox to connect securely to **www.billingsuccess.com**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Technical Details

www.billingsuccess.com uses an invalid security certificate.

The certificate is only valid for www.bestbillingcenter.com

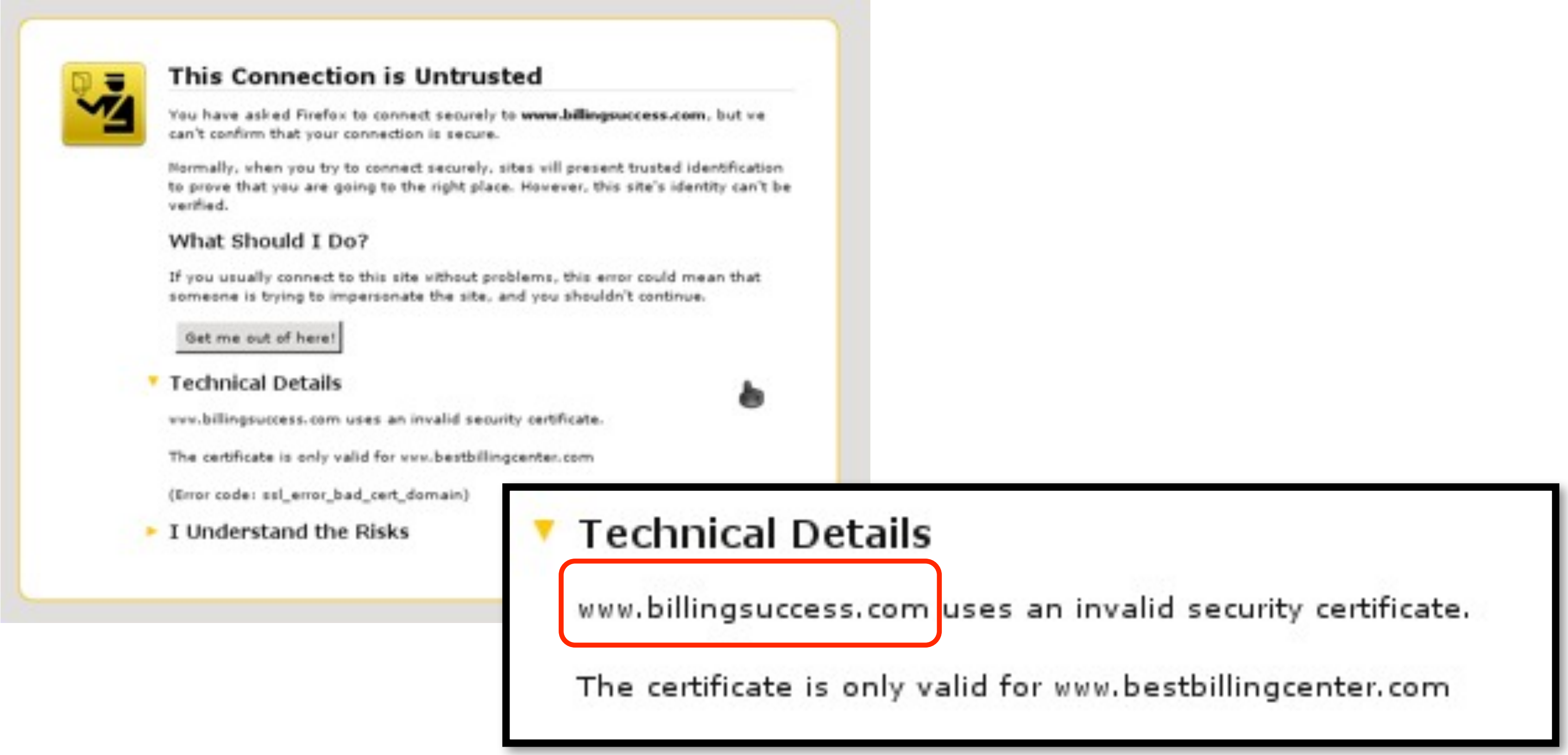
(Error code: ssl_error_bad_cert_domain)

Technical Details

www.billingsuccess.com uses an invalid security certificate.

The certificate is only valid for www.bestbillingcenter.com

SSL Certificate Re-use – FAIL!



