Multimodal Authentication

Audun Jøsang

– *University of Oslo*

Security Aspects of Trust Service Providers

ENISA Workshop, Brussels, September 2013

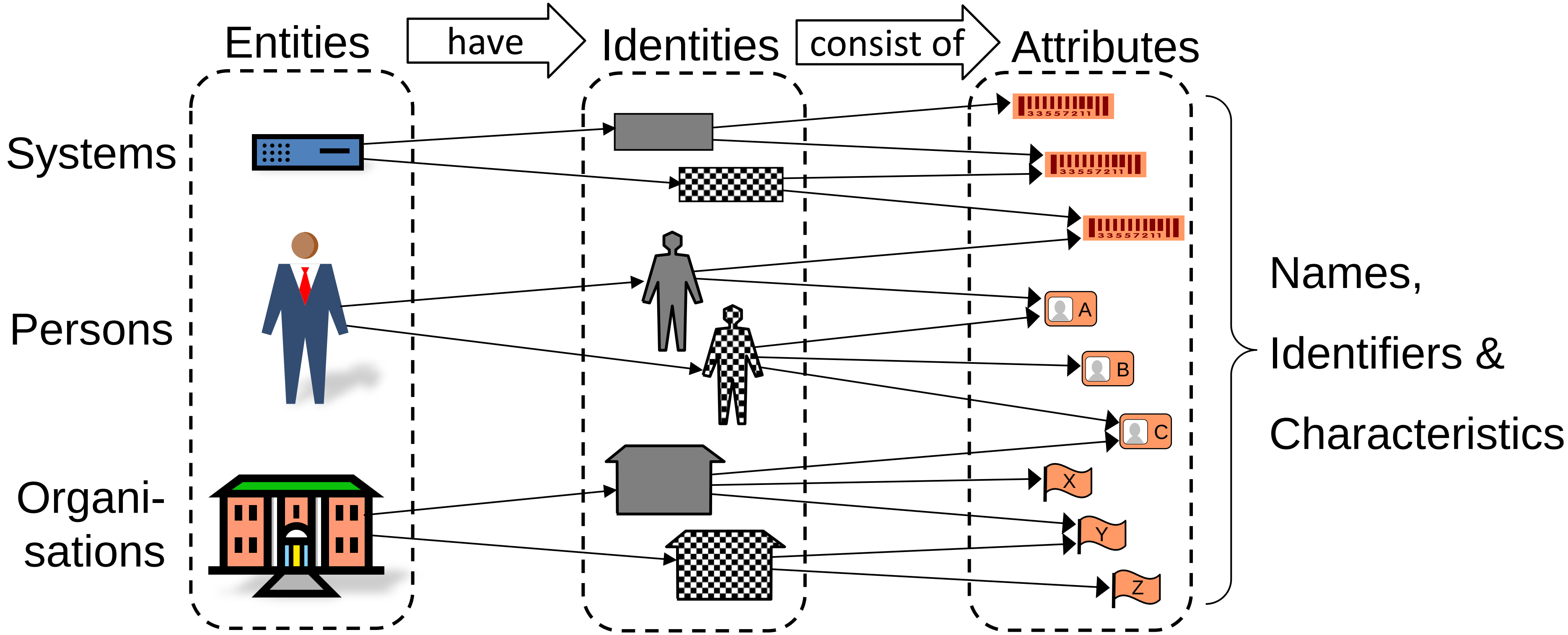
About me

- Prof. Audun Jøsang, Universitetet i Oslo
- Education
  - – Baccalaureat, Lycée Corneille France, 1981
  - – MSc Telecom, NTH, Norway, 1987
  - – MSc Info.Sec. Royal Holloway, London, 1993
  - – PhD Info.Sec, NTNU, Norway 1998
- Work
  - – SW Development Engineer, Alcatel, Antwerp 1988-1992
  - – Research Leader, DSTC, Australia 2000-2004
  - – Associate Professor, QUT, Australia, 2005-2007
  - – Professor IT Security, IfI, Oslo University, 2008 →

Identity

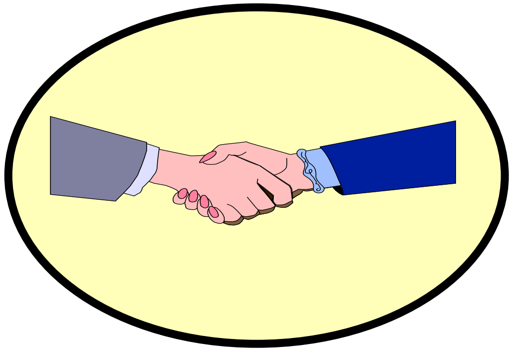
- Etymology of *“identity” :*
  - *“The same one as last time”.*
- “First-time” authentication not meaningful
- Authentication requires registered identity
- Registration based on
  - Pre-authentication of existing identity
  - Creation of new identity
- Names are difficult to interpret:
  - The name “apple” could be: “apple123@hotmail.com”, “www.apple.com”, “www.applecorp.com”, ”apple records”

