.se | Health Status 2012

1 Introduction

This is the sixth in a series of reports from .SE's survey of Internet reachability and the .se zone's health status with the latest results from 2012.

This year's study is largely, though not completely, a follow-up of earlier studies conducted from 2007 to 2011.

From a purely statistical perspective, there were minor deviations due to changes in the domain-name system for the survey group concerned. It is important to understand that we are providing a snapshot of the situation at a particular point in time, which can change quickly if, for example, someone changes their environment. However, we have not made any changes to the categories, which remain the same as in the preceding year.

As with the previous survey, the aim is to chart and analyze quality and reachability, primarily of the domain-name system (DNS), as well as other vital functions for domains registered under .se. The survey has been conducted for several consecutive years, which allows for the pinpointing of trends within the areas examined. As usual, the survey was conducted on a selection of domains representing vital functions in society and a random sampling corresponding to 1 percent of all domains under .se.

This report is primarily aimed at IT strategists and IT managers, but is naturally also intended for persons responsible for the operation and management of an organization's IT and information systems. The document is also intended to be suitable for reading by individuals with an advanced interest in technology.

This survey is a part of a larger initiative that will take shape in 2013 and fall under the designation, The Internet's Ecosystem. The aim of this initiative is to monitor the quality of the Internet infrastructure in Sweden and, in accordance with our charter, to contribute to the positive development of the Internet by identifying areas of improvement and to provide the market with tools where anyone can check the status of their own domain(s) as well as that of others.

.SE's ambition is to contribute to the high functionality and accessibility of infrastructure through the collection and analysis of facts, and the dissemination of results.

This health-status report is funded by .SE. The results of this year's survey have been analyzed and the report was compiled by Anne-Marie Eklund Löwinder, Security Manager at .SE. Patrik Wallström, Project Manager at .SE, held operational responsibility for the tools that were used. The review of the statistical analysis, as well as the charts and tables was carried out by Anders Örtengren of Mistat AB.

More information about the content of the report is available from Anne-Marie Eklund Löwinder, who can be reached at: anne-marie.eklundlowinder@iis.se. More information about the technology behind this survey is available from Patrick Wallström. He can be reached at patrik.wallstrom@iis.se.

2 Summary

This year's survey was conducted in October 2012. Like the studies of preceding years, this survey focuses on DNS quality. The development of IPv6 and DNSSEC are key parameters, particularly as a result of the development of both IPv6 and DNSSEC, as these factors received special attention in the Swedish government's strategy for the IT policy area "IT in the public service – a digital agenda for Sweden".[1]

For this year's survey, we can state that we have finally achieved an error rate of below 20 percent for the survey group as a whole, or closer to 18 percent. The percentage of warnings was also substantially reduced, from 37 to 30 percent.

2.1 About the survey group

For this year's survey, a total of 913 domains were tested, distributed among 1,445 unique nameservers (both IPv4 and IPv6). The term "unique" is defined as servers with unique IP addresses. A nameserver with a service provider can house several domains. The categories we have used and the number of domains existing under each of these categories is presented in the chapter 5.

A comparison was also made with a control group comprising 1 percent of the entire .se zone, corresponding to 11,806 randomly selected .se domains that are presented in chapter 0.

To enable the monitoring of trends from year to year, we endeavored in general to stick to roughly the same parameters and survey groups that had previously been used. No radical changes were implemented to this year's survey, apart from those brought about by the addition of new organizations, organizations that have been renamed or organizations that have been removed because they no longer exist.

For example, 912 domains were surveyed in 2011, compared with 913 this year, representing a minimal difference.

The results from the survey group were also compared with a survey of 11,806 randomly selected domains, corresponding to 1 percent of all domains in the entire .se zone.

2.2 Continued reduction in the volume of critical errors

In 2007, we conducted the first survey. The 2008 investigation provided us with an indication that there had been some positive development in the area compared with 2007. When we began to see trends in 2009, we were able to confirm that the changes were negligible and that there were still major problems, which we highlighted and proposed solutions for. These were sent to the Minister of Infrastructure of the time. Unfortunately in 2010, we were unable to see any significant improvements. The results for 2011 were positive in several regards. So, how does it look for 2012?

The overall percentage of critical errors and warnings was further reduced and, for the first time, the percentage of errors has fallen below 20 percent for the majority of the domains surveyed. The situation has substantially improved

1 http://www.regeringen.se/content/1/c6/17/72/56/99284160.pdf

since 2011, both in terms of the percentage of critical errors and the volume of error warnings.

2.3 Differences compared with the 2011 survey

Our goal with publishing the results of our survey of the domain-name system annually is to create attention for the problems and deficiencies plaguing a considerable number of domains in the .se zone. Conducting the surveys over the period of several consecutive years also provides us with an opportunity to see the development trend and to assess whether or not it is possible to track the effects of some of the advice and recommendations that we communicate and if this has resulted in any corrective measures among the surveyed organizations.

The results over time confirm our hypothesis that there is a general lack of knowledge about what is required to maintain a high level of quality in, for example, the domain name system (DNS), although the definition of "high quality" is always subject to discussion.

For this compilation, it is we, .SE, who define what we consider to be of high quality and this definition is based on recommended practices, or industry standards, internationally referred to as *Best Common Practice*.

2.4 Dominant players increase the risks

The array of service providers to which nameservers are connected remained essentially unchanged from 2011. The major Internet service providers are becoming increasingly large and the small service providers are fading. One exception is Telenor, which has increased its market share, from 6 to 9 percent. The risk of many players connecting to one and the same service provider is that if a single service provider dominates a certain category, an entire sector may be affected if the individual service provider experiences problems. Consequently, it is important to have several nameservers affiliated with various service providers.

2.5 Lack of competence among consultants and service providers

The results over time have led to a conclusion that there is a lack in knowledge about what is required to maintain a high level of quality in the domain name system (DNS). This conclusion has been confirmed through the requirements on DNSSEC implementation, the introduction of which leads to requirements on issues such as key management. There are also reasons to perform an analysis of individual capabilities within a DNS infrastructure. Re-delegating a domain is a fairly drastic measure with potentially major consequences if implemented in an incorrect manner, whether it is intentional or not.

The fact that some of the most serious problems are still relatively commonplace also confirms the hypothesis that the situation has not radically improved since earlier surveys. We emphasize the need for various organizations to sharpen their purchasing competency and to place relevant demands on consultants, registrars and the suppliers providing services related to nameservers, e-mail and the World Wide Web. As far as public-sector management is concerned, there should be central support for such requirements.

2.6 Nameservers with recursion remain activated

Between 2007 and 2012, the percentage of nameservers with recursion activated declined sharply, from 40 to 10 per cent this year. Since the preceding survey, there was a further decline of 1 percent. The category Municipalities, accounts for 16 percent -- the largest remaining block of recursive nameservers. Government agencies also account for a relatively high percentage, with 11 percent. For the categories of City Councils and ISPs, the percentage is down at 0 percent. Open recursive nameservers can be misused by others and employed in denial-of-service attacks.

2.7 Increased use of IPv6

In regard to the implementation of IPv6, there is an increase from 19 to 24 percent, throughout the categories. The largest increase took place in the category Registrars, which rose from 19 percent implementation of IPv6 in 2011 to 37 percent in 2012. Universities and colleges are the category with the most commonplace use of IPv6, at 73 percent. .SE is also working proactively to increase the deployment and use of IPv6.

2.8 Increase in DNSSEC signed domains

As a result of .SE's comprehensive campaign, which was implemented in December 2011, we have seen a strong increase of DNSSEC signed domains. For this year's survey, the number of signed domains in the survey group (913 domains) increased to 100 domains, corresponding to 11 percent.

At the time of the current survey, the control group (comprising a sample of 1 percent of the entire .se zone) had 1,182 signed domains, or an increase of 10 percent. This should be compared with the 2011 survey, when only 0.45 percent or a total of no more than 50 domains in the control group were signed.

The Swedish Civil Contingencies Agency, MSB, has the ability to provide annual funds from Appropriation Bill 2:4 Crisis Contingencies that can be applied for by the state agencies indicated. In 2012, the MSB prioritized reinforcement measures to facilitate secure online address searches, which are conducted via the domain name system. Government agencies have sometimes stressed the urgency that domains for public websites be signed with DNSSEC, which .SE considers being excellent.

.SE supports and encourages DNSSEC implementation in various capacities and consequently collaborates with MSB, the Swedish Post and Telecom Agency (PTS) and the Swedish Association of Local Authorities and Regions (SALAR) to produce package solutions that may benefit municipalities. In 2011, a total of 86 municipalities were provided funds for the implementation of DNSSEC.

2.9 Increase in e-mail servers in Sweden

The 2012 survey shows that a full 42 percent of the e-mail servers with IPv4 addresses are situated in Sweden compared with 24 percent in 2011 – a relatively strong increase.

2.10 Strong increase in use of cookies

Due to the amendment to the Electronic Communications Act (2003:389) concerning cookies, .SE has also been monitoring developments in this area. Despite the stricter regulations, the use of cookies appears to be increasing in all categories. The strongest increase can be noted among municipalities and state agencies.

The PTS has been assigned by the Swedish government to investigate whether the new “cookie law” has hindered the growth of or confidence in the Internet. Their assignment will be accounted for at the end of 2012.

3 Control points

In this year's study, we gathered facts concerning the following control points:

- How does the organization manage its DNS? Who is responsible for DNS within the organization, what is its structure (in relation to what can be considered to be industry standard or Best Common Practice, BCP), what are the most serious deficiencies and in what categories do they most frequently occur?
- What is the frequency of nameservers being open for recursion?
- How does the organization manage its e-mail? Are the servers situated within or outside Sweden, and do they employ TLS/SSL (transport-layer security)?
- How does the organization connect its websites to the Internet? What type of server software is used? How are cookies used?
- Has IPv6 been implemented in the organization's IT environment?

The domains and nameservers of a large number of important organizations in society were tested: public service and state-owned companies; banks, insurance and finance companies; Internet service providers; municipalities; county councils; media companies and state agencies, including county administrative boards and universities and colleges, as well as .SE's registrars for a total of 913 domains. The allocation by category is presented in chapter 5.

The data-collection process was automated and included testing of the most frequently occurring errors and deficiencies we associate with DNS operation, e-mail and web server management, in relation to what is considered standard practice.

Based on these tests, we investigated how well the organizations' systems function in various contexts, the areas in which the most serious errors arise and performed analyses of the possible consequences. The report enables a comparison with all previous surveys, meaning a total of five to six years of survey results.

We have also linked this information to general recommendations on what we would like the Swedish DNS infrastructure to be like. Finally, and we can hardly emphasize this enough, we have yet again provided some guidelines and recommendations containing proposals to the responsible authorities; corrective measures that we consider suitable to pursue and study in greater detail.

We are allowing these to remain essentially unchanged from last year's survey since the results from the survey clearly speak for themselves, namely that there are still inadequacies that need to and can be corrected.

By cultivating such strategic partners as the PTS and MSB, .SE has helped enable municipalities to apply for grants to pursue projects to implement DNSSEC, even for 2013. These funds will be granted and made available for claim as of 2013. We recommend that government agencies and individuals in decision-making positions adopt our advice and recommendations and take the actions to make improvements in all the areas concerned: DNS, DNSSEC and IPv6, as well as the protection of e-mail and web server communications.

4 Quality DNS service

The domain name system (DNS) is one of the Internet's cornerstones and its task is to simplify the addressing of Internet resources. .SE is responsible for Sweden's national top-level domain on the Internet, an assignment that is considered so important that it is regulated by a special law, the National Top-Level Domains for Sweden on the Internet Act (2006:24)[2]. Each Internet-connected unit has its own IP address, which, using DNS, can be connected to an address that is easier for people to handle, meaning a domain name.

We monitor that some 1,250,000 domain names with the .se suffix can delegate the right resources online by maintaining a registry of these names, and routing queries and responses placed with the domain name system. In this manner, connections to the correct web server or e-mail server are as a rule, virtually instantaneous.

We ensure that DNS queries to .se domains are responded to on the Internet round the clock and every day of the year. .SE's nameservers respond on average to 5,000 queries per second, with peaks that sometimes exponentially increase the number of queries.

We have applied the following definitions of quality DNS service to the survey in 2012 and in previous years, where quality for us means:

- That the organization has a robust DNS infrastructure with a high level of reachability.
- That all nameservers involved respond to queries correctly.
- That domains and servers are correctly set up.
- That data in the domain name system about individual domains is correct and up to date.
- That the organization's communication structure, when viewed as a whole, meets the requirements imposed by relevant Internet standards and other standards.

It is important that an organization's DNS infrastructure complies with the current standards and that it is designed in such a manner that it provides robust service with a high level of reachability, regardless of whether the organization operates its own DNS or has outsourced maintenance to an external partner.

Our basis for the investigation is an experience-based industry standard, or Best Common Practice (BCP), of what is considered to be a solid DNS infrastructure.

The fact that some of the most serious errors are still relatively commonplace also confirms the hypothesis that there has been no radical improvement to the situation since earlier surveys. We emphasize the need for various organizations to sharpen their sourcing expertise and to place relevant requirements on consultants, registrars and the suppliers providing services related to nameservers, e-mail and the World Wide Web. As far as public-sector

[2] https://lagen.nu/2006:24

management is concerned, this would be facilitated by central support for such requirements.

In Appendix 4, we present recommendations for more technically inclined readers as to what the industry standard requires to create a high-quality DNS infrastructure in Sweden.

5 Tests in 2012

The tests in 2012, as usual, comprised the domain configurations and statuses of the nameservers responding to queries about the domain, as well as what we consider to be some of the most vital parameters for e-mail and web servers. However, for this survey, we did not look into certificate management on web servers. The reason is that it is difficult to produce reliable data, which requires tools other than those we have access to at the moment. However, this is an area that we intend to examine in greater detail next year, in the same manner that we examined DNSSEC in greater detail (report[3] published in March 2012) and will now delve deeper into electronic mail (with a more detailed report that will be published in November 2012).

The tests that are the basis for this report made use of software that automatically checks the various control points stated in the industry standard for all domains included in the survey, for the survey group as a whole and by category. This was supplemented by certain queries, including those pertaining to the management of electronic mail and web servers.

The tests this year were implemented at the same point in time as in preceding years and included 913 domains on 1,445 unique nameservers. The test subjects were grouped into the following categories (the figures in parentheses pertain to the number of organizations that were included in each category last year):

- 57 public service and state-owned companies (60).
- 81 banks, financial institutions and insurance companies (79).
- 21 Internet service providers (ISPs) (22).
- 290 municipalities (290).
- 21 county councils (21).
- 36 media companies (34).
- 229 government agencies, including county administrative boards (excluding agencies under the Swedish Parliament) (228).
- 37 universities and colleges (39).
- 151 registrars (146).

The Registrars category, meaning resellers of .se domains, are often providers of nameservers and other services to domain owners. The number of registrars accredited by .se is continuously changing.

As in earlier years, we reported two different types of problems and categorized them as either errors or warnings.

3 https://www.iis.se/docs/Halsolaget-DNS-och-DNSSEC1.pdf

Error: Anything marked as an error in the survey pertains to such that directly affects operation and should be corrected immediately so that the organization can be assured of a high level of availability and reachability in DNS and other resources.

Warnings: The warnings constitute errors that may potentially influence operation, but which are deemed to be less critical and their rectification less urgent. If these errors were corrected, they would naturally raise the quality and level of reachability.

6 Observations in 2012

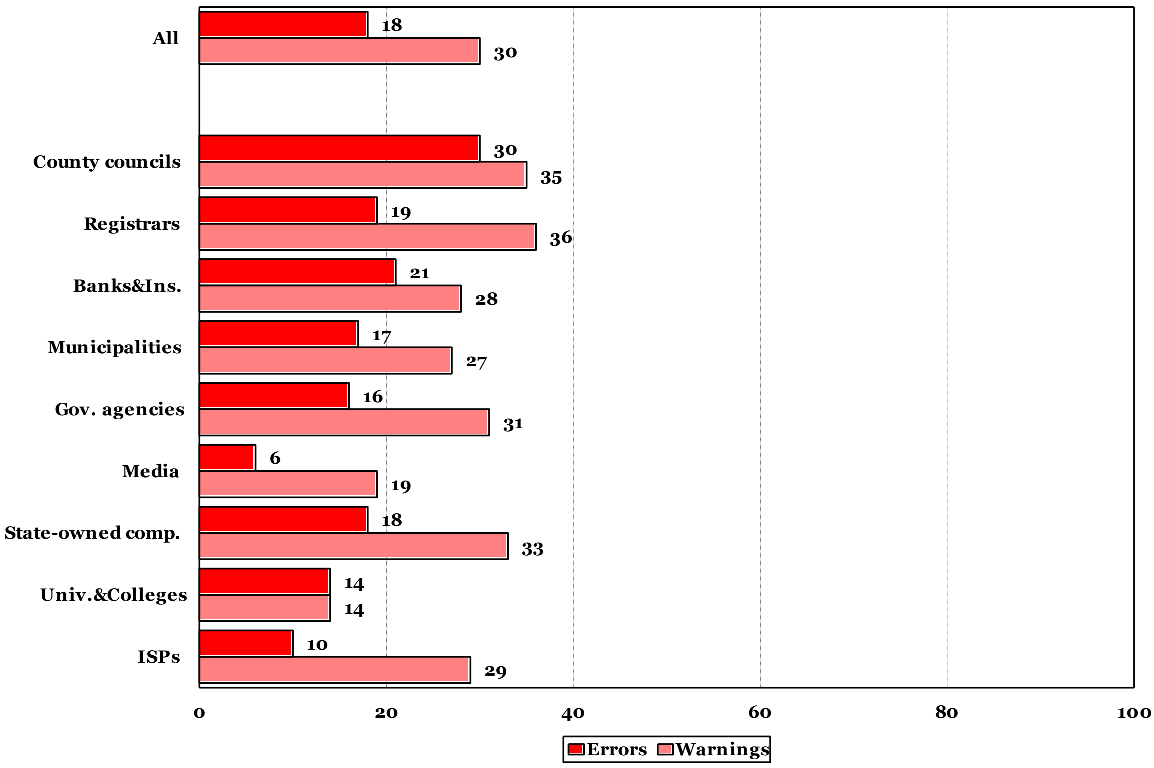
In 2007, we conducted the first survey to gain an understanding of the status of the .se zone. The 2008 survey gave us an indication that some positive developments had occurred in the area. When we began to see trends in 2009, we were able to confirm that the changes were negligible and that major problems remained, which we highlighted and proposed solutions for. In 2010, serious inadequacies remained and we were unable to observe any improvement, in fact, quite the opposite. Of the domains tested in 2010, 25.4 percent had critical errors and 43.4 percent had deficiencies of a nature that resulted in a warning. In the 2011 survey, the corresponding figures were: 21 percent with critical errors and 37 percent with deficiencies of a nature that resulted in a warning.

