



Certificates, an introduction

Greg Rose

Ir. Ivana Belgers



Content

- Some public key background
- The problem: trust
 - E-mail traffic
 - Surfing on the web
- Digital Certificates
 - Theory
 - CAcert
- Some examples from real life
- Your own CAcert certificate



Public key Crypto

- Also called “asymmetric”
- Keys come in pairs; keep one half secret
 - can’t derive the secret one from the public one
- Solves the key distribution problem... just publish the public keys



Public key Crypto

- Neat, we're done, right?
 - Oops, no.
- Replaces it with the authentication problem
 - How do you know that the key belongs to who you think it does? Still a research problem.



Hybrid systems

- Often use a combination of Public, symmetric and no-key cryptography.
- e.g.. SSL, SSH, PGP.
 - Public keys used for authentication, key exchange
 - Hash and public key for digital signature
 - Dynamic session key and classical cipher for security
 - Random numbers for all sorts of things.



Signatures

- With a piece of data, and a private key
 - you can sign things (*signing*)
- With a piece of data, a signature, and a public key
 - you can check that the corresponding private key made the signature, and
 - that the data is the same as when it was signed
 - (*verification*)



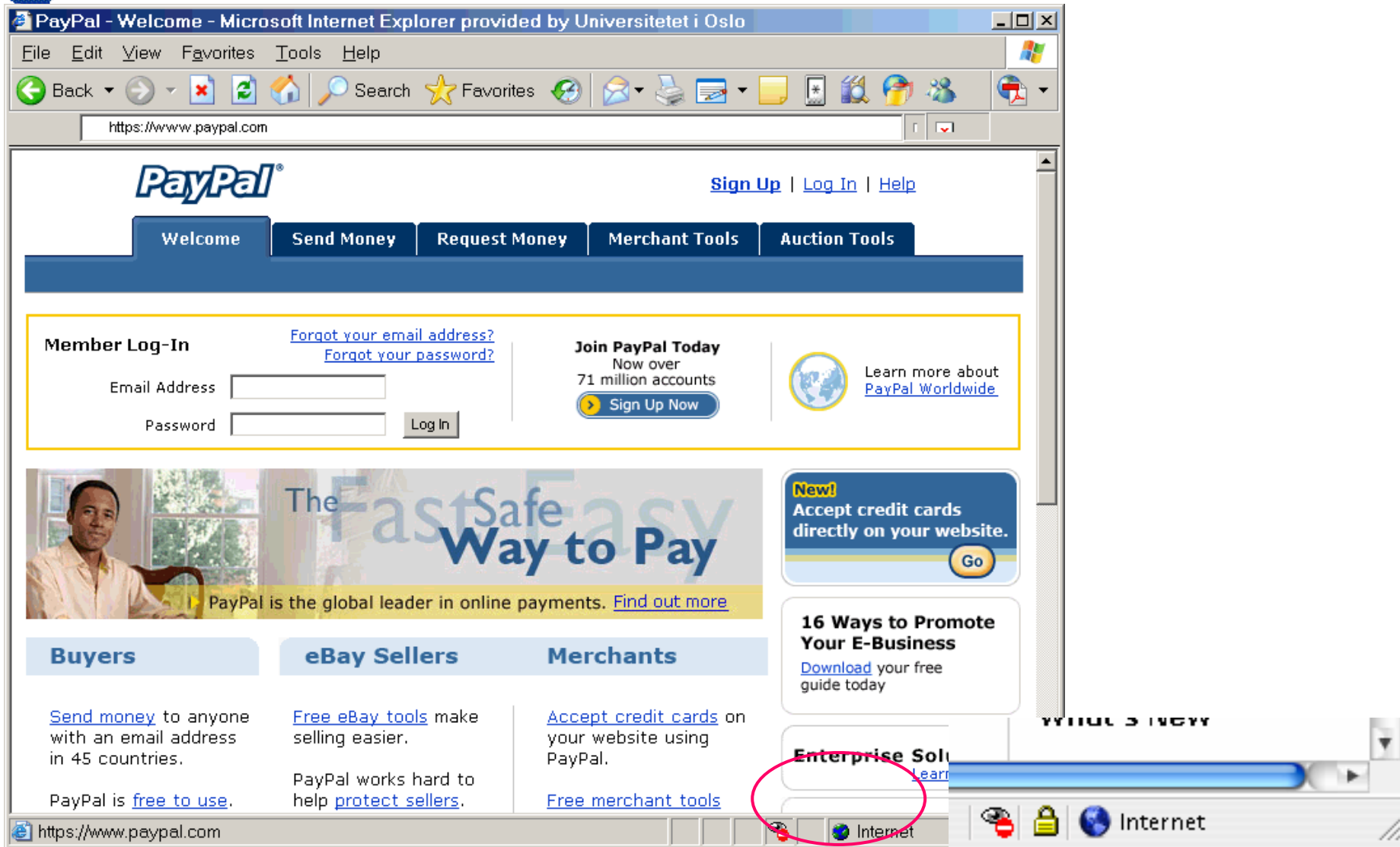
Certificates

- Just a blob of data that has been signed
- ...except that the data tells you about
 - a public key
 - who that key belongs to
 - what they can do with it
 - for how long (validity)
 - and maybe other stuff
- Who signs it?

On the internet, nobody knows you're a dog



"On the Internet, nobody knows you're a dog."

A screenshot of the PayPal website as seen in Microsoft Internet Explorer. The browser window title is "PayPal - Welcome - Microsoft Internet Explorer provided by Universitetet i Oslo". The address bar shows "https://www.paypal.com". The website features the PayPal logo, navigation tabs for "Welcome", "Send Money", "Request Money", "Merchant Tools", and "Auction Tools", and a "Member Log-In" section with input fields for email and