The Concept of Identity

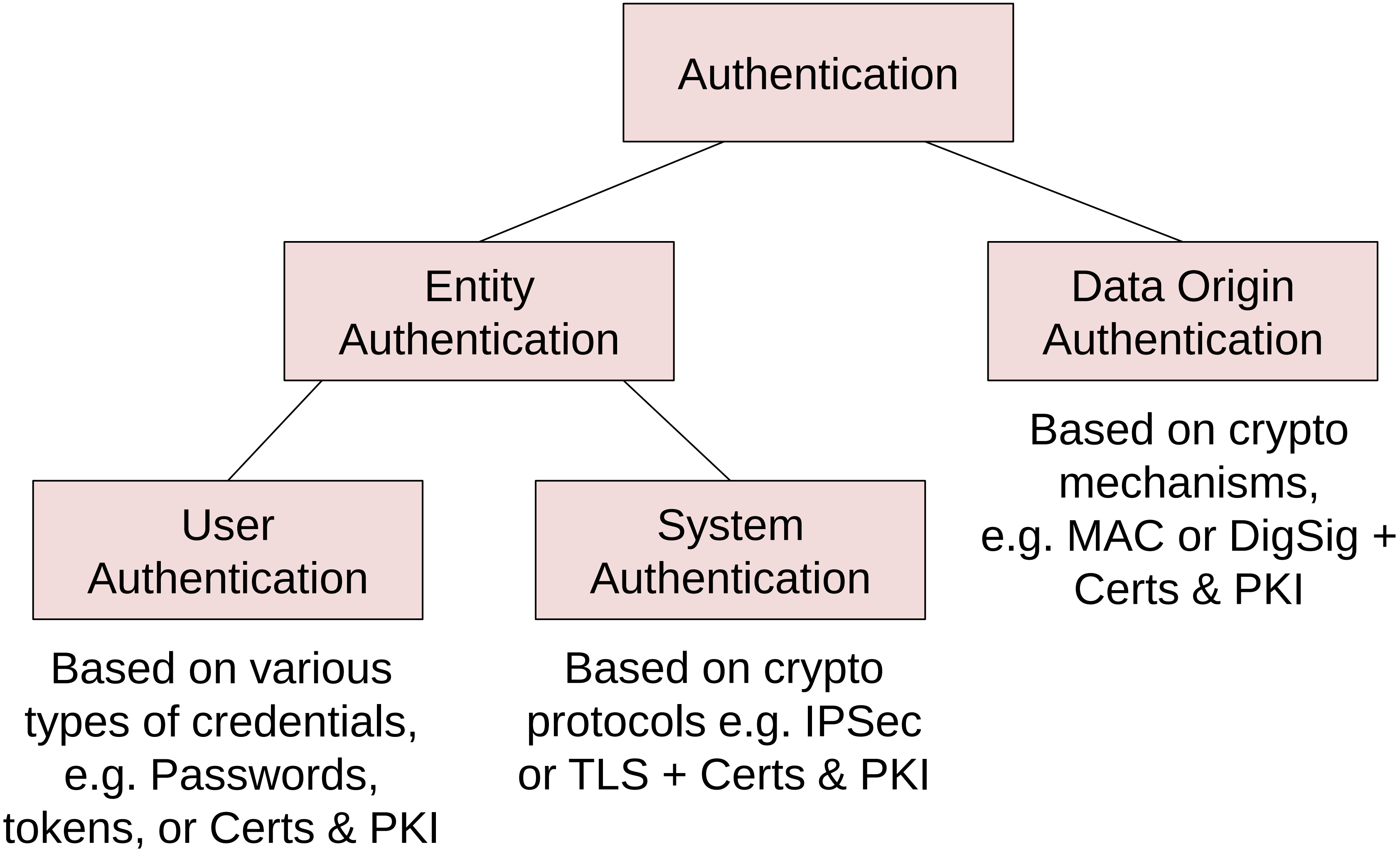


Explaining trust services

- Claims of identity must be verified
- Identity claims certified by 3rd party CA
- Verification of identity through certificates
- Trusting CA = Assuming honest & reliable CA
- Trust service = Issue & validate certificates



Taxonomy of Authentication



Authentication

Entity Authentication

Data Origin Authentication

User Authentication

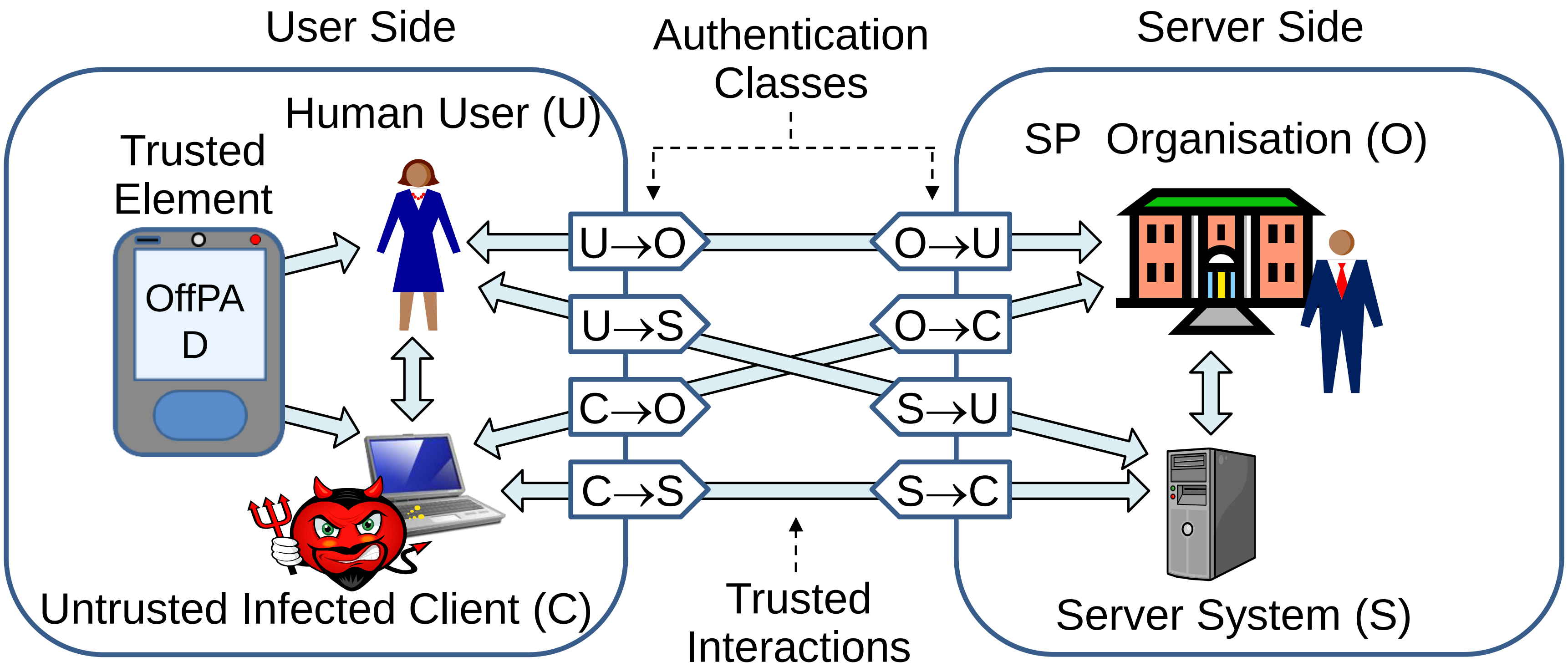
System Authentication

Based on various types of credentials, e.g. Passwords, tokens, or Certs & PKI

Based on crypto protocols e.g. IPSec or TLS + Certs & PKI

Based on crypto mechanisms, e.g. MAC or DigSig + Certs & PKI

Trusted Interactions & Untrusted Clients



- OffPAD Eurostarts Project: Solutions for trusted interaction in the presence of untrusted clients.

