IDN and SSL certificates

ICANN Cape Town, December 2004

Valentin Németh, senior engineer, Thawte Consulting

Who we are

- Thawte Consulting (Pty) Ltd., based in Cape Town, South Africa;
- the second largest Certificate Authority (CA) world-wide;
- started operating in 1995 and issued its first SSL certificate issued : 12 June 1996;
- the first Certificate Authority to issue a digital certificate outside of the U.S.;
- have issued over 480,000 SSL and Code Signing certificates and over 747,000 Personal Certificates in 172 countries;
- employ over 100 staff;
- support 28 languages;
- dedicated to the open source community;
- the company was acquired by VeriSign Inc. in 1999, but runs as a separate entity;
- a unique company. No one matches the precise mix of values, skills and assets we bring to our customers. Importantly, our commitment to the egalitarian ethos of the Internet and our focus on extending a trusted relationship on the Internet to anyone, anywhere mean that there is no other company quite like us .

IDN and Internet trust

Current Internet trust model:

- CA verifies that a domain name belongs to a given company and issues digital certificate.
- User visits company web site, browser downloads certificate.
- The browser matches domain name embedded in the certificate with the domain name of the download path.
  - If they match and the certificate signature verifies, browser displays closed padlock. User typically continues with transaction.
  - If domain names do not match or certificate signature does not verify, browser displays warning. User typically aborts transaction

IDN and Internet trust

What is the problem with trust in IDNs?

- The domain name as the user knows it in its native language form and the domain name that actually works are different!

Native language form	Punycode encoded form
www.szépjónapot.hu	www.xn--szpjnapot-c4a6i.hu
www.grützi.ch	www.xn--grtzi-lva.ch
www.欢迎.cn	www.xn--7jw659e.cn
www. здраствуйте.ru	www.xn--80aeeggp0cjjcj.ru

Would you trust the punycode encoded form?

