Reachability on the Internet

Health Status of .se 2010

.se

1 Introduction

In the fourth report from .SE's survey of Internet reachability and .SE's health status, we present results of the 2010 survey. The aim of the survey is to review and analyze the quality and reachability of the domain name system (DNS) in the .se zone and some other key functions for .se registered domains, through a selection of domains that represent central functions in society and a random selection of all .se domains.

This year's study is largely, though not completely, a follow-up of similar studies conducted in 2007, 2008 and 2009. In other words, this year we also have sufficient material to compare the results of these studies over a four-year period.

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.

The survey is included in one of .SE's focus areas, namely The health of the Internet in Sweden. The aim of this focus area is to monitor the quality of the Internet's infrastructure in Sweden. .SE endeavors 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. The objective for 2010 has been to implement advancement activities and improvements in terms of method support and the survey area.

The Health status report was financed by .SE and headed by Project Manager Patrick Wallström. The results of this year's survey have been analyzed and the report was compiled by Anne-Marie Eklund Löwinder, Quality and Security Manager at .SE. Anders Örtengren, from Mistat AB, reviewed the statistical analysis.

More information about the content of the report is available from Anne-Marie Eklund Löwinder, Head of Quality and Security at .SE. Her e-mail address is anne-marie.eklundlowinder@iis.se. More information about the Health status report is available from Patrick Wallström. He can be reached at patrik.wallstrom@iis.se.

2 Summary

Like the study conducted in earlier years, this year's study has primarily focused on DNS quality. We have also studied some other key parameters, such as e-mail and web servers. This year's study has also included a more in-depth analysis of the use of IPv6 and DNSSEC. The study was performed in October 2010.

2.1 670 investigated domains

The tests encompassed a total of 670 domains distributed among 908 unique name servers. The term "unique" is defined as servers with unique IP addresses. A name server with a service provider can house several domains. A comparison was also made with the .se zone in its entirety.

Although we have endeavored to keep to approximately the same test group as in the 2009 study, certain changes have occurred, which means that the studies conducted over the years are not entirely comparable. For example, 663 domains were investigated in 2009, compared with 670 this year. One of the main reasons for the change in number of domains is that changes have occurred among a number of government authorities, including closures, mergers and new additions. We also expanded the Bank and insurance category this year to include more of the registered companies subject to inspection by the Swedish Financial Supervisory Authority, meaning that this category has expanded from 21 to 67 domains. One domain name may also be included in several categories, although this only occurred once in the combined group. As a result, the sum of all domains in the various categories is 689, resulting in 19 duplicates.

2.2 More than one quarter experienced serious problems

In 2007, we conducted the first investigation to gain an impression of the status of the .se zone. The 2008 investigation gave us an indication that there had been some positive development in the area. 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 that we emphasized and for which we proposed solutions. These were sent to the Infrastructure Minister at the time, among others, and the report has also been addressed during debates in the Swedish Parliament.

In 2010, despite reporting serious deficiencies over several years, we were unable to detect any significant improvement. Of the 670 domains included in the test group, 25.4 percent experienced serious problems that should be addressed immediately and 43.4 percent have issues of a nature that generates warnings, which, although they are not as urgent as the serious problems, should also be resolved. In 2009, these figures were 23 and 34 percent, respectively.

In the survey, two domains had such serious problems that they could not even be tested. They were functioning, in the respect that users could reach the domain's websites, although they were probably not accessible by e-mail. However, as far as we can tell, these domains are not used for e-mail, only web traffic, which may be one of the reasons that the Registrant of these domains has not even noticed that the sites have serious reachability problems. If they were to use DNSCheck to test their domains, the response would have been that the domain does not exist.

Unfortunately, the total percentage of serious problems and warnings has increased since the last survey. The deterioration in results may be due in part to changes in the survey group, although not entirely. The conclusion remains that we were unable to see any significant improvements.

We are, in fact, unable to comprehend this development: whether it is a matter of carelessness, incompetence, a lack of resources or something else. The domain name system including name servers is critical for the Internet to function properly. Its importance must be advanced to the top level and it must be taken seriously.

2.3 No improvement since last year

In other words, our observations for 2010 indicate that there have not been any actual improvements in the area at all, despite all of the talk about the importance of having a robust infrastructure and how high the availability requirements are on, for example, public administration electronic government services.

The aim of publishing the results from the survey annually is to draw attention to the problems and deficiencies from which a number of domains in the .se zone suffer. Conducting the surveys over the period of several consecutive years also provides us with an opportunity to see the development trend, 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 study conducted in 2007 confirmed .SE's hypothesis that knowledge of what is required to maintain a high level of quality in the domain name system (DNS), for example, is generally deficient, although the interpretation of what constitutes "high quality" can of course be discussed. In this case, we have used our own definition of "high quality," but have based this definition on recommendations from international *Best Common Practice*. In addition, there is also reason to believe that these knowledge deficiencies apply to both operations and operational responsibility.

2.4 Dominant players increase the risks

The array of service providers to which users connect name servers is declining. The major Internet service providers are becoming increasingly large and the small service providers are fading. One of the risks associated with this is that a single service provider may dominate a certain category. The implications may, in the worst case, result in an entire sector being affected if the individual service provider experiences problems.

2.5 Lack of competence among name server operators

The survey results from previous years have led to the conclusion that there is a lack of knowledge regarding the measures required to maintain a high level of quality in the domain-name system (DNS). There is reason to believe that this lack of knowledge also pertains to maintenance and operational responsibility. The fact that some of the most serious problems are still relatively commonplace also confirms the hypothesis that the situation has not tangibly improved on earlier investigations, in fact quite the opposite. There is reason for the responsible authorities to begin imposing pertinent demands on those operating the name-server services for such organizations as public administrations.

2.6 Inadequate certificate management

The management of certificates in the survey group's web server environment remains inadequate in all respects addressed by the investigation. Among the organizations included in the survey, we had expected better results, particularly concerning the use of valid, current certificates issued by reliable issuers.

3 Control points

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

- How does the organization manage its own 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?
- How does the organization manage its e-mail? Are the servers located in or outside Sweden, is TLS/SSL (transport security) accepted, how widespread is the use of SPF (technology for reducing the amount of spam)?
- How does the organization connect its websites to the Internet? Where are the servers located, which server software is used, and does the organization use web certificates, meaning does it have support for TLS/SSL (transport security)? How are server certificates obtained?

In this year's survey, we removed a test in which the subject had name servers located with several operators (various Autonomous Systems, AS), since the results were too uncertain, it was simply too difficult to determine with a sufficiently high level of reliability. In addition, some of the major operators are currently building networks in which Anycast is used, or are otherwise built robustly enough to not be affected by having name servers placed with a single operator. ISP's incorporating the maintenance of the name servers into the organizations' own networks also appears to be a trend.

The domains and name servers of a large number of important organizations in society were tested: public service and state-owned companies; listed companies; banks and finance companies; Internet service providers; municipalities; county councils; media companies; government authorities, including county administrative boards; and universities and colleges, a total of 670 domains. The allocation by category is presented in section 5.

The data-collection process was fully automated and included testing of the most frequently occurring errors and defects we associate with DNS operation, e-mail and web-server management.

Based on these tests, we investigated how well the organizations' systems function in various contexts, the areas in which the most serious defects arise and the possible consequences. This year, we also had a better opportunity to compare the results with previous studies, since we now have access to the results from a total of four years, enabling us to arrive at conclusions on trends in the area.

We have also linked recommendations to this information on what we would like the DNS infrastructure to be like in more general terms. Finally, we have provided some guidelines and recommendations containing proposals to the responsible authorities that we consider to be suitable parties with which to pursue the study in greater detail. These questions are essentially the same as in the preceding year's study, since the results of the investigation are clear, namely that there have been no radical improvements to the situation. However, we would ideally like to see authorities with decision-making powers accept these proposals and take appropriate action in the areas of DNS, DNSSEC and IPv6.

4 Quality DNS service

The domain name system is one of the cornerstones of the Internet and is designed to simplify the process of addressing resources on the Internet. Every connected unit has its own IP address that, with the help of the DNS, can be linked to an address in a form that is easier for us to handle as humans. We applied the definition of quality DNS service also for this investigation.

In brief, a high-quality DNS service entails the following:

- That the organization has a robust DNS infrastructure with a high level of reachability,
- That all name servers 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 authentic,
- That the organization meets the requirements imposed by the relevant Internet standards and other standards.

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

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

Earlier investigations led to the conclusion that there is a lack of knowledge regarding the measures required to maintain a high level of quality in the domain-name system (DNS). There is reason to believe that this lack of knowledge also pertains to maintenance and operational responsibility. The fact that some of the most serious problems are still relatively commonplace also confirms the hypothesis that the situation has not tangibly improved compared with earlier investigations, in fact quite the opposite.

In Appendix 4, we have described the key measures that must be implemented to create a high-quality overall DNS infrastructure.

5 Tests performed in 2010

The tests performed in 2010 included the configuration of domains and the name servers that respond to queries about the domain. We also tested some of what we consider to be the principal parameters for e-mail and web servers. The tests made use of software that automatically checks the various control points stated in the industry standard for all domains included in the study, as a whole and per category. This was supplemented with questions regarding such areas as e-mail and web-server management. Part of the study was also performed to more closely examine various issues related to providing more secure, accessible and robust e-mail and web services.