Strategies for Internet security

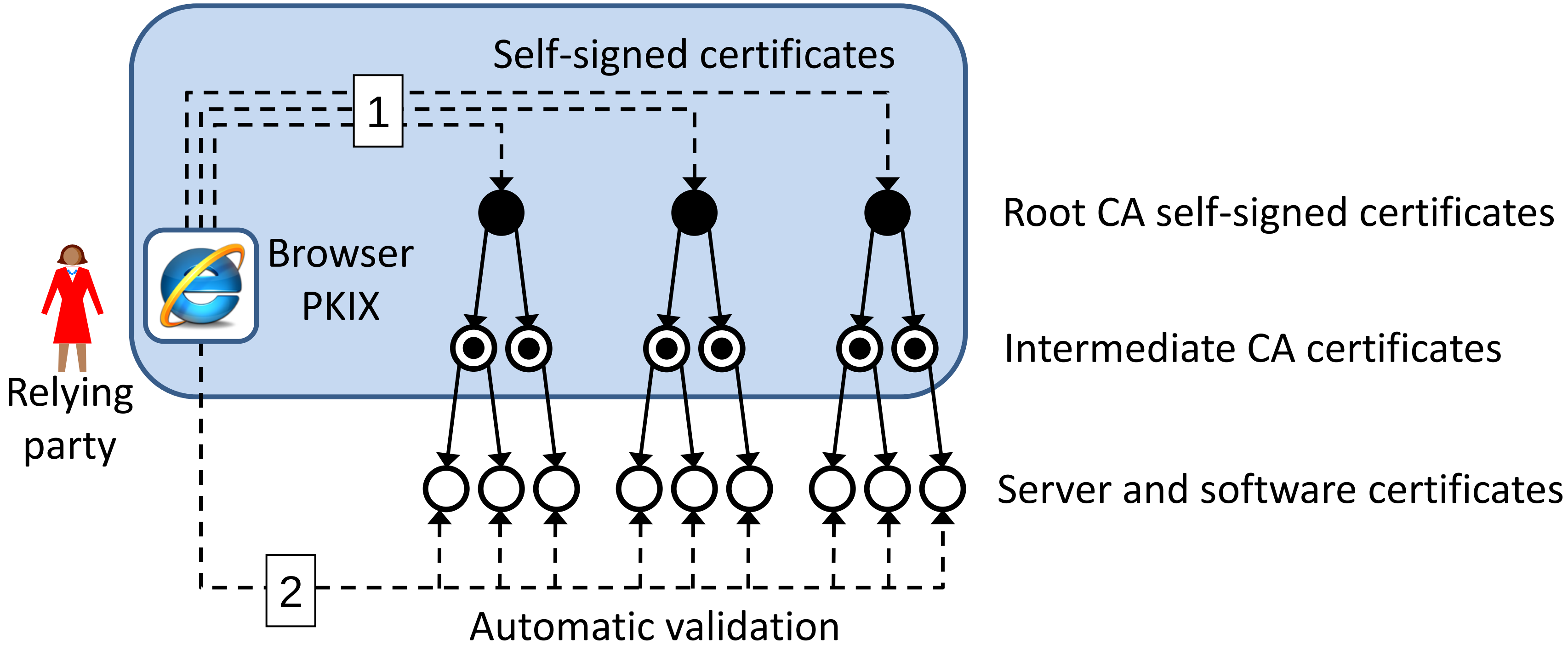
Smoke-and-Mirror strategy

- technology that doesn't solve the *real* problems
- jargon and confusion

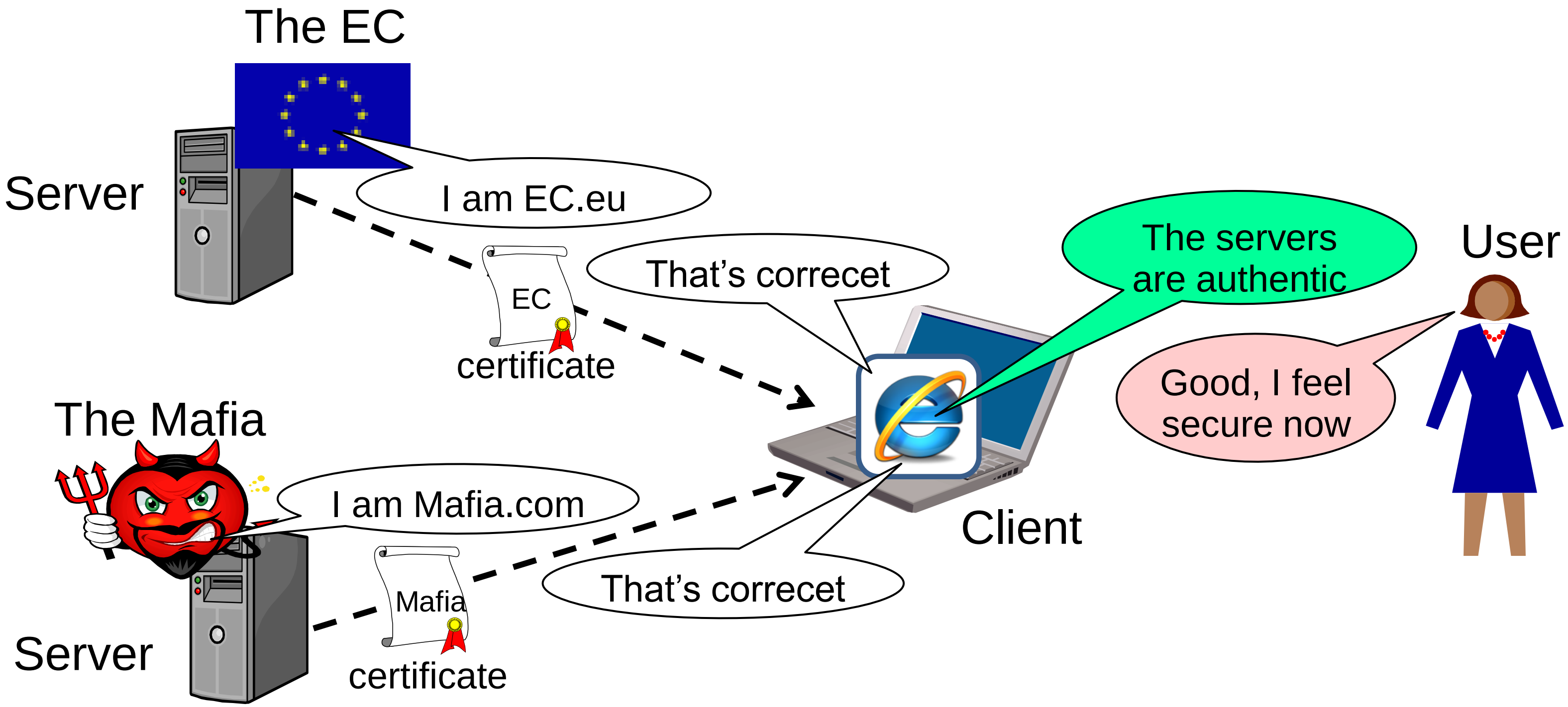
Real-Security strategy

- adequate security solutions
- clear and honest information

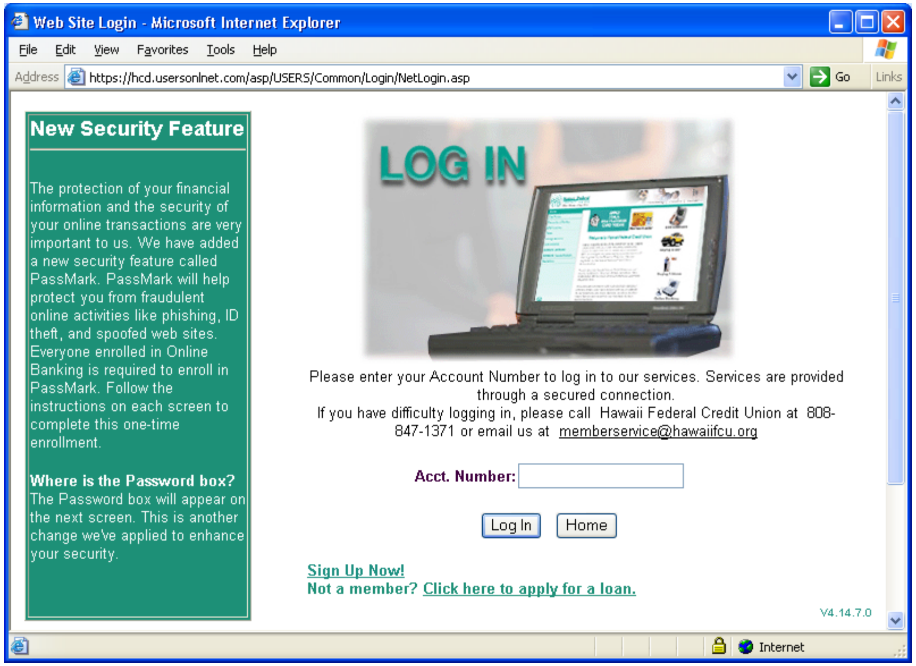
Browser PKIX


Self-signed certificates
1
Browser
PKIX
Root CA self-signed certificates
Intermediate CA certificates
Relying
party
Server and software certificates
2
Automatic validation

Meaningless PKIX System Authentication



A phishing example
Hawaii Federal Credit Union


Web Site Login - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address
Go
Links

https://hcd.usersonlnet.com/asp/USERS/Common/Login/NetLogin.asp

New Security Feature

The protection of your financial information and the security of your online transactions are very important to us. We have added a new security feature called PassMark. PassMark will help protect you from fraudulent online activities like phishing, ID theft, and spoofed web sites. Everyone enrolled in Online Banking is required to enroll in PassMark. Follow the instructions on each screen to complete this one-time enrollment.