For this year's survey, we can state that we have finally achieved an error rate of below 20 percent for the survey group as a whole, or closer to 18 percent. The percentage of warnings was also substantially reduced, from 37 to 30 percent.

6.1 Tests of DNS – errors and warnings

The distribution of errors and warnings between the various categories included in the survey are presented in the graph below.

Graph 1: Errors and warnings



The graph on the previous page shows the percentage of errors and warnings for all 913 domains in the entire survey group (referred to as "All"), and for each individual category. The bars of the graph indicate that of the 913 organizations included in the study, 18 percent had serious errors and 30 percent had errors of a nature that generated a warning. This is a clear improvement compared with the 2011 survey.

For a more detailed description of the distribution of errors and warnings by category and year, refer to chapter 0.

6.2 Most frequently occurring errors

The most common DNS errors among the tested domains and nameservers that generated either an error or warning in accordance with our definition have remained essentially the same throughout all the years we conducted the survey.

- The nameserver did not respond to a query via TCP (Transmission Control Protocol). This is probably attributable to the DNS server being incorrectly set up or an incorrectly configured firewall. We are attempting to determine the nature of the high percentage of this particular error occurring in the City Council category, but have yet to arrive at any conclusions.
  It is a fairly common misconception that DNS implementations do not need to be capable of communicating in accordance with the TCP protocol (unless they provide zone transmissions). However, TCP is a requirement under standard (RFC 5966, *DNS transport over TCP implementation requirements*), and the trend is that the need for TCP is increasing as new protocols such as IPv6 and DNSSEC result in it being used more extensively than in the past. This error indicates that the person who configured the nameserver or firewall has insufficient current knowledge of DNS.

- The organization has no consistent nameserver (NS) structure. The nameservers listed with NS records in a child zone differ from the information found in DNS in the parent zone and, accordingly, the nameservers cannot respond authoritatively and properly on behalf of the domain. If the information is not consistent, the reachability of the domain is negatively impacted, which indicates deficiencies in the internal DNS management. Examples of such inconsistencies are provided below:
  - The IP address of a nameserver in the child zone is not the same as in the parent zone in the level above. This is a configuration error and should be corrected as soon as possible. The likelihood is that the domain administrator forgot to perform an update when a change was made.
  - A nameserver is listed in the parent zone but not in the child zone. This is probably due to an administrative error. The parent zone must be updated as soon as possible so that it lists the same nameservers as those listed in the child zone. The consequence of such an error is that the redundancy that someone has tried to create essentially does not exist.

- The nameserver lacked EDNS support. This is an extension of the DNS protocol to handle DNS responses that exceed the UDP protocol's 512 byte limit. EDNS enables larger DNS response packets, which is becoming increasingly commonplace due to the increased use of DNS in conjunction with, for example, DNSSEC and IPv6.

- The DNS server did not respond to queries via UDP (User Datagram Protocol). This is probably attributable to the DNS server being incorrectly set up or an incorrectly configured firewall. A nameserver that responds to neither TCP nor UDP is essentially unreachable, the error may probably be found elsewhere, for example, in the connection to the nameserver, or the server may not have a correctly stated IP address. Our nameserver tests are immediately terminated if both these conditions are confirmed.

- Only one nameserver is found for the domain. There should always be at least two nameservers for one domain so that temporary problems with connections can be handled. If one of the servers or the connection to a server were to stop functioning, services pointed to by the nameserver would also be rendered unreachable. We count nameservers separately for IPv4 and IPv6. We consider that having an insufficient number of servers is a more serious problem for IPv4 (causes errors), while we currently consider it a less serious problem for IPv6 (generates a notification), since the latter is in its introduction phase. Naturally, it is preferable to have one nameserver that communicates through IPv6 than not to have one at all.

- The nameserver is recursive. The nameserver responds to recursive queries from third parties (such as DNSCheck). Open recursive resolvers can very easily be utilized for distributed denial of service attacks (DDOS), since the use of a very small DNS query can create a leverage effect, generating exponentially larger responses (amplification attack). It is also possible to forge sender addresses in the DNS, enabling those who wish to attack a system to create queries with spoofed sender addresses that are sent on to third parties. The queries are sent in a manner that generates large DNS responses which are returned to a presumed sender, which is in fact a third party whose services may more or less be blocked. (Refer to appendix 6).

- The start of authority (SOA) serial number is not the same on all DNS servers. This is usually due to incorrect configuration, but may occasionally be due to the slow dissemination of the zone to secondary DNS servers. This means that users searching for resources within the same domain may receive different responses depending on which nameserver receives the request, since the nameservers would then contain differing information on domains.

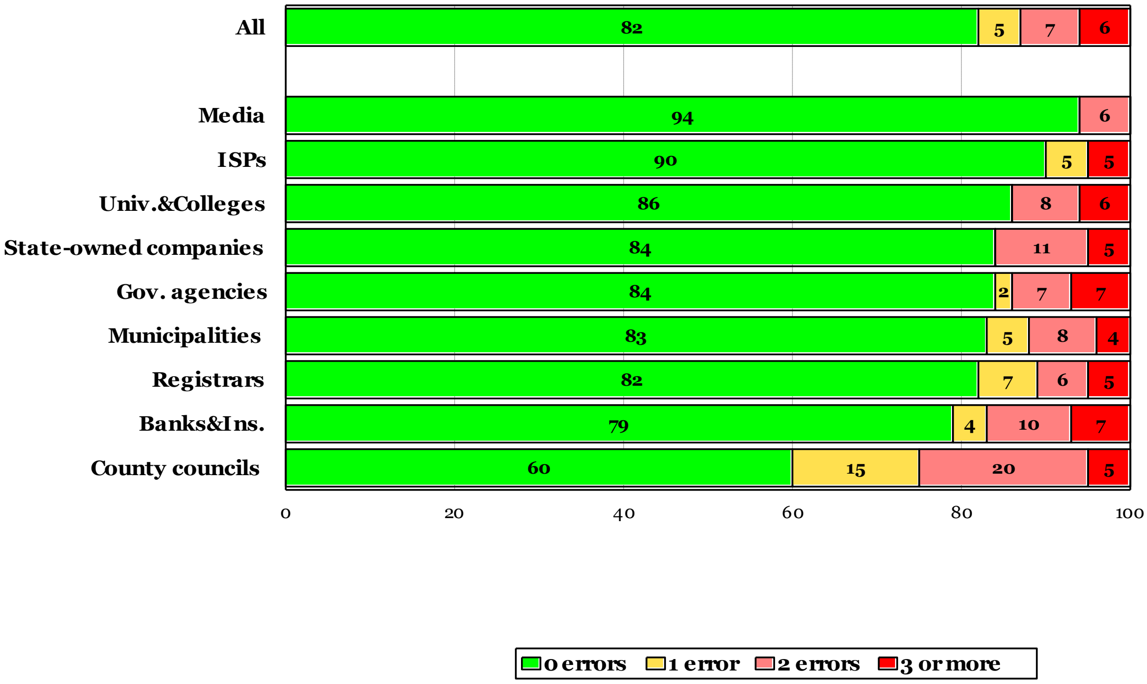
Incorrect configurations that are carried out by the same consultant on behalf of several organizations or one of the major nameserver operators are propagated in all the domains they manage and could, if this involves a large number of servers, naturally have a major impact on the results of our survey. This is especially the case if the errors appear within a single category.

It is worth noting that .SE's three largest registrars account for 50 percent of the market, while the seven largest command 60 percent of the market. Among the nameserver operators, the two largest control 36 percent of the market, while the five largest commands 50 percent. Also, the body of nameserver operators has a very long tail, meaning, there are a vast number of very small players.

6.2.1 Error volume by category

There is naturally a difference between a domain that only has one error and one that has several different errors that may often interact. For this reason, we also examined the spread of error volumes, both by number and category.

Graph 2: Distribution of the number of errors per category as a percentage



The distribution between 1, 2 and 3 or more errors is even throughout the survey group (All). The Media category has an abundance of ISPs, meaning Internet service providers, and in 2012 have the lowest percentage of errors, tightly followed by the ISP category. Bank and Insurance, and Government Agencies, are the two categories with the highest frequencies of errors, with three or more errors. The City Council category, as a whole, has the highest percentage of errors with a relatively large number showing more than one error.

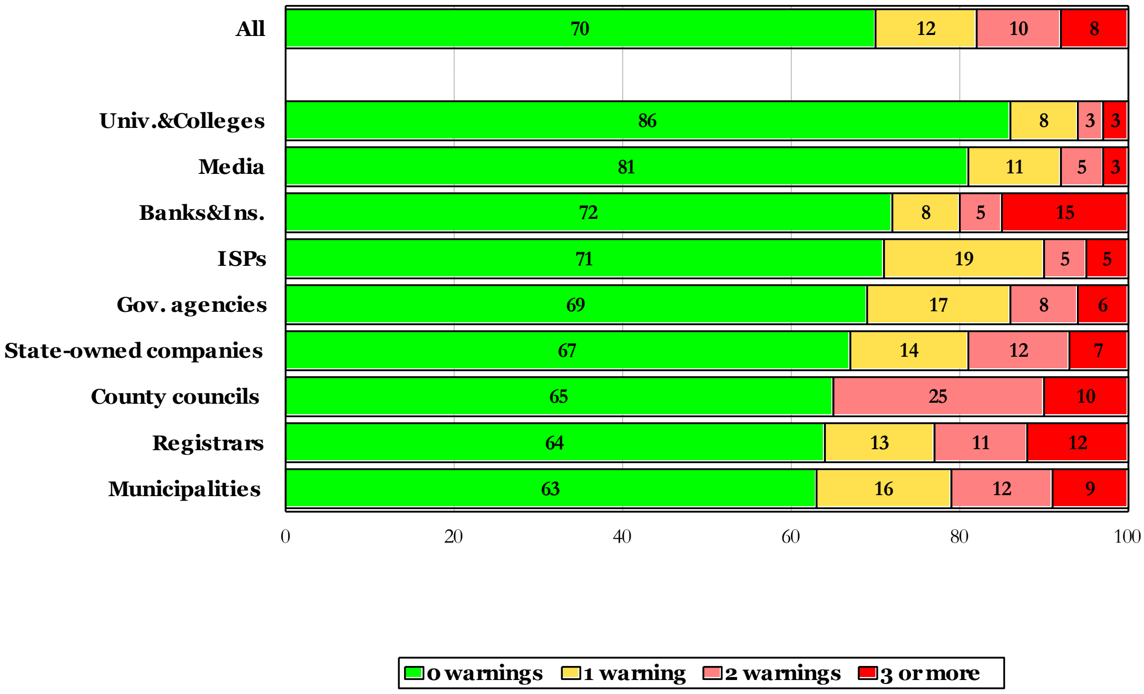
Through our contacts, we have recently called the attention of City Councils to the 2012 findings. The causes of the errors have been slightly varied, but most importantly, they are working to resolve the problems. Since our survey is a snapshot of the state of the Internet at the moment the measurements were taken, the situation can change very quickly.

We had earlier asserted that an error rate of below 20 percent was achievable without any major effort. In this year's survey, it appears that this target has been achieved for all the categories, apart from City Councils and Bank and Insurance. Achieving an error rate of below 15 percent requires a bit more than just correcting some basic hygiene factors, but it should not be impossible.

6.2.2 Volume of warnings by category

In 2012, we also investigated the corresponding distribution of the number of warnings in terms of quantity and in each category. The results are shown in the following graph:

Graph 3: Distribution of the volume of warnings per category as a percentage



The Municipalities category has the highest percentage of warnings, followed by Registrars, City Councils and State-owned Companies. Bank and Insurance and Registrars also have a high volume of warnings, meaning a high percentage with three or more warnings.

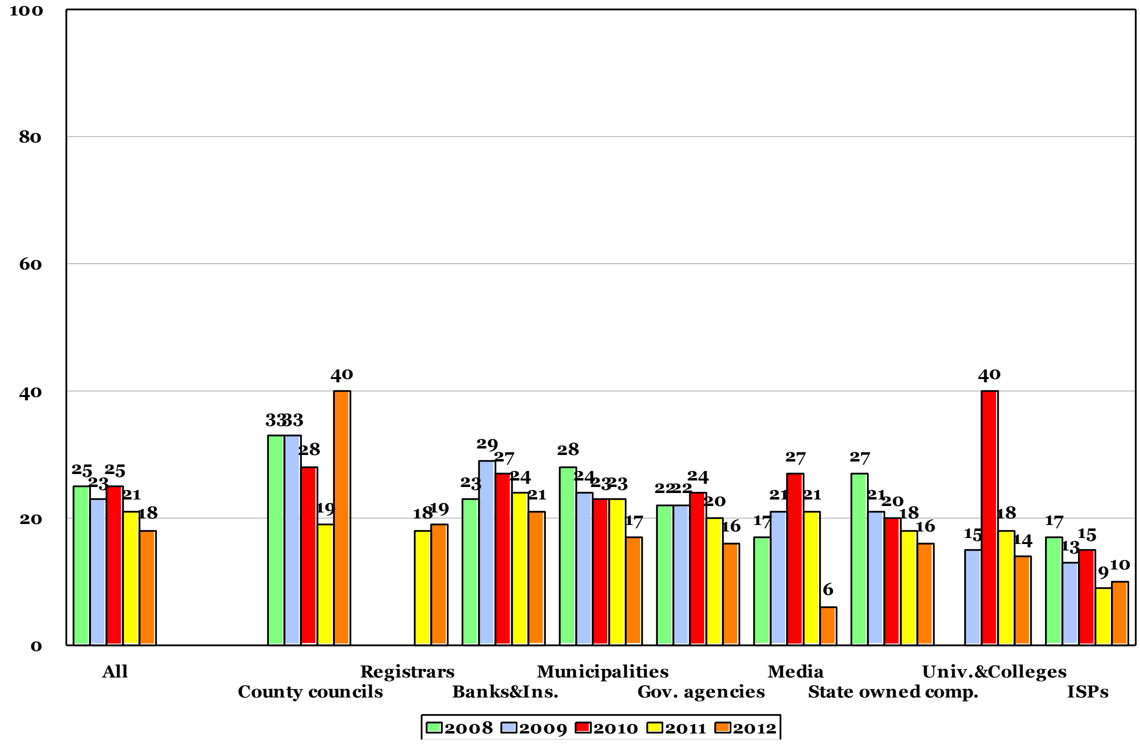
Our assessment is that this is primarily due to administrative shortcomings, such as incorrect e-mail addresses entered in the DNS. This is also generally more recurrent with warnings than with errors. However, both errors and warnings have a negative impact on reachability.

6.3 Comparison over time – errors and warnings

Saving the raw data from previous surveys enabled us to compare this year's results with those of the previous surveys for the categories that were included in the surveys for all five years. Some categories were not included until 2009 and we were thus only able to report results from the past three surveys for these categories. The Registrar category was introduced in 2011.

In the following graph, we compared the percentage of errors over time, from 2008 to 2012 (with the exception of Universities and colleges, and Registrars, which were added in 2009 and 2011, respectively).

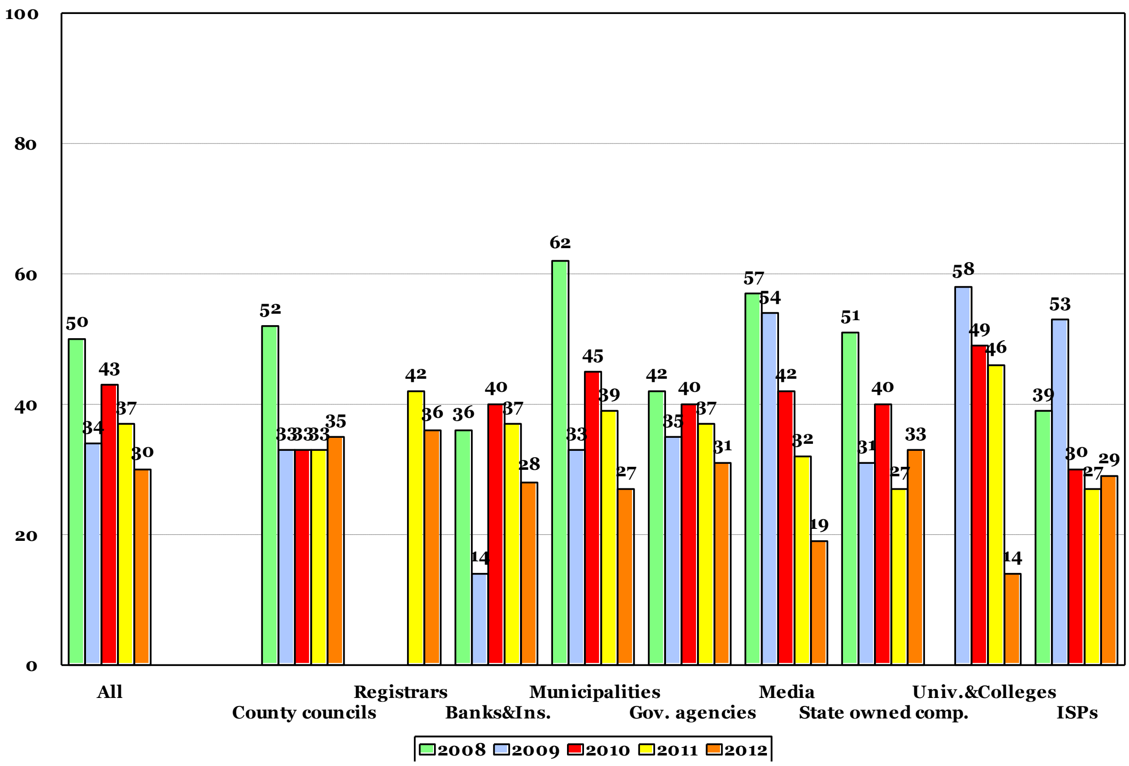
Graph 4: Percentage of errors over time



The graph shows that the situation has improved considerably in essentially all categories, compared with 2011. The Media category has fallen from a 21 percent error rate to only 6 percent in 2012.

The City Council category constitutes the largest exception, with an increase in errors from 19 to 40 percent – a situation that we have also called their attention to and which we hope will change relatively quickly. The Registrars and ISPs categories show a marginal increase but nothing alarming.