This Connection is Untrusted

You have asked Firefox to connect securely to **www.billingsuccess.com**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

▼ Technical Details

www.billingsuccess.com uses an invalid security certificate.

The certificate is only valid for www.bestbillingcenter.com

(Error code: ssl_error_bad_cert_domain)

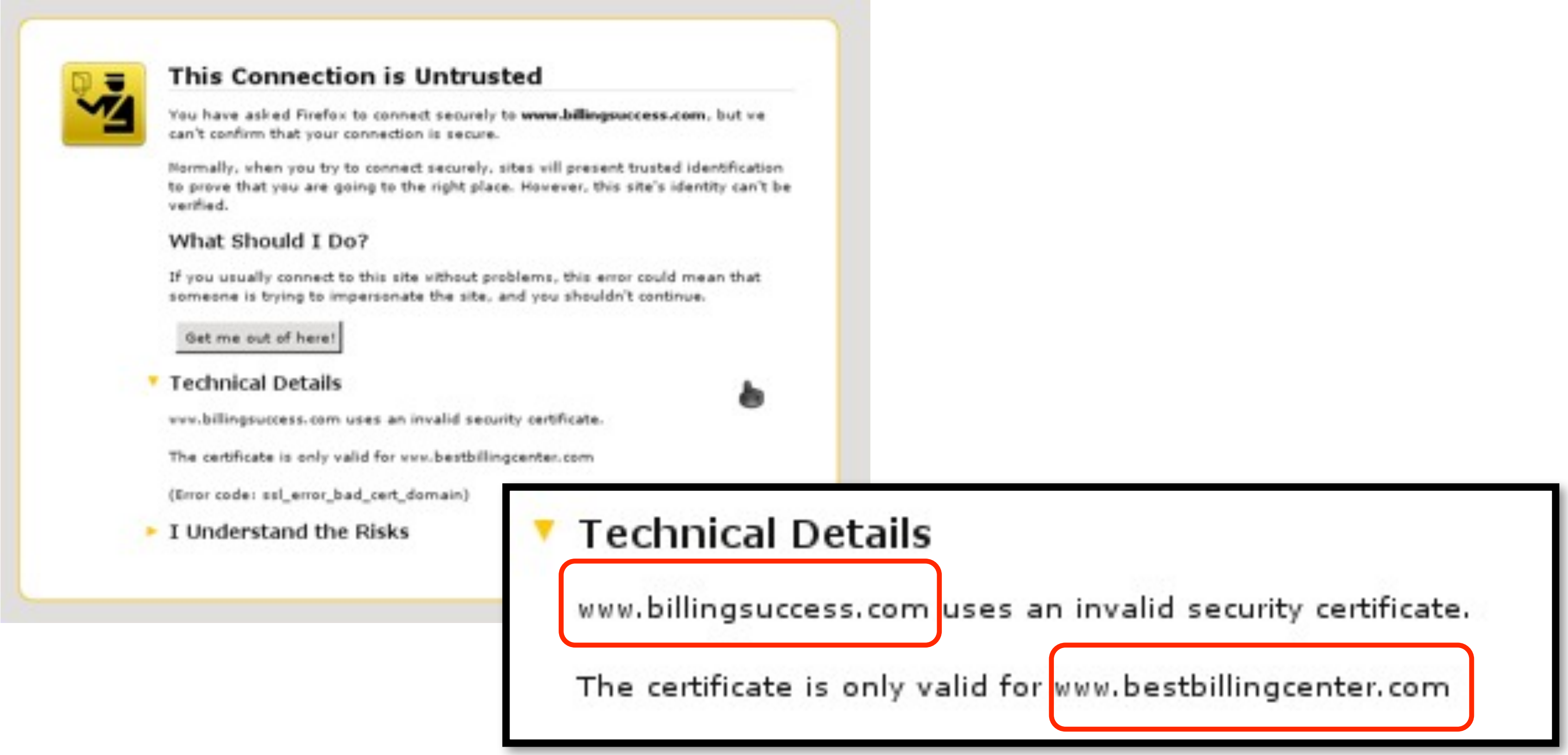
► I Understand the Risks

▼ Technical Details

www.billingsuccess.com uses an invalid security certificate.