Tests were performed on a total of 670 domains and 908 unique name servers. The test subjects were grouped into the following categories:

- Public service and state-owned companies (40)
- Banks and insurance companies (67)
- Internet service providers (ISPs) (20)
- Municipalities (290)
- County councils (21)
- Media companies (24)
- Government agencies, including county administrative boards (excluding agencies under the Swedish Parliament) (201)
- OMX-listed companies (28)
- Universities and colleges (35)

A total of 19 domains were duplicates, meaning that they were included in more than one category. All county councils are listed under a single domain.

We reported two different types of problems and categorized them as either errors or warnings.

Errors: Anything marked as an error in the study should be corrected immediately so that the organization can be assured of a high level of availability and accessibility in the DNS and other resources.

Warnings: Warnings also constitute errors that could affect operations, where although corrective actions are not deemed as urgent, they would naturally enhance quality and availability.

6 Observations for 2010

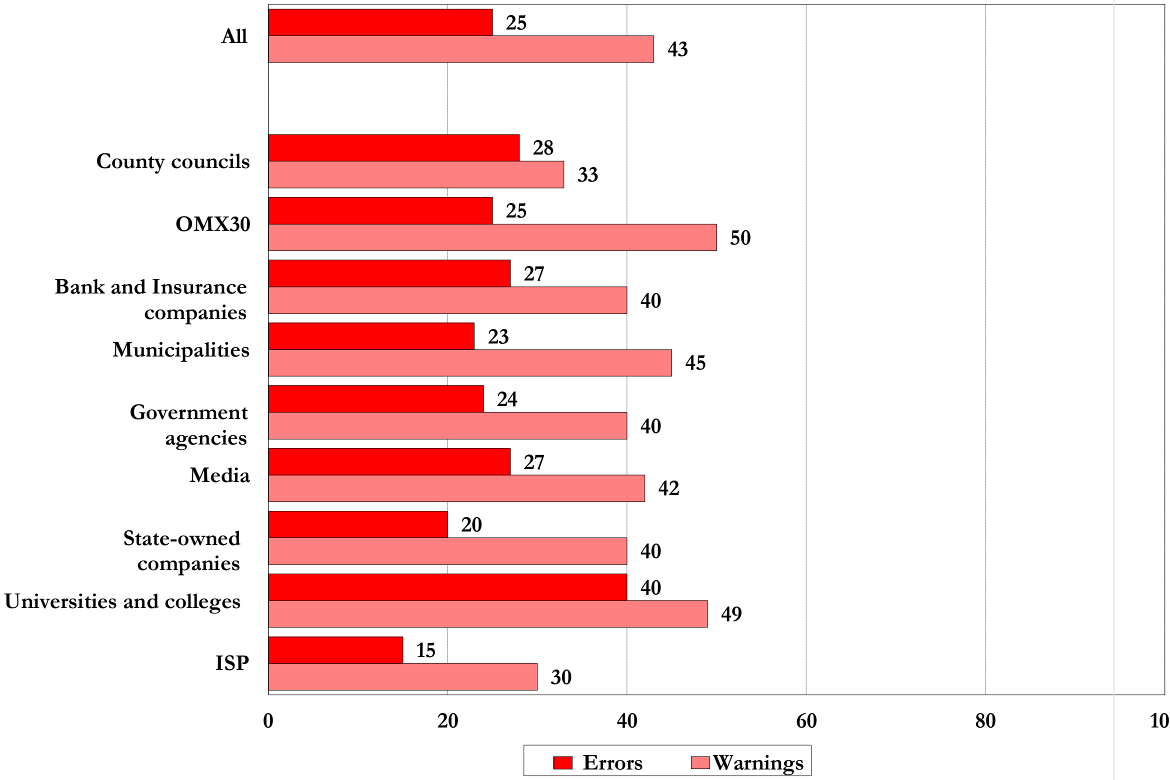
In 2007, we conducted the first survey to gain an impression of the status of the .se zone. The 2008 survey gave us an indication that some positive development had occurred in the area. When, in 2009, we began to see trends, we were able to confirm that the changes were negligible and that there were still major problems that we recognized and for which we proposed solutions. These solutions were sent to the Infrastructure Minister at the time, among others, and the Health-status report has also been addressed during debates in the Swedish Parliament, and during the Traffic and Defense Committees' public inquiry regarding IT security in 2008.

In 2010, we can confirm that serious deficiencies remain and that we were unable to recognize any improvements. Of the tested domains, 25.4 percent had serious errors that should be fixed immediately and 43.4 percent had defects of a nature that resulted in a warning.

6.1 Test of DNS – defects and warnings

The following graph shows the distribution between errors and warnings among the various categories included in the study:

Graph 1: Errors and warnings



The graph shows the percentage of errors and warnings for the entire test group (All) and for each individual category. The bars of the graph should be read so that of the 670 organizations included in the study, 25 percent had serious errors and 43 percent had defects of a nature that generated a warning. Of the 21 county councils studied, 28 percent had serious errors and 33 percent had defects of a nature that generated a warning, etc.

The situation for the investigated group as a whole has deteriorated since last year. Government agencies, media companies, universities and colleges, and ISPs had more errors in 2010 than in 2009. In the case of universities and colleges, there were far more errors this year than last. However, county councils, OMX30, bank and insurance companies, and state-owned companies experienced fewer errors than last year.

However, the percentage of warnings rose sharply for the OMX30 group, and increased among bank and insurance companies, municipalities, government agencies and state-owned companies groups. The percentage of warnings remained unchanged for county councils, while decreasing among media companies, universities and colleges, and ISPs.

The graph also indicates that in 2010, universities and colleges were the group that had the largest percentage of errors. In this group, nearly 40 percent of all name servers suffered from some type of error that was considered serious, up a full 25 percent, meaning a far worse result than last year. In other words, access to information and services in the operations in all categories was equally affected by errors and warnings as last year, if not more so. To view the distribution of errors and warnings by category and year, refer to section 6.3.

6.2 The most frequently occurring errors

Faulty configurations that are performed at any of the largest name-server service providers would have a major impact on the results of the investigation. It is worth mentioning that .SE's three largest registrars account for 50 percent of the market and the seven largest represent 75 percent of the market. Among the name-server operators, the largest two account for 36.6 percent of the market and the largest five for 50 percent of the market. Meanwhile, the name-server operation market has a long tail, with a large number of small operators.

Among the domains and name servers tested, the most common errors were:

- The name server did not respond to requests via the TCP (Transmission Control Protocol). The probable reason is that the DNS server was not correctly set up or the firewall was incorrectly configured. It is a fairly common misconception that the DNS does not need to be able to communicate according to the TCP protocol (if it does not provide zone transmissions). However, the truth is that TCP is a requirement under a standard (RFC 5966, *DNS transport over TCP implementation requirements*), and the trend is that the need for TCP is increasing as new protocols result in it being used more extensively than in the past. This error indicates that the person who configured the name server has insufficient current knowledge of the DNS.

- The organization has an inconsistent name-server structure (NS). The name servers listed with NS entries in a child zone are different from the information found in the DNS in the parent zone and, accordingly, the name servers cannot assume authoritative and proper responsibility for the domain. If the information is not consistent, the availability of the domain is negatively affected, which indicates deficiencies in the internal DNS management. Some examples of such inconsistencies are provided below:
    - The IP address of a DNS server 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 administrator of the domain has probably forgotten to make an update after a change took place.

  - A DNS server is listed in the parent zone but not in the child zone. This is probably an administrative error. The parent zone must be updated as soon as possible so that it lists the same DNS servers as those listed in the child zone. The consequence of such a defect is that the redundancy that someone has tried to create essentially does not exist.

- The name server lacked EDNS support. This is an expansion of the DNS protocol to handle DNS responses that exceed the UDP protocol limitation of packet size to 512 bytes. EDNS enables DNS responses in excess of this amount, which is also becoming increasingly normal along with the expanded use of DNS in conjunction with, for example, DNSSEC and IPv6.

- The DNS server did not respond to requests via UDP (User Datagram Protocol). The probable reason is that the DNS server was not correctly set up or the firewall was incorrectly configured. A name server that responds to neither TCP nor UDP is probably not reachable at all, and so the defect may be found elsewhere, for example in connection with the name server, or the server may not have a correctly stated IP address. The name-server tests are cancelled if both of these conditions have been confirmed.

- Only one DNS server is found for the domain. There should always be at least two DNS servers for one domain so that temporary errors with connections can be handled. If one of the servers or the connection to it were to stop functioning, services directed from the name server would also be rendered unavailable. We made separate calculations 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 warning).