Graph 5: Percentage of warnings over time

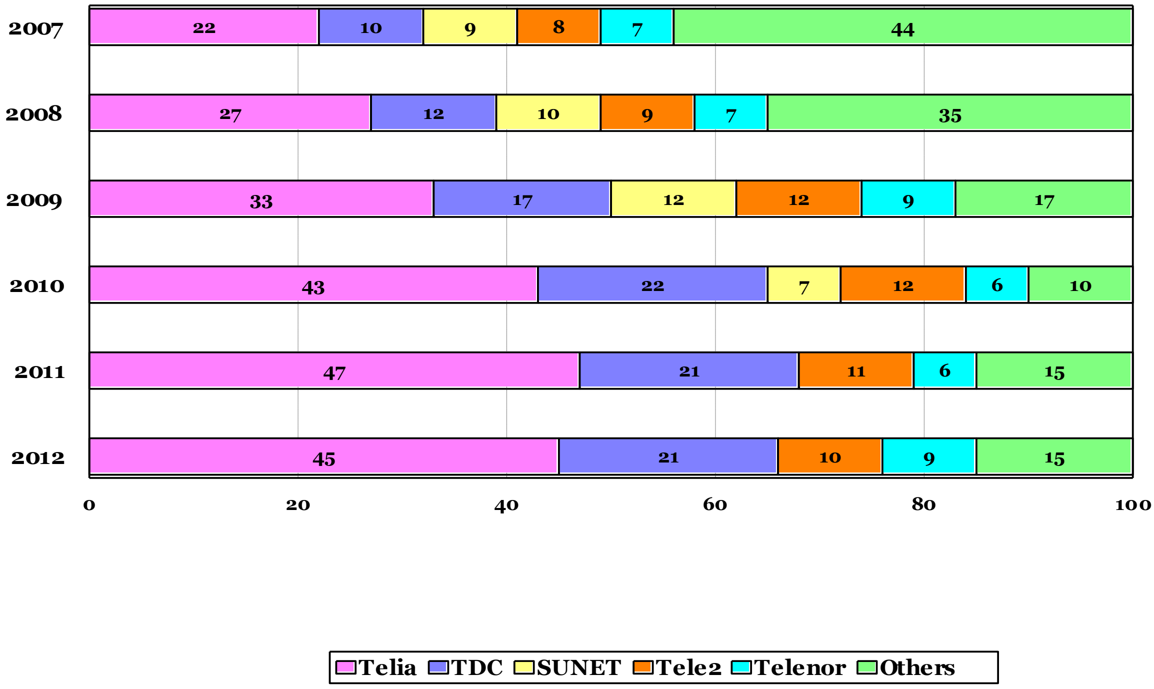


The percentage has also fallen in terms of warnings, from 37 to 30 percent for all subjects in the survey group. The largest reduction, from 46 to 14 percent, occurred within the Universities and colleges category. The reduction is distributed among all categories, except for the categories, City Council, State-owned companies and ISPs.

6.4 Nameserver connections to the Internet

As in earlier years, we examined in further detail which service providers the nameservers for the various organizations used for their Internet connections. The following graph does not show which service provider operated the nameservers for the domains; it only shows which service provider the nameserver used for its Internet connections.

Graph 6: Distribution by ISP – nameservers' Internet connections



We can confirm that the distribution among service providers, in terms of nameserver connections to the Internet, is declining from year to year relative to the total number of domains.

Without exception, we see small changes at the largest service providers, where Telia and Tele2, in particular, appear to have lost some share to the benefit of Telenor, which seems to have increased from 6 to 9 percent. In other words, the year-on-year changes were relatively minor. The percentage of "Others" remains at 15 percent in 2012.

Consequently, the distribution in nameserver operation by various service providers continues to develop in the same manner as before. The major companies are growing larger. A risk associated with this trend is for a single service provider to dominate a certain category. In the worst case, the consequence of such dominance is for an entire sector to be affected if the individual service provider experiences problems.

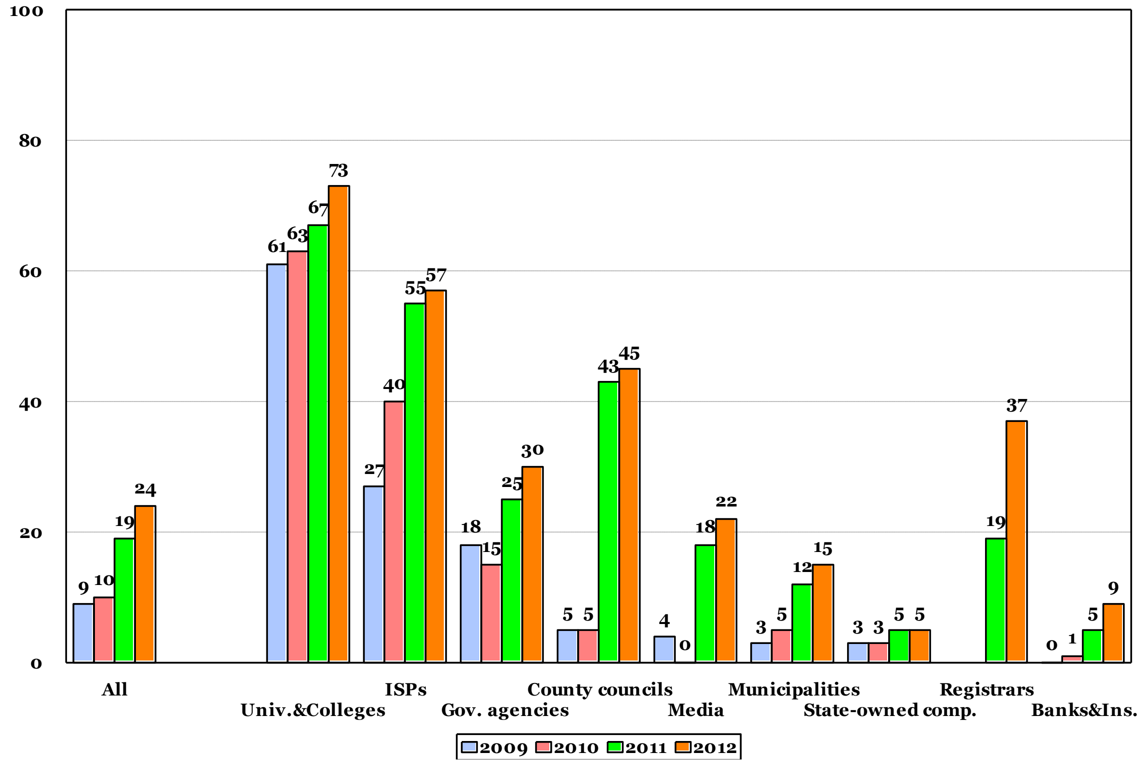
Redundancy would be increased if the nameservers were connected to more than one service provider.

6.5 Nameservers with IPv6

The introduction of IPv6 as a common communication protocol is the only way to guarantee a stable future Internet infrastructure.

The trend of increase in activity related to IPv6 has been steady and is continuing upward in 2012. As expected, universities and colleges are at the forefront of the trend, but all categories apart from one showed an increase. The very largest increase, from 19 to 37 percent, occurred in the category Registrars. It is only within the category State-owned Companies that proceeding is very slow. In fact, it had not changed at all, since the 2011 survey.

Graph 7: Percentage using nameservers reachable by IPv6



A total of 24 percent of the surveyed domains have some kind of nameserver that is reachable through IPv6, compared with 19 percent in 2011. Work is currently under way to fully implement the new protocol with ISPs. Companies and organizations must now follow suit. IPv6 is being introduced alongside IPv4 and the older protocol will not be phased out before the end of a transitional period lasting several years. .SE is acting in different capacities to facilitate and support the implementation of IPv6 in Sweden[4].

The shortage of addresses is already a fact and the implementation of IPv6 is far overdue. In 2011, the government charged the Swedish Post and Telecom Agency (PTS) with describing how to implement IPv6 at the government agency level in terms of accessibility, security and financial aspects. The description is aimed at serving as a support platform for government agencies, municipalities and other organizations in the public sector in their implementation of IPv6. The report was recently published and is available for reading at http://www.pts.se/upload/Rapporter/Internet/2011/2011-18_Att_infora_internetprotokollet_IPv6.pdf (Swedish).

The Swedish Post and Telecom Agency (PTS) have now also been tasked by the government with following up the implementation of IPv6 by government agencies. In conjunction with this, the Swedish Post and Telecom Agency launched a website, "Authorities with IPv6,"[5] where the implementation of IPv6 in the Swedish public sector can be followed.

4 https://www.iis.se/lar-dig-mer/ipv6/om/

5 http://e-tjanster.pts.se/internet/ipv6

It is important to understand that a transition of this type requires about 12 to 18 months of preparation and work. There is a risk of being on our way toward a new Y2K scenario. Everyone will want to claim a limited amount of resources in the form of training and experienced consultants. Our advice is to plan in advance – far in advance. Do not wait for D-day. Let your technicians commence testing now. They will be able to accomplish a great deal with just a single firewall and a computer. .SE provides a comprehensive e-course for IPv6, for which we recently added five new chapters: [https://www.iis.se/lar-dig-mer/ipv6/e-utbildning/ (Swedish only)](https://www.iis.se/lar-dig-mer/ipv6/e-utbildning/).

6.6 Service providers offering nameserver maintenance

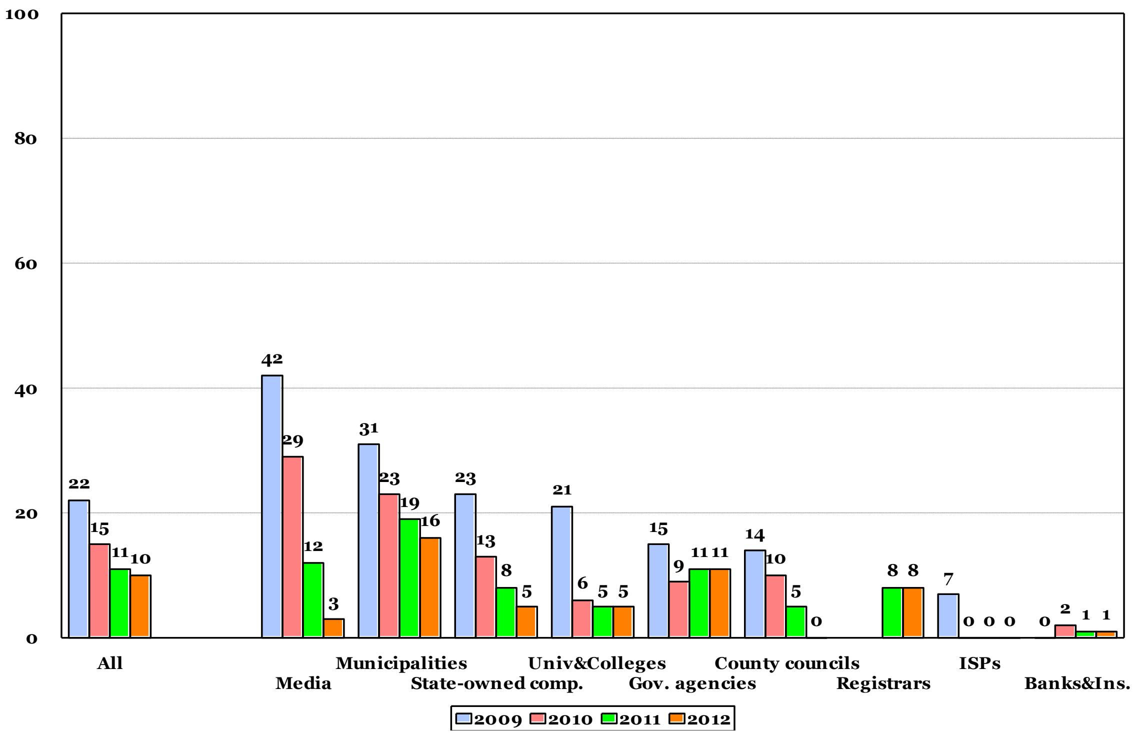
Normally, a registrar is also responsible for the maintenance of nameservers for a domain. As mentioned earlier, .SE's three largest registrars account for 50 percent of the market, and if we look at the seven largest, they command nearly 60 percent of the market. Among the nameserver operators, the two largest control 36 percent of the market, while the five largest command 50 percent of the domains in the .se zone. Critically incorrect configurations at any one of these registrars that also offer nameserver maintenance for its customers will naturally be quite significant.

6.7 Nameservers with recursion activated

In 2012, we are also repeating our message from preceding years: Open recursive nameservers have very few legitimate areas of use and may be abused in conjunction with denial-of-service attacks. Accordingly, we strongly recommend eliminating the possibility of abusing open recursive resolvers with the assistance of available methods as described in the references stated in appendix 6.

The share of nameservers open for recursion declined further in 2012 and is down to 10 percent, compared with 11 percent in 2011. This is excellent considering the risks involved.

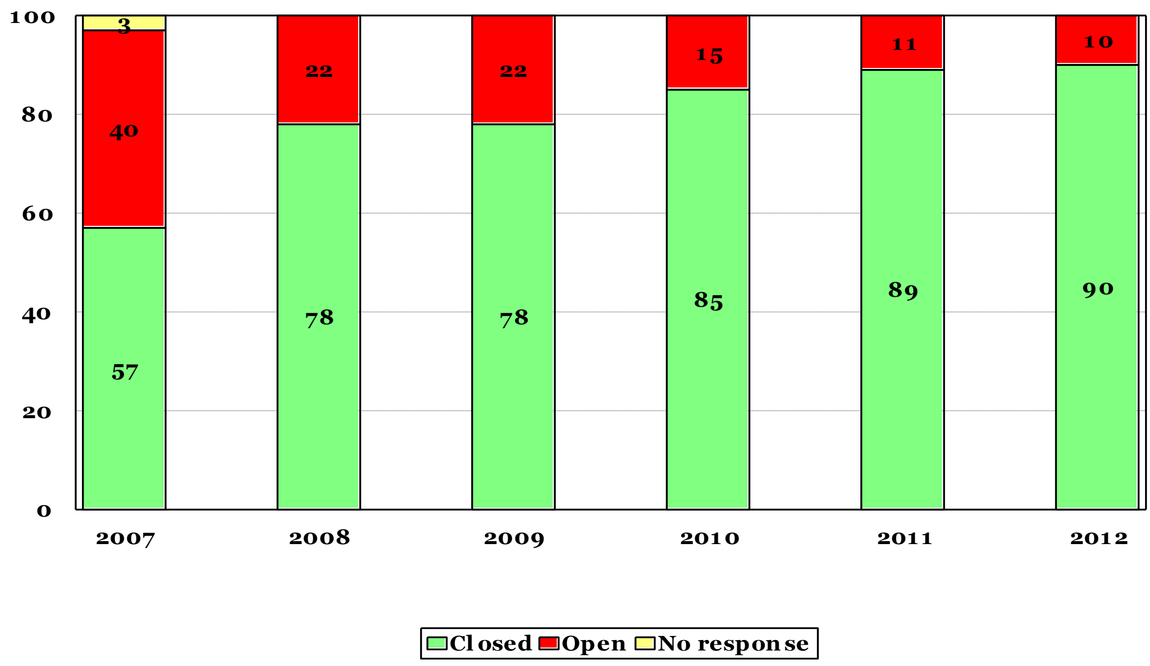
Graph 8: Nameservers open for recursion by category



We are seeing a continued improvement that is in part attributable to nameservers now being delivered with recursion inactivated as a default setting. We also believe that those responsible for DNS infrastructure have become more proficient at implementing a separation between authoritative nameservers (those that actually respond to queries) and resolvers (those that simply mediate queries and responses). The Municipalities category accounts for 16 percent – the largest remaining block of recursive nameservers. Government agencies also account for a relatively high percentage, with 11 percent. For the categories of City Councils and ISPs, the percentage is down at 0 percent.

In the graph on the next page, we can follow the development trend from 2007 to the 2012 survey.

Graph 9: Nameservers open for recursion 2007-2012



Between 2007 and 2012, the percentage of nameservers with recursion activated declined extensively, from 40 to 10 percent. Since the preceding survey, there was a further decline of 1 percent. We have a highly favorable view of this trend and hope that it will continue. First and foremost, municipalities and government agencies should review their infrastructure in this regard.

6.8 Use of DNSSEC

Secure DNS (DNSSEC) is an add-on to the DNS protocol that is based on encryption keys and is used for signing zone file content for both top-level and second-level domains.

.SE's launch of DNSSEC service for more secure DNS in 2005 has also contributed to a greater focus on DNS and DNS operation. Companies wishing to make their DNS infrastructure more secure by using DNSSEC realize relatively quickly that they cannot introduce the mechanism until they first review their own DNS infrastructure as a whole.

We are particularly interested in finding out the extent of readiness of .se domains for DNSSEC, specifically because DNSSEC has received considerable attention in the government's strategy for the IT policy area, "IT in the public service – a digital agenda for Sweden,[6]" in PTS' activities and in MSB's action plan, "Public information security – National action plan 2012[7]."

MSB's action plan states that the goal is to implement DNSSEC in the majority of public organizations by the end of 2014. The measures that government agencies will adopt are to follow up the efforts undertaken in 2011 and also to

[6] http://www.regeringen.se/sb/d/14216/a/177256
[7] https://www.msb.se/RibData/Filer/pdf/26290.pdf

continue on the work implementing DNSSEC for the remaining domains in cooperation with .SE, PTS and SALAR.

This – as well as the fact that we are responsible for the Swedish top-level domain – is the crucial reason why our tests focus specifically on DNS quality. The Internet's root zone was signed in summer 2010, accelerating the proliferation of DNSSEC. The root zone's location at the pinnacle of the DNS hierarchy facilitates the implementation of DNSSEC for underlying top-level domains.

DNSSEC protects Internet users from forged or manipulated DNS information through, for example, what is known as DNS cache poisoning. Responses to DNS queries that are secured using DNSSEC are assigned a digital signature, the verification of which ensures that the DNS information has not been tampered with en route from the nameserver to the recipient system.

6.9 How extensive is DNSSEC use?

Among the 912 domains in the 2012 survey group, 6.69 percent, or 61 domains, were signed using DNSSEC. Municipalities, government agencies, county councils and ISPs are the primary organizations that have begun to implement the more secure technology.

As a result of a comprehensive campaign implemented in December 2011, we have seen a highly extensive increase in the number of DNSSEC-signed domains. In February 2012, .SE performed an in-depth analysis of DNSSEC tests, which was presented in a report[8] published in March 2012, and which had a special focus on DNSSEC quality.

For this year's survey, the number of signed domains in the survey group (913 domains) increased to 100 domains, corresponding to 11 percent.