The certificate is only valid for www.bestbillingcenter.com

SSL Certificate Re-use – FAIL!



This Connection is Untrusted

You have asked Firefox to connect securely to **www.billingsuccess.com**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Technical Details

www.billingsuccess.com uses an invalid security certificate.

The certificate is only valid for www.bestbillingcenter.com

(Error code: ssl_error_bad_cert_domain)

Technical Details

www.billingsuccess.com uses an invalid security certificate.

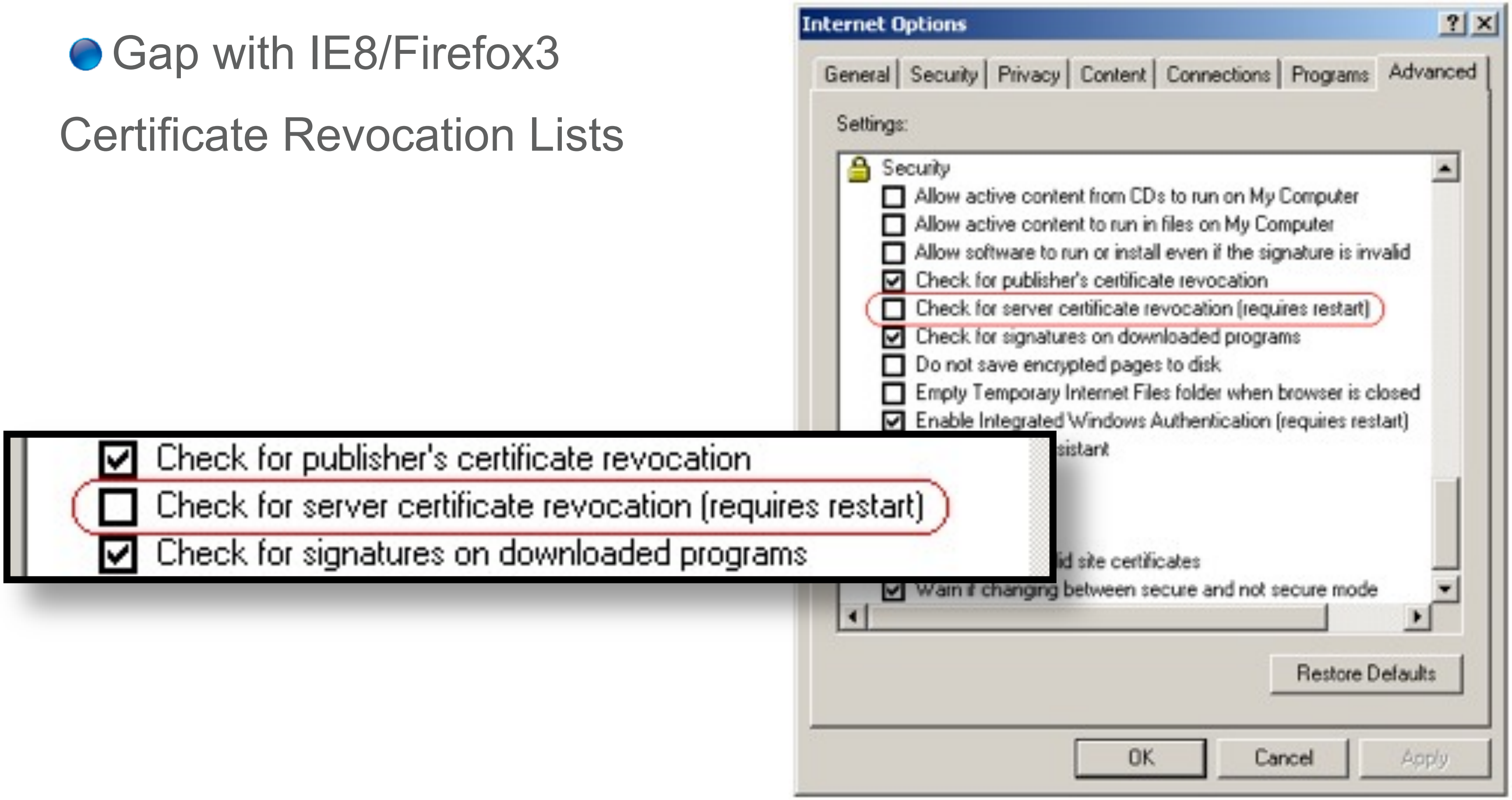
The certificate is only valid for www.bestbillingcenter.com

