.SE's experience testing and presenting Internet Health

Anne-Marie Eklund Löwinder

Quality & Security Manager

amel@iis.se

Three years of trial and learning

- From quite rudimentary tools 2007 – to a flexible reusable tool with historic data 2009.
- Showing slow progress in some areas, but not as much as you want.
- Digging deeper and deeper for each year.

Survey

- In all, 663 domains and 867 unique name servers were tested.
  - Public authorities at the central level (231)
  - Public authorities at the local level (290)
  - County councils (21)
  - Public utilities and state-owned companies (40)
  - Internet service providers (15)
  - Companies within media (24)
  - Banks and insurance companies (21)
  - Largest listed companies (30)
  - Universities and university colleges (33)
  - Comparison with a control group of 10,000 randomly selected .se domains.

Check up

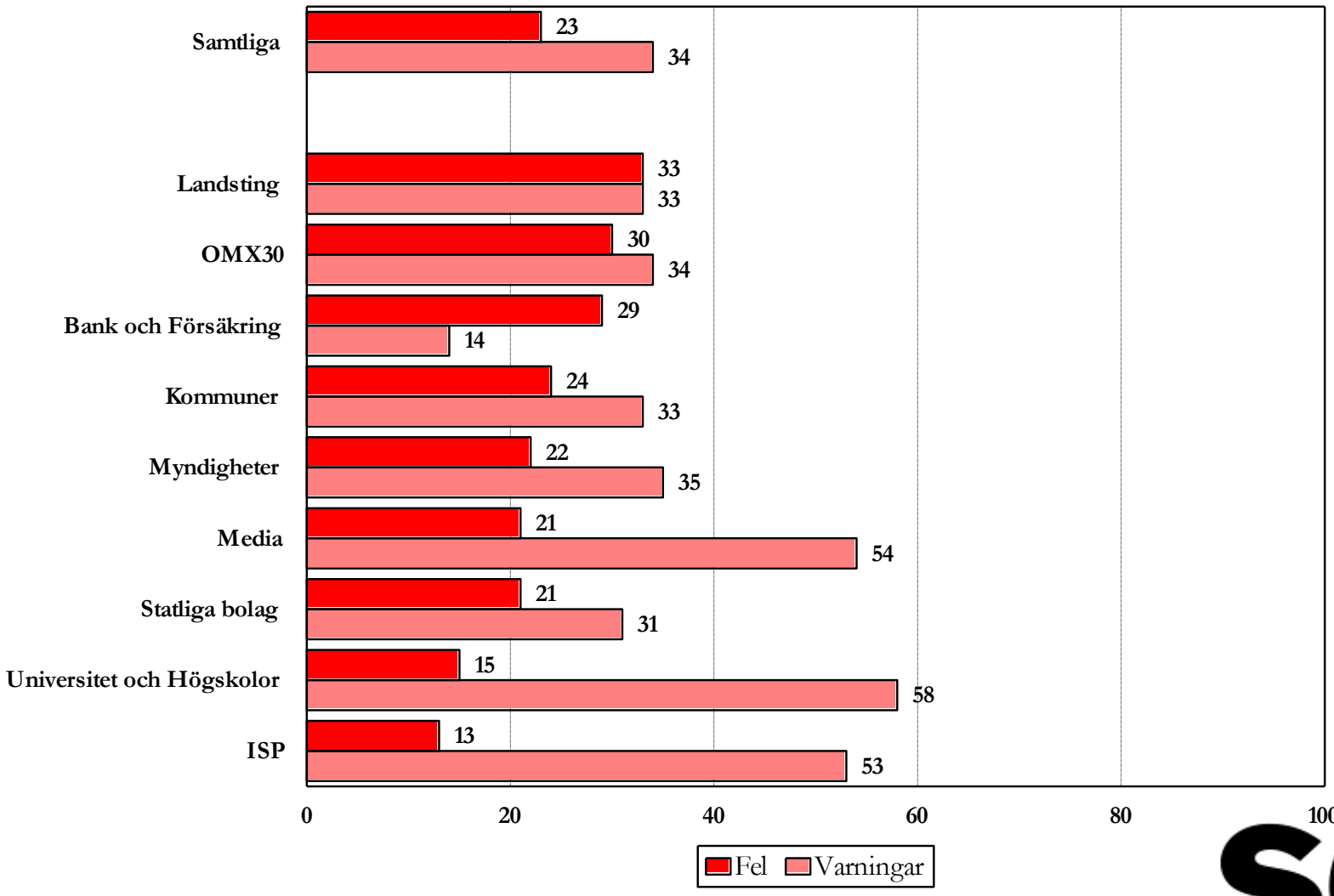
- Quality and reachability in the domain name system (DNS).
  - Compliance to Best Common Practice.
  - Open recursive name servers, Kaminsky vulnerability.
  - Deployment of DNSSEC.
- Deployment of IPv6.
- Important details relating to e-mail and web.
- Comparison of test results from 2007-2009.

