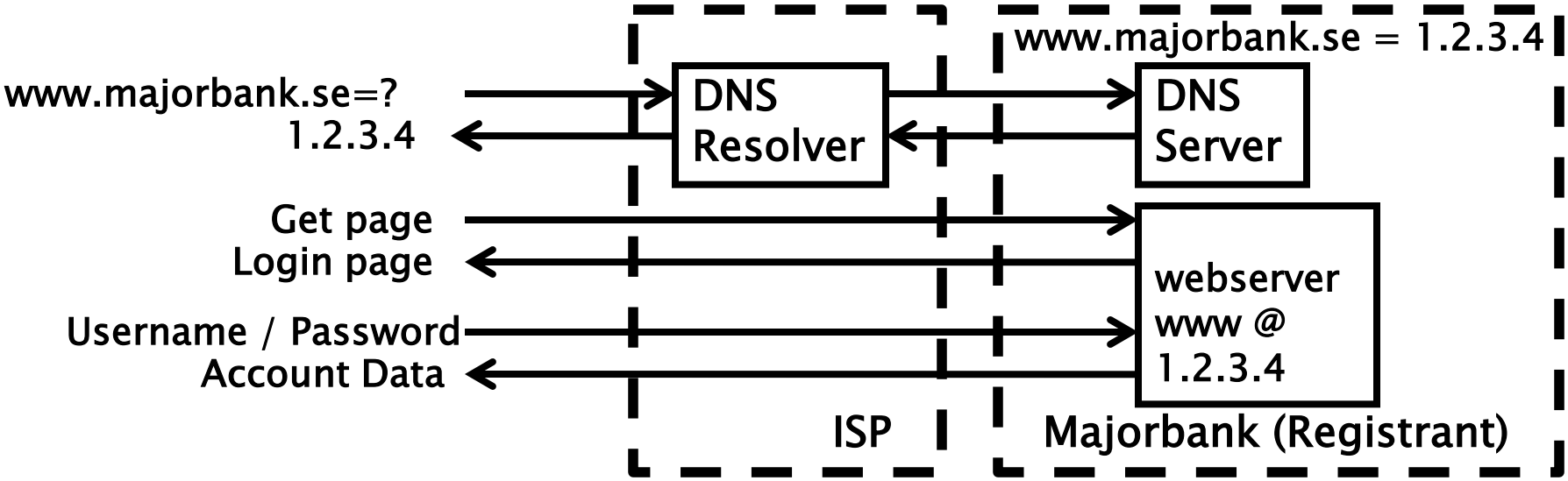
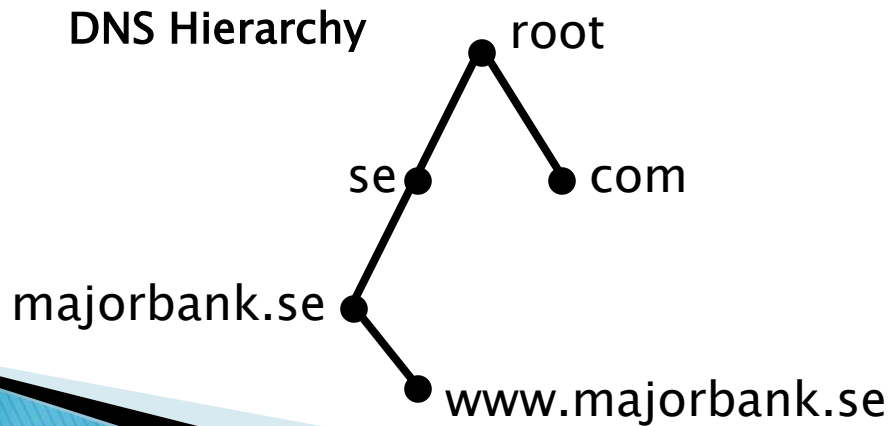
# DNSSEC 101