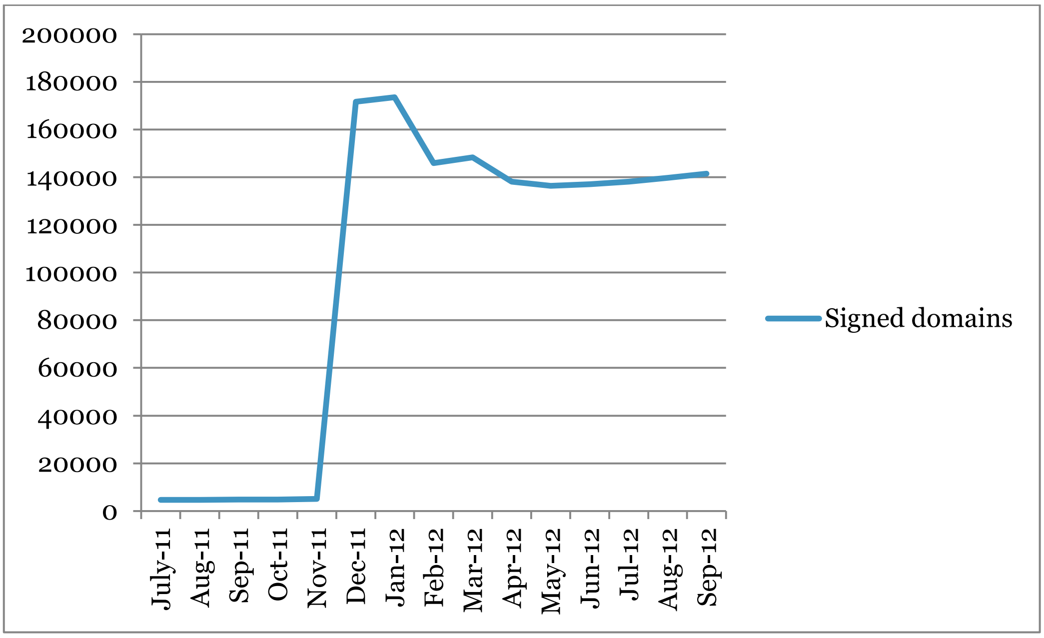
At the time of the current survey, the control group (comprising a sample of 1 percent of the entire .se zone) had 1,182 signed domains, or an increase of 10 percent. This should be compared with the 2011 survey, when barely half a percent, or a total of just 50 domains of the more than 10,000 domains in the control group, were signed.

However, in comparison with the report from March, we are observing a reduction, since a number of DNS operators were forced to shut down DNSSEC due to problems encountered in the technical environment.

The graph on the next page presents the growth of DNSSEC signed domains for the entire .se zone – not just the survey group or control group.

[8] https://www.iis.se/docs/Halsolaget-DNS-och-DNSSEC1.pdf

Graph 10: Growth – domains with DNSSEC in the entire .se zone.



On October 6, 2011, the Ministry of Enterprise, Energy and Communications published the report,[9] *IT in the public service – a digital agenda for Sweden*, which includes proposals on new IT policy targets. In the digital agenda, the Minister in charge declares that:

> *"Sweden must strive to ensure an accessible, open and robust Internet within the country and globally. To achieve more secure communication for authorities, there is a need for requirements for an Internet specification that can be used in the procurement of Internet connections by authorities. A joint Internet specification with different robustness and security requirements (model cases) is therefore due to be produced by 2013. In addition, all authorities should make use of DNSSEC and be reachable with IPv6 by 2013."*

In partnership with the Swedish Civil Contingencies Agency (MSB), the Swedish Post and Telecom Agency (PTS) and the Swedish Association of Local Authorities and Regions (SALAR), .SE has made preparations to enable municipalities to apply for funds from Appropriation Bill 2:4 Crisis Contingencies through the county administrative boards. Consequently, municipalities had the opportunity to apply for funds in autumn 2011. Despite a tight schedule, applications were received from 120 municipalities. The MSB granted funding to 86 of these, which corresponds to approximately 71 percent of the applications. Applications from 35 municipalities were rejected in the first batch of applications.

In October 2011, 24 municipalities had signed domains. In October 2012, the number was 36, which is an increase of 12 municipalities. When considering that there are 290 municipalities to sign in total, at the current growth rate it will take another 20 years before all municipality domains are signed. However,

[9] http://www.regeringen.se/sb/d/14216/a/177256

the hope is that the pace will accelerate with the assistance of the policy targets and the support that municipalities may receive from MSB.

Just as for IPv6, it is vital to engage the right expertise for the implementation of DNSSEC. Fatal errors could be made if the installer does not understand the workings of DNSSEC. So if you do not know what you're doing, it would be preferable to leave it aside until you obtain qualified assistance!

An example of what could happen is that the DNSSEC signatures have a certain lifespan and must therefore be renewed regularly. If they are not renewed in time, the domain will stop working, which means that all resources associated with the domain, such as e-mail and web servers, will also stop working.

We have seen examples of organizations that have signatures with a lifetime of less than one week and other parameters that leave very little room for an organization's ability to react and repair.

Having DNSSEC does not automatically increase the stability of your DNS environment. Consequently, monitoring is vital in order to be aware when situations arise. It is important to be able to handle various types of disruptions in the system relatively quickly and improperly set parameters could, for example, pose a problem during vacation periods or long weekends, unless there is operational maintenance round the clock, every day of the week and year round.

6.10 DNSSEC specific testing

Following some initial difficulties in the December campaign, we performed a closer examination of the actual procedures used by DNS operators when signing their domains. Above all, we feel it is important to gain an early insight into the number of domains that do not function. We would also like to have an indication and advance warning of which domains are within the risk zone of losing their accessibility, which is why we have also examined such parameters in what are known as the "child zones" (second-level domains under .se, which is then the parent zone) that are associated with DNSSEC. This involves the life span of DNSSEC signatures, and the extent of the time margin before they expire and the domain stops working.

Our standard tool, DNSCheck, is not adequately developed to handle these values, which is why we developed a new tool that solely examines DNSSEC for signed domains[10]. It was mainly the results of these tests that we presented in the DNS and DNSSEC report from March 2012. Following the report in March of 2012, we have repeated some of these tests in this report and the results are presented in chapter 6.11 below.

6.11 Works, does not work

For surveying DNSSEC, we initially examined the entire .se zone, meaning all delegated domains. For the current survey, 125,647 of the 1,177,113 delegated domains were signed. (Approximately 50,000 registered domains lack any delegation (are not delegated) in the .se zone and consequently, are not affected by our survey.)

[10] https://github.com/dotse/dnssec-analysis

The error message received when a domain's DNSSEC is dysfunctional is SERVFAIL. Unfortunately, this is also the very same error message received when server-side settings are incorrectly configured, or when the nameserver software is experiencing other problems with processing queries. This does not make it easy to determine whether an error is due to DNSSEC.

Every domain has a number of records connected to itself in the DNS, which serve as delegations to nameservers, to e-mail servers and similar resources. A crucial record associated with DNSSEC is called the DS record. The DS record comprises DNSSEC information specific to a DNSSEC-signed domain.

By "DNSSEC signed domains" we are referring to domains that have a DS record published in the .se zone, which means that the zone must function with DNSSEC activated. A DS record must match a published DNSKEY in the zone, which in turn generates signatures for all the records that are published within the zone.

Of the total of 125,647 signed domains, at the measurement point in time 112,947 were functioning and the remaining 12,700 domains (8.9 percent) were completely dysfunctional when the nameservers with activated DNSSEC on the resolver side attempted to verify the signatures. There were some major difficulties in initiating .SE's DNSSEC campaign in December, but the worst problems have mostly been rectified. However, the total percentage of DNSSEC signed domains that are completely dysfunctional increased from 6 percent to 8.9 percent in the latest survey.

Since virtually all ISPs in Sweden have activated DNSSEC validation, we find it remarkable that the number of domains that are dysfunctional for customers are actually increasing in number. We have not arrived at a reasonable explanation for this. .SE is actively working to reduce the number of dysfunctional domains through dialog, surveys and reports such as this one.

6.12 DNSSEC in other top-level domains

The proliferation of DNSSEC has gained momentum among other top-level domains worldwide, particularly after the signing of the root zone, which took place in 2010. Of all 316 top-level domains that are announced in the root zone, 101 are currently signed using DNSSEC, of which 94 have published information about their keys in the root zone.

In conjunction with the establishment of new generic top-level domains (new gTLD) that ICANN is working with, the number will increase due to the requirement that new top-level domains should be signed with DNSSEC.

Current statistics are available at
http://stats.research.icann.org/dns/tld_report/

7 Key parameters for e-mail

Electronic mail (e-mail) has been available for quite some time and was one of the first truly used and usable applications. There are many advantages to using electronic mail as a communications channel. As is often the case, it depends on **how** it is done. It is vital that an e-mail system is set up correctly from the beginning and that functions are utilized to increase security in e-mail use. Failures to do so will likely lead to problems and complaints from frustrated recipients.

In the 2012 survey of the health status of .se, we have examined a handful of parameters affecting e-mail, which is presented below. However, in November, we will publish an in-depth report on e-mail, where we will not only conduct a poll of e-mail administrators, but will present history and statistics, and explain how e-mail should work, as well as examine some technical parameters in greater detail through tests and the use of our tool, MailCheck[11].

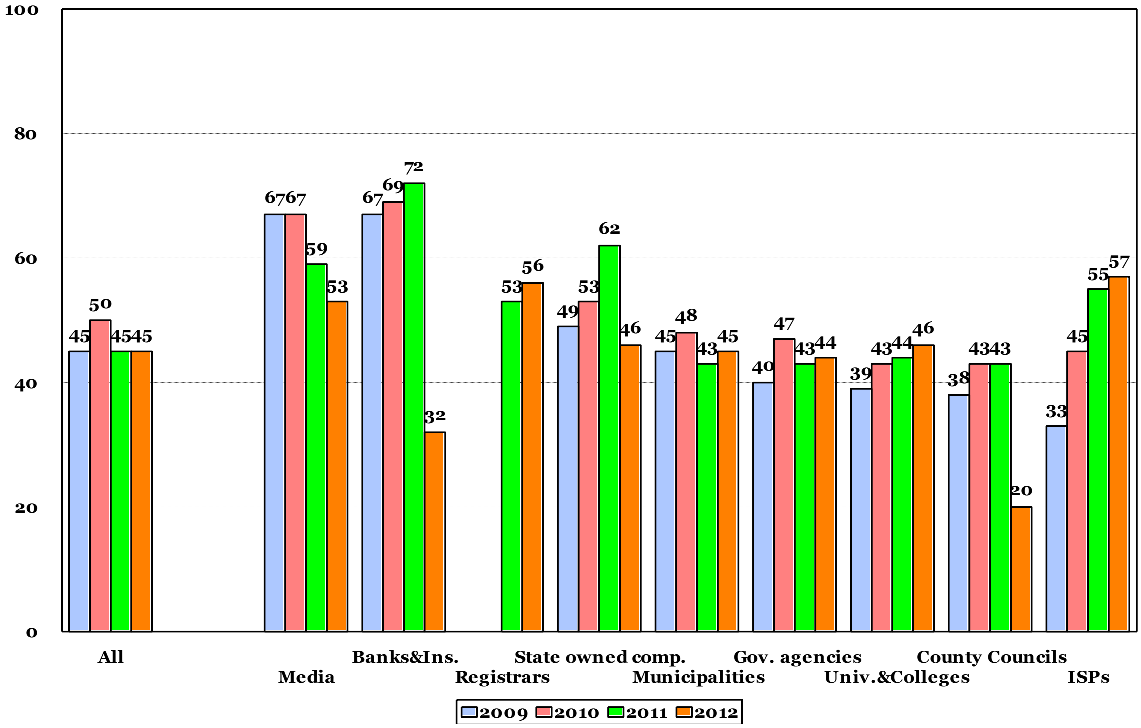
7.1 Support for transport layer security (TLS)

To ensure the secure exchange of information between e-mail servers, the communication should be protected during transit. Transport layer security, or TLS, is an open standard for the secure exchange of encrypted information between computer systems. TLS is advancement on version 3 of the SSL protocol and is governed by the IETF. In addition to confidentiality (encryption), TLS offers accuracy (data integrity) and, depending on use, authenticity protection (source protection). TLS/SSL can be used in such tasks as the transfer of electronic mail (SMTP).

Of the organizations surveyed in 2012, only 45 percent supported TLS/SSL in their e-mail servers. This is unchanged from 2011 and means that there has certainly not been an increase in the number of people taking sufficient actions to protect their e-mail traffic against eavesdropping.

[11] https://mailcheck.iis.se/

Graph 11: E-mail servers offering TLS support

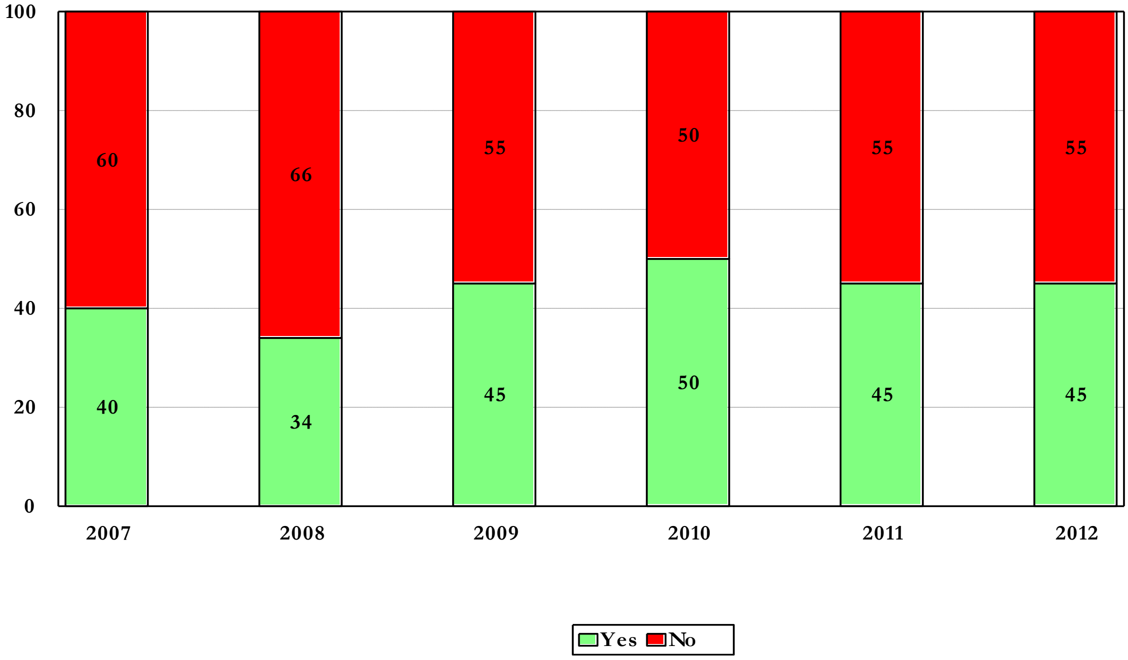


While we are seeing a modest increase in most categories, there is also a relatively sharp decline in the Banks and Insurance and County Councils categories. All modern software currently has built-in support for TLS, which is not difficult to implement.

TLS is used to encrypt the communication between two units, of which one usually comprises a web server and the other a browser. The idea of securing the information exchanged between these units is that no other parties on the network, such as the Internet, should be able to eavesdrop or distort the information. When shopping or if you are expected to submit sensitive information to an online service through the Internet, it falls naturally on TLS to be used in the encryption of, for example, credit-card information or personal information.

Naturally, the vast decline in the Media category since this portion of the survey was initiated in 2009 is of particular interest, from the perspective of an individual's legal right to anonymity, meaning the importance of protecting informants who provide journalists with information. Unfortunately, we do not have any information as to the reasons behind this. The graph on next page shows the trend in the past six years.

Graph 12: E-mail servers offering TLS support 2007-2012

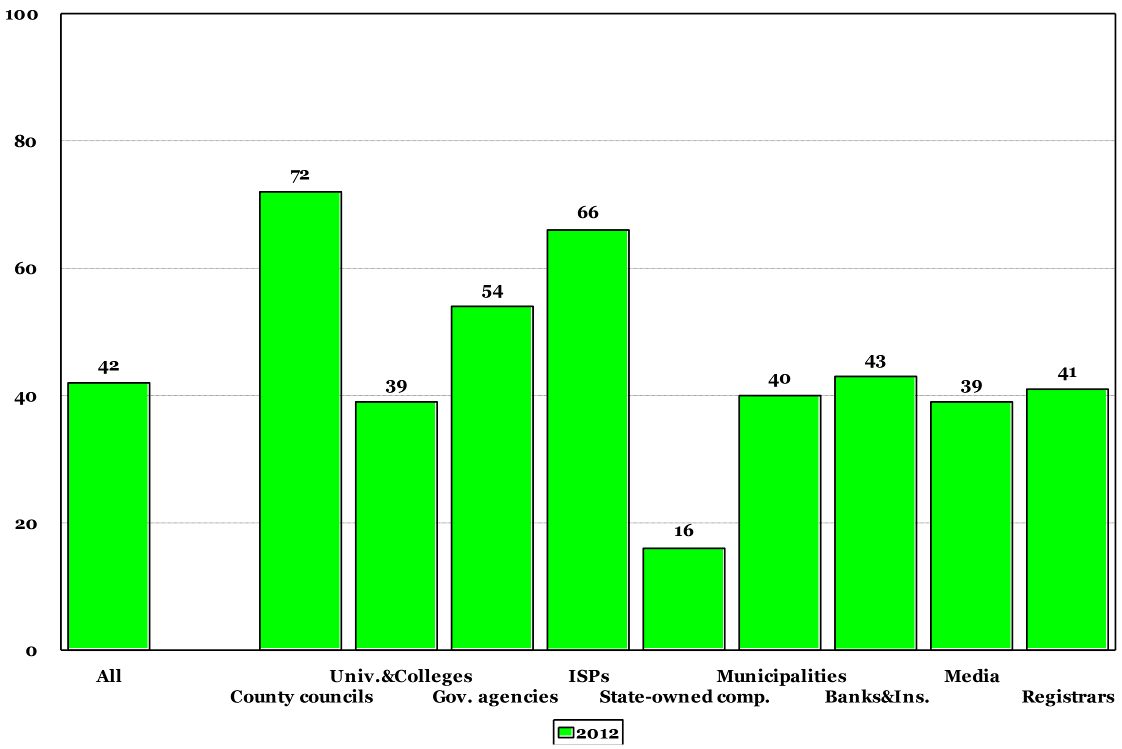


7.2 Location of e-mail servers

Since there are now an even greater number of e-mail servers using IPv6 addresses in 2012 than in 2011, and since their location cannot be determined with any certainty, we will continue to separately report the results for the servers that use IPv4 addresses.

The graph on the next page presents the percentage of email servers located in Sweden, distributed by category.

Graph 13: Percentage of e-mail servers located in Sweden



What we can see is that in 2012, 42 percent of the e-mail servers with IPv4 addresses are located in Sweden, compared with 24 percent in 2011 – a relatively sharp increase. County Councils experienced the greatest increase by far, from 5 percent to 72 percent. We essentially see a robust increase in all categories, apart from the Registrars and State-owned companies' categories.