.se

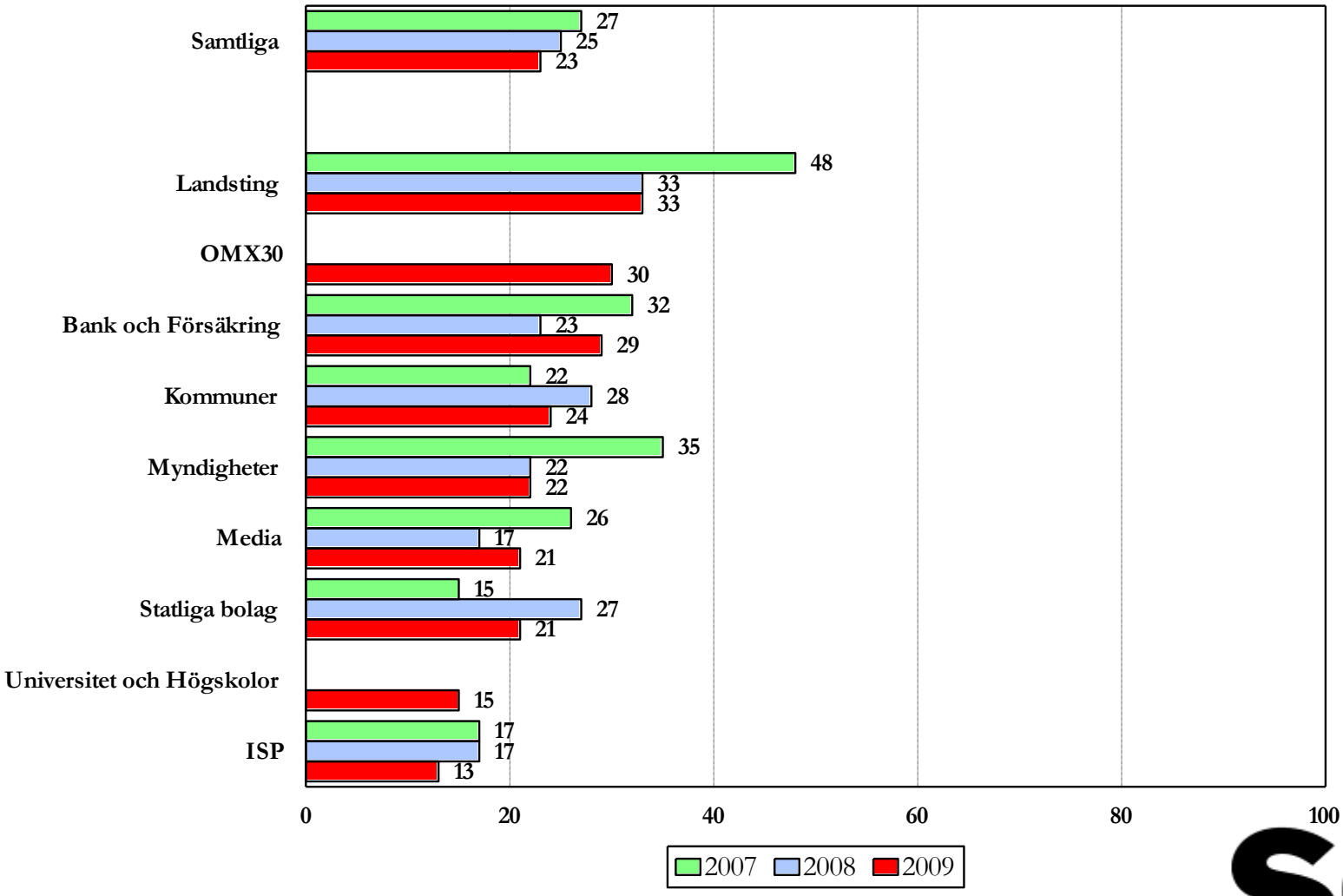
Definition - quality in DNS

- A robust DNS infrastructure with high reachability.
- All name servers involved answers all queries correctly.
- Domains and name servers are correctly implemented.
- DNS data in DNS about certain domains is valid and updated.
- The organisations DNS is compliant to standard.