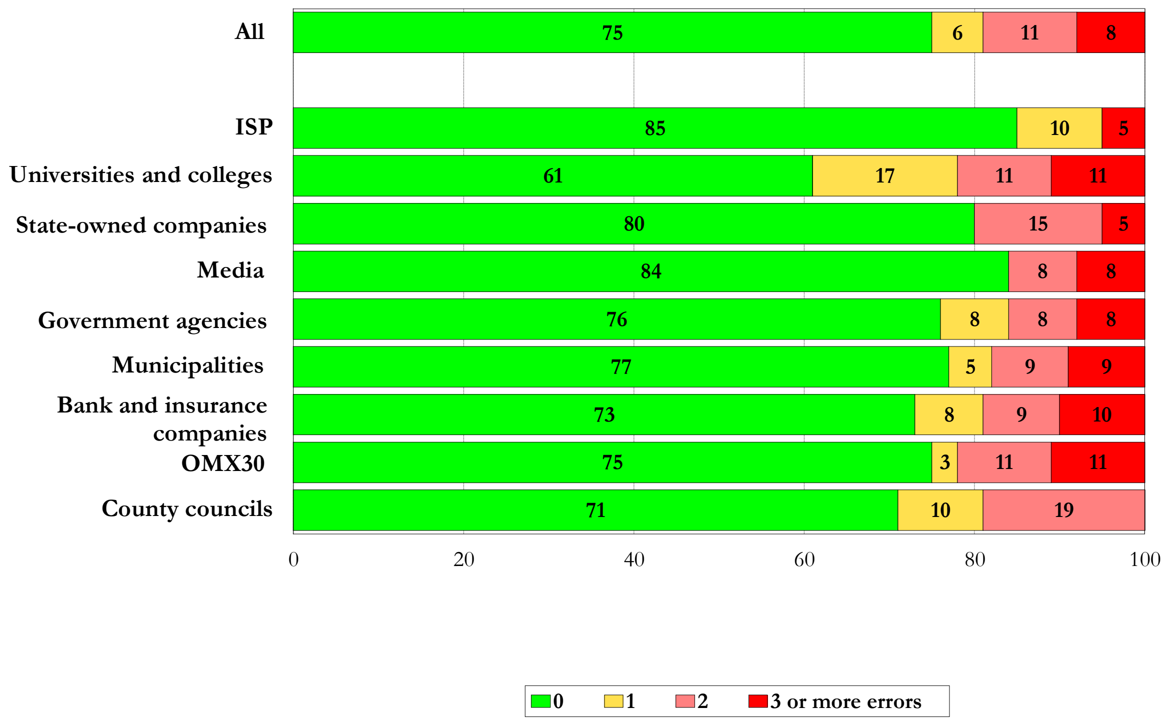
- The DNS server is recursive. The DNS server responds to recursive requests from third parties (as in DNSCheck). It is very easy to abuse open recursive resolvers during distributed denial of service attacks (DDOS), since the use of a very small DNS query can create a leverage effect generating exponentially larger responses. False source addresses can be generated using DNS, and those who want to attack a system create queries under a false source address that produce major DNS responses that are sent to the presumed source, which is in fact a third party whose services more or less will be blocked (refer to appendix 6).

- The SOA serial number is not the same in all DNS servers. This is usually due to an incorrect configuration, but is sometimes due to slow dissemination of the zone to secondary DNS servers. This means that users searching for resources under a domain may receive different responses depending on which name server receives the request.

6.2.1 NUMBER OF ERRORS PER CATEGORY

Naturally, there is a difference between whether a domain has one error or several errors which also often interact. Accordingly, as in earlier years, we have also examined the distribution of the number of errors in terms of quantity and among the different categories.

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



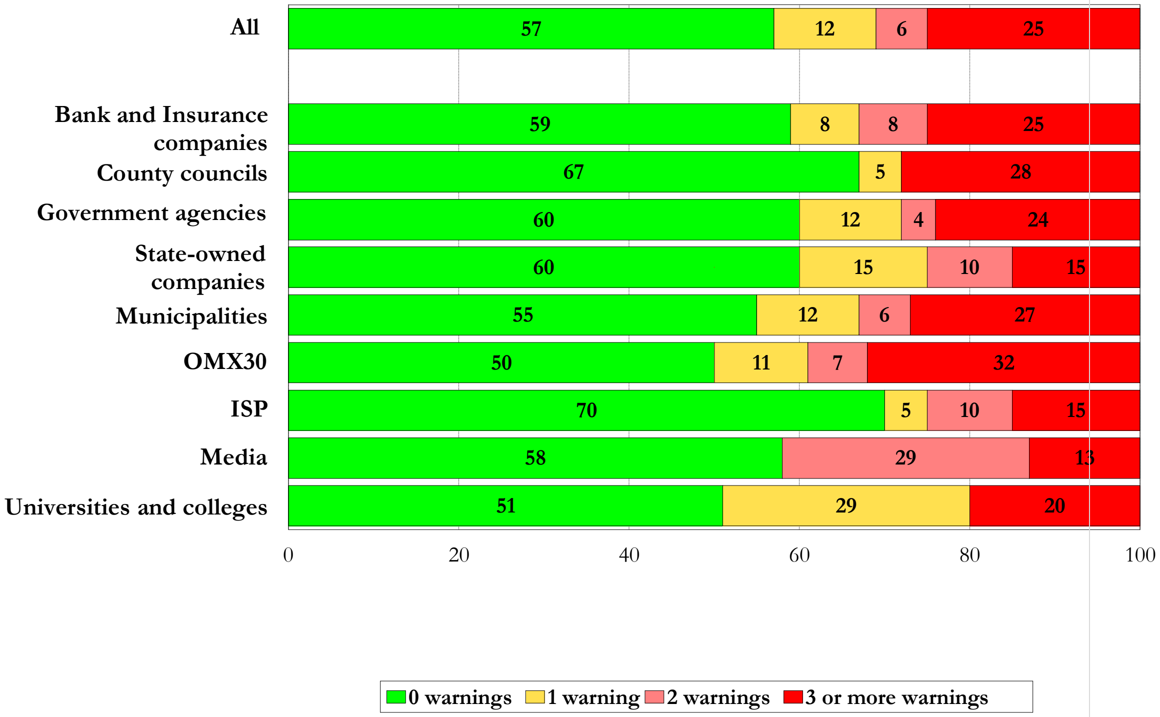
Internet service providers have the lowest error percentage, while universities and college had the highest in 2010. In this area, it might have been expected that the knowledge and expertise regarding DNS would be found among these institutions, as well as the experience of how to conduct maintenance and administration. In the Universities and colleges category, there appears to have been a change that has resulted in a significant deterioration.

In 2010, the County councils category had a lower share of errors at 29 percent compared with last year's 33 percent. The OMX30 category also had fewer errors at 25 percent compared with last year's 30 percent. The only categories to fall short of 20 percent errors were ISP and Media, which really should be the benchmark for all categories. Any organization should be able to fall short of 20 percent without any efforts. Falling short of 15 percent errors requires slightly more effort.

6.2.2 NUMBER OF WARNINGS PER CATEGORY

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 graph on the next page.

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



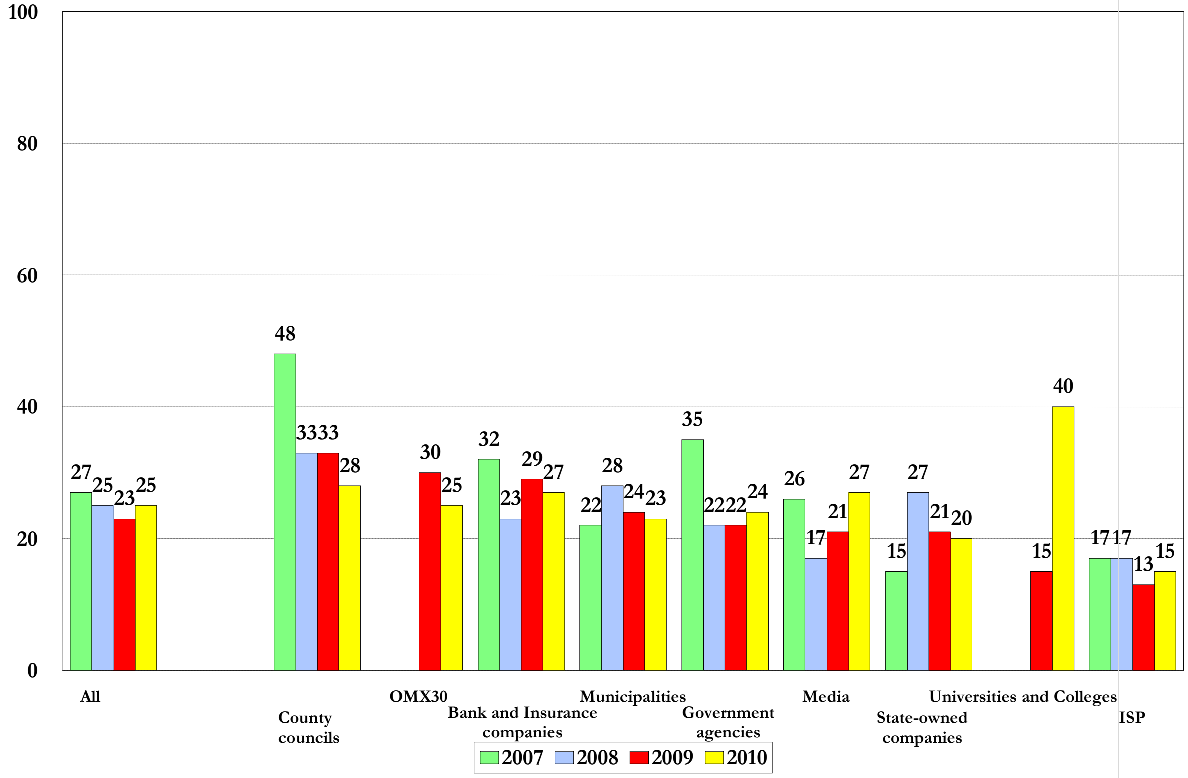
The OMX30 category had the most warnings in terms of percentage and number, followed by universities and colleges. Among municipalities and county councils, 27 and 28 percent respectively had three or more warnings. Our assessment is that this is primarily due to administrative shortcomings, such as e-mail addresses that are entered in DNS not functioning. This is generally also much more commonplace with warnings than errors. However, both have a negative impact on reachability.