For the Registrars category, part of the explanation as to why so many of them have servers beyond the country's borders is that a large portion of the accredited registrars have their operations in countries other than Sweden. Registrars also operate a large number of e-mail servers, since they often deliver e-mail as a service to customers.

It appears that state-owned companies have had a year of outsourcing e-mail management, since a considerably smaller percentage of e-mail servers for this category are located in Sweden. In 2011, 35 percent of the e-mail servers of state-owned companies were located in Sweden, while the results of this year's survey show a total of 16 percent.

The main reason for locating servers outside Sweden is in all likelihood the same as before, meaning that organizations engage third-party suppliers to handle the filtering of viruses and spam on their behalf.

One consequence of locating the e-mail servers of such organizations as government agencies and municipalities outside Sweden is that a considerable amount of the e-mail communication of these public administrations passes through a foreign country on its way to the recipient. In the case of the media, this also applies to e-mail communications between informants and journalists. When considering that this communication is often unsecured, it represents an unnecessary risk for the exposure of sensitive information.

In conclusion, we can state that organizations still seem to frequently send their e-mail abroad to be "washed" from spam and malicious code. At the same time, we know that less than half of the organizations surveyed use encryption for transport layer security of their e-mail. Only 45 percent of the domains surveyed support transport layer security using encryption for incoming e-mail.

This means that not only Swedish but also foreign intelligence services can eavesdrop on traffic without major difficulty. The location of servers outside Sweden means that all information passes beyond Sweden's borders, which entails that foreign governments and other parties can very easily access information that may be sensitive in one form or another. It is impossible to determine the level of awareness of this problem among those responsible for the organizations and, in such cases, whether they have carried out any consequence analysis.

7.3 Actions against spam

The standard protocol for sending e-mail, SMTP, enables the sending of messages stating any domain of choice as the sender's address. There are several solutions aimed at limiting the distribution of spam by attempting to verify that the sender of the message is legitimate. The most common solution is to employ DomainKeys Identified Mail (DKIM) or Sender Policy Framework

(SPF) or a combination of the two. Both methods are based on some form of sender authentication on a server and domain level.

7.3.1 DKIM

DomainKeys Identified Mail (DKIM) is a technology that uses a digital signature to protect selected parts of an e-mail header and the content of an e-mail message from being modified by a third party.

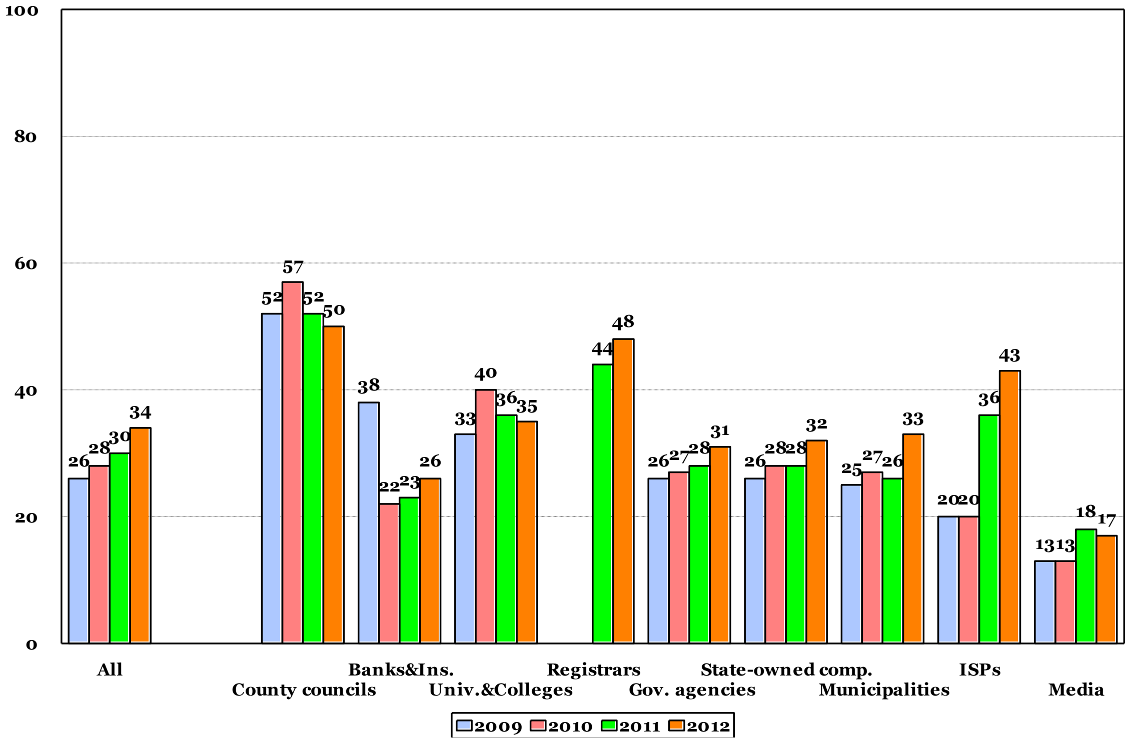
Unfortunately, due to the design of the DKIM standard, it is impossible to precisely determine whether or not a domain uses DKIM. We are still unable to report the results on the expansion of DKIM since the existence of DKIM for a domain cannot be determined with certainty until the use of Author Domain Signing Practices (ADSP) becomes more of the norm. DKIM itself does not protect against spam unless it is combined with an ADSP policy. Currently, the use of ADSP is quite rare. We will not be reporting on the prevalence of ADSP and DKIM until we have a reliable survey method and we note that there is more than just a marginal presence. The option of conducting measurements exists, since this is information that is published in the DNS.

7.3.2 SPF

The second solution is designated Sender Policy Framework, or SPF, which can also be effective against spam, as long as its limitations are taken into consideration. SPF is, for example, unable to handle situations in which e-mail is automatically forwarded or in which an e-mail message takes an unexpected route. This may become messy in a structure that includes several levels of forwarding and SPF checks.

There are also arguments against the use of SPF, but since its use is relatively widespread, we have opted to check whether domains have a published SPF record. We did not perform an assessment of the SPF content.

Graph 14: SPF use



The graph shows a continued increase in the use of SPF in the 2012 survey as well, from 30 percent in 2011 to 34 percent in 2012. SPF use in the City Council category continues to decline, from 52 to 50 percent, but they remain at the top, despite the rivaling of the Registrar category with 48 percent, which is an increase from 44 percent in 2011. SPF use in the ISP category continues its relatively sharp increase, from 36 to 43 percent. Usage in the categories of Banks and Insurance, Government Agencies, State-owned Companies and Municipalities is increasing, while use in the categories of Universities and Colleges is declining.

8 Key parameters for online services

A large number of organizations currently broker information and services through web interfaces, and many organizations are entirely dependent on their online services being functional and accessible to their customers, business partners and the public at large. Increased use leads to the imposing of stricter requirements on accessibility and reachability.

Concrete actions can be taken to also increase redundancy for web services. It may be a good idea to take these into consideration, if any critical functions are provided through web services, and if their dysfunction would prompt a strong reaction from users. On the other hand, a website may not be a critical function of an organization and consequently, it would not matter if it was offline for several hours per year. Regardless of which may be the case, it is vital that the adopted measures stem from a balanced decision about the level of availability and reachability required.

The demand on availability is a vital component that is becoming increasingly relevant, particularly in the light of the distributed denial-of-service attacks (DDoS) that several Swedish websites were subjected to, most recently in autumn 2012.

8.1 Web server connections to the Internet

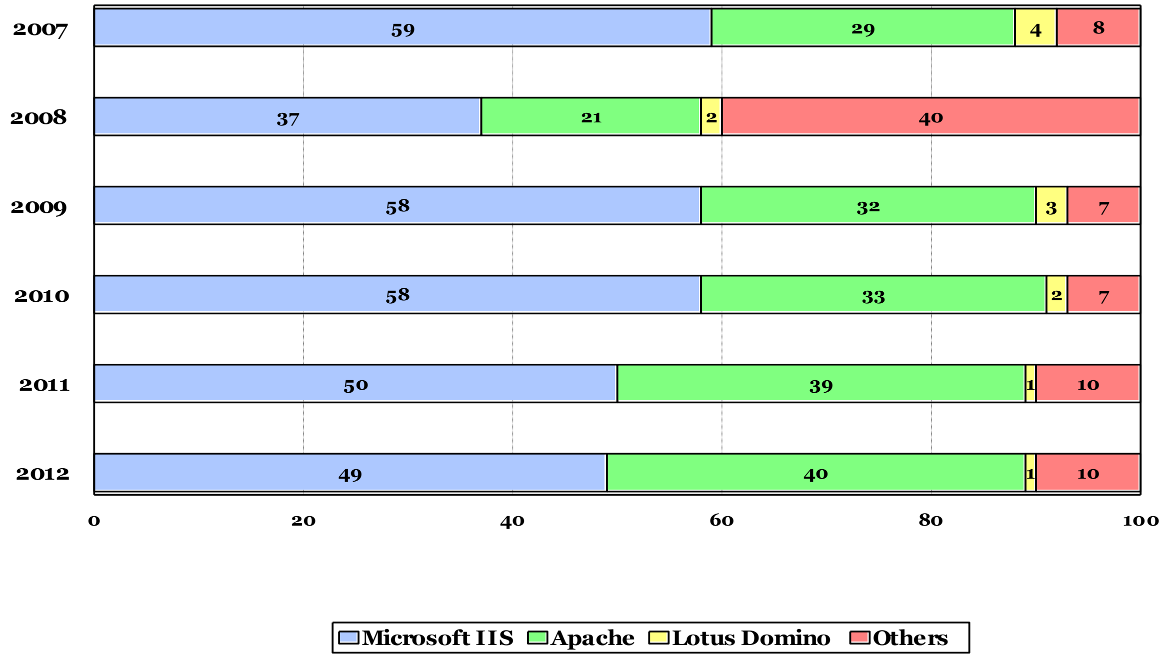
If all of an organization's nameservers are connected to one single Internet service provider, and if the web server is also connected to the same provider, there will be major problems if the service provider experiences accessibility problems.

This would not only affect the nameservers, but also the web servers, thus rendering the system unreachable. An organization should have at least one additional nameserver located with another service provider, and consider establishing a reserve site somewhere to achieve the greatest possible redundancy.

8.2 Software for web servers

We are continuing to monitor which particular web server software is used in the surveyed organizations. Microsoft Internet Information Server (Microsoft IIS) and Apache were still clearly dominantly featured. We are noting minor changes from 2011 in this area.

Graph 15: Software used for web servers



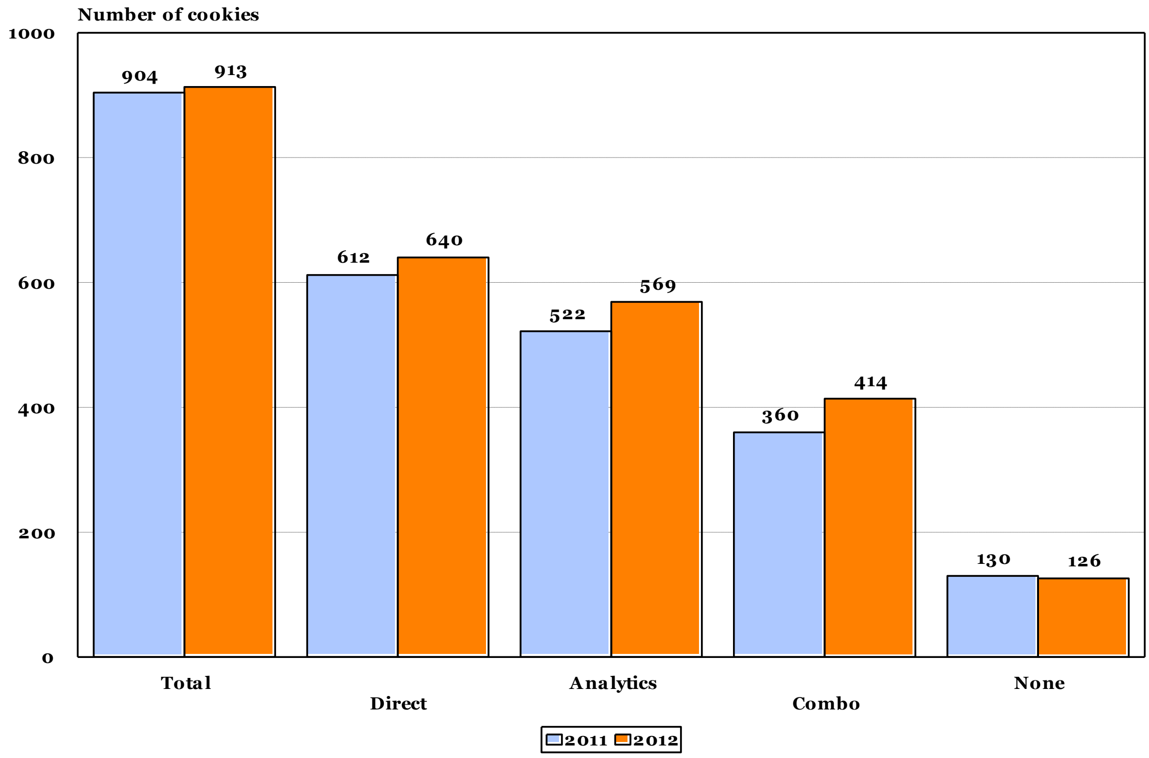
8.3 Other interesting observations regarding web servers

For the second consecutive year, we have checked a number of parameters that are of particular interest for web applications. For the 2012 survey, we have deliberately omitted the in-depth analysis of SSL certificates and their use. Our goal is to conduct an in-depth survey of this particular area next year.

8.3.1 Cookies

On July 1, 2011, the Swedish Electronic Communications Act (2003:389) was amended. As a result of this amendment, everyone who actively visits a website may have to consent to the website's use of what is known as "cookies."

Graph 16: Usage of cookies



The graph shows the number of domains utilizing cookies of various types. The type Direct Cookies pertains to cookies originating from the website itself. The type Analytics pertains to websites using Google Analytics and thereby utilizing third-party cookies. The type Combo refers to websites that use both Google Analytics and Direct Cookies. The type None refers to websites that neither use Google Analytics nor Direct Cookies, but which may nevertheless connect to third-party resources that utilize cookies.

The use of cookies appears to be on the rise despite the new regulations. Of the survey group's 913 domains, 640 of them, or 70 percent, utilized direct cookies on the websites, which is an increase of 3 percent from the preceding year.

A significant share (62 percent) of the websites surveyed in 2012 used Google Analytics and thus attached third-party cookies to collect visitor statistics, which is an increase from 57 percent in 2011. It is important to be aware that Google Analytics utilizes cookies regardless of the organization's policy on cookies, without requesting prior permission to do so.

In addition, 45 percent of the websites utilized a combination of both Google Analytics and direct cookies.

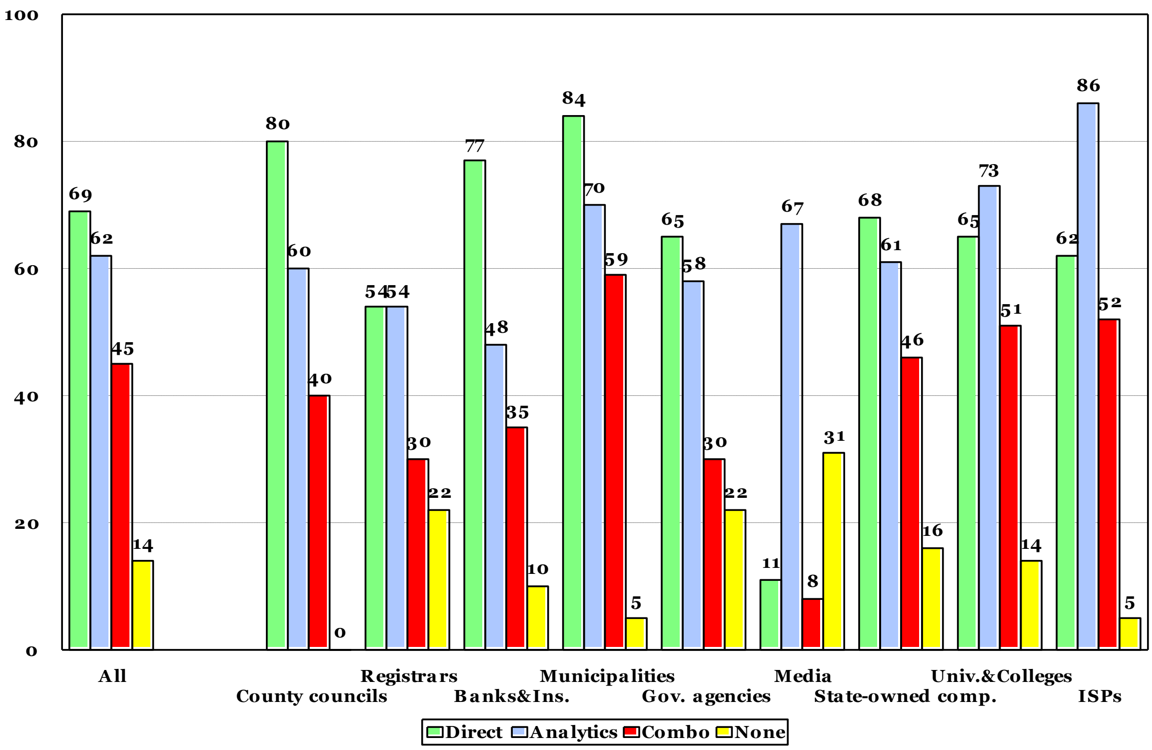
The graph on the next page shows that there has been a sharp increase in the use of cookies within the Municipalities and Government Agencies categories.

Graph 17: Difference in the use of cookies of some form in 2011 and 2012.

Category	2011	2012	Increase/decrease
Banks and Insurance	140	137	-3
ISPs	40	43	+3
Municipalities	578	632	+54
City Councils	32	36	+4
Media	36	42	+6
Government Agencies	388	429	+41
Registrars	242	241	-1
State-owned companies	108	109	+1
Universities and Colleges	79	75	-4

The graph below shows the distribution of cookies by type among the various categories.

Graph 18: Cookies by type and category, 2012



The most common type of cookies is what is known as direct cookies, although Google Analytics is frequently used in all categories of the survey group. Among the City Council and Municipalities categories, more than 80 percent utilized direct cookies, but were also frequent users of Google Analytics. At a full 86 percent, ISPs were the biggest users of Google Analytics.