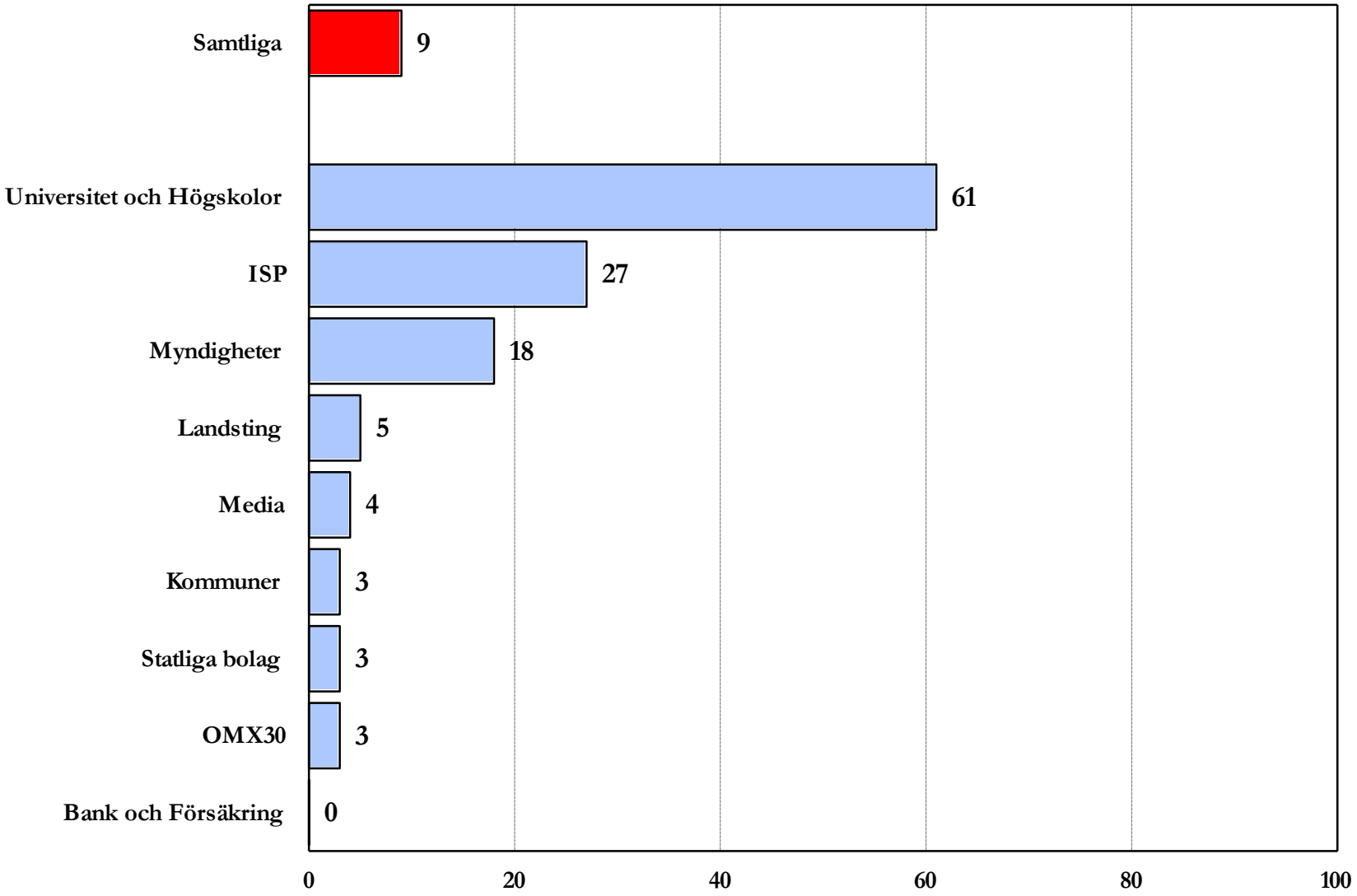
Findings 2009 – Errors and warnings



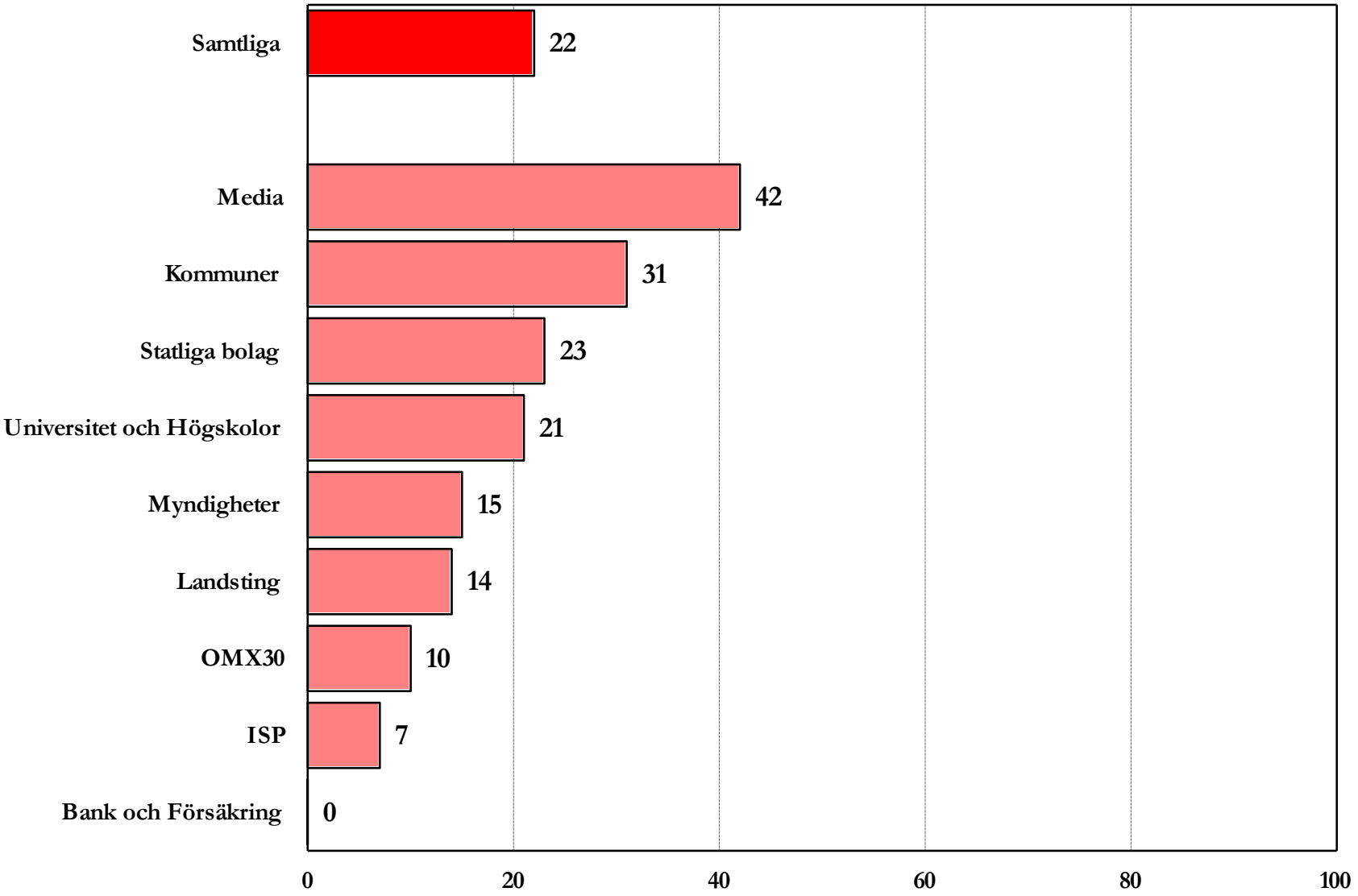
Errors and warnings 2007-2009



IPv6 on name servers



Open recursive name servers



KAMINSKY BUG!SE

SVENSKA / ENGLISH

PRESENTED BY .se

About the Kaminsky bug | Test your computer | **Test your domain** | We have the solution

Is your domain safe?

To minimize the risk of Kaminsky attacks, it is important that your name servers don't answer recursive queries from just anyone. The risk of a Kaminsky attack also increases when you mix the authoritative function for a domain with the function of acting as a recursive resolver. This tool both indicates if your name servers act as recursive resolvers and test the vulnerability of these when it comes to the Kaminsky bug.