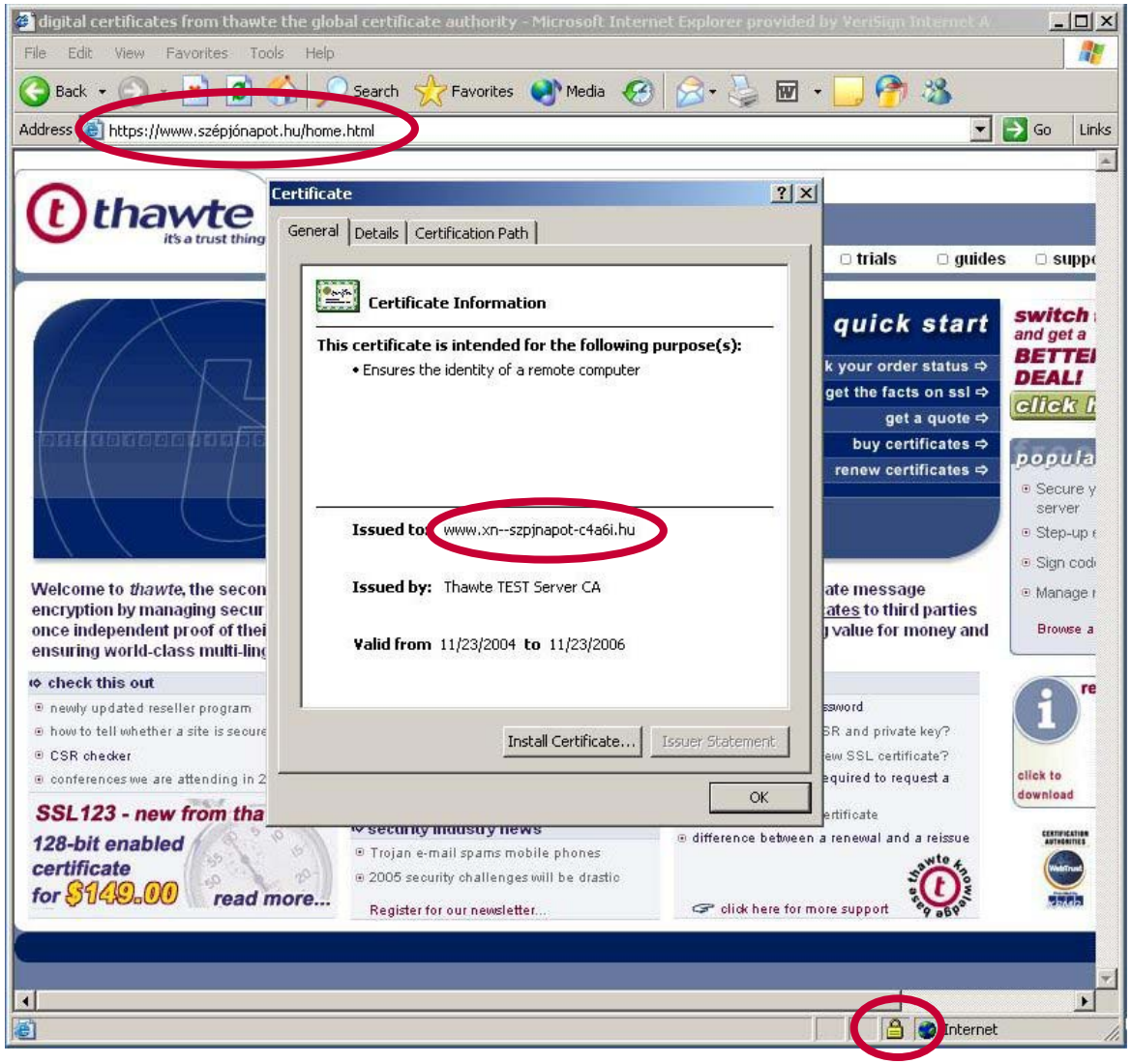
IDN and Internet trust

What is the problem with IDN in SSL server certificates?

- Basic trust model still the same, but what domain name should be embedded in the digital certificate?
  - The native language one?
    - This is what the user expects.
    - However, the embedded domain name doesn't match the domain name of the download path – browser issues warning.
    - User will not trust and typically aborts the transaction.
  - The punycode encoded one?
    - This is not what the user expects.
    - However, the embedded domain name does match the domain name of the download path – browser shows '"closed padlock"
    - User will still not trust and typically aborts the transaction.

- Biggest limiting factor in ecommerce is users' trust!

IDN and Internet trust



Would you trust this site?

Securing IDN

Why should IDNs be secured?

- 92% of the world speaks a primary language other than English (*)
- 48% of Internet users are non-native English speakers (*)
- By 2003, non-English speakers represented two-thirds of all Internet users (*)
- By 2007, Chinese will be the #1 web language (*)
- Additional vulnerability in a foreign language environment.
- Phisers are likely to attack using “similarly looking/sounding” names.

- Although IDN is considered as an early adopter market, there are already roughly 1 million delegations world-wide.
- Studies show that approximately 2-3% of domain names have been secured with SSL certificates. 2% of 1 million is a significant number!
- Important drive is to securing Intellectual Property and trade-mark company and product names in their original form.
- The number of IDN delegations has been growing exponentially.