6.3 Comparison over time – errors and warnings

Because we saved the raw data from previous studies we had the opportunity to compare this year's results with those of the previous studies for the categories that were included in the studies for all four years. Some categories were first included in 2009 and we were thus only able to report results from the past two investigations for these categories.

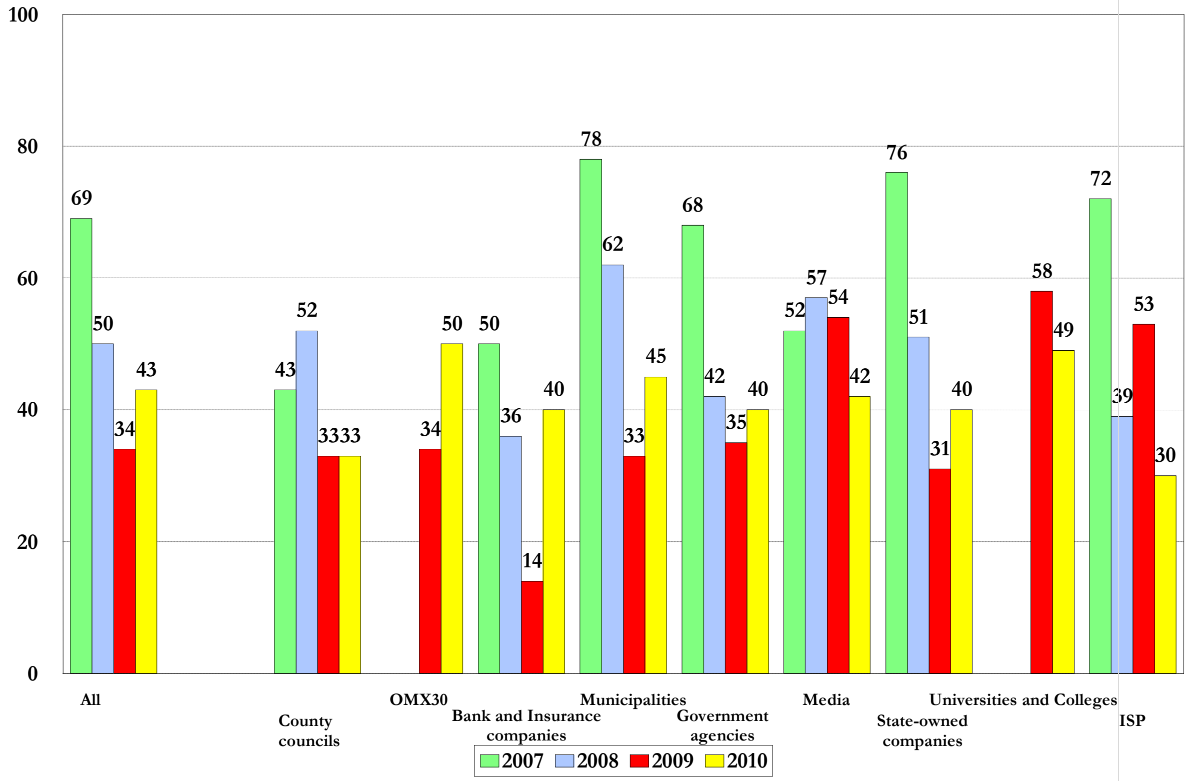
In the following graph, we compared the percentage of errors over time, from 2007 to 2010 (with the exception of universities and colleges and OMX 30, which were added last year and for which we can only compare 2009 with 2010).

Graph 4: Number of errors over time



The graph shows that the situation has improved somewhat compared with the first investigation. However, this year's results are worse than last year's for the All category. The number of errors has increased in the Government agencies, Media, Universities and colleges, and ISP categories. Meanwhile, a decline was noted among the OMX30, Bank and insurance companies, Municipalities, State-owned companies and County council categories, which also indicated a trend of improved results over time.

Graph 5: Number of warnings over time

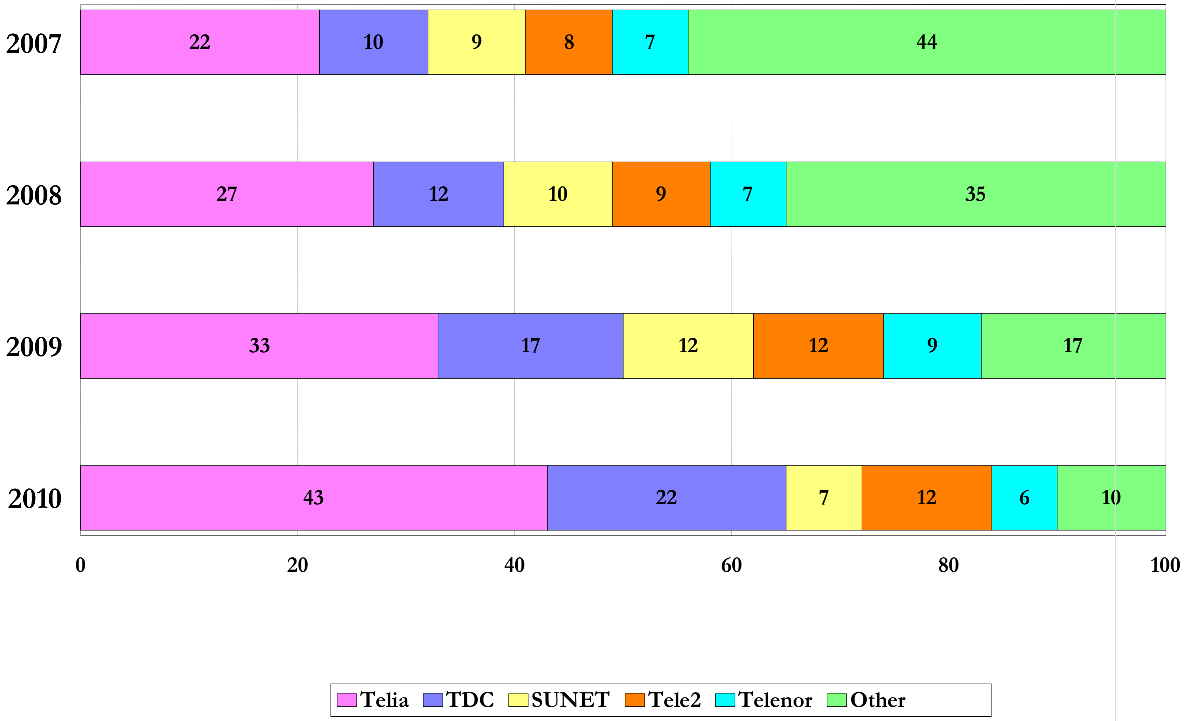


Warnings declined significantly between 2007 and 2009. The relatively sharp rise in 2010 broke this trend – in the wrong direction. OMX30, Bank and insurance companies and Municipalities increased considerably. Government agencies and State-owned companies showed a rise. County councils remained unchanged at 33 percent, while the number of warnings declined in Media, Universities and colleges and ISP.

6.4 Name server connections to the Internet

As in earlier years, we took a closer look at which service providers the name servers for the various organizations used for their Internet connections. **The following graph does not show which service provider operated the name servers for the domains; instead, it only shows which service provider the name server used for its Internet connections.**

Graph 6: Allocation of ISPs – name servers' Internet connections



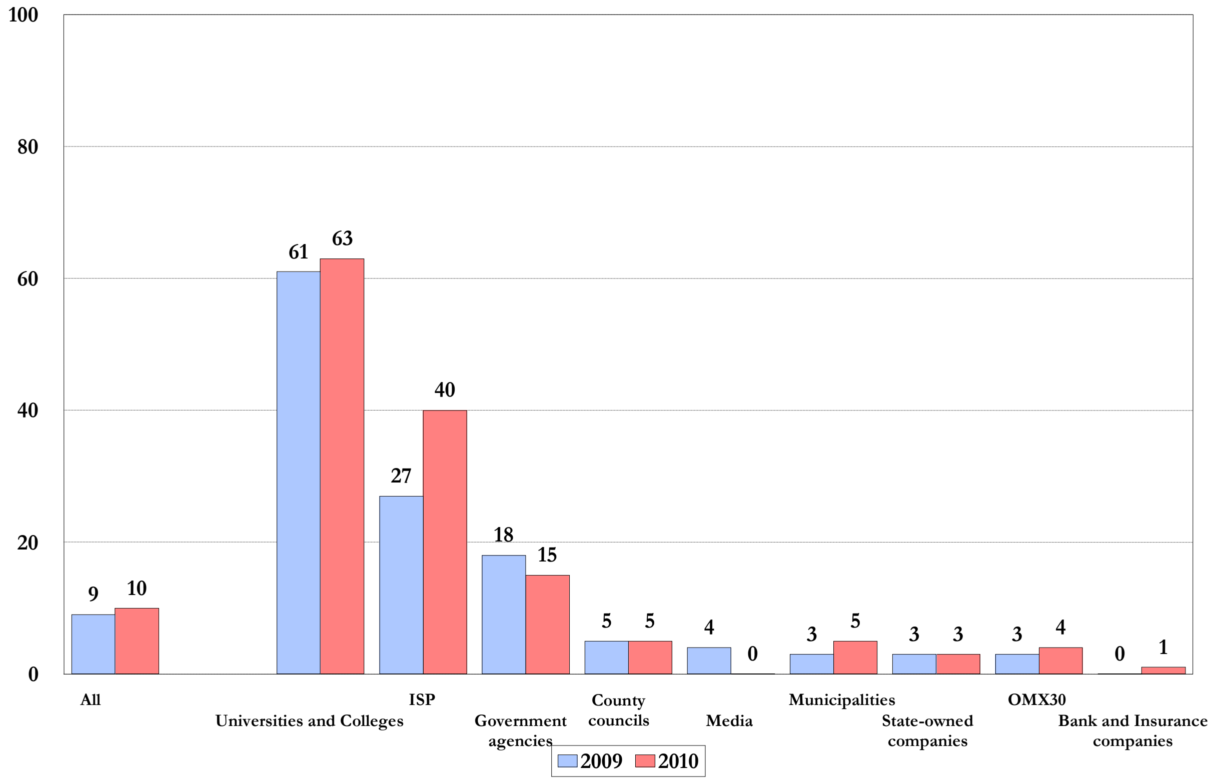
We can confirm that the distribution among service providers, in terms of name-server connections to the Internet, is declining from year to year relative to the total number of domains. The percentage of "Other" decreased sharply in 2010 and has declined from 44 percent in 2007 to 10 percent this year. We noticed a general rise among the largest service providers, among which Telia in particular appears to increasingly dominate the market and increased its share to 43 percent this year from 33 percent last year. TDC also bolstered its share, while Tele2 remained unchanged at 12 percent. Sunet and Telenor declined considerably. The year-on-year changes were significant.