Implementation issues

Revocation Issues – Safe Defaults

- Major browsers lack safe defaults
  - Gap with IE8/Firefox3

Certificate Revocation Lists



Internet Options

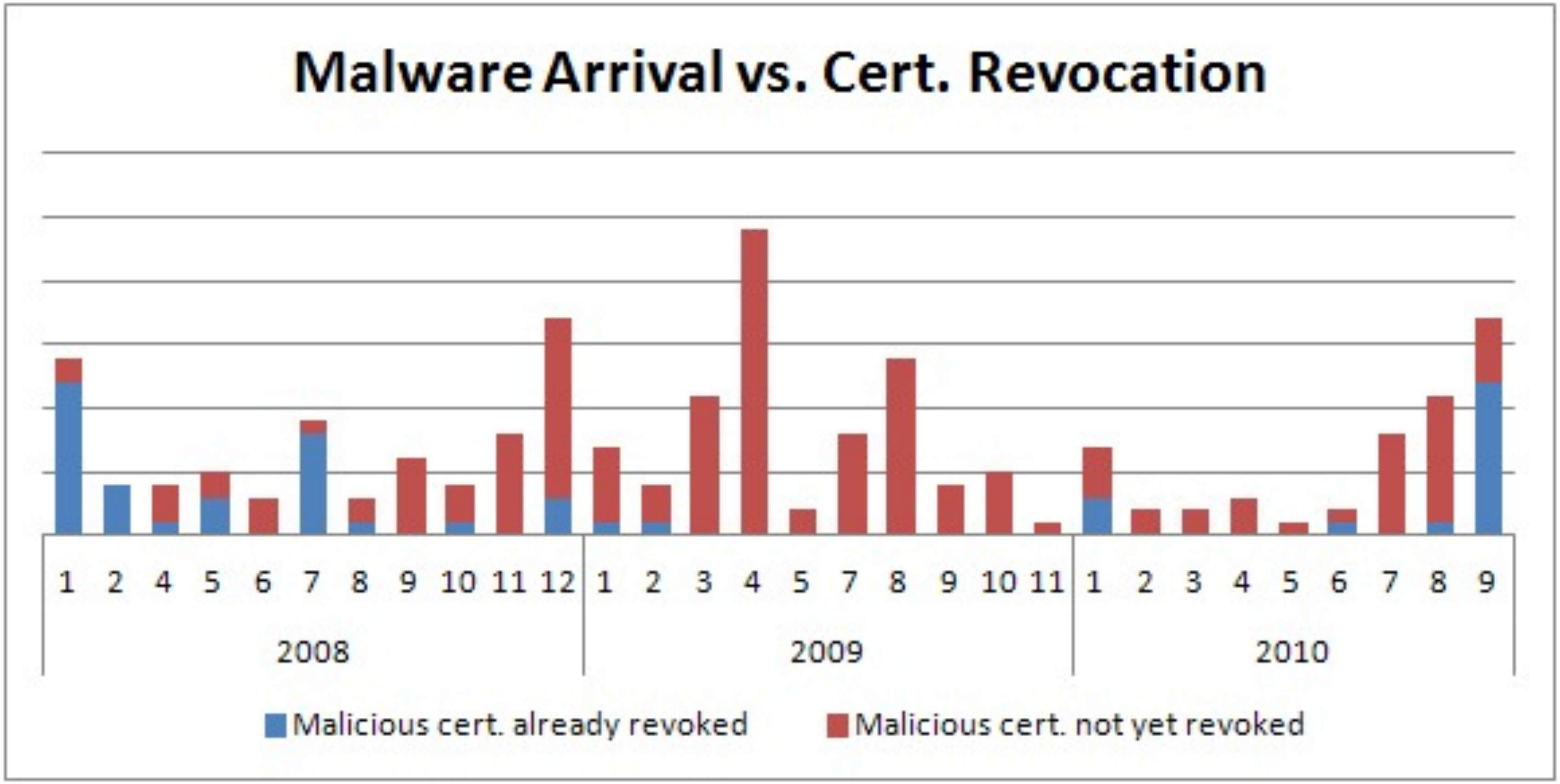
Settings:

Security

- □ Allow active content from CDs to run on My Computer
- □ Allow active content to run in files on My Computer
- □ Allow software to run or install even if the signature is invalid
- ☑ Check for publisher's certificate revocation
- □ Check for server certificate revocation (requires restart)
- ☑ Check for signatures on downloaded programs
- □ Do not save encrypted pages to disk
- □ Empty Temporary Internet Files folder when browser is closed
- ☑ Enable Integrated Windows Authentication (requires restart)
- sistant
- id site certificates
- ☑ Warn if changing between secure and not secure mode

- ☑ Check for publisher's certificate revocation
- □ Check for server certificate revocation (requires restart)
- ☑ Check for signatures on downloaded programs

Revocation Issues – Response Time

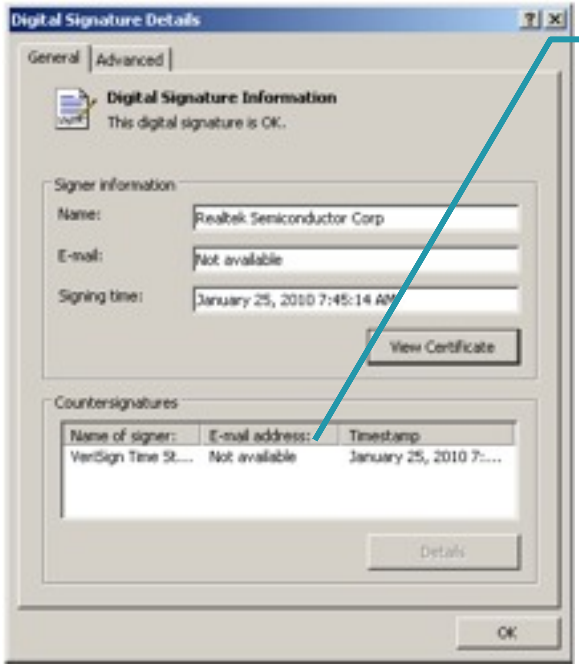


* NB: 2010/09 only up to Sept 15

SOPHOS

Verification Issues – Permanent Timestamping

- Authenticode timestamps preserve signature indefinitely



Digital Signature Details

Digital Signature Information

This digital signature is OK.

Signer information

Name: Realtek Semiconductor Corp

E-mail: Not available

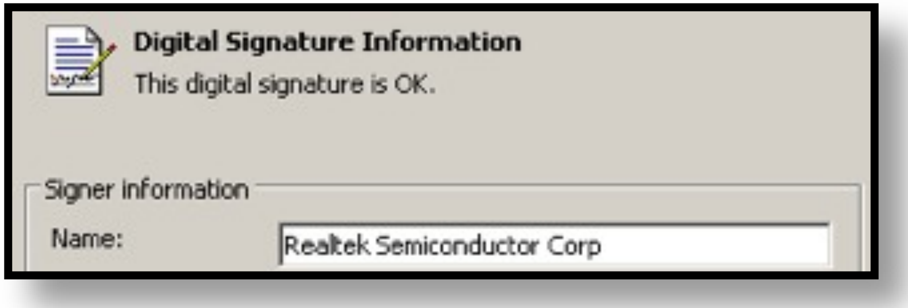
Signing time: January 25, 2010 7:45:14 AM

Countersignatures

Name of signer:	E-mail address:	Timestamp
VeriSign Time St...	Not available	January 25, 2010 7:...