6 March 2012

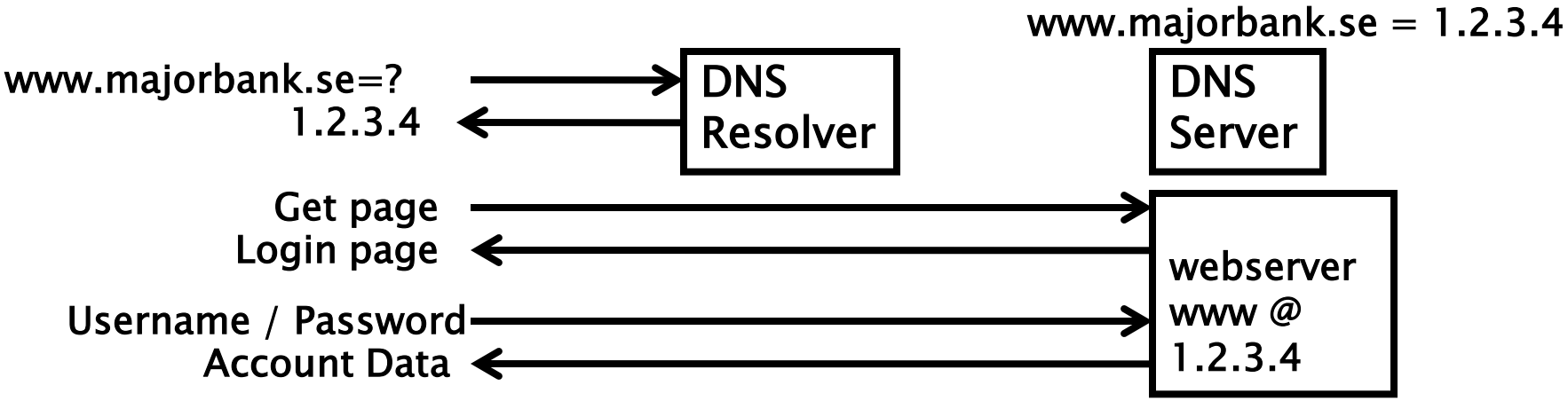
richard.lamb@icann.org

# The Internet's Phone Book – Domain