Enter a domain name to analyse [redacted] Test the domain

Insecure

The name servers tested for [redacted] are vulnerable to a Kaminsky attack. Since the recursive name servers use randomly selected ports, a Kaminsky attack is more difficult to carry out, but the risk is still there.

(Note! All authoritative name servers could not be reached. There could be unrevealed problems.)

DNSSEC not activated

The domain does not have a DNSSEC signature and is thus not secured against the Kaminsky bug in the long term.

Read more on .SE DNSSEC here.

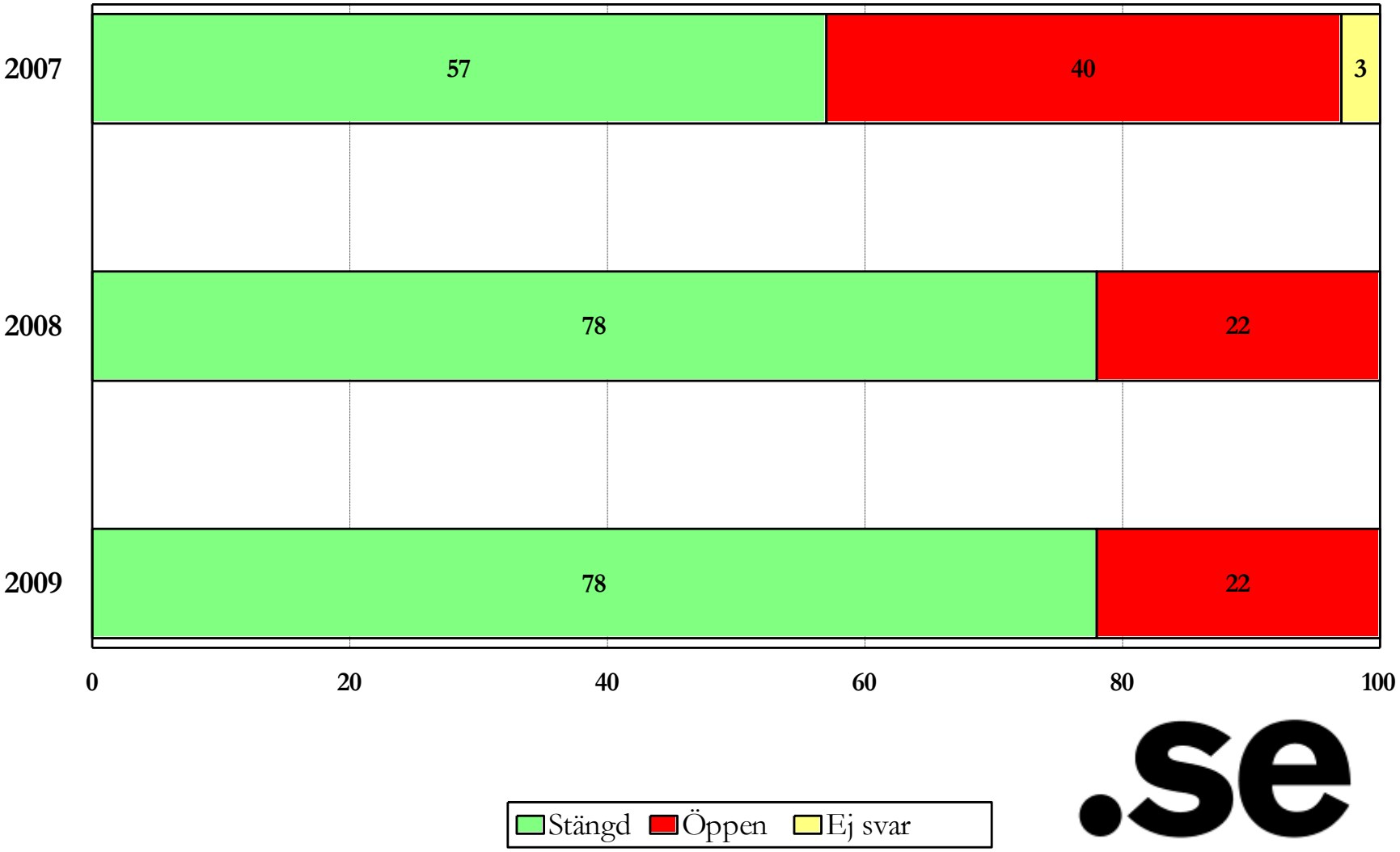
Name server	IP-address	Results
[redacted]	[redacted]	Is recursive, with random port selection