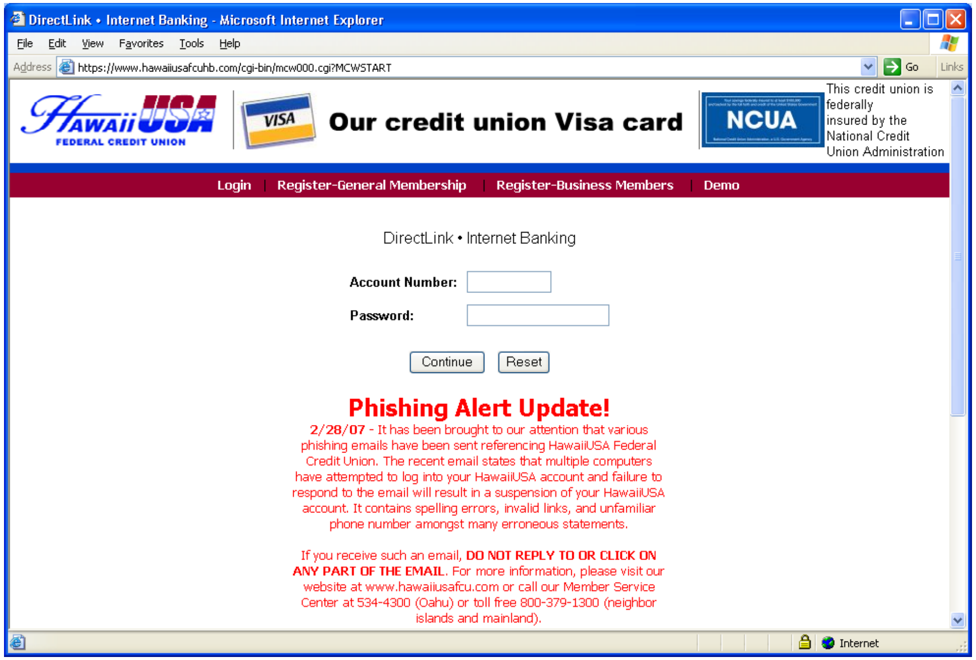
Where is the Password box? The Password box will appear on the next screen. This is another change we've applied to enhance your security.

Please enter your Account Number to log in to our services. Services are provided through a secured connection.
If you have difficulty logging in, please call Hawaii Federal Credit Union at 808-847-1371 or email us at memberservice@hawaiifcu.org

Acct. Number:

Sign Up Now!
Not a member? Click here to apply for a loan.

V4.14.7.0


DirectLink • Internet Banking - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address
Go
Links
HawaiiUSA
FEDERAL CREDIT UNION
VISA
NCUA
Login
Register-General Membership
Register-Business Members
Demo

https://www.hawaiiusafcuhb.com/cgi-bin/mcw000.cgi?MCWSTART

Our credit union Visa card

This credit union is federally insured by the National Credit Union Administration

DirectLink • Internet Banking

Account Number:

Password:

Phishing Alert Update!

2/28/07 - It has been brought to our attention that various phishing emails have been sent referencing HawaiiUSA Federal Credit Union. The recent email states that multiple computers have attempted to log into your HawaiiUSA account and failure to respond to the email will result in a suspension of your HawaiiUSA account. It contains spelling errors, invalid links, and unfamiliar phone number amongst many erroneous statements.

If you receive such an email, **DO NOT REPLY TO OR CLICK ON ANY PART OF THE EMAIL**. For more information, please visit our website at www.hawaiiusafcu.com or call our Member Service Center at 534-4300 (Oahu) or toll free 800-379-1300 (neighbor islands and mainland).