We also noticed how the distribution of the operation of name servers declined among service providers. The large providers are expanding and the small providers appear to be fading away. One of the risks associated with this is that a single service provider may dominate a certain category. The implications may, in the worst case, result in an entire sector being affected if the individual service provider experiences problems. We examined the databases more closely to attempt to assess their condition. However, there do not currently appear to be any cases in which an entire group of domains is dependent on a single supplier, and where this is closest to being the case the service provider concerned is Telia. We already know that if Telia experiences problems, this has major implications in a number of areas.

6.5 Name servers using IPv6

While the trend of increased activity in the IPv6 area has sustained, it remains far too modest. The only exceptions are the University and colleges and ISP categories.

Graph 7: Use of IPv6 on name servers



A total of 10 percent of the investigated domains have a name server that is accessible via IPv6, compared with 9 percent in 2009. Despite initiatives by the Swedish government that require IPv6 support during public procurement processes, the survey does not indicate any positive changes in the Government agencies category and a highly negligible change in the Municipalities category.

The lack of addresses will soon become urgent and it is high time to shift to IPv6. It is important to understand that such a transition requires 12-18 months of preparation and work.

Switching to IPv6 is the only way to guarantee a stable, future Internet infrastructure. .SE has taken an active role in facilitating cooperation and coordination concerning the transition. As a result of this, we have launched a website to continuously report on IPv6 in Sweden. These reports are available at http://ipv6.iis.se/.

6.6 Service providers offering name-server operations

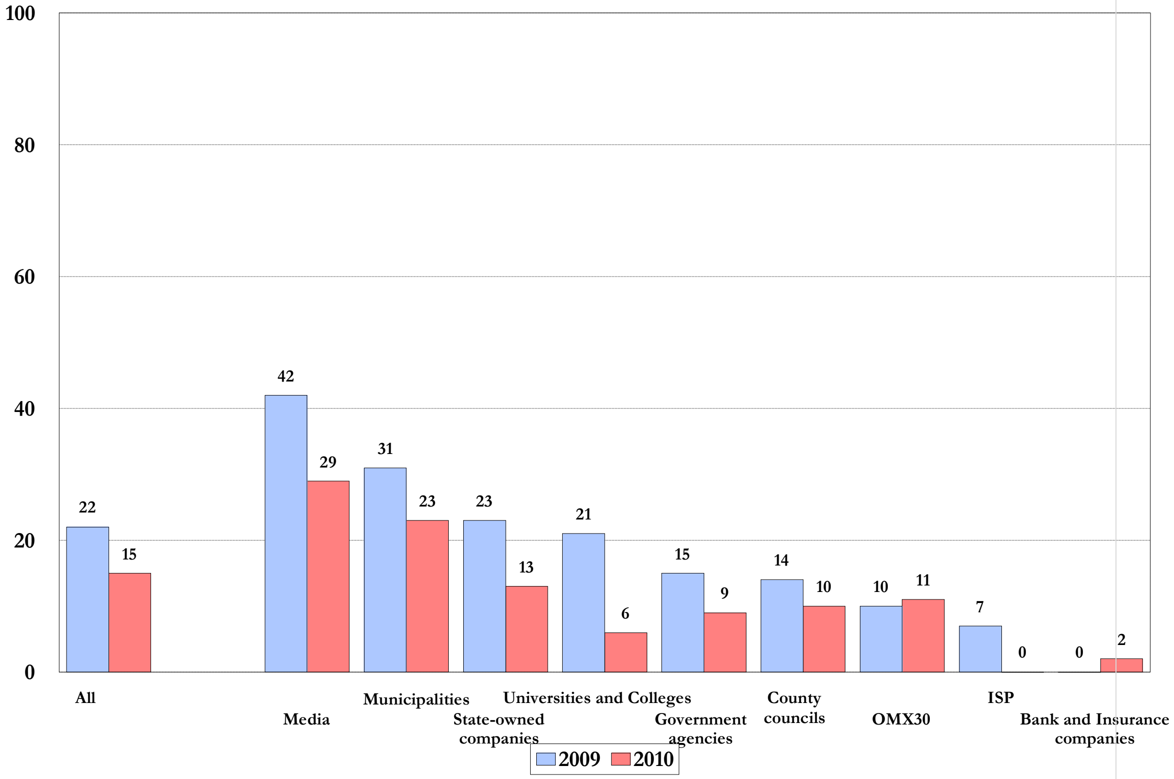
Normally, a registrar is also responsible for the operations of name servers for a domain. The seven largest registrars manage 75 percent of the domains in the .se zone.

6.7 Name servers with recursion activated

Open recursive name servers have very few legitimate fields of application and may be used in conjunction with Denial of Service attacks. Accordingly, we strongly recommend eliminating the possibility of abusing open recursive resolvers by using the methods described in the references stated in appendix 6.

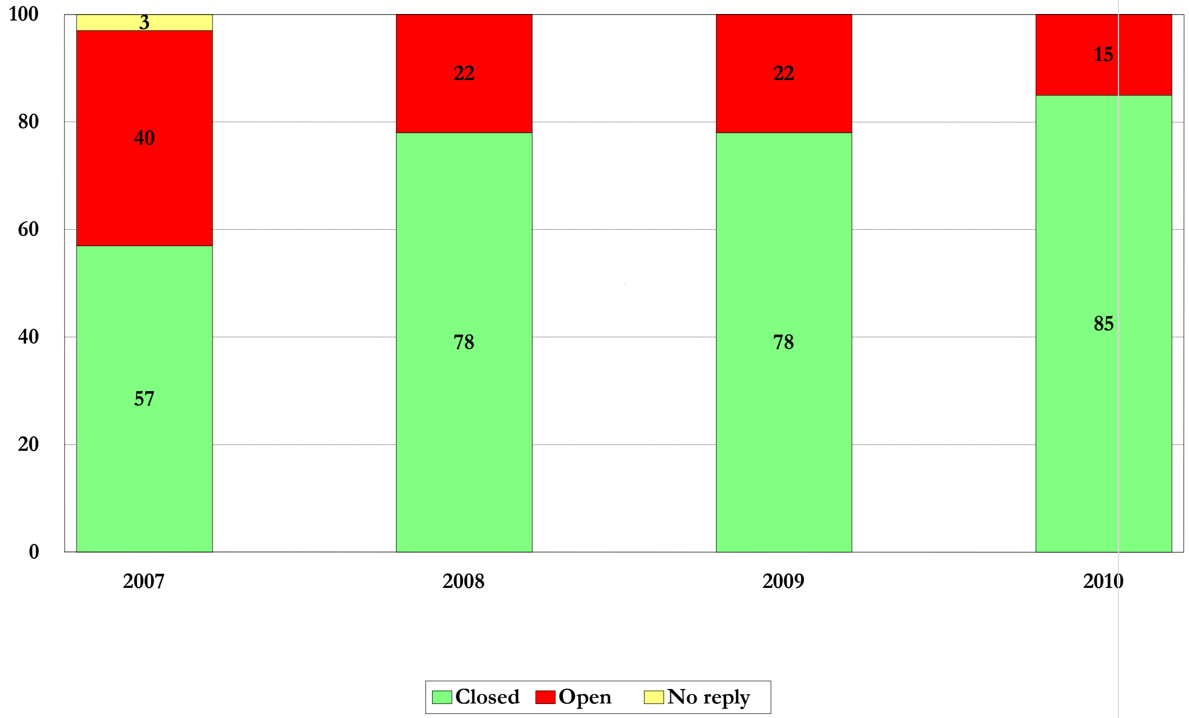
The share of name servers that are open for recursion also declined in 2010 and is currently down to 15 percent. This is excellent considering the risks involved. This most frequently occurred in the Municipalities and Media categories, although these areas also declined compared with 2009, which is indicated in the graph below.