password. A banner for "The Fast Safe Easy Way to Pay" is visible, along with a "New! Accept credit cards directly on your website" promotion. The footer contains sections for "Buyers", "eBay Sellers", and "Merchants". A red circle highlights the "Enterprise Solutions" link in the bottom right corner. The Windows taskbar at the bottom shows the "Internet" icon circled in red.

PayPal - Welcome - Microsoft Internet Explorer provided by Universitetet i Oslo

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites

https://www.paypal.com

PayPal

[Sign Up](#) | [Log In](#) | [Help](#)


Welcome Send Money Request Money Merchant Tools Auction Tools

Member Log-In [Forgot your email address?](#) [Forgot your password?](#)

Email Address

Password

Join PayPal Today
Now over 71 million accounts

 Learn more about [PayPal Worldwide](#)

The Fast Safe Easy Way to Pay

PayPal is the global leader in online payments. [Find out more](#)

New! Accept credit cards directly on your website.

16 Ways to Promote Your E-Business
[Download](#) your free guide today

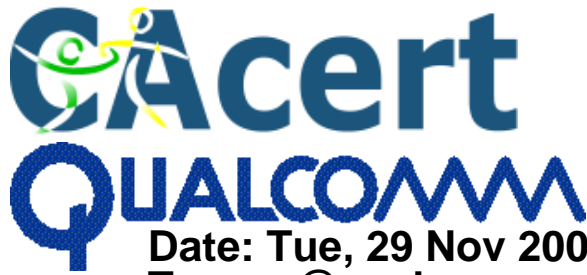
Enterprise Solutions [Learn](#)

Buyers [Send money](#) to anyone with an email address in 45 countries. PayPal is [free to use](#).

eBay Sellers [Free eBay tools](#) make selling easier. PayPal works hard to help [protect sellers](#).

Merchants [Accept credit cards](#) on your website using PayPal. [Free merchant tools](#)

Internet



Phishing

Date: Tue, 29 Nov 2005 17:17:04 -0500

To: ggr@qualcomm.com

Subject: Reactivate Your Account!

From: "service@amazon.com" <service@amazon.com>

Amazon.com

Dear Amazon member,

We regret to inform you that your Amazon account was been suspended for a period of 3-4 days,after that it will be terminated.

Your credit card on file with Amazon

Card number: XXXX-XXXX-XXXX-XXXX (Not shown for security purposes) Expiration date: XX/XX

Please sign in to your Amazon account and update your billing information:

<http://www.amazon.com/gp/css/homepage.html>

If your account information is not update, your account on Amazon will be terminated.