8.3.2 Assignment to monitor the Cookies Act

In October 2011, the government charged the PTS with assessing whether the Cookies Act had hampered the growth of or trust in the Internet. A report on the assignment will be published in late 2012. It is too early to tell whether it will entail any amendments to Swedish legislation, which is derived from an EU directive.

As part of the assignment, the PTS has conducted a poll and field survey on a selection of Swedish organizations, within both the private and public sectors. The preliminary results indicate that in every case, survey participants were aware of the existence of the regulations.

Many of those surveyed are of the opinion that the Act's requirement for consent potentially complicates their efforts at making websites user-friendly and thus hampers the user experience. There is also concern that users may not understand what they are consenting to. Several of those interviewed consider the Act to be divorced from reality and delegate to websites that are currently dependent on cookies to be able to function. At the same time, they understand the idea behind the legislation and regard its purpose as something positive. Nevertheless, it is difficult to comply with the regulation in practice, since a cookie is attached by default when a website is visited, to enable the request for consent.

8.3.3 Google Analytics for visitor statistics

Google Analytics is the more or less established industry standard for measuring visitors at websites and is widely used by Swedish websites to measure and compare visitor traffic between other websites within such networks as the SIS Index.

Sharing visitor statistics with Google Analytics also enables Google to draw its own conclusions of visitor traffic to the websites of Swedish government agencies, for example. It cannot be ruled out that Google may choose to perform cross-references to examine which of the visitors to an agency's website also visit another agency's website, for example. Prior to selecting a tool to assess visitor statistics, it is important to perform an consequence analysis that takes into consideration where and with whom the information is stored.

In August 2012, the Norwegian Data Security Agency, which corresponds to Sweden's Data Inspection Board, contended that the government agencies utilizing Google Analytics were in violation of the Norwegian Data Integrity Act[12]. According to the Data Security Agency, the violation of data integrity occurs through the loss of control over the manner in which Google utilizes the information about its users. Google Analytics collects IP addresses and information about the behaviors of a website's visitors. The Data Security Agency was concerned that data could be traced and analyzed down to an

[12] http://computersweden.idg.se/2.2683/1.461378/olagligt-anvanda-google-analytics (Only in Swedish)

individual level. However, the Swedish Data Inspection Board has not treated the issue in the same manner or drawn the same conclusions, in any case, not as yet.

8.4 Support for transport layer security (TLS/SSL)

TLS/SSL is the technology that protects traffic against eavesdropping during Internet use, and which enables a user to trust that he or she is communicating with the right organization when, for example, performing online banking. A more detailed description is available in chapter 6.3.

Using certificates and the accompanying encryption keys, a web browser can establish a secure, encrypted connection for communication with the web server. As with e-mail, TLS/SSL is used to establish a secure connection between two parties, in this case, a web browser and a website (https); refer to appendix 9.

It does not suffice to have a certificate issued for the domain or the web server. The certificate must also be considered reliable through the fulfillment of certain fundamental requirements that should be imposed on this type of security mechanism. For example, the certificate must be issued by a reliable certificate authority, be valid, it must use secure algorithms, the keys must be of sufficient length, and so on.

Among the reasons why a certificate may sometimes not be trustworthy are:

- The certificate is used before becoming valid.
- The certificate is used after the expiration of its period of validity.
- The domain for which the certificate was issued does not correspond to the domain for the website.
- The certificate has been revoked (blocked).
- The certificate is self-signed.
- The issuer is not a well-known CA (certificate authority).
- The issuer certificate is deemed unreliable.
- The certificate chain is incomplete.

Measuring the existence and quality of certificates is not entirely easy, and we are testing various approaches to identifying a solid method of measurement. Accordingly, in 2012, we have not undertaken any operations to specifically explore certificates and their quality. On the other hand, we plan to perform such a survey next year.

In our earlier surveys, the results indicated that the management of certificates in the survey group's website environments was of very poor quality in all the aspects revealed through the survey. This type of encryption use has existed for some time and is apparently commonplace. Among the organizations included in the survey, we had expected better results, primarily in terms of the use of valid, current certificates issued by credible issuers. In this part of the survey, we want to mention that the substandard use of web certificates undermines the credibility of this type of security solution.

Anything that results in a user being forced to click on icons that in practice mean "Yes, I know that this is incorrect, but I want to proceed anyway," including self-signed certificates or expired certificates, contributes to the establishment of a substandard security culture among Internet users. This counteracts the fundamental concept behind server certificates – namely users' ability to know with reasonable certainty that they are connected to the correct server (refer to appendix 9).

All organizations that, on their websites, request some form of information from users, such as a login with userid and password, personal information, user information, payment information, credit card numbers, telephone numbers, et cetera should use TLS/SSL with certificates issued by generally accepted certificate authorities, which are installed in the most common web browsers. These organizations must have someone with internal responsibility for such tasks as monitoring when certificates expire and must be renewed.

Consequently, they should consider:

- Managing the organization's certificates as assets and keeping a record of which certificates are used, including their purposes.
- Using EV certificates [13] where warranted.
- Avoiding the use of wildcard certificates [14] for web services, especially for the subcontracted operation of web hotels or cloud services, where organizations do not control their own key material and certificates.
- Using hardware support to save private keys for sensitive web servers.

At https://www.ssllabs.com, those who use certificates to protect web services can learn more about how this works and personally check whether a website has adequate security in terms of SSL.

8.4.1 Attacks on the SSL

In 2011, there were several highly serious attacks on several major certificate authorities, and there is reason to wonder about the reliability of the SSL system and what can be done about the existing problems.

In this case, we are referring to traditional security. Among the CAs that was attacked during the year, crisis management has been highly varied, and some of the affected CAs acted slowly and inadequately concerning the communication of information to their customers and the general public. They have simply proven to be inadequate at crisis management.

In this context, we want to remind you that the certificate warnings should not be ignored, but given very serious consideration. It is important to monitor the https-connection and try to ensure that it is authentic. We also recommend that users learn more about how to have an extra look at the certificate to verify its authenticity.

[13] Certificates with extended validation (EV)

[14] A wildcard certificate activates SSL encryption on several subdomains using a single certificate.

Following the latest incidents, web browser suppliers such as Google, Mozilla, Microsoft and others have raised the requirements for issuers to join the list of trusted root certificates that accompany every web browser.

8.4.2 Measures to counteract attacks on the SSL

Many different parties are pondering potential solutions, but for now, one of the most interesting initiatives is the DNS-Based Authentication of Named Entities (DANE) created by the Internet Engineering Task Force, whose findings recently became a completed standard and were published as a Transport Layer Security (TLS) Protocol: TLSA, RFC 6698[15].

With TLSA, certificates are stored in the DNS, so that they can be verified using DNSSEC. The approach supplements the certificate issuer's signatures by verifying the certificate through DNS. This helps reinforce the quality of the certificate and thus also its reliability. It also enables users to forego the traditional CAs and rely solely on DNS if they only want to verify the domain name and not the legal entity behind a service.

Another relatively standard variety of attacks against websites that use SSL involves various types of downgrade attacks. This means that the user is tricked into using a simpler form of encryption, or no encryption at all, to communicate with the website. In such a case, not even a valid website certificate is needed to effectively perform what is known as a man-in-the-middle-attack. The IETF is working on the development of HTTP Strict Transport Security (HSTS), which forces the web browser to run SSL on the website, regardless of other commands. HSTS remembers whether a website that has been visited before has used SSL and forces communications to the same level during recurrent visits.

The Chrome web browser includes a number of extensions, including *certificate pinning*[16], which is the feature that revealed this year's CA attack on DigiNotar. Other Chrome extensions include *HTTPS-preloading*[17], which means that websites are preprogrammed to always use SSL.

A plug-in is also available for Mozilla Firefox and other web browsers for enhanced certificate management, such as *HTTPSEverywhere*[18], which was co-developed by the Electronic Frontier Foundation (EFF) and the Tor project.

15 http://tools.ietf.org/html/rfc6698
16 http://www.imperialviolet.org/2011/05/04/pinning.html
17 http://dev.chromium.org/sts
18 https://www.eff.org/https-everywhere

9 Comparison with the .se zone

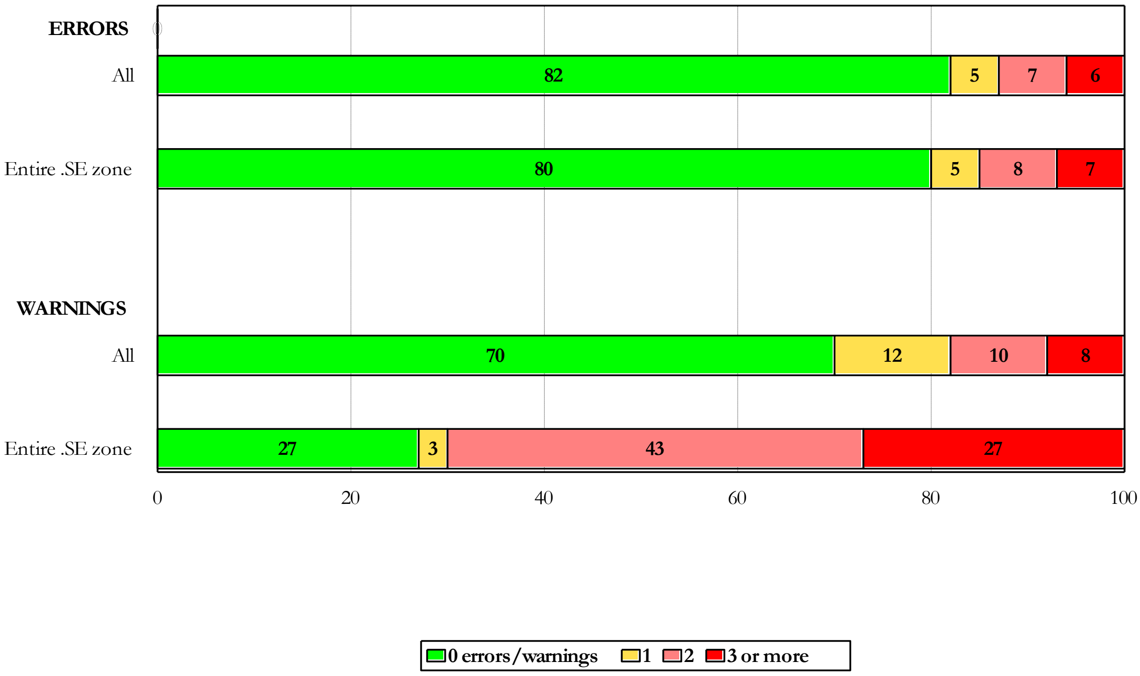
In the 2012 survey, we also examined a 1 percent cross-section of randomly selected domains from the .se zone to assess whether our survey group was better or worse than the .se zone as a whole.

In the graphs below, “All” represents the current survey group with its 913 domains, while the “Entire .se zone” represents the random selection of 1 percent or 11,806 domains derived from a version of the zone file dated October 2, 2012.

9.1 Distribution of errors and warnings

Above all, we examined the distribution of errors and warnings, and how the All survey group, which included several critical functions and organizations, compared with the Entire .se zone.

Graph 19: Percentage of errors and warnings



In contrast to 2011, there were fewer errors this year in our survey group than in the .se zone as a whole, in other words, a somewhat different situation than in earlier years. The percentages of visible warnings were far fewer in our survey group than in the comparative group. Only 27 percent of the entire .se zone do not show any form of warnings at all.

The reason for this is partly due to misconfigured nameservers for the DNS, and partly due to the fact that ever more users are employing various filtering functions for detecting spam.

One method for filtering is to use DNS-based blacklists to determine if the sender IP address has been listed as a sender of spam or known as an infected computer. So, what we are seeing here is the result of our attempts at sending e-mails to more than 12,000 domains. In other words, this particular portion of the results is not entirely trustworthy and no definite conclusions may be drawn from it, other than that filtering of this type is increasingly commonplace.

Later in 2012, we will publish a report that deals solely with e-mail and how it should be set up to function optimally for all parties concerned, including senders, service providers and recipients. For this survey, we used one of the methods that would prevent us from being blacklisted as easily.

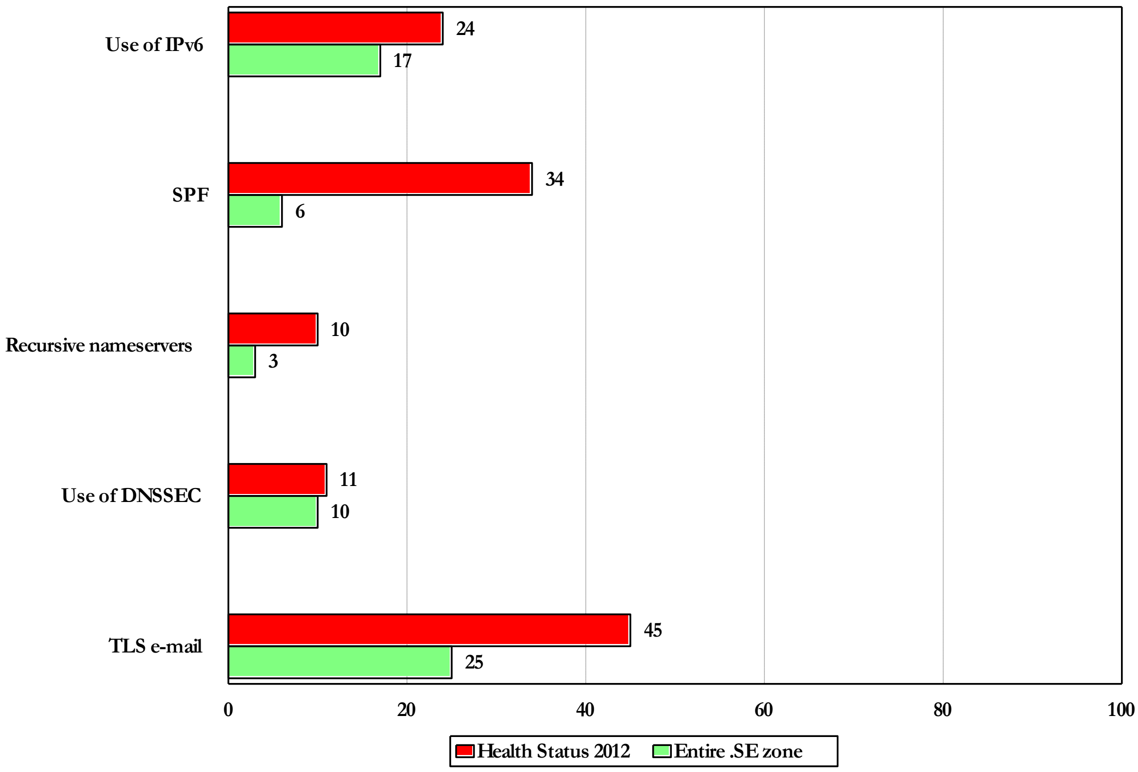
9.2 Differences between the survey group and the comparative group

On closer examination of the specific areas we reviewed for the parameters associated with DNS quality as defined in Appendix 4, the major differences have more to do with incorrect pointing, or delegations, in the comparative group for the .se zone as a whole than in the survey group, and more organizations that were dependent on just one nameserver. Meanwhile, there were more organizations in the survey group that had open recursive nameservers (10 percent compared with 3 percent in the comparative group).

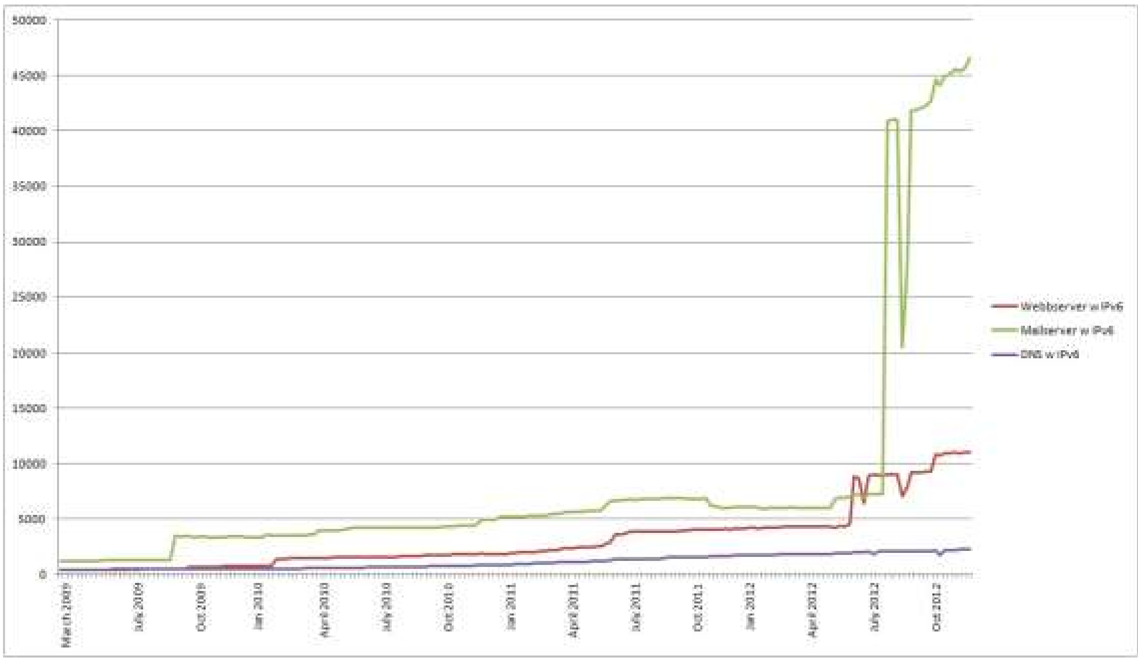
In 2012, there was an increase in those who implemented IPv6 in both groups (24 percent in the survey group and 17 percent in the comparative group). Far more were using DNSSEC (11 percent in the survey group and 10 percent in the comparative group for the .se zone as a whole) and there was an increase in the use of TLS for the protection of e-mail (45 percent in the survey group and 25 percent in the comparative group for the .se zone as a whole). SPF was also used more frequently in the survey group (34 percent) than in the comparative group (6 percent).

In the graph below, we can see the differences between the survey group and the comparative group for the .se zone as a whole, for the various sections that we have studied. In other words, there were generally more positive aspects in the survey group than in the comparative group, but also some less positive aspects, such as open recursive nameservers.