One domain– three name servers – three different responses

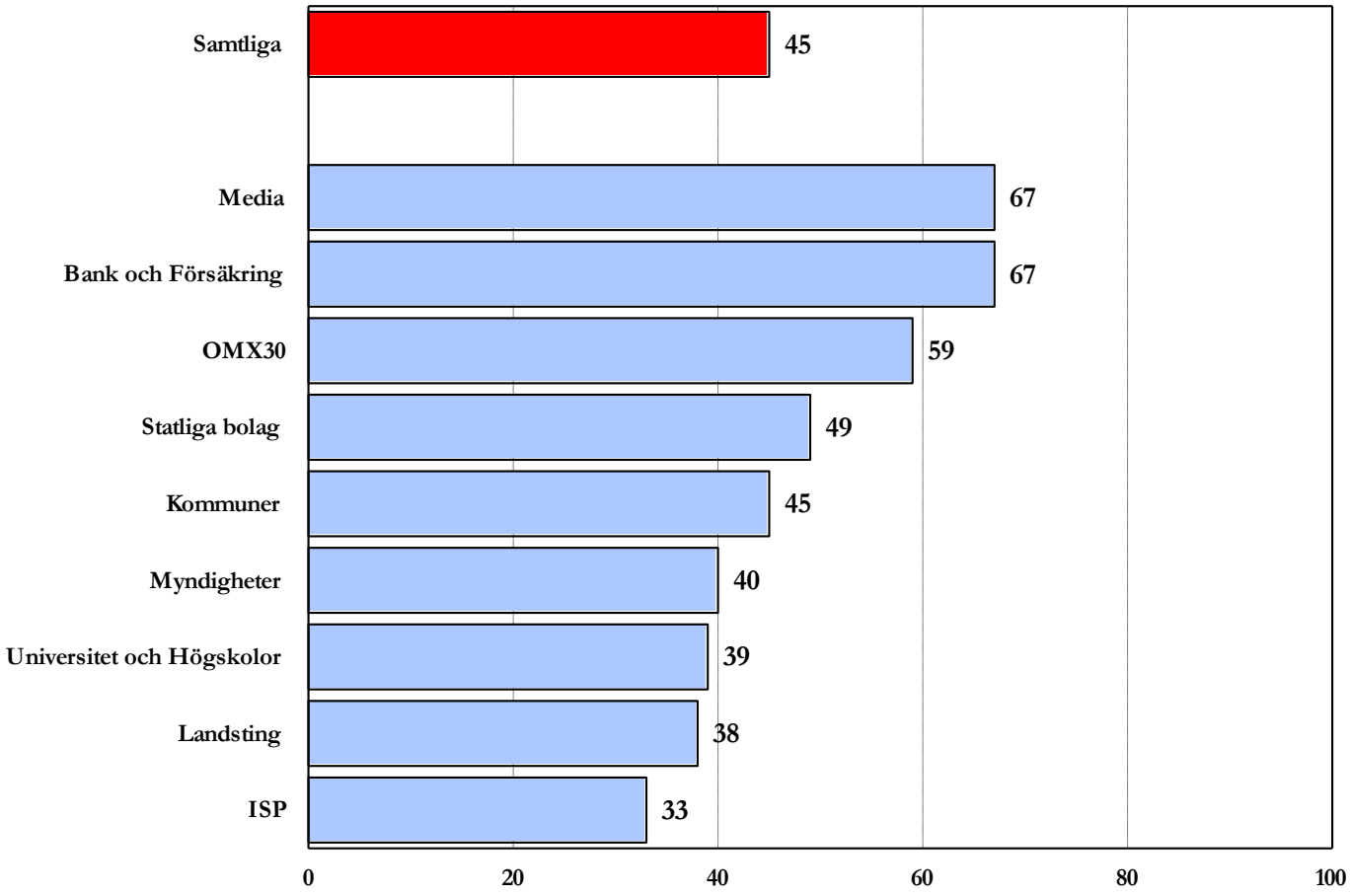
- DNS1- Is recursive, with random port selection.
- DNS2 – Not recursive.
- DNS3 - Is recursive, but doesn't seem to have random port selection.
- Note to self 1: tell the operator of DNS1 and DNS3 that they are supposed to deliver an authoritative name service.
- Note to self 2: Resolving and authoritative name servers should be separated.