(*) source: http://www.walid.com

Securing IDN

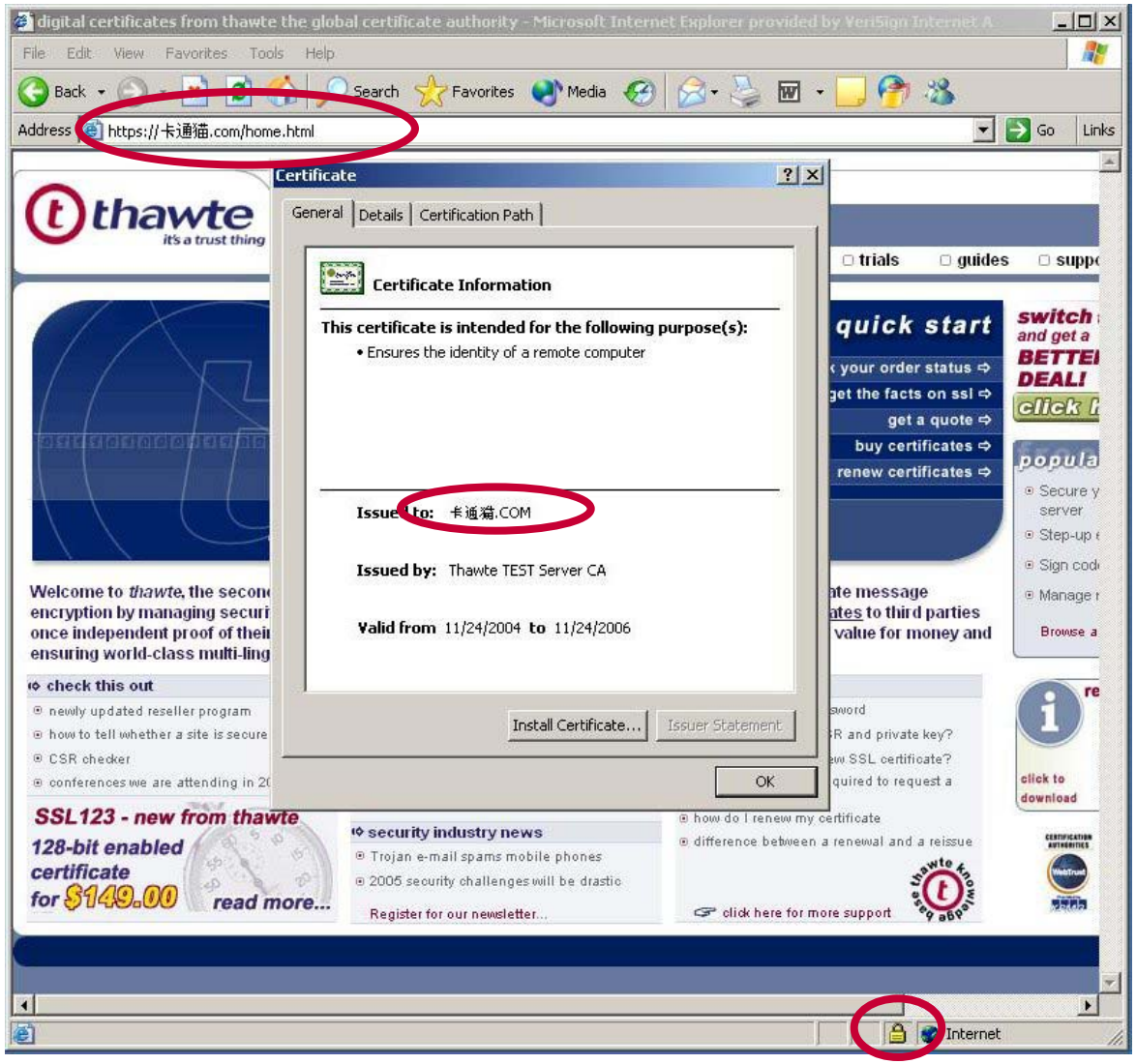
Synopsis

- User instinctively trusts the native language IDN and distrusts machine readable, encoded forms.
- Network transactions are done in encoded form.
- X509 specification supports UTF-8 to display native language characters.
- X509 specification supports multiple domain names in a single certificate.