Name System (DNS)

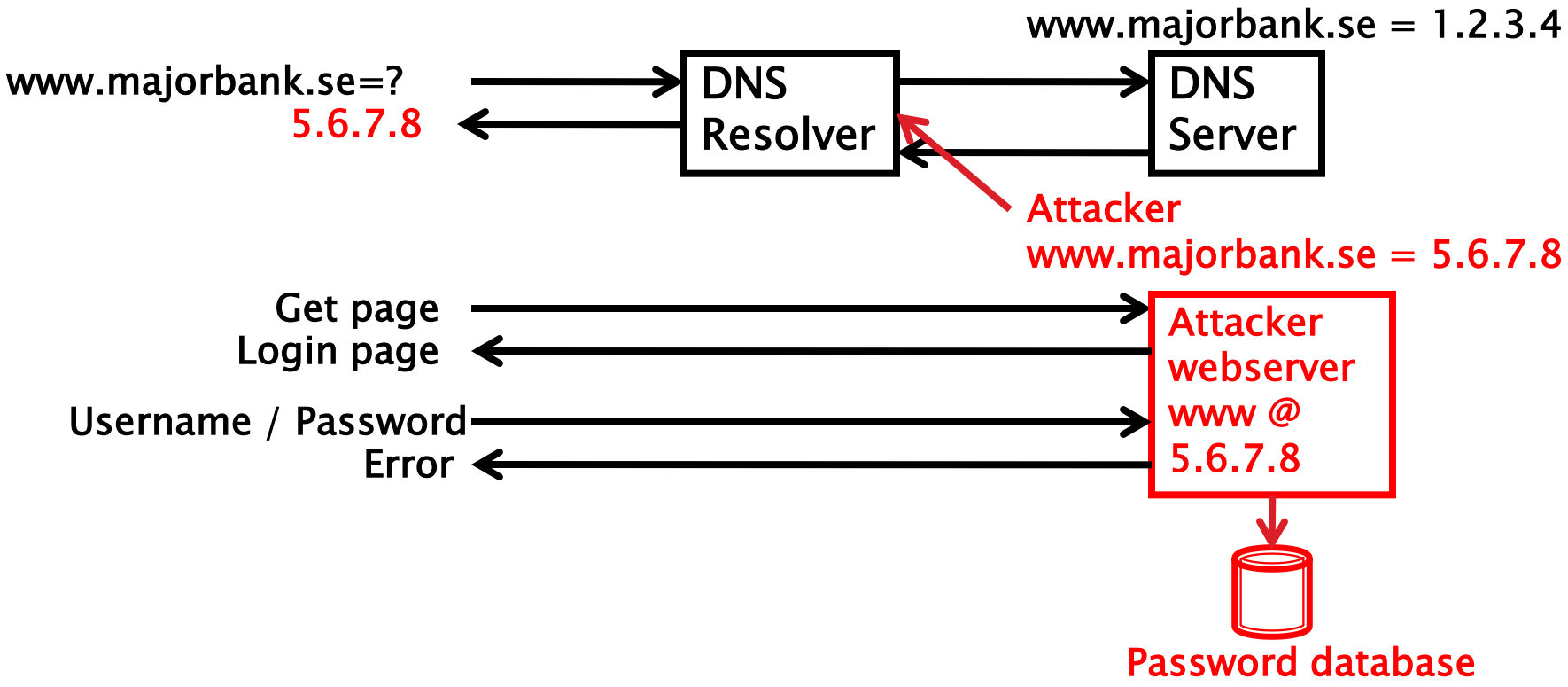


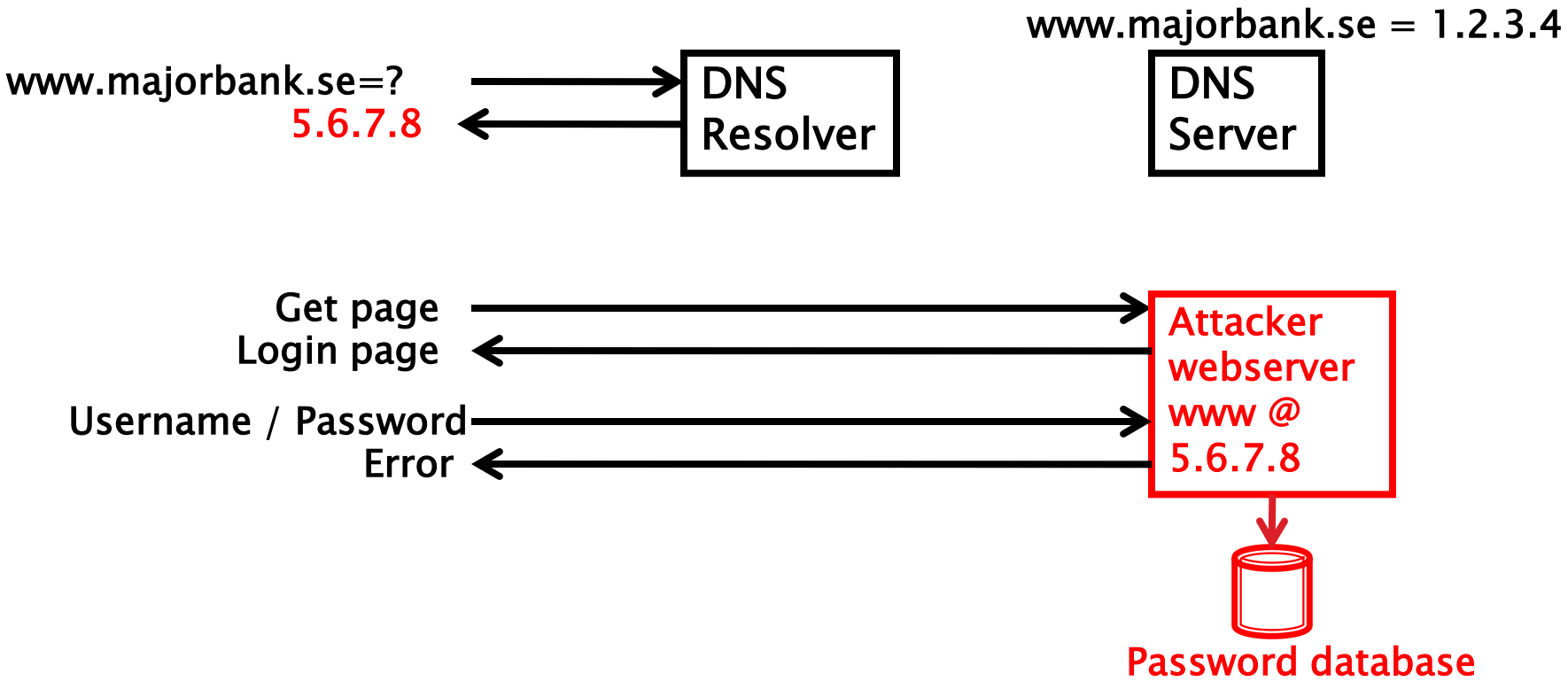