Graph 20: Comparison between the survey group and the .se zone



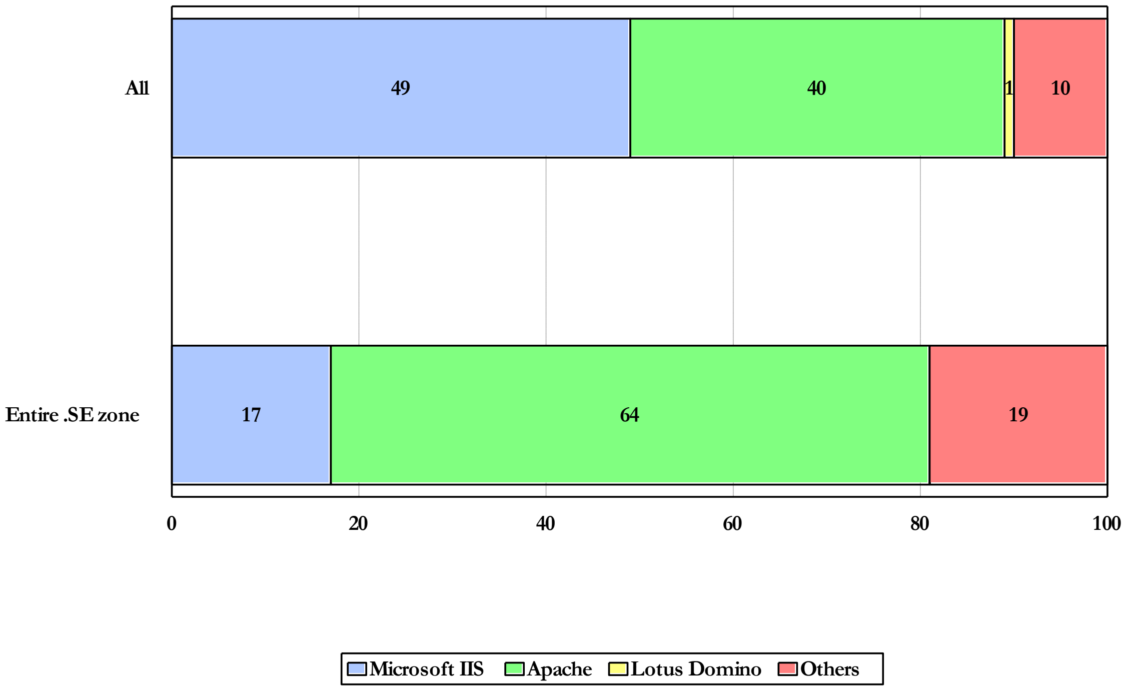
The extent of the actual growth of IPv6 for the entire .se zone is presented in the graph below:



9.3 Differences in the use of software for web servers

The difference between which software is used for web servers in the survey group, where Microsoft IIS dominates, and the .se zone as a whole, which resembles what we see in the rest of the world that Apache remains the dominant software, still remains. Microsoft IIS continues to lose ground to Apache and other software, but the differences are negligible. Lotus Domino has declined further and disappeared from the map.

Graph 21: Software for web servers

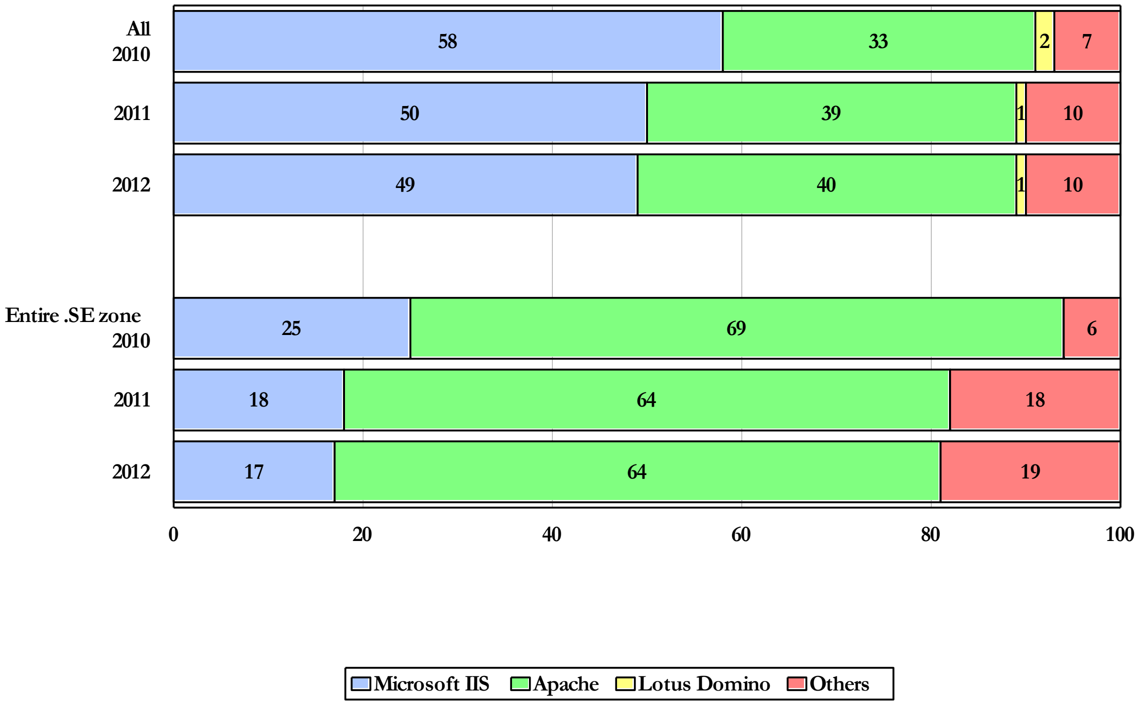


In Graph 22, we performed the same comparison, but for the years 2010 to 2012. In this comparison, we can state that Microsoft IIS lost ground in both the survey group and the comparative group. However, it remains well entrenched in the survey group.

The Other category rose even further for the comparative group and was three times larger in 2012 than in 2011. This indicates the existence of other software that is also gaining popularity.

An explanation for Microsoft IIS' strong domination in the survey group can probably be found in the system of public procurement and framework agreements, which contributes to a homogenization of the IT environments of public administration, which may not always be optimal.

Graph 22: Software for web servers – changes over time



10 Advice and recommendations

After performing yet another round of tests with relatively positive results compared with 2011, we still see a strong need for greater coordination between various stakeholders in order to improve security and reachability on the Swedish part of the Internet and, in particular, potential for major gains in efficiency-enhancements and cost savings. In this area, we hope that the government's digital agenda will have a positive impact on developments.

First of all, public-administration organizations must be able to agree on recommendations and an action plan for the implementation of some important activities:

- Critical resources in Sweden should have nameservers that are connected to several service providers simultaneously; for example with the use of Anycast technology. Suppliers that offer such quality services are scarce. At a central level, someone must establish a definition for critical resources.
- Shared secondary DNS operations should be set up for critical services; for example through the Swedish Internet exchange nodes where these could be connected as an extra measure to create redundancy. Such a function could be regulated by agreement.
- Implement joint procurement functions for virus checking and spam filtering, subject to the requirement that the servers be located in Sweden. This would be more efficient and probably save resources and make it easier to conduct audits. It would also prevent the information of government agencies from leaving the country.
- Issue guidelines on what is acceptable in terms of managing spam and virus filtering in public administrations. It should be unacceptable for Swedish government authorities and municipalities to send their e-mail abroad, at least not without imposing relevant, uniform requirements for transport layer security and encryption.
- Issue recommendations stating that e-mail servers for critical operations at Swedish government agencies should be physically located in Sweden to protect the traceability of information sent between government agencies, and to protect against the consequences of what is known as the FRA law.
- Establish requirements for public administrations regarding the use of both e-mail and web servers with TLS for source and transport layer security.
- Make all services available over IPv6 and promptly establish plans for a systematic transition to IPv6 in the entire public administration. This process itself is an operation lasting 12-18 months.
- Protect web servers with certificates issued by generally accepted certificate authorities and maintain control of their validity. A Swedish issuer would be preferable.
- Introduce DNSSEC for all domains in public administration.

In addition to the above measures, further actions should be taken, including at the service provider level, to strengthen Internet infrastructure. These actions fall primarily on the Swedish Post and Telecom Agency (PTS), which is the agency that is the supervisory authority for such issues as the Electronic Communications Act and in this regard, involves the formulation of requirements that should be placed with service providers.

In this context, we have a particularly positive view of the proposal made in the government's Digital Agenda for Sweden, stating that achieving more secure communications for government agencies requires documentation for an Internet specification, which could be used when government agencies are procuring Internet connections.

The government has proposed that a joint Internet specification featuring various reinforcement and security requirements (typical cases) be prepared for government agencies not later than 2013. The government has also proposed that all government agencies should adopt the use of DNSSEC and be reachable by IPv6 not later than 2013.

Appendix 1 - Abbreviations and glossary

ADSP Author Domain Signing Practices are used to detect unauthorized removal of the signature in DKIM.

Child zone The underlying *zone* – for example, .example.se is the child zone of the parent zone .se.

BCP Best Common Practice, industry standard.

DANE A working group within the IETF. Short for DNS-Based Authentication of Named Entities.

DKIM Domain Keys Identified Mail. DKIM enables e-mail servers to send and receive electronically signed e-mail.

DNS Domain Name System. An international, hierarchically designed, distributed database that is used to find information about allocated *domain names* on the Internet. The domain name system is the system that translates domain names (for example, iis.se) to IP addresses used for communication over IP networks (for example, the Internet).

DNS data Information stored with a *Registry* that states which *nameservers* are to respond to requests for a particular *domain*.

DNSSEC Secure DNS. DNSSEC is an internationally standardized extension of DNS that ensures more secure domain name lookups and reduces the risk of manipulation of information and forgery of domain names. DNSSEC's fundamental mechanism is cryptographic technology that uses digital signatures.

DNS server See *Name server*.

Domain The designation of a level in the domain name system.

Domain name A unique name, comprising parts of a name, in which a domain at a lower level in the domain name system comes before a higher level domain. A registered *domain name* is a *domain name* that is allocated to a certain *registrant*.

DS record A record type in the DNS that comprises DNSSEC information specific to a DNSSEC signed domain.

Parent zone The overlying *zone* – for example, .se is the parent zone of example.se. See also *Child zone*.

IP address Numerical address that is allocated to each computer that will be reachable over the Internet. Available in IPv4- and IPv6-addresses.

Nameserver A computer with software that store and/or distribute *zones*, and that receives and responds to domain-name queries.

Nameserver operator
An operator that provides a *DNS function* to Internet users.

Registrar Accredited resellers of .SE-domains.

Resolver	The software that translates names to *IP addresses* and vice versa.
SOA	Start of Authority. A pointer to where information about a zone begins.
TLS/SSL	SSL (Secure Sockets Layer) is a standard for encrypting communications over networks such as the Internet. Communications using HTTP over SSL are known as HTTPS. Now replaced by the IETF's (Internet Engineering Task Force) open standard TLS (Transport Layer Security).
TLSA	The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA
Zone	Delimitation of the administrative responsibility for the domain name tree. A *zone* comprises a cohesive part of the domain name tree that is administered by an organization and stored on its *nameservers*.
Zone file	A data file containing the information required about a *zone* that enables the use of *DNS* addressing.

Appendix 2 -- About DNS and the survey

According to its charter, the purpose of .SE (the Internet Infrastructure Foundation) shall be *"to promote positive stability in Internet infrastructure in Sweden and to promote research, training and education in data and telecommunication, with a specific focus on the Internet. By so doing, the Foundation must assign priority areas that increase the efficiency of the infrastructure for electronic data communication, whereby the Foundation shall, inter alia, disseminate information concerning R&D efforts, initiate and implement R&D projects and implement high-quality inquiries."* Secure Internet infrastructure is a very important and key area for us.

The considerable interest shown in the results of the surveys of earlier years convinces us at .SE that the survey is valuable and we will continue to conduct it. The study is being conducted for the sixth consecutive year. The study is part of a long-term project, which from next year will be called the Internet Ecosystem and will comprise additional areas and measurements.

.SE has been responsible for the operation and administration of all nameservers for .se domains since 1997 and, over the years, has amassed solid experience with regard to the domain name system (DNS). International Best Common Practice for DNS has gradually emerged from the organization's mistakes and experiences, and those of other parties, and this practice can also be applied to environments other than only top-level domains. DNS is somewhat of an unknown system that has existed for nearly 30 years. Throughout the years, DNS has proven to offer exceptional scalability and robust design. Essentially no changes have been required in the basic protocols, despite the enormous growth of the Internet. However, DNS has become increasingly important to the existence of functioning communication between Internet users worldwide, and this requires that all areas of DNS maintain a high level of quality.

DNSSEC

When DNS was created in the 1980s, the main idea was to minimize central administration of the network and make it easy to connect new computers to the Internet. However, no major importance was attributed to security. The deficiencies in this area opened the way for various types of abuse and attacks where the responses to DNS lookups are falsified. This way, Internet users can be misguided; for example, people can be tricked into disclosing sensitive information such as passwords and credit card numbers.

Accordingly, security extensions have been developed for DNS that are designated DNSSEC (DNS Security Extensions). DNSSEC is based on cryptographic keys that are used to sign the content of the zone files. The validation of signatures ensures that the responses truly derive from the right source and have not been changed during transmission.

.SE's launch of the DNSSEC service for more secure DNS in 2005 has also contributed to a greater focus on DNS and DNS operation. Companies wishing to make their DNS infrastructure more secure by using DNSSEC realize relatively quickly that they cannot introduce the mechanism until they first review their own DNS infrastructure as a whole.

For this reason, we are naturally interested in finding out how well prepared .se domains are for DNSSEC. This – as well as the fact that we are responsible for Swedish top-level domains – is the crucial reason why our tests focus specifically on DNS quality.

The signing of what is known as the root zone in summer 2010 accelerated the proliferation of DNSSEC. The root zone's location at the pinnacle of DNS hierarchy facilitates the implementation of DNSSEC for the underlying top-level domains.

IPv6

For computers and other equipment to be able to communicate with one another over the Internet, they must use a shared communication architecture. This means that they must use the same structure rules for communication, or the same protocol. The shared communication architecture is based on Internet Protocol (IP). Today's Internet is dominated by IPv4 (IP version 4), which was developed as early as 1981.

The IP addresses, meaning the unique number series that identify each unit connected to the Internet, comprise 32-bit numbers in the IPv4 version. This means that for IPv4, there can only be slightly more than four billion unique IP addresses. As the world becomes more connected, we are simply approaching a point where a shortage of Internet addresses will arise. The last IPv-4 addresses were allocated in 2010.

The solution for this shortage of addresses is to introduce a new version of the IP protocol, IPv6, with 128-bit addresses. There is no doubt at all that these IP addresses will be sufficient and will remain so for a long time after the transition to IPv6 has been carried out. While the IPv4 system did not even offer one IP address per person in the world, under the IPv6 system, every living individual could have 5×10^{28} addresses. In other words, everyone could have 50,000,000,000,000,000,000,000,000,000 personal IP addresses at their disposal. Rich access to IP addresses also paves the way for applications that would otherwise be difficult to realize in practice, such as the Internet of Things and intelligent homes.

For these and other reasons, the implementation of IPv6 has become more or less imperative. Accordingly, we are also looking at the current expansion of IPv6 in Sweden in closer detail.

The government, in the Digital Agenda report spearheaded by IT Minister Anna-Karin Hatt, will lead by example by proposing that IPv6 be implemented at all Swedish government agencies before 2013. However, the private sector has yet to get on board.

Services for e-mail and the Internet

At .SE, we are also interested in looking more closely at how organizations handle their communication in other respects, mainly in terms of security, availability and robustness for the most common services of electronic mail and Internet traffic. We continuously work on further development of measurement tools to be able to study more details, particularly with regard to parameters that concern Internet applications, but also concerning e-mail use. The

MailCheck tool is the latest addition to be developed. MailCheck aims to improve the quality of e-mail-related services in general by pointing out possible configuration problems, weaknesses in software and deviations from standards for both system administrators and end-users.

Appendix 3 - About DNSCheck test tool

We used the software for .SE's DNSCheck service as the engine for performing the study. DNSCheck is a program designed to help Internet users check, measure and, hopefully, better understand how the domain name system functions. When a domain (also known as a zone) is sent to DNSCheck, the program investigates the health status of the domain by analyzing DNS from its root (.) via the TLD (top-level domain – for example, .se) up to the nameservers containing information about the specified domain (for example, iis.se). DNSCheck also performs a number of other tests, such as controlling DNSSEC signatures, checking that the various host computers are accessible and that the IP addresses are valid.

The tool is available for use at http://dnscheck.iis.se. The source code for this tool and others is available for download at http://github.com/dotse/.

Our standard tool, DNSCheck, is not adequately developed to handle these values, which is why we developed a new tool that solely examines DNSSEC for signed domains. The source code for this tool and others is available for download at https://github.com/dotse/dnssec-analysis.

Other tools being used include Page analyzer and Whatweb. Page analyzer measures performance and performance affecting parameters, such as the number of external resources loaded and the sizes of the resources. Whatweb analyzes web technology. A specially developed tool is also used for measurement of DNSSEC-related parameters.

Full processing of the groups surveyed and the control group takes approximately 24 hours to complete. We then utilize a proprietary interface developed by .SE which collects data from the database and compiles it for the selected groups according to the parameters set. In addition, we can also obtain an insight by using the results of multiple different measurements concurrently to be able to rapidly identify variations and trends.

Appendix 4 - Industry standard for high-quality DNS service

For the more technically skilled reader, we have provided a more detailed description of the industry standard for high-quality DNS service in terms of recommendations in this appendix. You can easily test your domain yourself on .SE's website.

DNSCheck tool can also perform what are known as undelegated domain tests. An undelegated domain test is a test carried out on a domain that can be (but does not have to be) published entirely in DNS. This function is highly useful for those who, for example, want to relocate a domain from one nameserver operator to another. For instance, let us say that the domain example.se is to be relocated from the nameserver "ns.nic.se" to the nameserver "ns.iis.se". In this case, an undelegated domain test can be carried out on the domain (example.se) using the nameserver to which the domain will be moved (ns.iis.se) BEFORE the move itself is implemented. When the test shows a green light, it is relatively certain that the domain's new home at least knows that it should respond to queries regarding the domain. However, errors in the zone information may still exist and may not be detected by this test.

This function is available in both Swedish and English at:

http://dnscheck.iis.se/

1. At least two nameservers

Recommendation: DNS data for a zone should be located on at least two separate nameservers. For reasons of availability, these nameservers should be logically and physically distinct so that they are located in different service-provider networks in different autonomous systems (AS).

Explanation: At least two functioning nameservers should exist for each underlying domain. They should be listed as NS records for the domain in question. They should be physically separated and located in different network segments to obtain optimum functionality. This will ensure that the domains continue to function even if one of the nameservers stops working.

Consequence: When the sole server or sole service provider experiences a disruption, DNS service will be rendered unreachable for the domain on that server or in the service provider's network. Accordingly, the services under the domain will not be reachable, even if they are located with entities other than the organization's own nameserver operator.