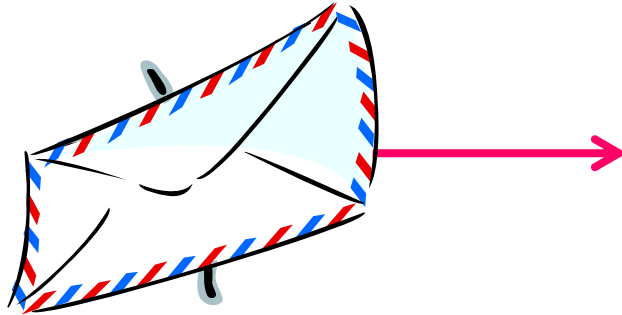
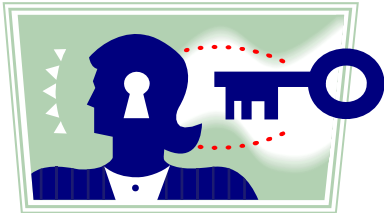
Thank you for your time!

Amazon Security Departament

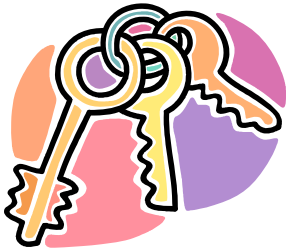
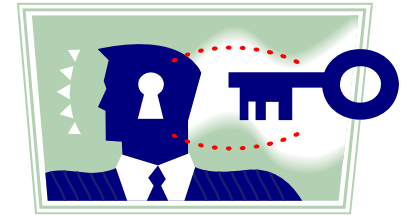
Encryption (1)



Alice



Bob



Code for a rotation of 13 letters: ROT-13

10. ~~Zkrcpdcyrlg thvak lpbu spxakv d q d fish~~
9. ~~SoivthguP Cclgyttematbrf~~
8. ~~Zkrcy lsr d r f s s v p l h y g t b e N g u i o A a g S l e a n y i t f r a g e n g l y N t r a p l~~
7. ~~Kerep Q d a w i d M r g t j e e z n a n s f e o z n f s t e a y i r a g l y o u e z n a g r e v a l y~~
6. ~~Zkrcn y l g . c o n s p i r a c y l r a e i o b u s~~
5. ~~Bepabfrenabj h e r e l o p o z r e a b j o w e r e p y r e l e d r p e z o r c l e s k ,
p a r e g r e e n t e p l a z b f e o r a e s g r e e n~~
4. ~~B a f s k e y n e w b i e s~~
3. ~~N'g'fcheape r e t g a n a t h e C R p p e c r e h p o v c~~
2. ~~Azrenipa B a l i m e r u s f e e s p a a " g d e p b d e l y o e r z r f e s t s f a g e s a v a d
f i n g j u r t g m b a t e r d u i k a s a y i n g~~
1. ~~Zkrci' b a g u t h e / a r g e r a g t g o b~~