Graph 8: Open recursive name servers per category



Open recursive name servers have declined in all categories, except OMX30 and Bank and Insurance companies, where there was in fact a small increase. Perhaps most notable was that the ISP category declined from 7 to 0 percent, indicating that ISPs have improved their infrastructure through better separation between authoritative name servers and resolvers.

Graph 9: Name servers with recursion activated, 2007-2010



Between 2007 and 2010, the proportion of name servers with recursion activated declined strongly, from 40 to 15 percent. In other words, since the last investigation, there was a decline of a further 7 percent. This is one of the truly gratifying results from this year's survey.

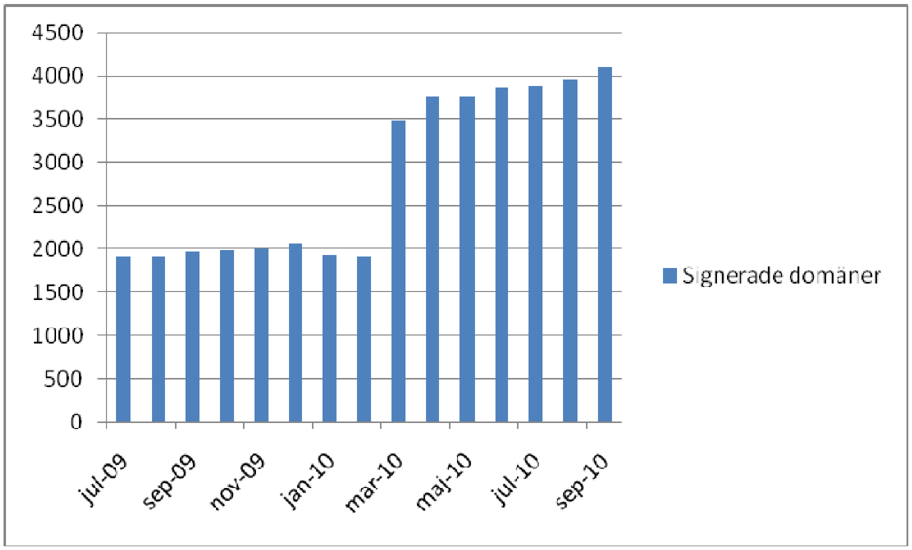
6.8 Use of DNSSEC

For the first time, we are reporting the number of domains that are signed using DNSSEC separately. We also made certain changes to the measurement tool since DNSSEC is no longer to be considered in an experimental phase but rather fully operational. This entailed us tightening requirements somewhat and thus altering the level of that which is considered an error or a warning in a few regards. This does not otherwise affect the results of the report since we did not include DNSSEC in previous years.

6.8.1 How widespread is the use of DNSSEC?

Among the domains in the 2010 investigation group, 3.88 percent were signed using DNSSEC. Municipalities, government agencies, county councils and ISPs are the organizations that have begun to adopt the safer technology. As a comparison, it can be noted that in the entire .se zone, there are currently nearly 4,000 domains in total that have implemented DNSSEC, meaning twice as many as last year, yet still only 0.4 percent of the total number of domains. We noted some growth, although perhaps not at the rate that we would have wanted. The following graph shows the growth of DNSSEC-signed domains throughout the entire .se zone.

Graph 10: Growth – domains using DNSSEC throughout the .se zone



Source: .SE's website

To date in 2010, for example, only three municipalities have signed their domains. If growth continues at this rate, it will take 80 years before all 290 municipalities are signed.

The e-Government Delegation recently began publishing a list of the government agencies that have implemented IPv6 and DNSSEC. The aim of the publication is to emphasize the government agencies that have implemented IPv6 and DNSSEC as solid examples and role models to thus encourage more agencies to follow suit. On its website, the e-Government Delegation says that DNSSEC ought to be implemented among government agencies no later than summer 2011.

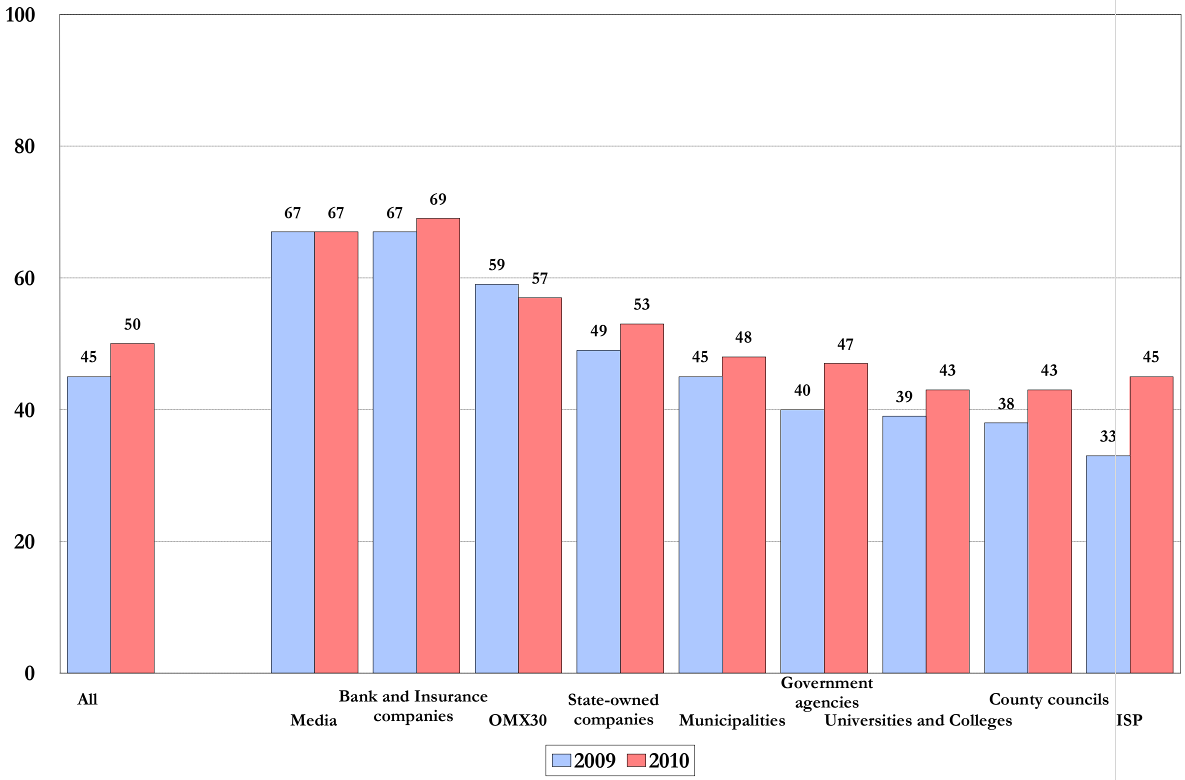
The use of DNSSEC has also gained momentum among top-level domains after signing of the root zone. In the past weeks alone, a number of new top-level domains have been signed. Further information regarding DNSSEC is available in appendix 5.

7 Key parameters for e-mail

7.1 Support for transport security (TLS)

To ensure the secure exchange of information between e-mail servers, transport security should be added to communication. Of the organizations investigated in 2010, nearly half, or 49.5 percent, had support for TLS/SSL in their e-mail servers. While this is a minor increase on last year (44.5), it means that many are not taking sufficient measures to protect their e-mail traffic against eavesdropping, although the situation has improved somewhat. All software now a day features built-in support for this purpose.

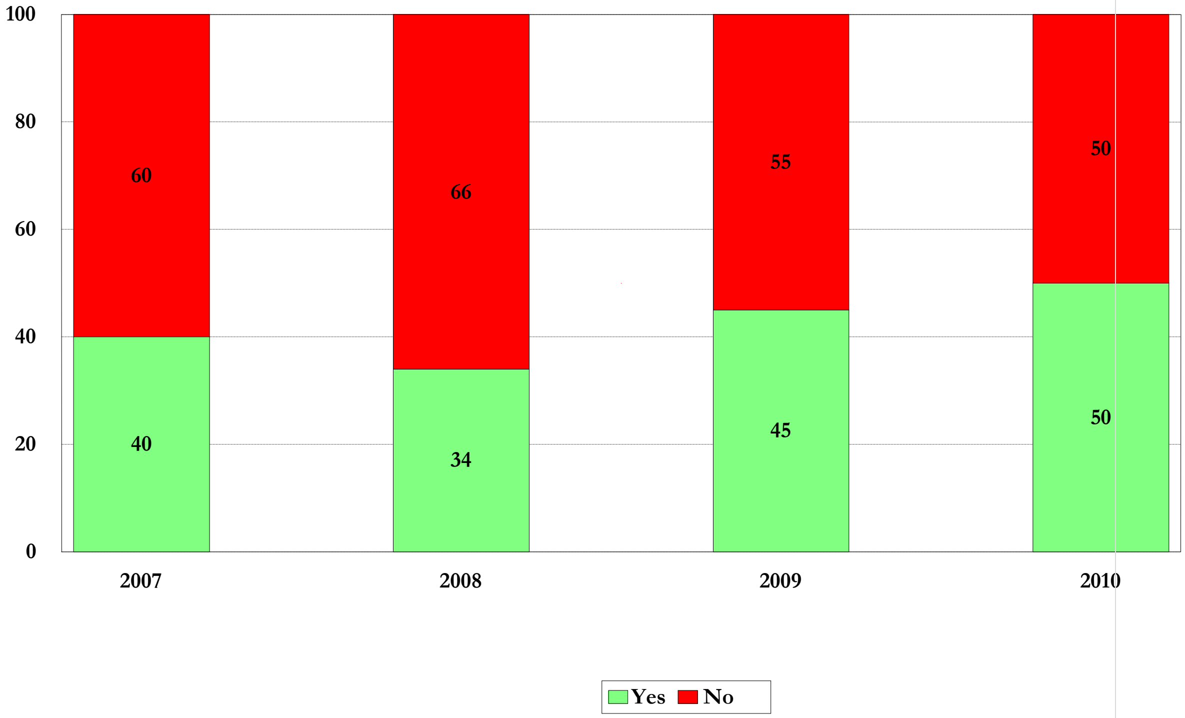
Graph 11: E-mail servers with support for TLS



The use of StartTLS has increased in all categories except Media, which remained unchanged, and OMX30, which declined somewhat. We do not have any information as to the reasons behind this.