# Caching Responses for Efficiency



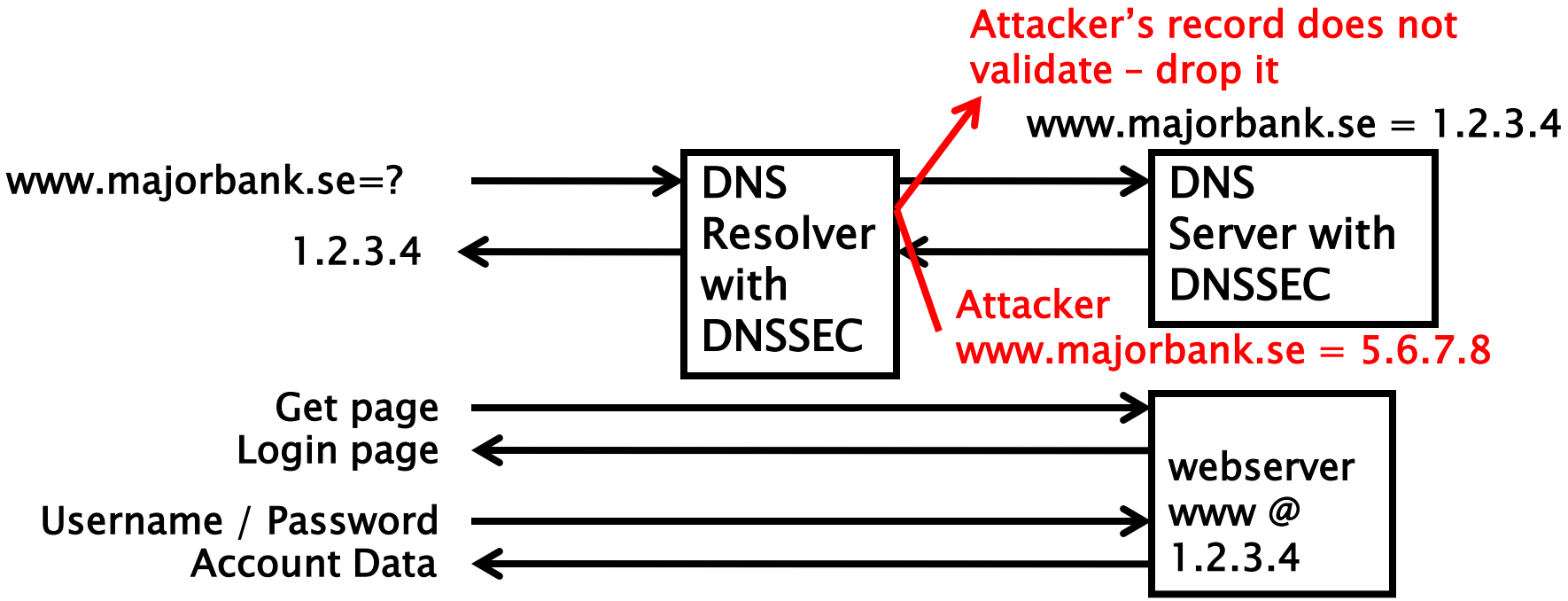
# The Problem:
# DNS Cache Poisoning Attack