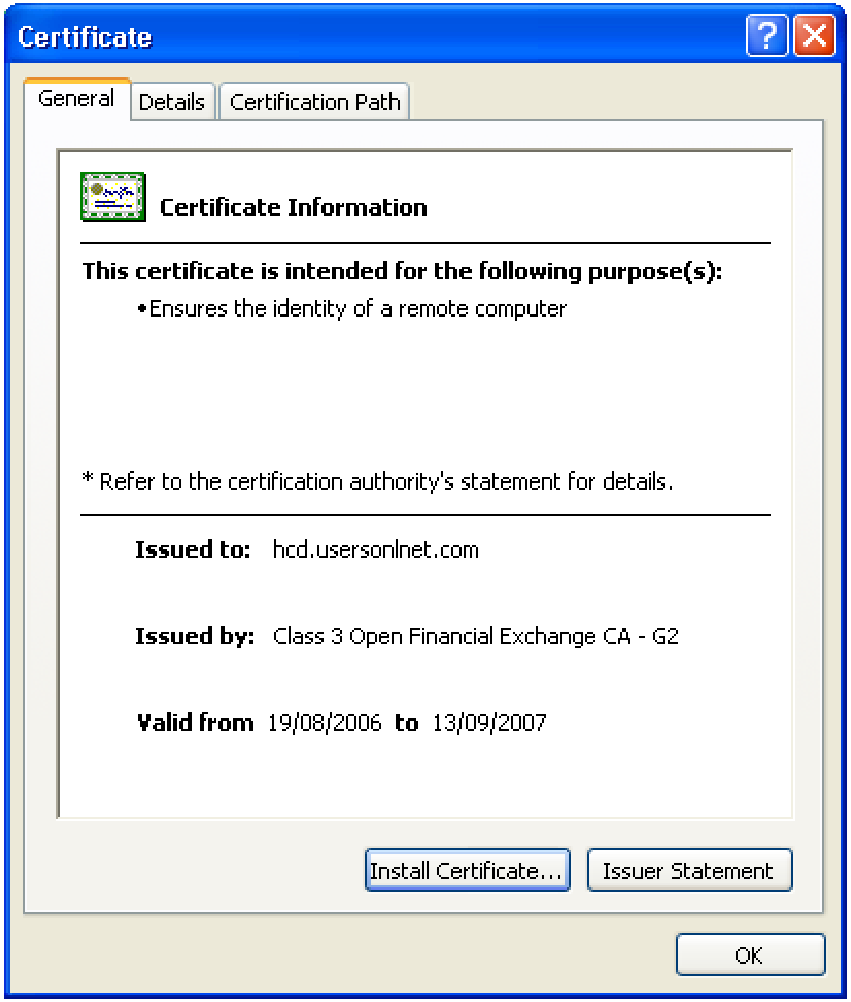
Genuine bank login

https://hcd.usersonlnet.com/asp/USERS/Common/Login/NettLogin.asp

Fake bank login

https://hawaiiusafcuhb.com/cgi-bin/mcw00.cgi?MCWSTART

Certificate comparison 1



Certificate Information

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

- Ensures the identity of a remote computer

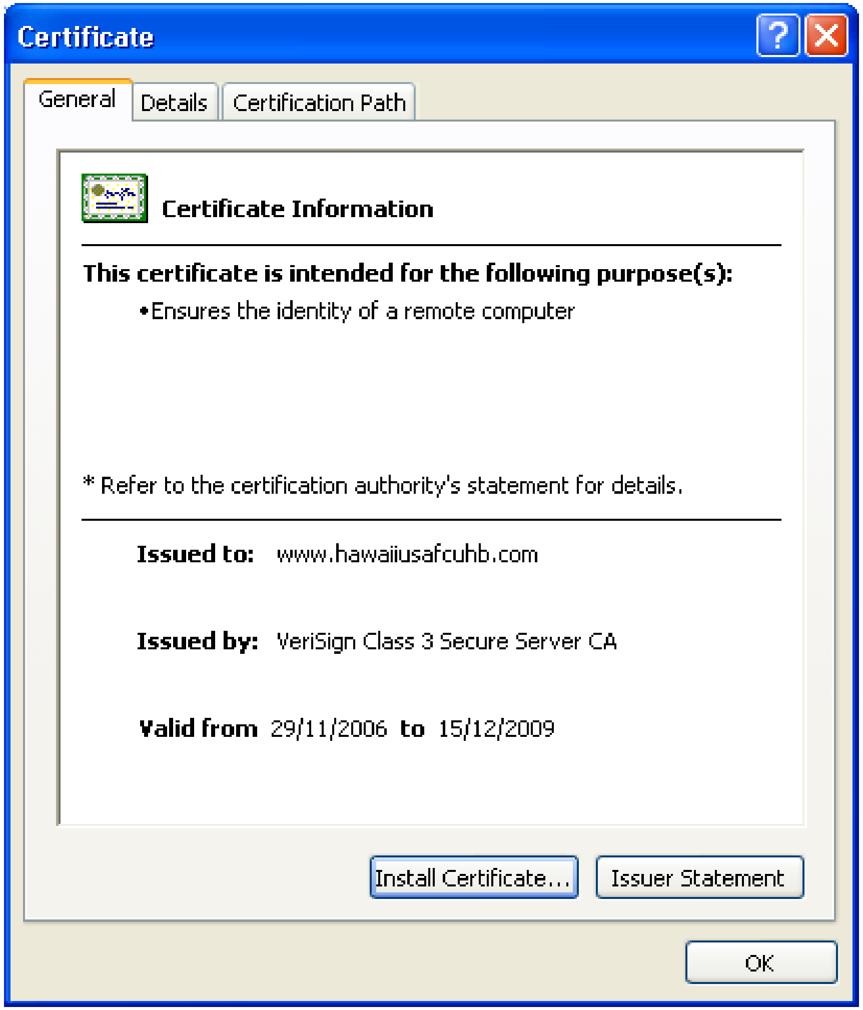
* Refer to the certification authority's statement for details.