2. All nameservers specified in a delegation should exist in the underlying zone

Recommendation: All of the NS records listed in the overlying zone (.se or equivalent) in order to point out (delegate) a certain domain should also simultaneously exist in the underlying zone.

Explanation: NS records are used in the overlying zone to transfer responsibility for (delegate) a certain domain to other servers. According to DNS documentation, this list of computers should also be found in the zone file that "receives" the responsibility and that contains other data about the zone. The lists must be kept synchronized so that all NS records included in the parent zone are also found in the child zone. The list in the parent zone is not automatically updated; it is only updated after a “manual” report is submitted to the responsible registration unit. If changes are required that entail a change to the overlying zone, the administrative contact for the underlying zone shall immediately inform the registration unit.

Consequence: If the parent zone contains information about the child zone that de facto does not exist in the child zone, this means that anyone submitting queries about the domain will not receive a response, thus resulting in an impact on availability.

3. Authority

Recommendation: All nameservers listed with NS records in a delegated zone shall assume authoritative responsibility for the domain.

Explanation: When checking the subdomain servers, it should be possible to obtain consistent and repeatable authoritative responses for SOA and NS records for the subdomain. This applies to all servers listed in the underlying zone’s DNS for the domain in question.

Consequence: DNS usually functions even if this error exists. However, the existence of this error in a zone indicates inadequate administrative procedures of the party responsible for the content of the domain’s DNS.

4. Serial numbers for zone files

Recommendation: All nameservers listed with NS records in the delegated zone shall respond with the same serial number in the SOA record for the domain.

Explanation: The serial number in the SOA record is a type of version number for the zone, and if the servers have the same serial numbers for their zones, this indicates that they are synchronized. This is controlled by sending SOA-entry queries to each server and comparing the serial numbers of the responses. SOA is the acronym for Start of Authority.

Consequence: If the nameservers are not synchronized and do not have the same version of the zone file, the entity submitting a query about a domain risks not receiving a response. Availability will be affected.

5. Contact address

Recommendation: The zone contact address in the SOA record must be reachable.

Explanation: The SOA record for a domain includes, along with other sub-entries, an e-mail address that is to serve as a contact point if the administrator of the domain in question needs to be reached. In simple checks, e-mail servers for the e-mail address shall not provide obvious error messages (for example “user unknown”). In more detailed checks, it should be possible to send test messages to the address and receive responses to these within three days.

Consequence: The reason for maintaining a current e-mail address for contacts is that it must be possible to quickly call attention to problems relating to the reachability of a domain. If such an address does not exist, it will become more difficult to solve problems arising in DNS due to an individual domain.

6. Reachability

Recommendation: All NS records in the underlying zone must be reachable for DNS traffic from the Internet.

Explanation: The NS records for a domain comprise the list of the computers that function as nameservers for the domain. All listed servers must be reachable via the Internet at all of the addresses listed in the corresponding address entries in DNS for the computers in question.

Consequence: If a name server is not reachable despite its name being included in the list of name servers that respond to queries about a domain, this means that entities submitting queries will not receive responses. Availability will be affected.

Appendix 5 – More information about DNSSEC

DNSSEC stands for DNS Security Extensions and is an expansion of DNS that ensures safer Internet address look-ups for web and e-mail servers, for example. The rising importance of DNS has made DNSSEC increasingly relevant over time.

Many other Internet protocols depend on DNS, but the DNS information in the resolvers has become so vulnerable to attacks that it is no longer reliable. The greater security provided by DNSSEC means that such attacks no longer have an effect.

Some of the most well-known and greatest threats to DNS are cache poisoning and pharming.

Cache poisoning is a situation whereby, either by attack or inadvertently, DNS data is introduced into a nameserver that did not originate from an authoritative source. One of the most notorious examples of this was the much discussed Kaminsky bug in 2008.

Pharming is when someone makes the actual DNS content point to the wrong servers. This specifically means that an Internet address for a bank, for example, may be redelegated to an entirely different server, although for the visitor, the address field still makes it appear as though he/she is visiting the right server.

Accordingly, there is no doubt that DNSs need to become more secure. DNSSEC is a long-term solution that protects against several different types of manipulation of DNS queries and responses transmitted between different servers in the domain name system.

Over the years, .SE has achieved an international breakthrough for its work with more secure DNS lookups. As early as autumn 2005, .SE was the world’s first national top-level domain to sign its zone with DNSSEC and in 2007 we were also the first to offer DNSSEC to all our domain holders. We currently have some 30 resellers (registrars) that offer DNSSEC.

It is not simply a coincidence that one of .SE’s employees was selected as a Trusted Community Representative (TCR) in order to act as a Crypto Officer (CO) and participate in the key ceremonies that are performed for the root zone four times a year; twice at the site located on the west coast of the US and twice at a corresponding site on the east coast of the US.

In contrast to the traditional domain name system (DNS), DNSSEC look-ups have a cryptographic signature, which makes it possible to ensure that these look-ups come from the right user and that the content is not changed during transmission. The aim of the service is to ensure that domain registrants can secure their domains using DNSSEC. The aim of the service is to ensure that domain registrants can secure their domains using DNSSEC.

DNSSEC is used to secure DNS from abuse and man-in-the-middle attacks including cache poisoning. For several years, .SE has been a driving force for the implementation and dissemination of DNSSEC.

What DNSSEC protects against

The purpose of DNSSEC is to safeguard the content of DNS using cryptographic methods requiring electronic signatures. Through the validation of signatures, DNSSEC allows the user to determine whether the information returned from a look-up in DNS comes from the correct source and whether it has been manipulated en route. Thus, it is difficult to falsify information in a DNS that is signed with DNSSEC without it being detected.

For ordinary users, DNSSEC reduces the risk of being defrauded, for example, when conducting bank transactions or shopping on the Internet, since it is easier for the user to determine whether he or she is really connected to the correct bank or store rather than to an impostor.

However, it is important to note that DNSSEC does not stop all types of fraudulent activity. It is only designed to prevent attacks in which attackers manipulate responses to DNS queries for their own gain.

What DNSSEC does not protect against

A number of other security issues and problems on the Internet remain that DNSSEC cannot solve, including Distributed Denial of Service (DDOS) attacks.

DNSSEC provides some protection against phishing (websites that resemble or are identical to genuine websites to trick users into revealing passwords and personal data), pharming (redirecting a DNS query to the wrong computer) and other similar attacks against DNS. DNSSEC does not prevent attacks at other levels, such as at the IP or network level.

.SE's role in DNSSEC

Many have been waiting for the root zone, meaning the parent zone of .se, to be signed and this became a reality in 2010. To date, .SE has been responsible for signing .SE's zone file and for acting as a *trust anchor* in the chain for the Swedish part of the Internet. A *trust anchor* signs the keys of the underlying zones and acts as the starting point in the verification chain. Signing means that .SE assumes responsibility for managing and verifying the DS entries of the underlying zones. This is comparable with the management of NS records in DNS.

.SE will still sign .SE's zone file, although since .SE publishes its DNSSEC keys in the root zone, it is now the root that constitutes the *trust anchor* for the Internet. This makes it easier for all resolver operators that would otherwise be forced to manage all keys for all signed top domains, which are *trust anchors* for each of their underlying domains. With the root signed, they only need to keep track of the root key. Modern standards also offer simpler handling of key exchanges, and new tools have been developed to make it easier (refer to Open DNSSEC below).

Further information on .SE's DNSSEC service is available at http://www.iis.se/domaner/dnssec/.

.SE provides additional information on DNS vulnerabilities at https://www.iis.se/domaner/dnssec/kaminskybuggen

The website's features include a link to a film that demonstrates how an attack is carried out and the ability to test whether the resolver being used is vulnerable to the Kaminsky bug.

Here are some links to further information:

Information on DNSSEC and the advances in both its use and tools. http://dnssec.net

A practical guide on how to implement DNSSEC. http://www.nlnetlabs.nl/publications/dnssec_howto/index.html

In addition, an update is ongoing of the RFC-draft-4641-bis, which also focuses on practical implementation. This is under discussion within the IETF.

News from the DNSSEC Deployment Initiative is distributed regularly at: http://www.dnssec-deployment.org/

The Initiative also has an e-mail list that anyone can subscribe to and thus stay abreast of developments in the field.

Internet Society (ISOC) is also striving to drive the development of DNSSEC. It has compiled a substantial amount of useful and useable information at: http.

OpenDNSSEC

DNS is relatively complex, as are electronic signatures. Naturally, the combination of these in DNSSEC is also complex.

After .SE noted that the lack of high-quality, accessible tools in the market for signing zone files with DNSSEC was a barrier for many parties who wished to start implementing DNSSEC, a development project was launched in conjunction with some of the foremost developers in the area. The result was OpenDNSSEC, which is a turnkey program, or a tool for facilitating the implementation and use of DNSSEC. OpenDNSSEC secures DNS information the moment before it is published on an authoritative nameserver. OpenDNSSEC takes an unsigned zone file, adds signatures and other items for DNSSEC and sends the file on to the authoritative nameservers for the relevant zone.

The purpose of OpenDNSSEC is to manage these difficulties and relieve system operators of responsibility for them once the operators have set up the system.

By participating in the development of a turnkey system for signing zone files with DNSSEC, .SE hopes to facilitate the spread of DNSSEC.

OpenDNSSEC is developed under a special company owned by .SE (The Internet Infrastructure Foundation).

The software, OpenDNSSEC, is the result of a collaboration between developers from .SE, Nominet, NLNet Labs, SIDN, SURFnet, Kirei AB and Sinodun. More information is available at http://www.opendnssec.org/

The software, which is openly available, can also be downloaded and tested from the website.

Appendix 6 – Open recursive name servers

A **recursive nameserver** not only responds to queries about DNS records for which it itself is responsible, but also goes further and asks other nameservers to respond to queries. Queries can be both labor-intensive (meaning that they utilize extensive computer capacity) and result in a relatively large amount of data, which means that organizations normally want to limit the number of persons permitted to use the recursion function.

An **open recursive nameserver** responds to all queries it receives for which recursion has been requested. This makes it possible for external parties to launch Denial of Service attacks; for example, via the open nameserver; for example, by allowing these parties to submit queries that will result in unusually large responses (what is known as an Amplification Attack). Combined with a false sender address that leads to the response being sent somewhere else, this comprises a Denial of Service attack.

The fundamental problem is not actually open recursive nameservers, but the fact that service providers do not filter traffic by sender addresses. If they did, open recursive resolvers might not be considered a problem. Since such filtering is relatively difficult and costly to implement for the service providers, which causes reluctance to do so, we need to attempt to limit the damage caused by DDOS attacks in the meantime until the service providers have solved the fundamental problem. Closing a recursive resolver is a relatively simple task that is worth the trouble of implementing, since it will help ease problems arising from DDOS attacks.

Pointers to further information

Below, we have gathered some links to high-quality, informative material about DDOS and open recursive nameservers.

Secure Domain Name System (DNS) Deployment Guide
http://csrc.nist.gov/publications/nistpubs/800-81r1/sp-800-81r1.pdf

DNS Amplification attacks
An excellent description of how these attacks occur and what they entail.
http://www.isotf.org/news/DNS-Amplification-Attacks.pdf

Official advice from the US CERT
The Continuing Denial of Service Threat Posed by DNS Recursion
http://www.us-cert.gov/reading_room/DNS-recursion033006.pdf

ISC BIND. Here you can find source codes and binaries for BIND and links to highly interesting and useful information.
https://www.isc.org/downloads/all/

BIND 9 Administrator Reference Manual.
Includes examples of configuration, practical tips and detailed descriptions of BIND functions.
http://www.isc.org/files/arm97.pdf

Appendix 7 - Action against spam

DKIM

Domain Keys Identified Mail (DKIM) is a method for preventing e-mail messages from being sent with a false domain name in the sender address, that is to say that the sender uses an address other than his or her own as the sender address. DKIM is based on cryptography; the sender's post office signs ("stamps") all outgoing post. Recipients can, in turn, verify this stamp.

The purpose of DKIM is to counteract phishing, which is a type of spam with a false sender used to trick Internet users into providing sensitive information.

Any modifications can be detected by the receiving party as the sender uses cryptography to sign a control sum of these parts with a private key. Along with the private key, a public key is required to verify that the signature is correct. This public key is published by the sender in its DNS.

The DKIM signature is subsequently sent with the message as part of the e-mail header. The receiving software validates the message received against the signature and the public DKIM key. As a result, any changes can be detected.

Author Domain Signing Practices (ADSP) is used to detect unauthorized removal of the signature. Using ADSP, the sender can inform the recipient whether or not the domain in question signs its messages. This information is also distributed via the sender's DNS. ADSP has been a proposed standard since August 2009[19]. Its function is documented in RFC 5617. In brief, the RFC defines a type of record that can announce whether a domain signs its outgoing e-mail and how other servers can access and interpret this information.

By searching for the public DKIM keys, it is possible to determine which domains sign their e-mail using DKIM. However, the method used to find these domains cannot distinguish between domains that use DKIM and those that use its predecessor, DomainKeys. The main reason is that DKIM and DomainKeys publish their keys in similar ways.

Read more about DKIM at http://www.dkim.org.

SPF

Sender Policy Framework (SPF) is a method for preventing e-mail messages from being sent with a false domain name in the sender address, meaning that the sender uses an address other than his or her own as the sender address.

SPF gives the domain registrant the option of publishing rules in DNS that specify the computer addresses from which e-mails from the domain are to originate. When a receiving e-mail server receives a message, it checks this message against the SPF information in DNS according to the rules there. If the message comes from a sending server that is not published in the rules, the receiving server interprets this as an indication that something is wrong.

Based on this information, the receiving server can determine the fate of the message, such as refusing to accept the message or filtering it as spam. The SPF

[19] http://tools.ietf.org/html/rfc5617

standard does not define what will happen to messages that do not meet the SPF validation criteria.

Read more about SPF at http://tools.ietf.org/html/rfc4408.

Appendix 8 - Actions for transport security

Electronic mail

Since e-mail is most commonly transmitted in cleartext, it is often compared with postcards. A few years ago, a standard for transmitting e-mail with transport security was introduced; it can most closely be compared with continuing to send postcards, but actually locking the “mail van” during transport. This means that anyone attempting to read the e-mail en route between the post offices cannot see what is being sent. E-mail transport security is often known as STARTTLS.

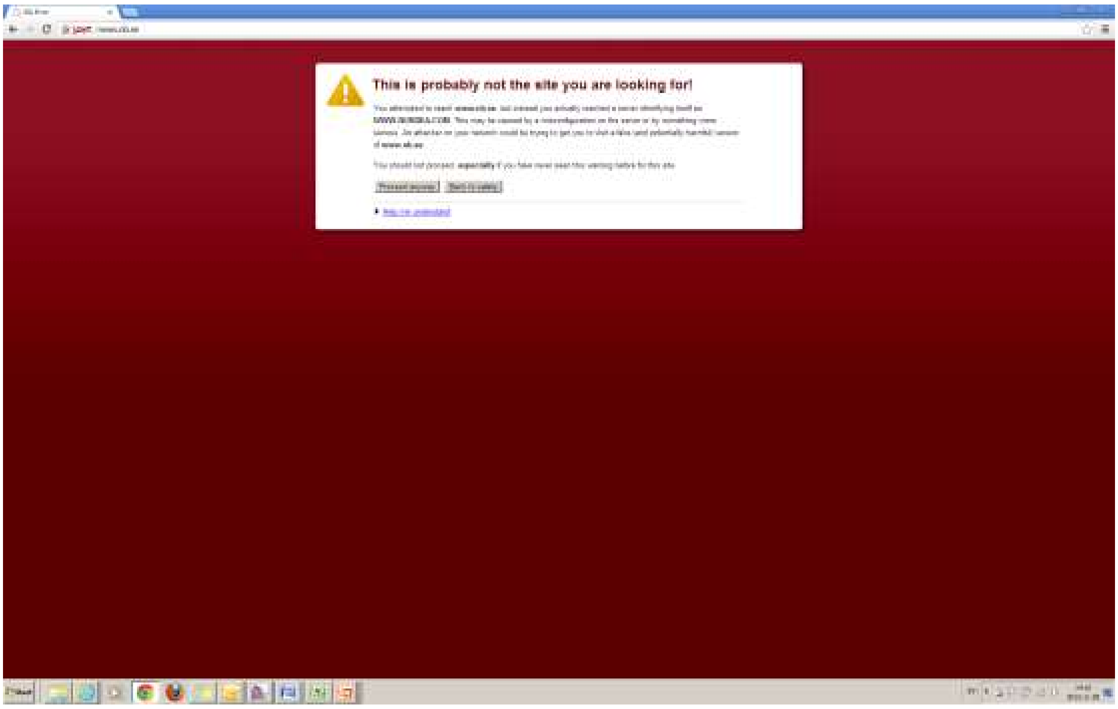
Additional protection is required if the sender wants to send e-mail that nobody else can read, not even those responsible for the e-mail system (or those who “work at the post office”). In these cases, the entire letter can be encrypted by “gluing the envelope shut and sending it by registered letter,” to make an analogy with the traditional postal service. The two most common methods for this type of encryption are PGP and S/MIME.

Web traffic

For a user who wants to contact a Swedish government authority or a bank, for example, it is important to know that the server being contacted is the correct server, and that the user has not for some reason connected to the wrong service or server due to an incorrect configuration or intentional fraud.

One of the methods used also for this purpose is Transport Layer Security (TLS). TLS/SSL gives users the opportunity to check that a connection has been made with the correct server or service.

The web browser checks that the address entered in the web browser is the server address included in the web certificate. If the addresses are not the same, the user receives a warning that something may be wrong, as shown in the example below using Chrome as the web browser.



.SE (The Internet Infrastructure Foundation) is a not-for-profit public-service organization that acts to promote the positive development of the Internet in Sweden. .SE is responsible for the Internet's Swedish top-level domain, .se, encompassing domain-name registration and administration, as well as the technical operation of the national domain name registry. Proceeds from domain-name registrations are used to support projects that contribute to the Internet development in Sweden, through proprietary operations and the financing of independent projects.

This survey is included in of .SE's Health status focus area. The aim of this focus area is, among other things:

- To monitor the quality of the Internet's infrastructure in Sweden by compiling and analyzing facts,
- To disseminate the results from the surveys, and
- To use advice and recommendations to contribute to ensuring that the infrastructure functions well and has a high level of accessibility.

Another aim is to, when necessary, detect deficiencies and improprieties.

.SE (The Internet Infrastructure Foundation)
P.O. Box 7399, SE-103 91 Stockholm, Sweden
Tel +46 (0)8 452 35 00, Fax +46 (0)8 452 35 02
Org. nr 802405-0190, www.iis.se, info@iis.se

.se
Moving the Internet forward