Design guidelines

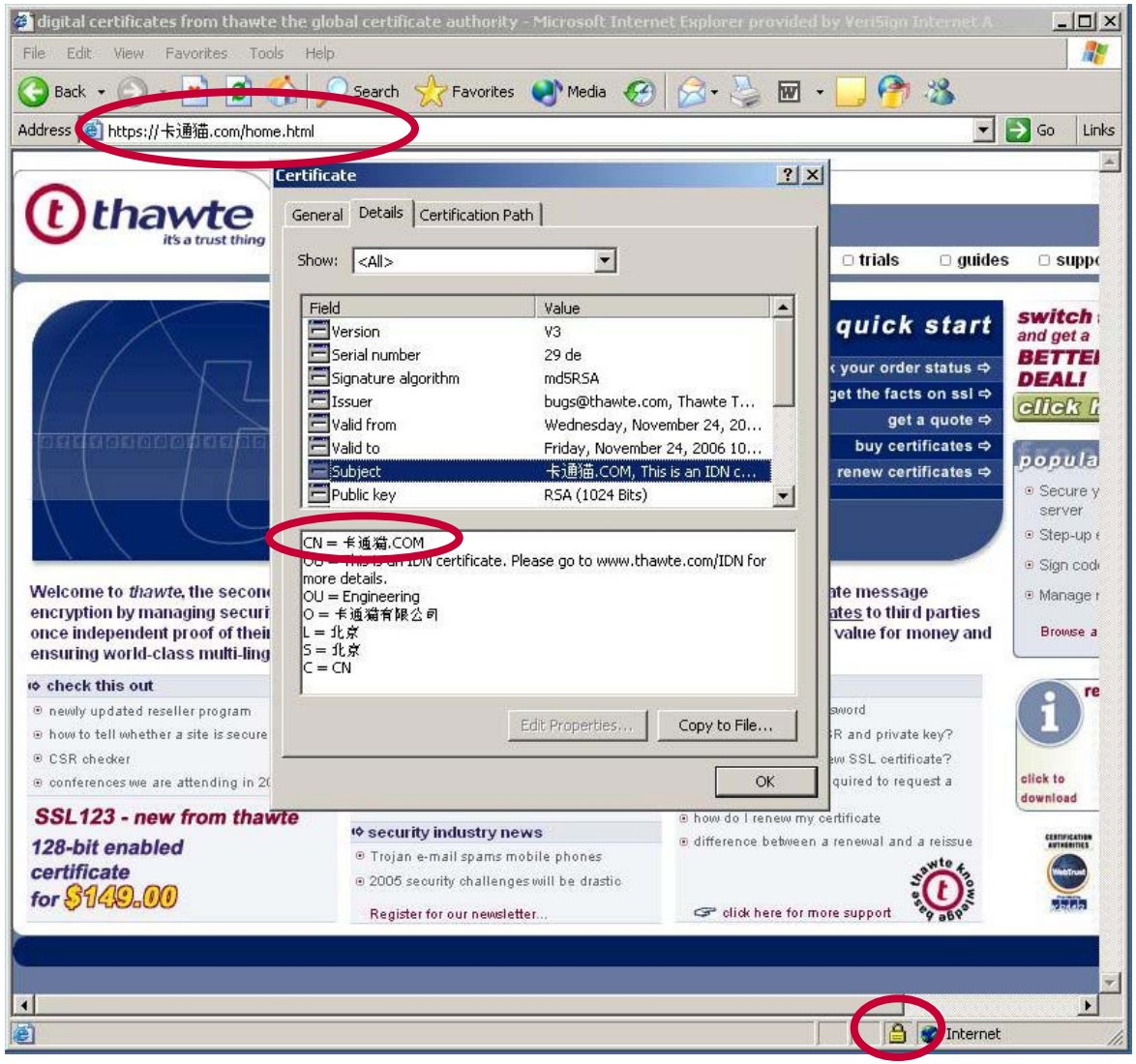
- Establish users' trust by
  - Maximize the presence of the native language form in displays to the user;
  - Minimize the presence of the punycode encoded form in displays to the user.
  - Provide sufficient amount of punycode data to allow network transactions to continue working
- Secure IDN must work in current browser environment without additional software or updates.

Secure IDN



Would you trust this site?

Securing IDN



You can trust this site!

Secure IDN

http://www.thawte.com/IDN

- Fully internationalized SSL certificate enrollments.
- Fully internationalized code signing certificate enrollments.
- Fully internationalized SSL certificates supporting IDNs.