Signature Timestamp Jan 25, 2010

Certificate Revoked July 16, 2010



Digital Signature Information

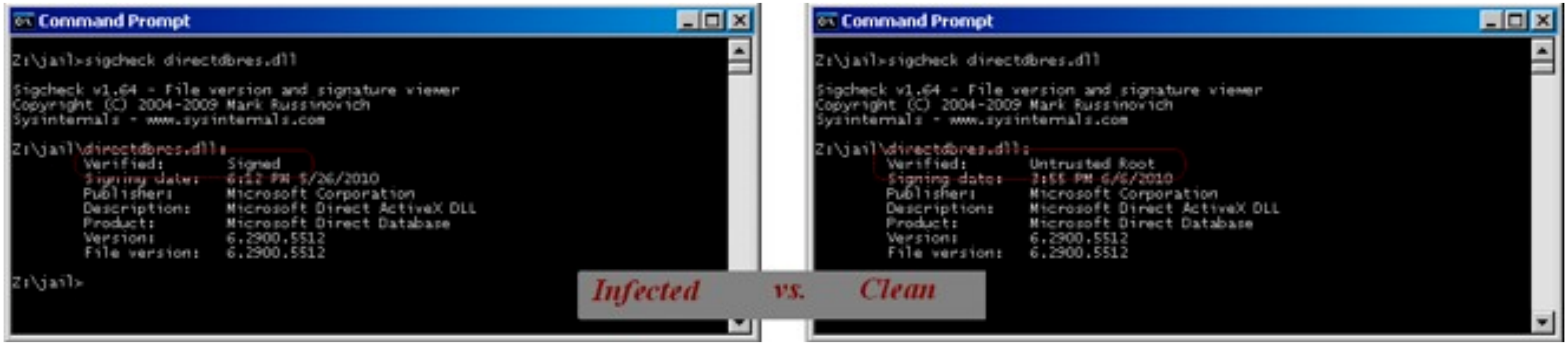
This digital signature is OK.

Signer information

Name: Realtek Semiconductor Corp

Verification Issues – Any Root Cert. Will Do…

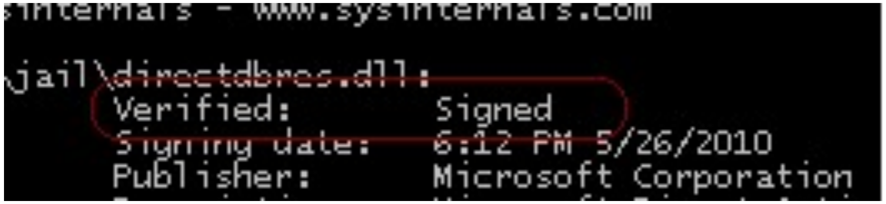
- Troj/BHO-QP installs a rogue “Verisign” root certificate



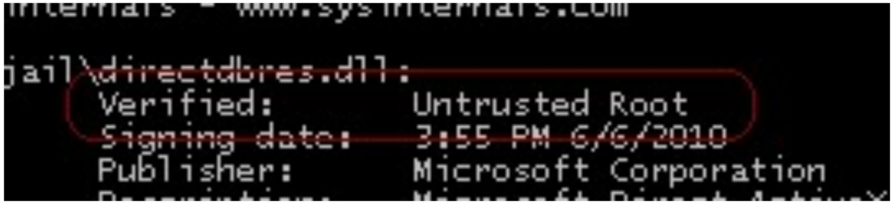
```
Command Prompt

Z:\jail>sigcheck directdbres.dll

Sigcheck v1.64 - File version and signature viewer
Copyright (C) 2004-2009 Mark Russinovich
Sysinternals - www.sysinternals.com

Z:\jail\directdbres.dll:
        Verified:       Signed
        Signing date:   6:12 PM 5/26/2010
        Publisher:      Microsoft Corporation
        Description:    Microsoft Direct ActiveX DLL
        Product:        Microsoft Direct Database
        Version:        6.2900.5512
        File version:   6.2900.5512

Z:\jail>
```

```
Command Prompt

Z:\jail>sigcheck directdbres.dll

Sigcheck v1.64 - File version and signature viewer
Copyright (C) 2004-2009 Mark Russinovich
Sysinternals - www.sysinternals.com

Z:\jail\directdbres.dll:
        Verified:       Untrusted Root
        Signing date:   3:55 PM 6/6/2010
        Publisher:      Microsoft Corporation
        Description:    Microsoft Direct ActiveX DLL
        Product:        Microsoft Direct Database
        Version:        6.2900.5512
        File version:   6.2900.5512
```