.se

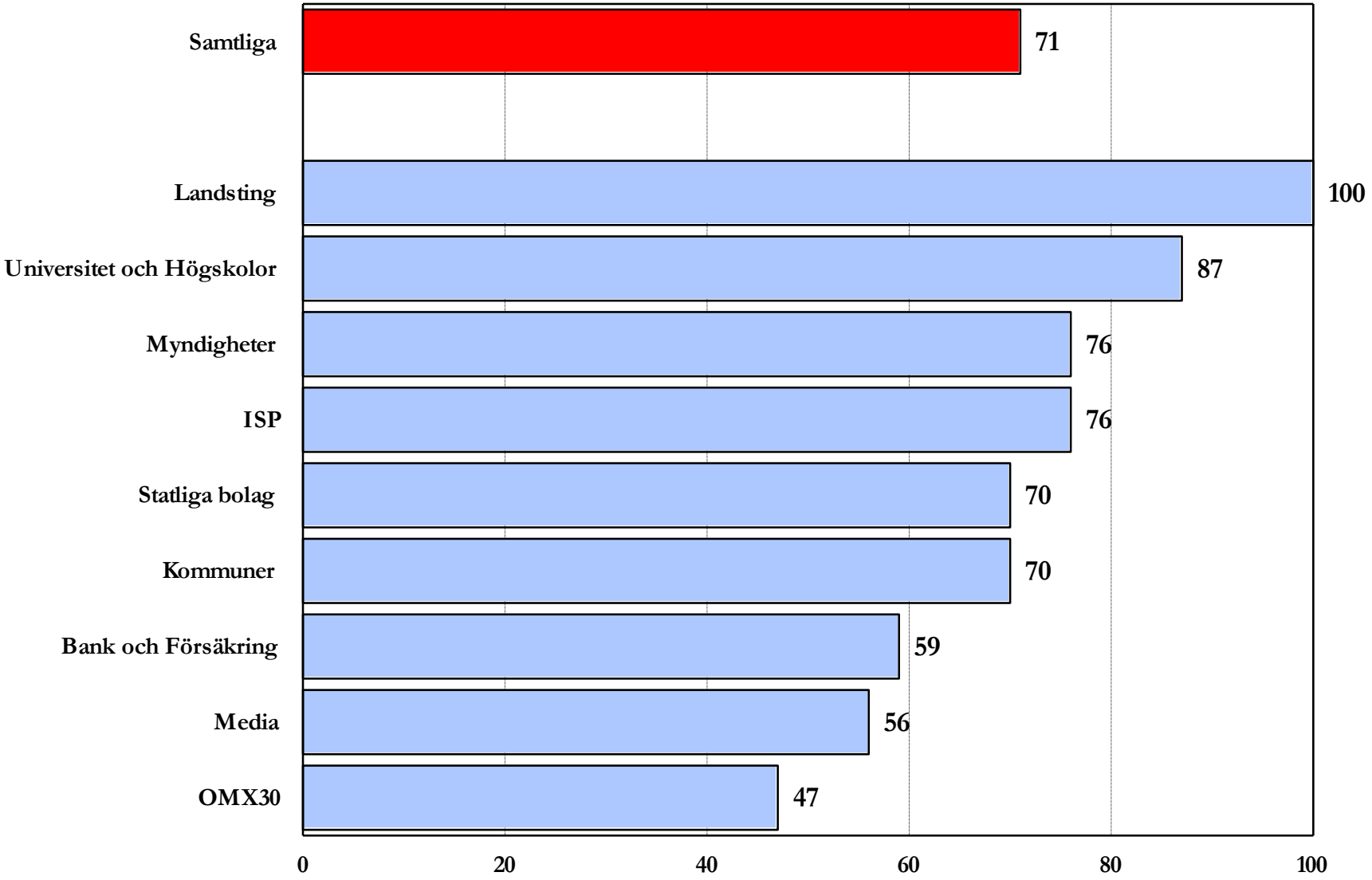
Open recursive name servers 2007-2009



E-mail servers supporting TLS



Mail servers placed in Sweden



Web servers supporting TLS/SSL using web certificates

- No more than 25 per cent has support for TLS/SSL.
- Just about 20 per cent out of the 25 have certificates issued by a well known and accepted CA (in the Mozilla Firefox browser).
- More than 20 certificates had expired, one 2004 in July.
- Many uses a weak hash algorithm (MD5) and/or short RSA keys.
- Few uses Extended Validation certificates.
- About 40 uses wild card certificates or certificates not related to the domain.

.se

Nordeas Internetbank Privat

Nordea Bank AB (SE) https://internetbanken.privat.nordea.se/nsp/eng

Google

Mest besökta | Kom igång | Senaste nytt | Verifierat av: VeriSign, Inc. | Newseum | Today's ... | Freak Kitchen | 8.0TODO - FreeBSD ...