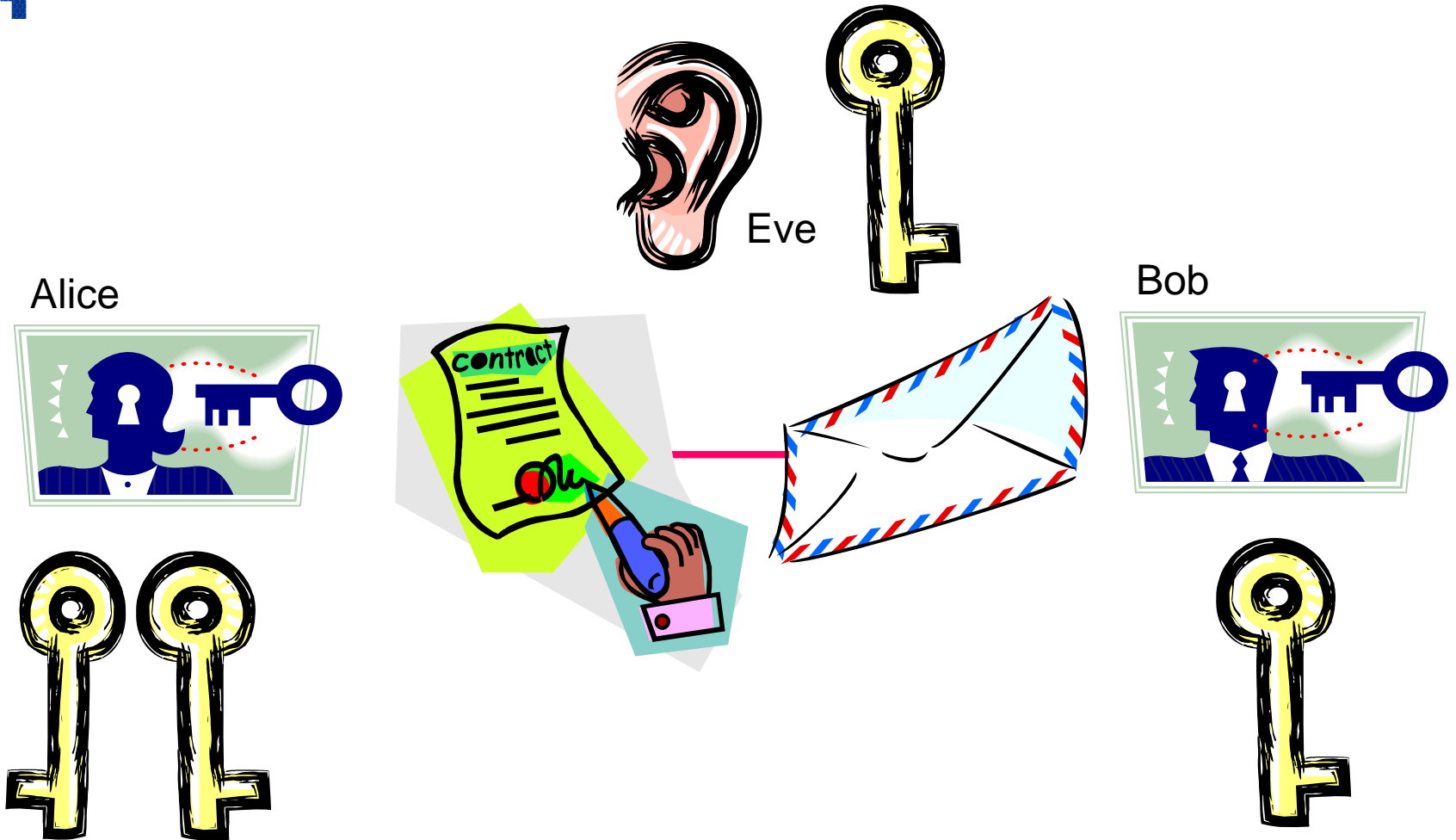
Disadvantages

- Sharing the secret
- Big keyring, many keys to protect
- Key exchange
- Not suitable for digital signatures

Advantage:

Relatively fast algorithm

Encryption (2)





Advantages

- Create keys for yourself
- One key pair per person
- Your public key can be... public
- Digital signatures are possible

Disadvantage:

Slow algorithms, big keys.