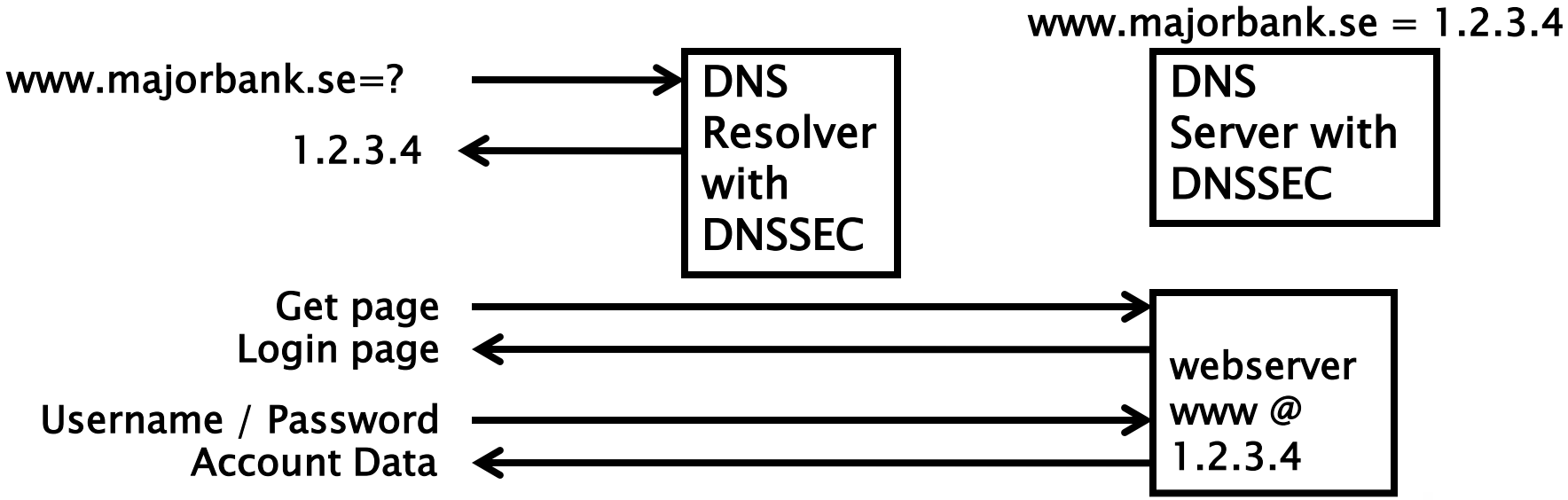
# Argghh! Now all ISP customers get sent to attacker.



# Securing The Phone Book – DNS Security Extensions (DNSSEC)



# Resolver only caches validated records



# History

- DNS developed: 1983.
- Discovered vulnerability:1995
- Triggered15+ years DNSSEC work in IETF
- 2007 Some ccTLDs have deployed DNSSEC.
- Community presses ICANN to deploy DNSSEC at root
- Aug 2008 Dan Kaminsky reveals DNS vulnerability shortcut
- Root signed June 2010 with direct international participation
- Nov 2011 report: DNSChanger/Ghost Click: 4M PCs across 100 countries suffer redirection. Large scale Brazilian ISP DNS poisoning attack
- Recognition of global PKI spurs development of innovative security solutions beyond DNS.