Nordeas Internetbank Privat

Nordea Internetbanken Privat

Hem | Privat | Om Nordea | Företag

Logga in

e-kod | e-legitimation | Förenklad inloggning

Personnummer:

Kontrollkod: **978 128** (Anges i kortläsaren)

Svarskod: (Visas i kortläsaren)

Logga in

Instruktioner för inloggning

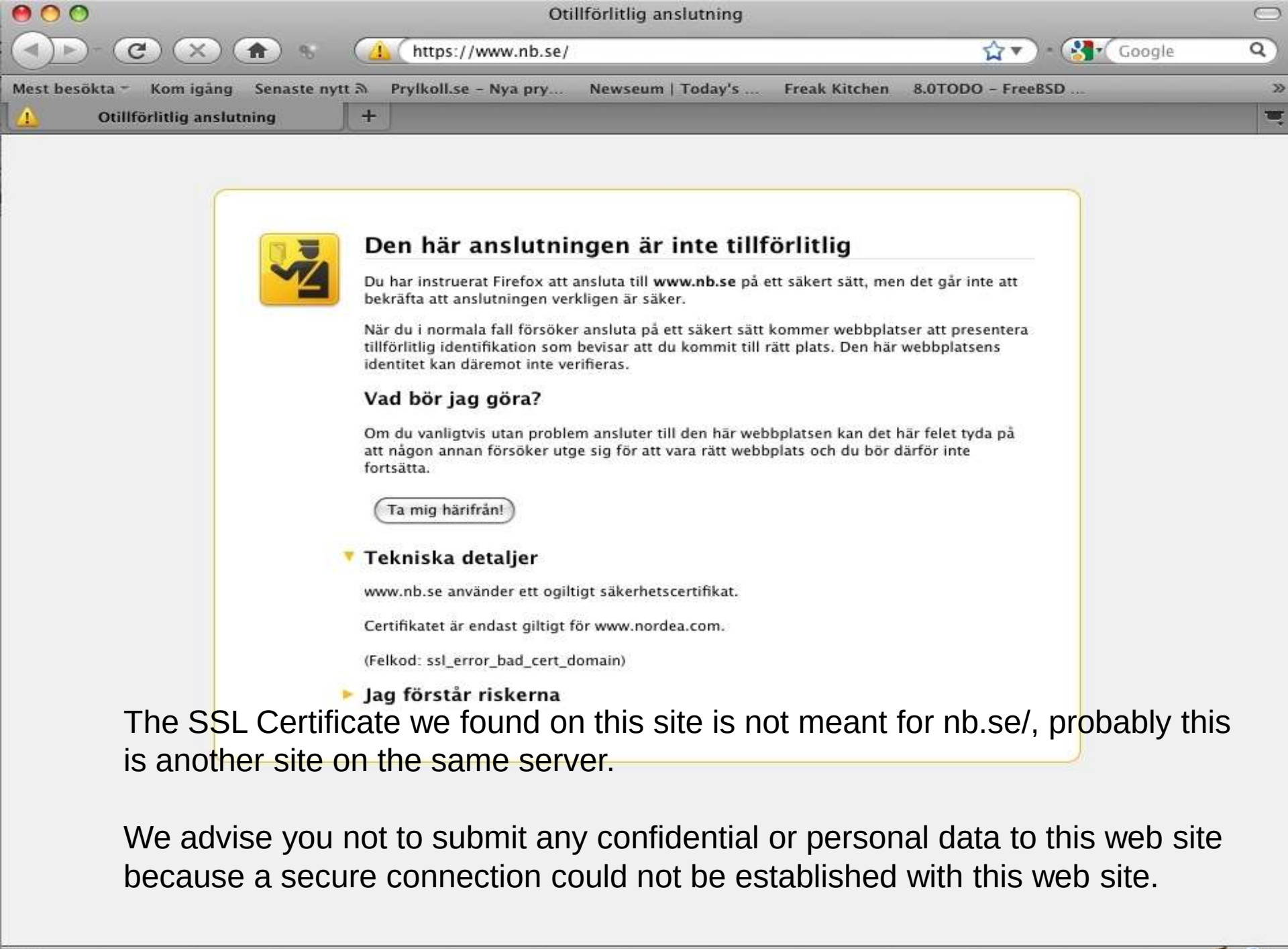
1. Starta kortläsaren genom att sätta in ditt kort utan att använda sladden. Chippet ska vara vänt nedåt och mot dig.
2. Texten "Välj Funktion" visas i kortläsarens fönster. Tryck på knappen LOGIN.
3. Knappa in ovanstående kontrollkod i kortläsaren. Tryck OK.
4. Texten "KortPIN" visas i kortläsarens fönster. Knappa in den PIN-kod du använder till ditt kort (MasterCard-, Visa- eller Inloggningskort) och tryck OK på kortläsaren.
5. Ange den niosiffriga svarskoden som kortläsaren skapat i fältet märkt "Svarskod" ovan.
6. Klicka på "Logga in" ovan.

Viktiga meddelanden

Viruskontroll

Är du orolig för att din dator kan vara smittad med virus? Gör en viruskontroll med Virusverktyget Norman Malware Cleaner

Demo och användarhandledning



The SSL Certificate we found on this site is not meant for nb.se/, probably this is another site on the same server.

We advise you not to submit any confidential or personal data to this web site because a secure connection could not be established with this web site.