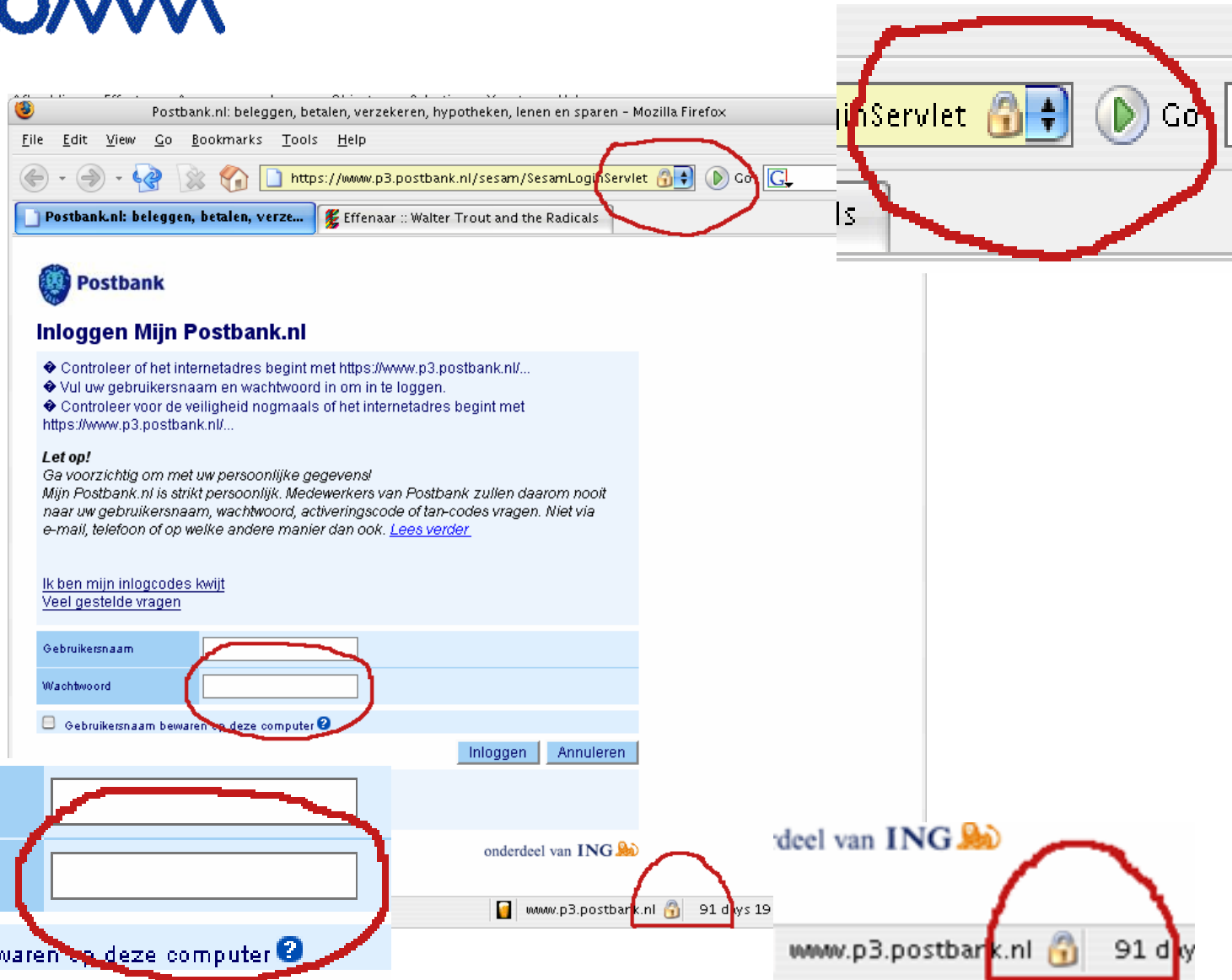
- X.509
 - Hierarchical structure
 - Certificate Authority (CA)
 - Verisign, Thawte, ...
- PGP
 - Web of trust
- Support for E-mail and Web clients.