The graph below indicates the trend over the past four years. It is evident that the percentage of e-mail servers with support for TLS increased during the period, although the progress is slow.

Graph 12: E-mail servers with support for TLS, 2007-2010



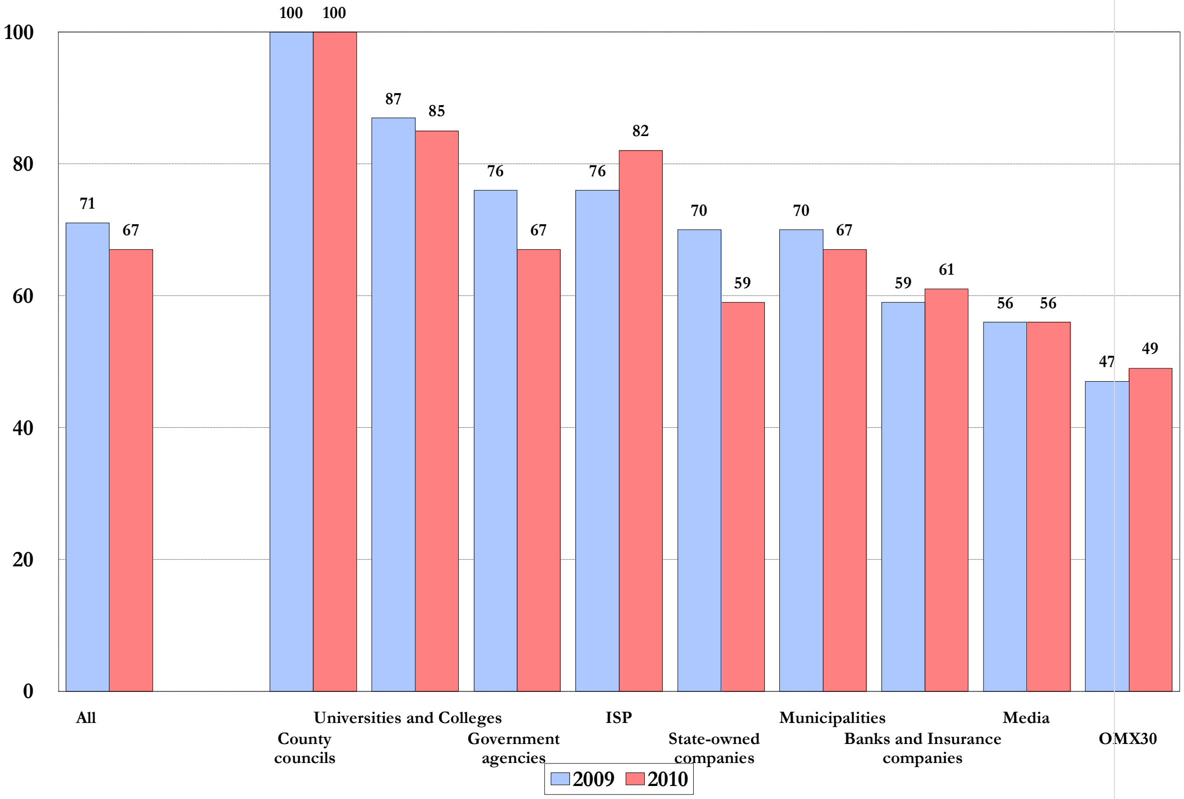
Transport Layer Security (TLS) is an open standard for the secure exchange of information. TLS offers confidentiality (encryption) and correctness (data integrity), and also authenticity protection (source protection) depending on use. The older version of the method is called Secure Socket Layer (SSL). The uses of TLS/SSL include the transmission of e-mail (SMTP). For further information, refer to appendix 9.

7.2 Location of e-mail servers

For 2010, 67 percent of the investigated organizations had e-mail servers located in Sweden, which is somewhat less than last year. It is important to note that since we were unable to identify the geographic location of IPv6-addressed e-mail servers, these servers were listed in the “abroad” category. In the investigation group, 1 percent of the domains have e-mail servers with IPv6 addresses.

The following graph shows the percentage of e-mail servers located in Sweden, divided by category:

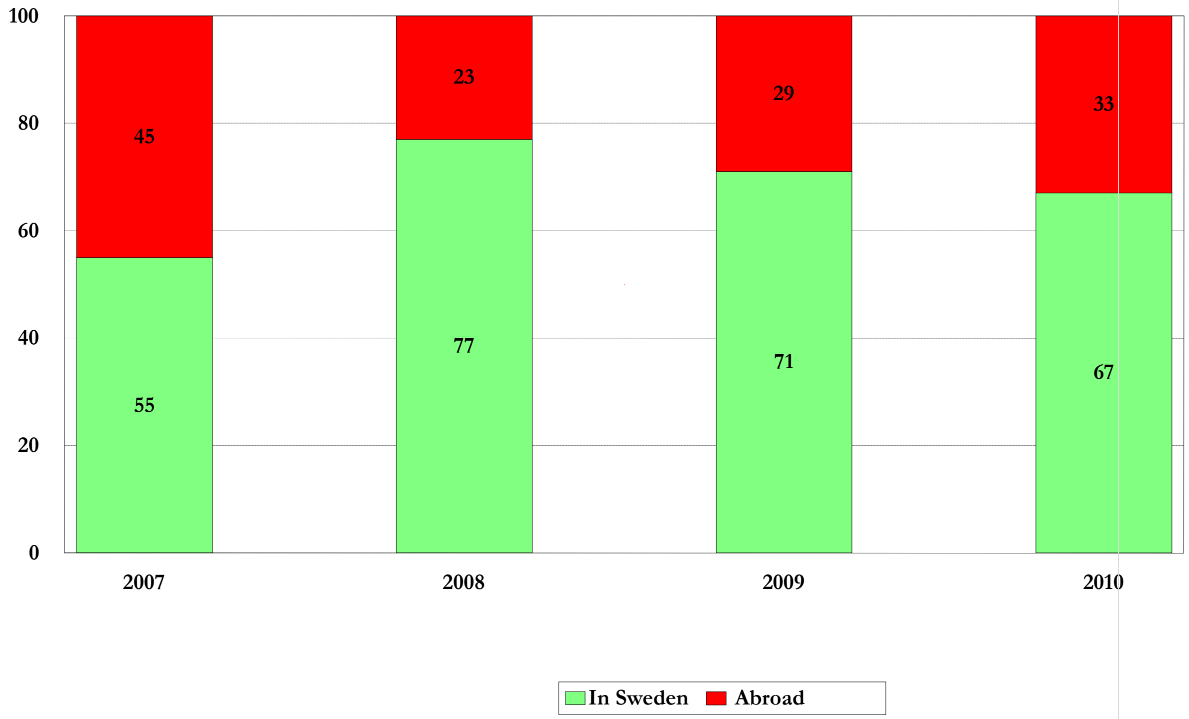
Graph 13: Percentage of organizations with e-mail servers in Sweden



The main reason for locating servers outside Sweden probably remains the same, meaning that organizations engage third-party suppliers to handle the filtering of viruses and spam. For the OMX30 category, the reason may also be that the companies are multinational, with centralized IT operations located in countries other than Sweden.

When the e-mail servers of such organizations as government authorities and municipalities are located outside Sweden, a consequence is that the e-mail communication of these public administrations passes through a foreign country on its way to the recipient.

Graph 14: Percentage of organizations with e-mail servers located in Sweden, 2007-2010



The graph shows that the percentage of e-mail servers located outside Sweden has increased since 2009. In summary, we can state that organizations still frequently send their e-mail outside Sweden for "washing".

At the same time, we know that still only about half of the organizations investigated use encryption for transport security of their e-mail. Only 50 percent of the domains investigated accept transport security using encryption for incoming e-mail, although we are unable to say whether they use this function for outgoing e-mail.