Infected vs. *Clean*



```
sinternals - www.sysinternals.com

jail\directdbres.dll:
  Verified:         Signed
  Signing date:     6:12 PM 5/26/2010
  Publisher:        Microsoft Corporation
```



```
internals - www.sysinternals.com

jail\directdbres.dll:
  Verified:         Untrusted Root
  Signing date:     3:55 PM 6/6/2010
  Publisher:        Microsoft Corporation
```

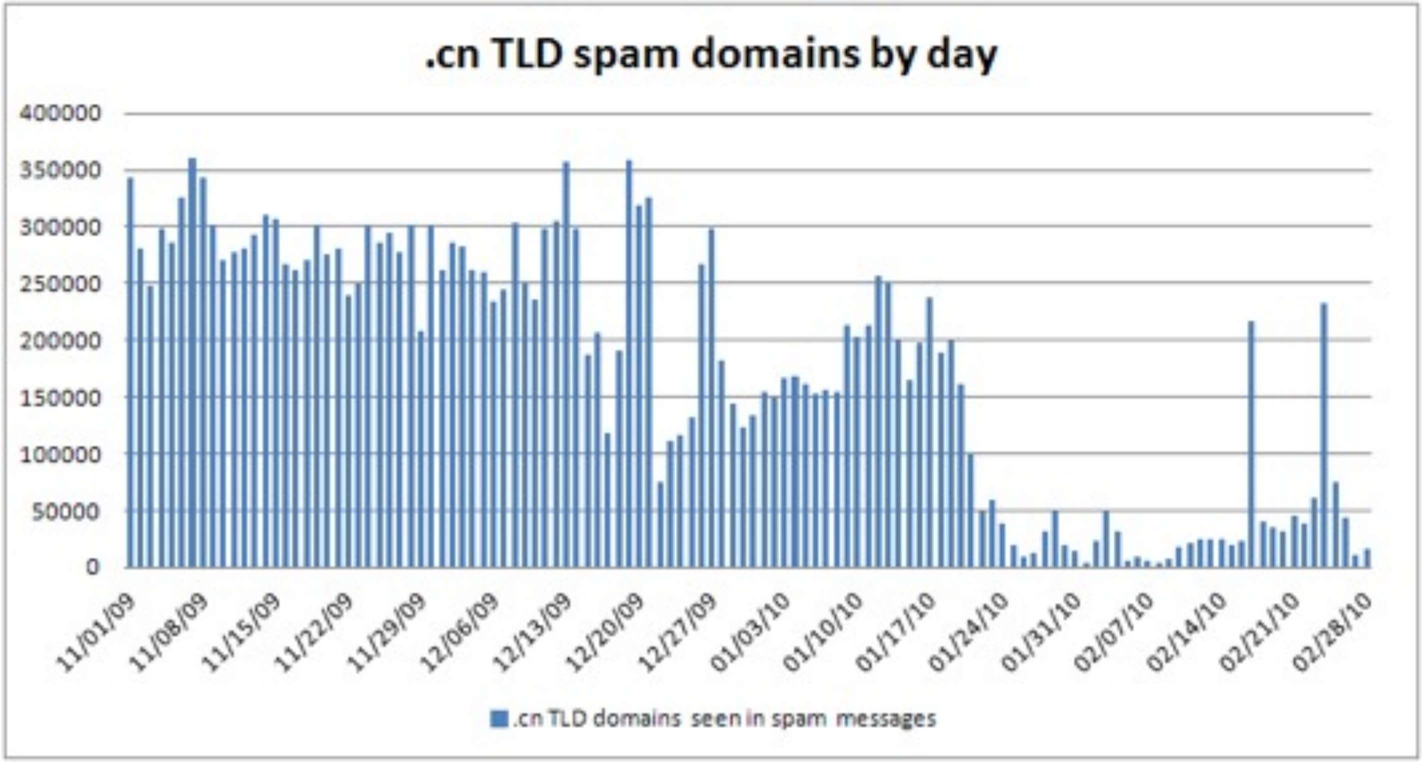
Rogue ¨Verisign¨
Certificate installed

Rogue ¨Verisign¨
Certificate absent

What have we learned?