Issued to: hcd.usersonlnet.com

Issued by: Class 3 Open Financial Exchange CA - G2

Valid from 19/08/2006 **to** 13/09/2007

Genuine certificate



Certificate Information

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

- Ensures the identity of a remote computer

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

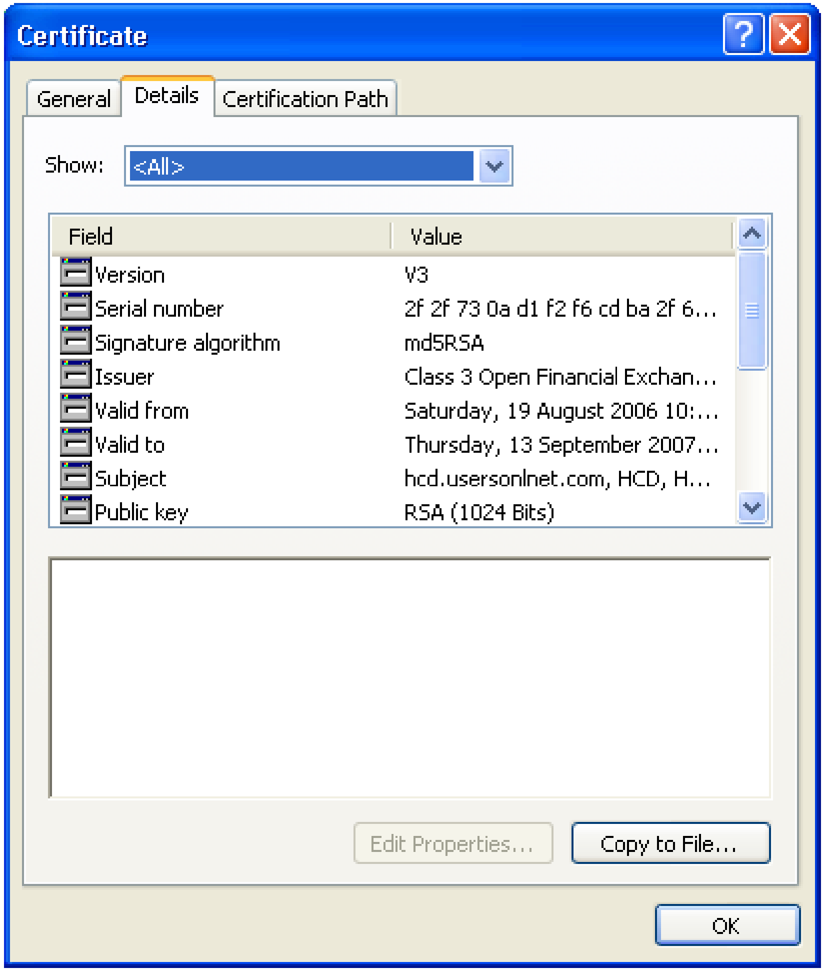
Issued to: www.hawaiiusafcuhb.com

Issued by: VeriSign Class 3 Secure Server CA

Valid from 29/11/2006 **to** 15/12/2009

Fake certificate

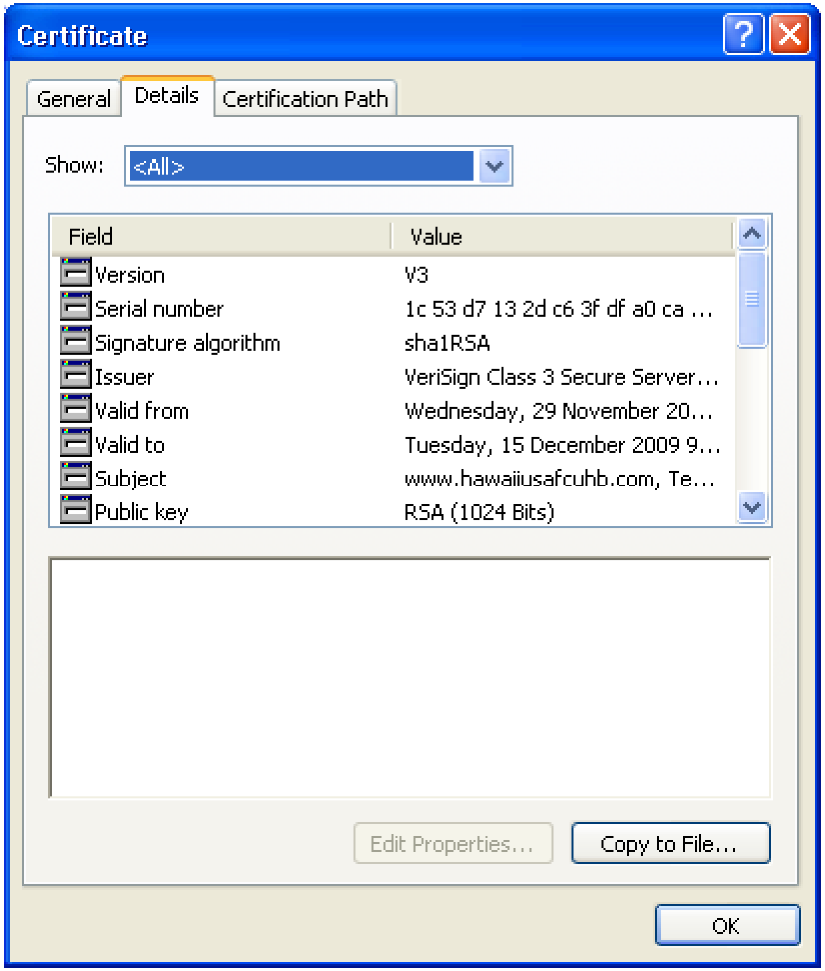
Certificate comparison 2



Show: <All>

Field	Value
Version	V3
Serial number	2f 2f 73 0a d1 f2 f6 cd ba 2f 6...
Signature algorithm	md5RSA
Issuer	Class 3 Open Financial Exchan...
Valid from	Saturday, 19 August 2006 10:...
Valid to	Thursday, 13 September 2007...
Subject	hcd.usersonlnet.com, HCD, H...
Public key	RSA (1024 Bits)

Genuine certificate

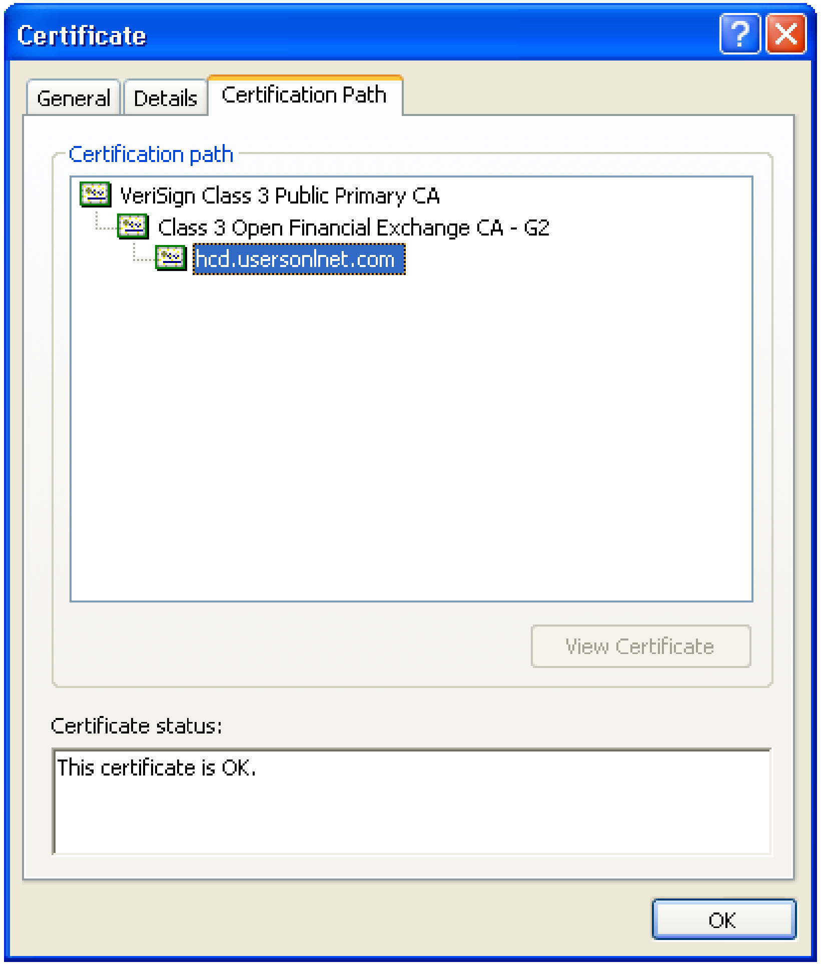


Show: <All>

Field	Value
Version	V3
Serial number	1c 53 d7 13 2d c6 3f df a0 ca ...
Signature algorithm	sha1RSA
Issuer	VeriSign Class 3 Secure Server...
Valid from	Wednesday, 29 November 20...
Valid to	Tuesday, 15 December 2009 9...
Subject	www.hawaiiusafcuhb.com, Te...
Public key	RSA (1024 Bits)

Fake certificate

Certificate comparison 3

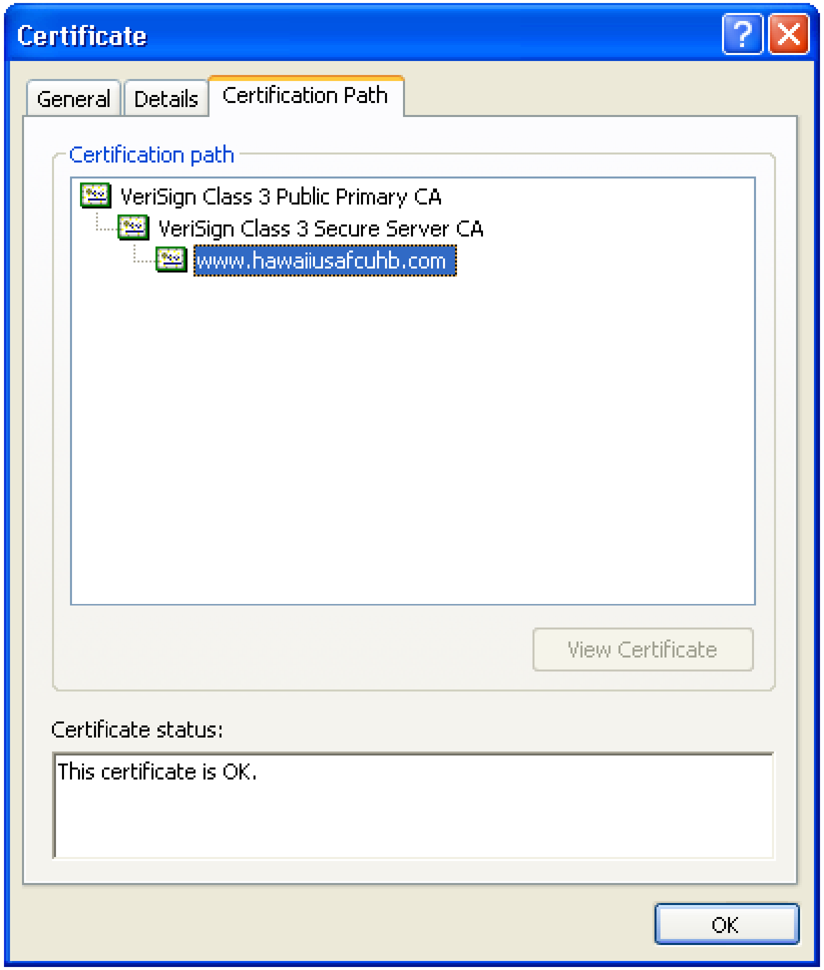


VeriSign Class 3 Public Primary CA
Class 3 Open Financial Exchange CA - G2
hcd.usersonlnet.com

Certificate status:

This certificate is OK.