ICANN

# DNSSEC Deployment: Where we are now

- Passed the point of no return
- Deployed on 84/313 top level domains (e.g., .se, .com,台灣 …) and the root.
- 84% of domain names can have DNSSEC deployed on them.
- Large ISP has turned DNSSEC “on”*.
- Supported by most DNS implementations.
- But deployed on < 1% 2nd level domains (e.g., paypal.com).

*10Jan12 17.8 M COMCAST Internet customers. Other ISPs include Vodafone, Telefonica CZ

6 March 2012 rhl

# How it Works

- DNSSEC uses public key cryptography where the private half of keys are used to create digital signatures for records and the public halves used to verify that they have not been modified.
- The Zone Signing Key (ZSK) public-private key pair is used to sign each record of a zone file, i.e, web server IP address, mail server, etc.
- The Key Signing Key (KSK) pair is used to sign the ZSK and KSK itself.
- All someone needs is the public KSK half to validate all records in the zone.
- By having each zone sign the KSK of its subordinate zone, a chain of trust is created from registrant to ISP/end user.



ICANN

# *Trust us with your Money Bank (Registrant)*

**www.mybank.se**

**IP address = 192.101.186.8**

*Signature of mybank.se-ZSK1234*

**mybank.se ZSK signature**

*6 march 2012*

**Date**

# *Trust us with your Money Bank (Registrant)*

**mybank.se ZSK = 1234**
**mybank.se KSK = 5678**

*Signature of mybank.se-KSK5678*

**mybank.se KSK signature**

*6 march 2012*

**Date**

Dot SE

*Trust us, we are Swedish (Registry)*

**mybank.se KSK = 5678**

Signature of se-ZSK9012

**se ZSK signature**
1 march 2012

**Date**

Dot SE

*Trust us, we are Swedish (Registry)*

**se ZSK = 9012**
**se KSK = 3456**

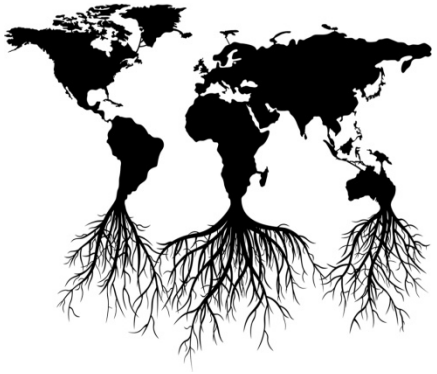
Signature of se-KSK3456

---

**se KSK signature**
1 march 2012

---

**Date**



# *Multi-stakeholder Root*

**se KSK = 3456**

*Signature of root-ZSK7890*

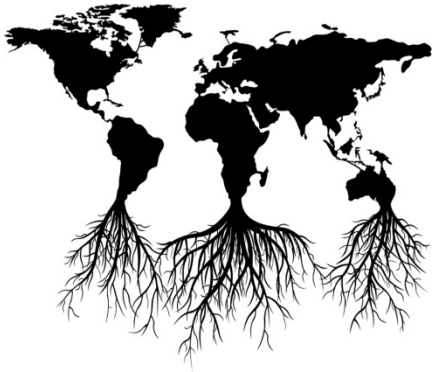
**root ZSK signature**

*28 February 2012*

**Date**



ICANN



# *Multi-stakeholder Root*

**root ZSK = 7890**
**root KSK = 1903**

*Signature of root-KSK1903*

**root KSK signature**

*2 February 2012*

**Date**



ICANN

# *End User Trusted Operating System or ISP*

**root KSK = 1903**

*O/S Vendor Signature*

**O/S Vendor Signature**

*1 January 2012*

**Date**

# Roles and responsibilities at the registry, registrar, registrant

- Registrant is responsible for generating, signing their records with, and publishing KSK and ZSK.
- Registrar manages DS (derived from KSK) record at the Registry on behalf of the Registrant.
- Registry generates, signs Registrant DS records with, and publishes its own KSK and ZSK.
- The root generates, signs Registry DS (derived from KSK) records with, and publishes its own KSK and ZSK.
- ISP/End User uses a copy of the public half of the root KSK above and uses it to recursively validate and cache responses on behalf of end user DNS lookup requests.