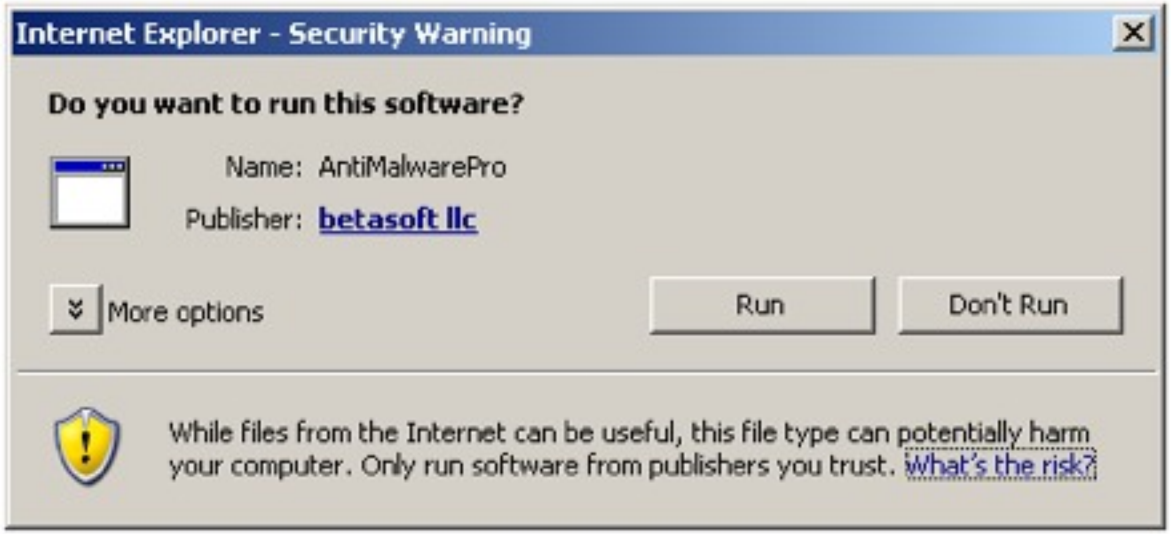
Some things that we already knew…

- Cheap and anonymous helps out the bad guys
  - … a lesson from .cn tld registrar



Some things that we already knew…

- End users will get themselves into trouble



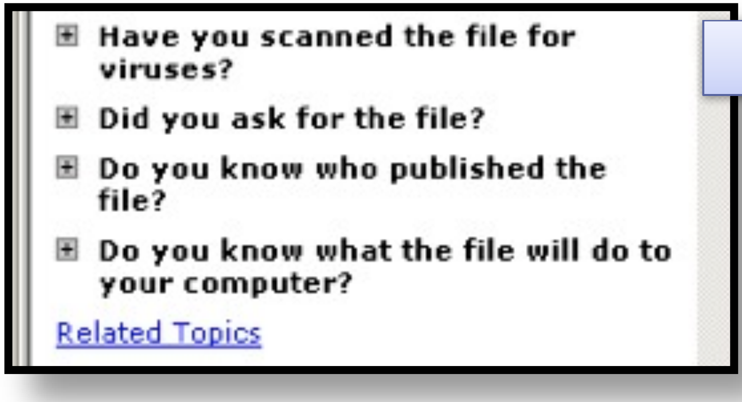
Internet Explorer - Security Warning

Do you want to run this software?

Name: AntiMalwarePro

Publisher: betasoft llc

While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust. What's the risk?



⊞ Have you scanned the file for viruses?

⊞ Did you ask for the file?

⊞ Do you know who published the file?

⊞ Do you know what the file will do to your computer?

Related Topics

No, that's what AntiMalwarePro is for!

Yup, I clicked on that 'cleanup' link.

The good folks at betasoft, of course.

It will cleanup my malware infection.

The AV Advantage… Automation

- Plenty of improper use/abuse fodder for detection
  - Broken signatures
  - Certificate x-domain reuse

The AV Advantage… Reputation Management

- Revocation is broken
- Certificate reputation
  - Fraudulent certs - Blocklist
  - CAs -- root vs. intermediate vs. compromised - Greylist

The AV Advantage… Enforcement Flexibility

- Auto-update mechanisms already in place
- Escalate decision to the IT admin

Thank you

Questions …?