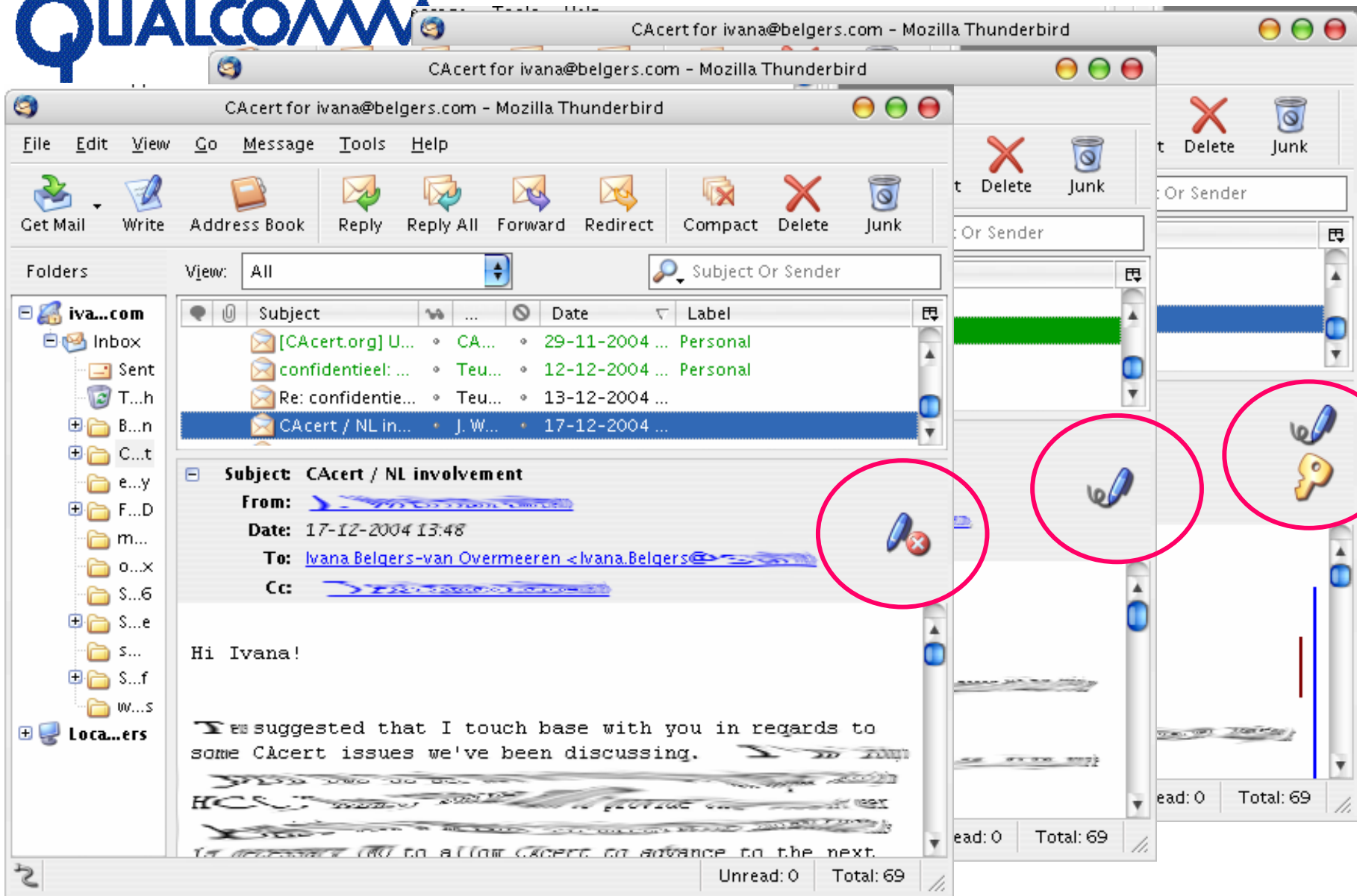


CAcert

- Makes Digital Certificates
- Functions as a CA
- Free!
- Web-of-trust
- Began in Australia, now worldwide
 - 2000 certifiers, growing \pm 150/month
 - 77000 certificates, growing \pm 5000/month



The image shows a screenshot of a Mozilla Firefox browser window displaying the Postbank.nl login page. The browser's address bar shows the URL `https://www.p3.postbank.nl/sesam/SesamLoginServlet`. A red circle highlights the address bar and the status bar, which shows a lock icon and the text "www.p3.postbank.nl 91 days 19". Another red circle highlights the "Go" button in the address bar. A third red circle highlights the "Wachtwoord" (password) input field in the login form. A fourth red circle highlights the "Gebruikersnaam" (username) input field. A fifth red circle highlights the "Gebruikersnaam bewaren op deze computer" checkbox. The page content includes the Postbank logo, the heading "Inloggen Mijn Postbank.nl", and instructions for logging in. The text "onderdeel van ING" is visible at the bottom of the page.



The screenshot shows the Mozilla Thunderbird email client interface. The main window displays an email from CAcert.org with the subject "CAcert / NL involvement". The email content includes a greeting "Hi Ivana!" and a paragraph starting with "It is suggested that I touch base with you in regards to some CAcert issues we've been discussing." The interface also shows a folder tree on the left, a message list, and a toolbar with icons for "Delete" and "Junk". Three red circles highlight specific icons: a blue key icon, a blue key icon with a red 'X', and a yellow key icon.

CAcert for ivana@belgers.com - Mozilla Thunderbird

CAcert for ivana@belgers.com - Mozilla Thunderbird

CAcert for ivana@belgers.com - Mozilla Thunderbird

File Edit View Go Message Tools Help

Get Mail Write Address Book Reply Reply All Forward Redirect Compact Delete Junk

Folders View: All Subject Or Sender

Subject	Date	Label
[CAcert.org] U...	29-11-2004 ...	Personal
confidentieel: ...	12-12-2004 ...	Personal
Re: confidentie...	13-12-2004 ...	
CAcert / NL in...	17-12-2004 ...	

Subject: CAcert / NL involvement
From: ...
Date: 17-12-2004 13:48
To: Ivana Belgers-van Overmeeren <Ivana.Belgers@...>
Cc: ...

Hi Ivana!

It is suggested that I touch base with you in regards to some CAcert issues we've been discussing.

Unread: 0 Total: 69



And you?

- <http://www.cacert.org/>
- Do your account registration, supply some private data
- <https://secure.cacert.org/cap.php>
- Print the form
- Find an assurer (or can be done by mail with notarized ID)

- Questions?