**Registrant→Registrar→Registry→Root→ISP→End User**

# Walkthrough Typical Example

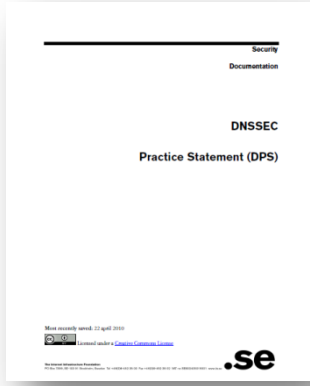
1. Registrant goes to Registrar to get domain name.
2. Registrant selects Registrar provided DNS hosting and DNSSEC signing services.
3. On behalf of Registrant, Registrar generates KSK and ZSK and submits KSK (DS records) to Registry.
4. Registry automatically signs DS record with Registry's ZSK. Registry KSK/DS has previously been incorporated into the root and signed by root ZSK.
5. Registrant edits DNS records on Registrar (www, etc) and Registrar automatically signs records with ZSK.
6. ISP follows the chain of signatures to validate DNSSEC signed DNS records and only sends valid entries to end users.



ICANN

# Common Issues (but all getting better)

- Expiring signatures: monitoring, automation
- Complexity: experience, automation, training
- High equipment cost: $20K→$5
- Security and Trust: multi-person access, transparency (lessons learned from CAs)
- Lack of Registrar and ISP support: Raise registrant and end user awareness
- Random number generation: careful consideration, standards




```
int getRandomNumber()
{
    return 4;  // chosen by fair dice roll.
               // guaranteed to be random.
}
```

ICANN

# Links

- IETF RFCs
  RFC 4033 DNS Security Introduction and Requirements
  RFC 4034 Resource Records for the DNS Security Extensions
  RFC 4035 Protocol Modifications for the DNS Security Extensions
- ISOC Deploy360 Program

http://www.internetsociety.org/deploy360/dnssec/

- DNSSEC Deployment Initiative

http://dnssec-deployment.org/

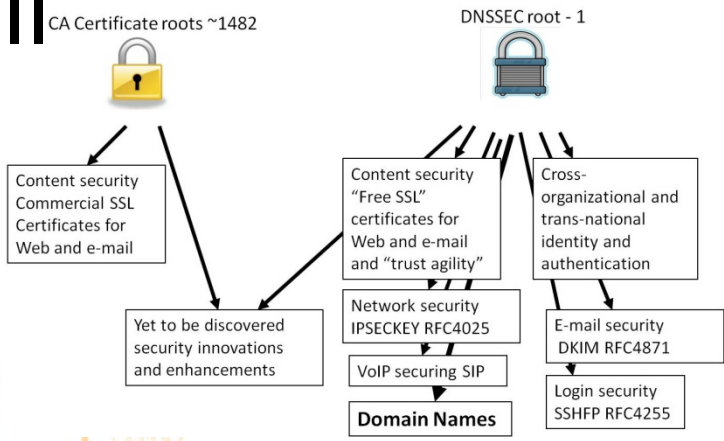
- Contact ICANN if interested in training