Genuine certificate



VeriSign Class 3 Public Primary CA
VeriSign Class 3 Secure Server CA
www.hawaiiusafcuhb.com

Certificate status:

This certificate is OK.

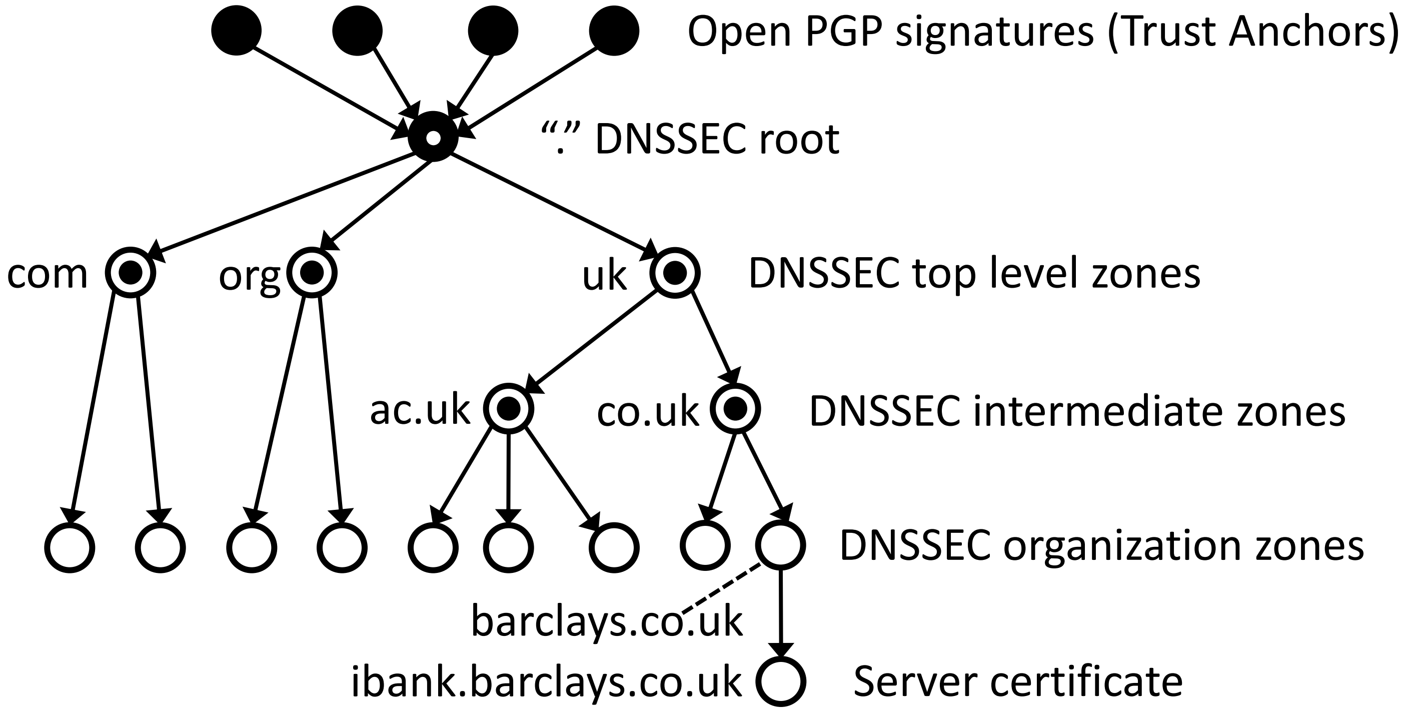
Fake certificate

Self-signed root keys: Why?

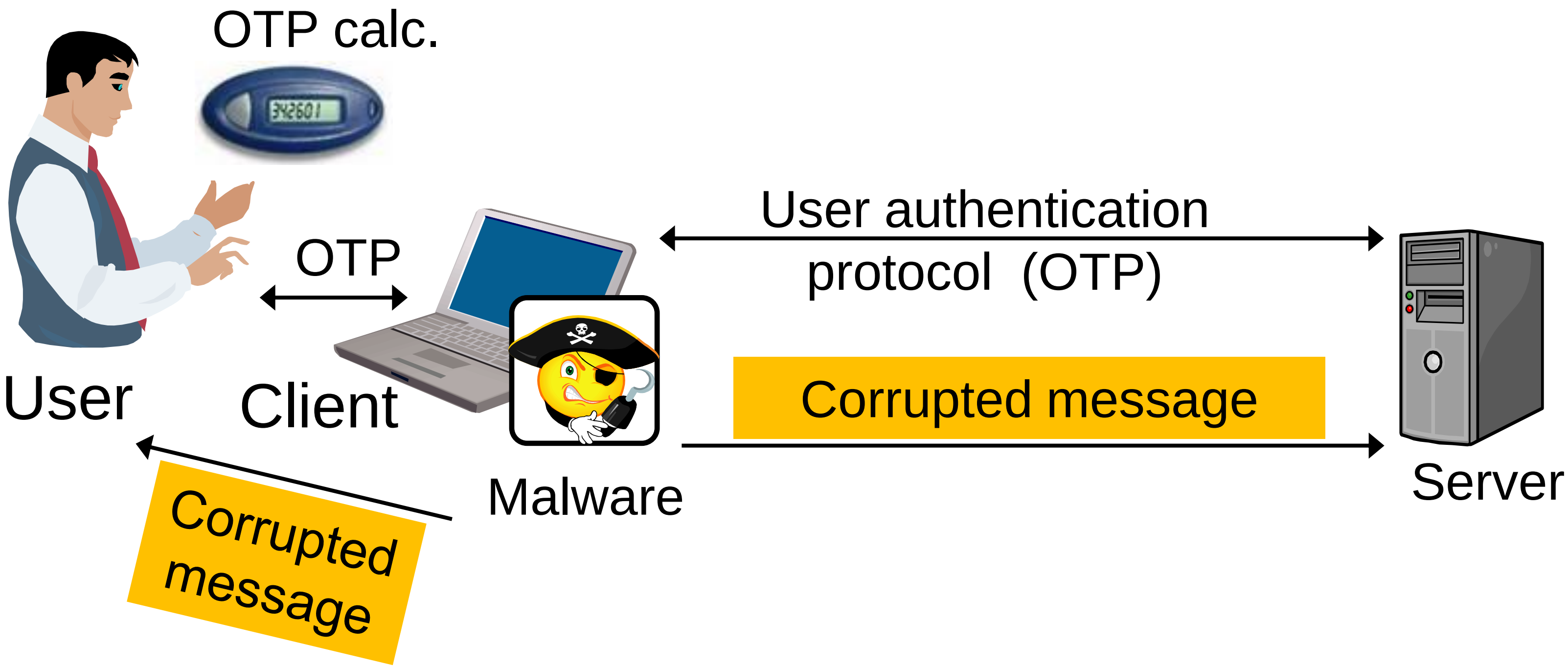
- Most people think a root public key is authentic just because it is self-signed
- Self-signing is deceptive propaganda