Good example 1- local authorities

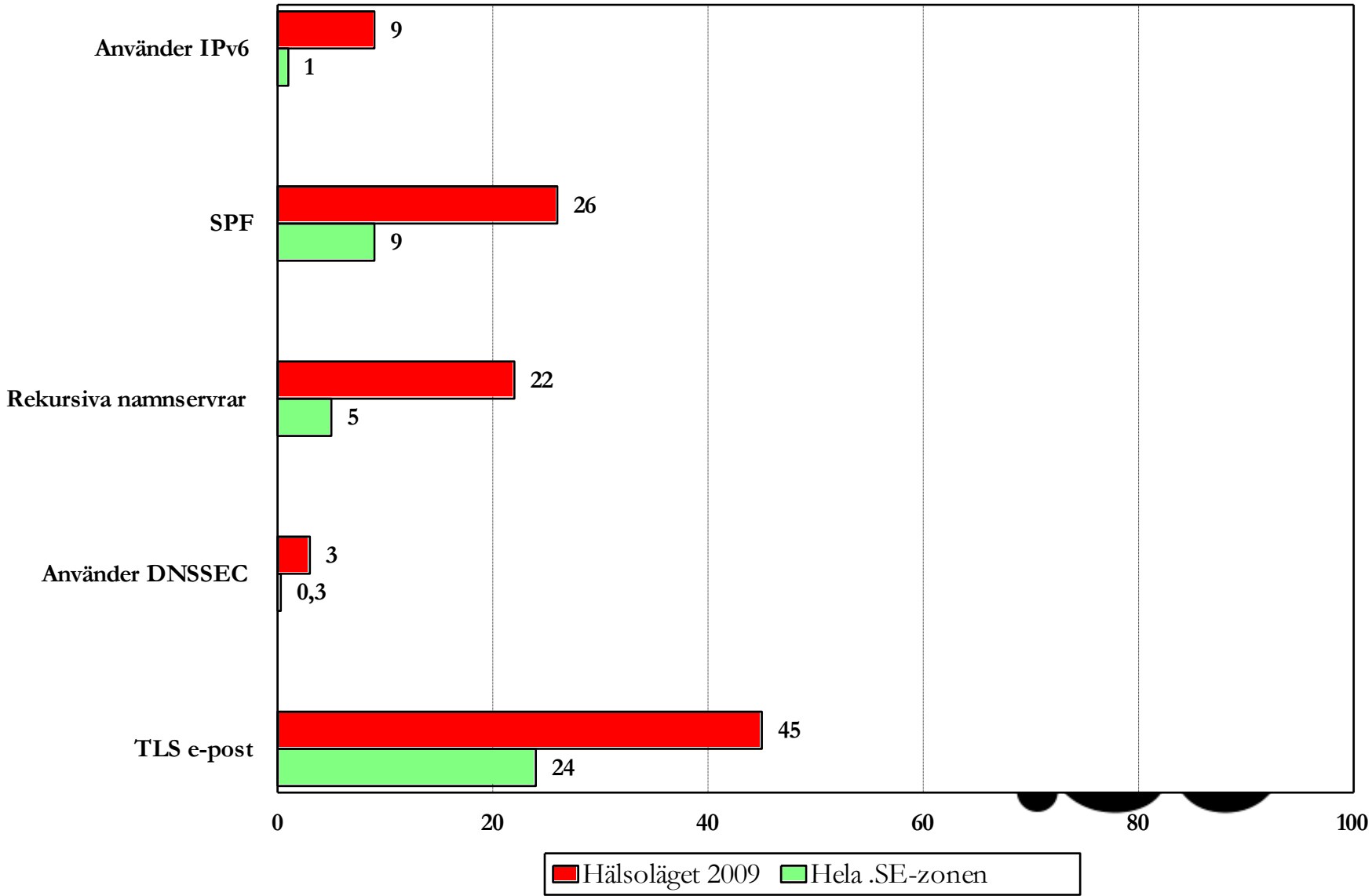
- Local authorities – recommendation for improvement of the information security:
  - Analyze the DNS with DNSCheck.
  - Check DNS-servers behind firewalls.
  - Check that SOA Expire is at least one week.
  - Check for Kaminsky vulnerability.
  - Deploy DNSSEC,

Good example 2 - Banks

- Agreed upon a common e-mail policy.
- #1: ”Valid sender of e-mail”.
  - Case 1: Bank sends e-mail to customers.
  - Case 2: Bank uses external distribution service for e-mail to customers.
  - Case 3: Bank uses external distribution to send e-mail to the banks own staff (surveys).
- #2: ”Secure e-mail communication between banks”.
- Written generally on a high level. Mentions that banks should introduce techniques to secure e-mail.

.se

Comparing with the .se-zone



Comparison – **EU TLD's (28)**

- 100 per cent have at least one server for DNS, SMTP or HTTP that has an IPv6 address announced.
- 100 per cent have domains announced in more than one AS.
- 0 per cent have name servers for the domain that allows recursive queries.

.se

Comparison – **EU TLD's (28)**

- DNS:NO_EDNS – 3,57 per cent
- DELEGATION:EXTRA_NS_PARENT – 3,57 per cent
- ADDRESS:PTR_NOT_FOUND – 42,86 per cent
- CONNECTIVITY:NOT_ANNOUNCED – 39,29 per cent
- CONSISTENCY:SOA_SERIAL_DIFFERENT – 17,86 per cent

.se

Thank you.
Questions?