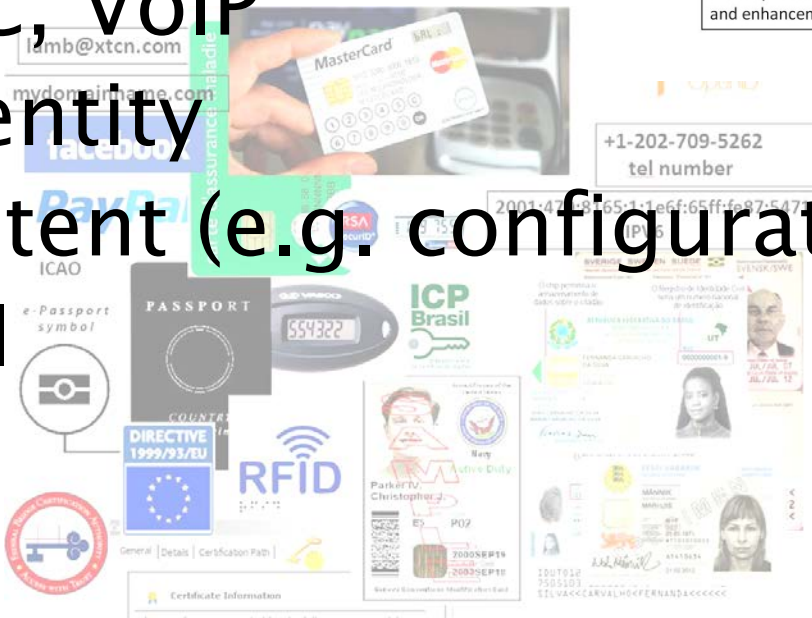


ICANN

# But wait, there is more..

- DANE
  - Improved Web TLS for all
  - Email S/MIME for all
- Other…
  - SSH, IPSEC, VoIP
  - Digital identity
  - Other content (e.g. configurations)
  - Global PKI



+1-202-709-5262
VoIP

US-NSTIC

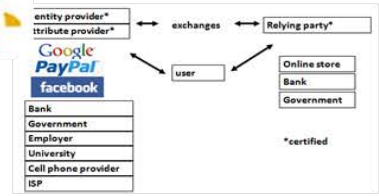
# DNS is a part of all ecosystems

Google
OpenID

facebook

PayPal

AADHAAR





e-Passport symbol

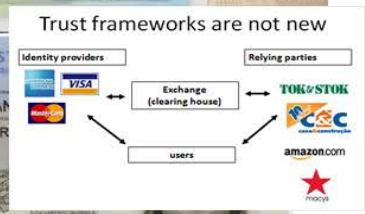


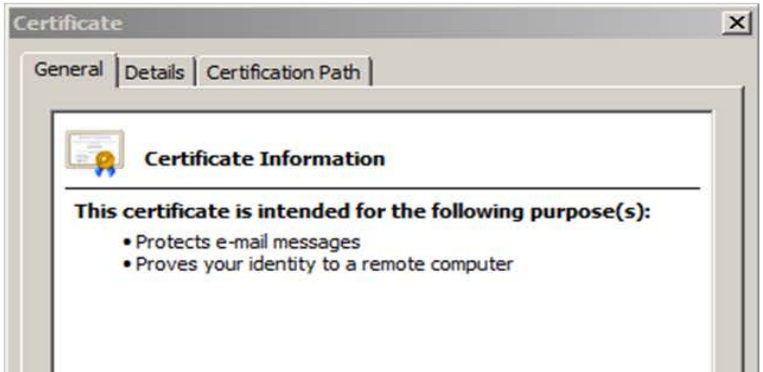
ICP Brasil
O Brasil na era da certificação digital


DigiNotar
A VASCO COMPANY

COMODO
Creating Trust Online

Smart Electrical Grid





lamb@xtcn.com

# Summary

- DNSSEC is the biggest improvement to the Internet's core infrastructure in over 20 years.
- Deploying DNSSEC need not be complicated or costly.
- DNSSEC does not solve all the ills of the Internet but can become a powerful tool in improving security.
- DNSSEC is a cross-organizational and trans-national platform for cyber security innovation and international cooperation.
- In order to realize the full benefits of DNSSEC, greater end user and registrant awareness is needed to drive a virtuous cycle of trustworthy deployment.



ICANN

# Thank You