- Self-signing has absolutely no purpose for trust

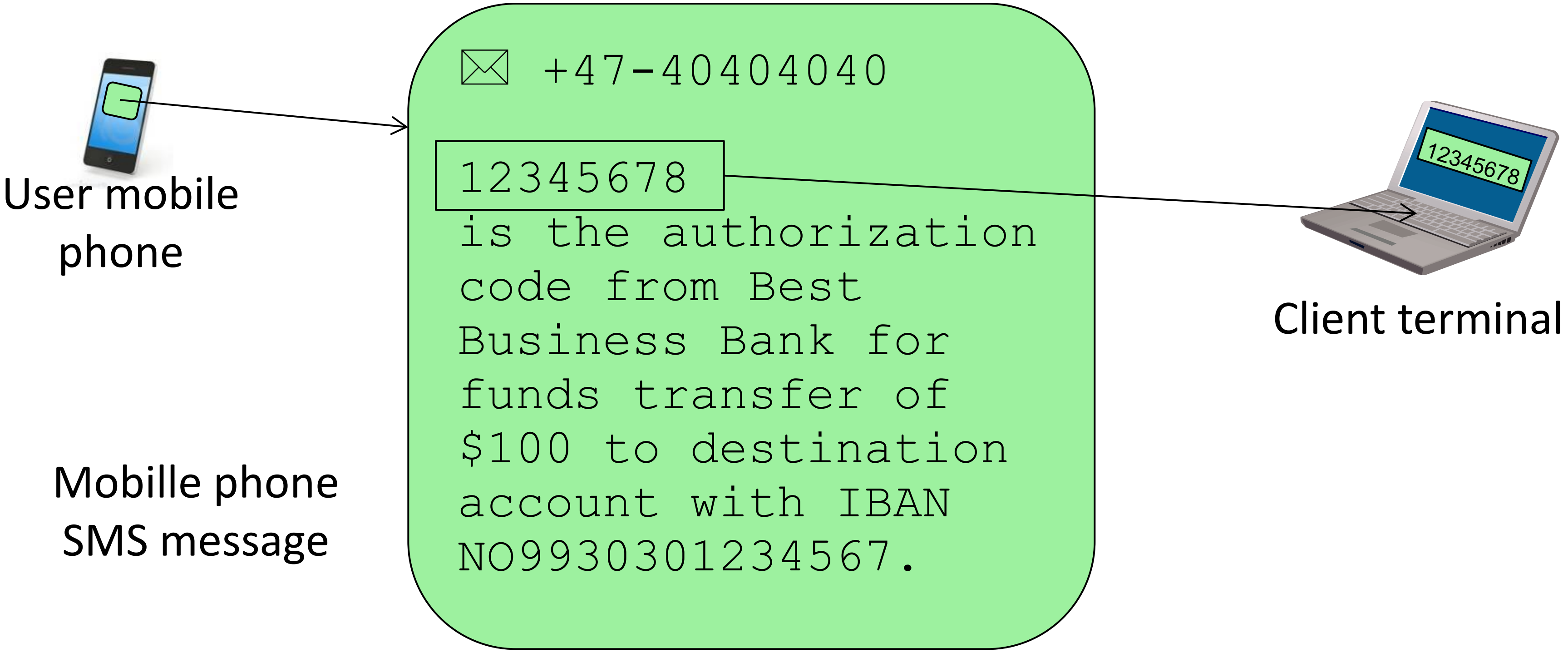
Server certificates with DNSSEC



Entity authentication is insufficient (also need for data authentication)



SMS-based message authentication



User mobile phone

✉ +47-40404040

12345678 is the authorization code from Best Business Bank for funds transfer of $100 to destination account with IBAN NO9930301234567.

Client terminal

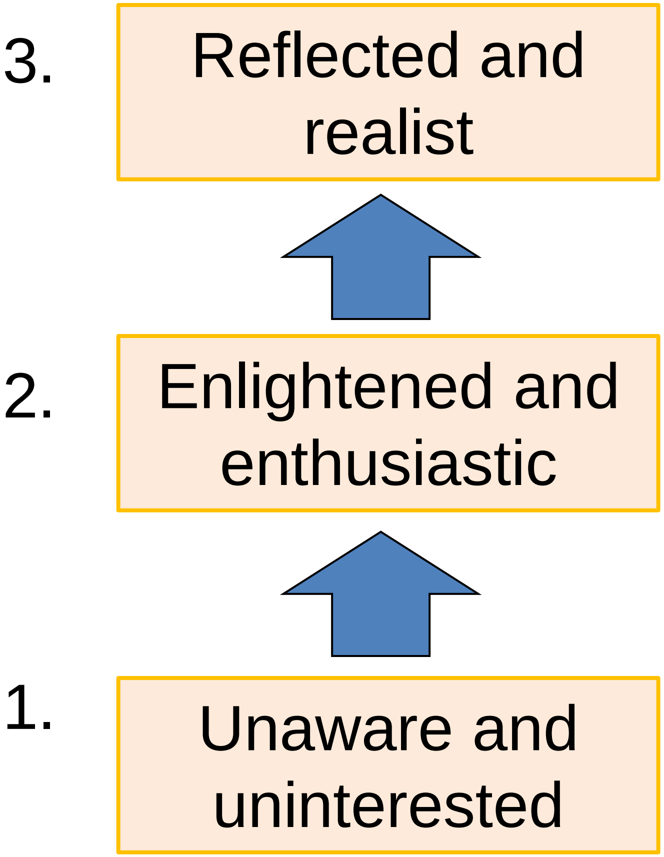
Mobille phone SMS message

- > 30% of users will not notice attack on transactions,

Authentication Framework	***User Authentication Assurance Levels***				
EAG **(USA) 2006**	Little or no assurance (1)		Some (2)	High (3)	Very High (4)
IDABC **(EU) 2007**	×	Minimal (1)	Low (2)	Substantial (3)	High (4)
FANR **(Norway) 2008**	Little or no assurance (1)		Low (2)	Moderate (3)	High (4)
NeAF **(Australia) 2009**	None (0)	Minimal (1)	Low (2)	Moderate (3)	High (4)
ePramaan **(India) 2012**	None (0)	Minimal (1)	Moderate (2)	Strong (3)	Very Strong (4)

- Assurance levels also needed for
  - – Server system authentication
  - – Data authentication

Conclusion:
3 Stages of Security Learning



3. Reflected and realist

2. Enlightened and enthusiastic

1. Unaware and uninterested

- *This is far more complex than I first thought. I actually don’t think this can ever be made secure.*
- *I understand it now, it’s great, and I know how to operate it*
- *I don’t understand it, and I don’t want to know about it. Why can’t security simply be transparent?*