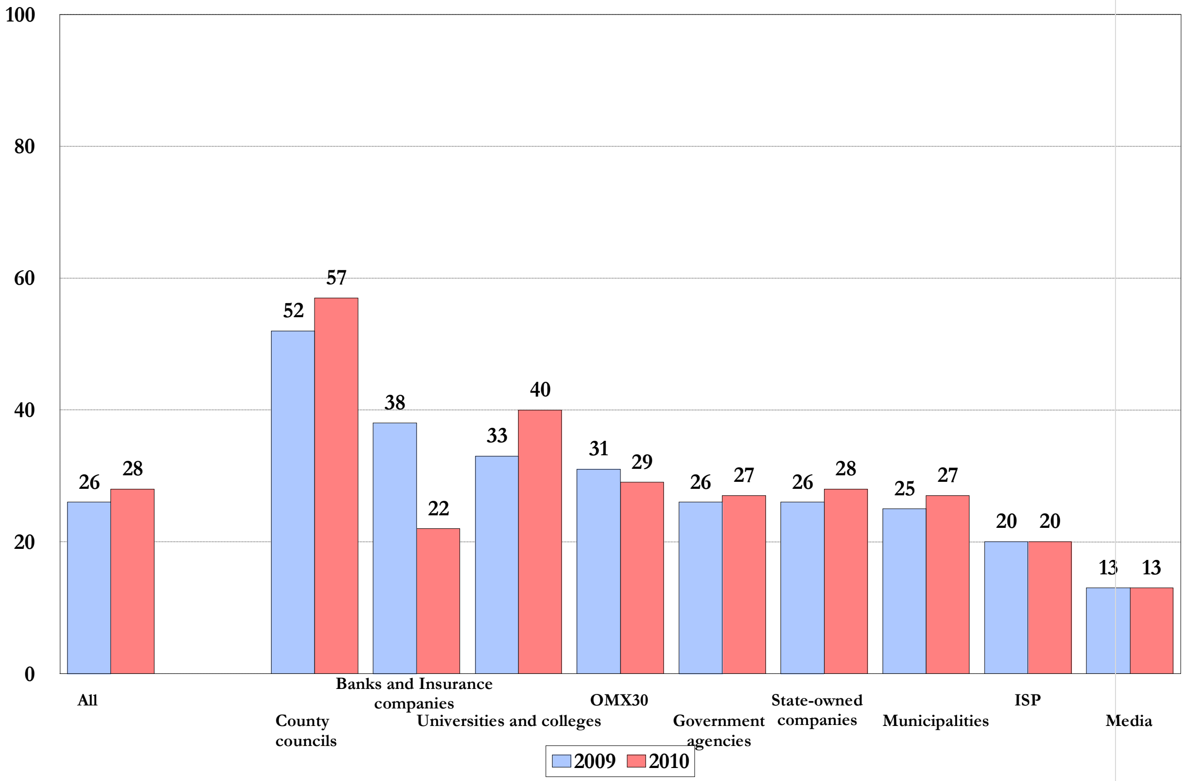
One of the goals of this part of the study was to show that there could be consequences for e-mail sent from Swedish companies and organizations together with the regulations formulated in the highly controversial FRA law (law on signal surveillance), which was passed by the Swedish Parliament in 2009. Having e-mail servers located abroad means de facto that the information will pass Sweden's borders and then return, which will make it more or less impossible to determine whether or not it is Swedish traffic.

This also means that foreign intelligence services can eavesdrop on the traffic in a similar manner. The location of servers outside Sweden means that all information passes Sweden's borders, which entails that foreign governments and others can very easily access information that can be perceived as sensitive from various perspectives. It is impossible to determine the level of awareness of this problem among those responsible for the organizations and, if they are aware of the defect, whether they have carried out analyses of the consequences.

7.3 Actions against spam

The standard protocol for sending e-mail, SMTP, makes it possible to send messages using any domain as the sender address. There are several solutions aimed at limiting the ability of spam to reach recipients by attempting to verify that the sender of the message is legitimate. One of these solutions is designated Sender Policy Framework, or SPF.

Graph 15: Usage of SPF



A total of 28 percent of the organizations investigated use SPF. County councils top the list at 57 percent, while its use decreases sharply in the Banks and Insurance companies category, which is attributable to the growth of the category, from previously only including the central banks to now encompassing a larger number of the registered companies under the regulation of the Swedish Financial Supervisory Authority.

In the current measurement, we only considered whether or not the domain has an SPF item published. We did not assess the content, except to verify that it was an SPF item.

Domain Keys Identified Mail (DKIM) is a standard that protects selected parts of an e-mail header and the content of an e-mail message from being modified by a third party.

Because of the way the standard for DKIM is designed, it is impossible to precisely determine whether or not a domain uses DKIM. In the 2008 study, we found only two domains with DKIM activated and, in principle, the result for 2009 was equally poor. In 2010, we opted to not report any of the results from the test since it is not possible to determine the existence of DKIM for a domain before the application of ADSP becomes more widespread (see appendix 8).

It is also possible to combine the SPF and DKIM technologies if desired. However, in this year’s study, we decided not to look into how many organizations chose to do this.

8 Key parameters for web servers

Information and services provided via web interfaces have become increasingly commonplace, and many organizations are entirely dependent on having functional web services that are accessible to their customers or to citizens in the community. Actions can be taken to ensure redundancy for web services. It can be a good idea to consider these whether critical functions are provided online.

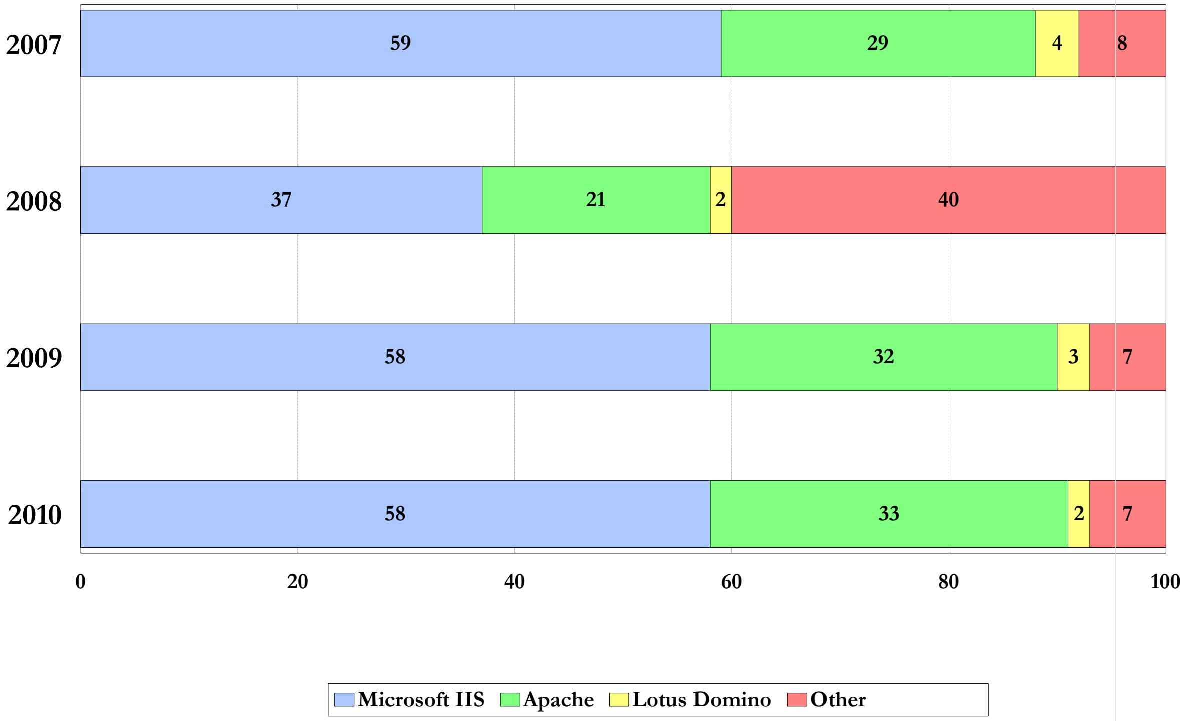
8.1 Connection of web servers

If all of an organization's name servers are connected to a single Internet service provider, it does not matter whether the web servers are also located with this provider. If the service provider experiences availability problems, then the web servers will be unreachable. If the name servers are located with two different service providers, the organization could also consider locating the web servers with a third service provider to ensure the greatest possible redundancy.

8.2 Software for web servers

This year, as in past years, we looked at which software for web servers was used in the organizations investigated. The clearly dominant software remained Microsoft Internet Information Server (Microsoft IIS) and Apache.

Graph 16: Software used for web servers



8.3 Other interesting observations regarding web servers

Through the advancement of our investigation tools we were able this year to control a number of other parameters of interest, particularly for web applications. Some of the most notable results are presented below. Many of these will be of greater interest next year, when we will actually be able to compare and assess whether there has been any progress and, if so, how much.

A significant share (44 percent) of the investigated websites uses Google Analytics to collect visitor statistics. Google Analytics is more or less recognized as the industry standard for measuring visitors to websites, and is widely used by Swedish sites to measure and compare visitor streams with other sites in such networks as SIS Index.

Sending visitor data to Google Analytics naturally also entails allowing Google to draw its own conclusions of visitor streams to, for example, the websites of Swedish government agencies. Also, Google may well choose to perform cross references to see which visitors to an agency's website have also visited another agency's website. Before choosing a tool to analyze visitor statistics, it is important to conduct a consequence analysis taking into account where and with whom the information will be stored.

By far the most popular publishing system (CMS) used in the investigation is the commercial EPiServer system, developed by a Swedish company with the same name. There are surprisingly few organizations that use alternatives based on open source code, although it is reasonable to assume that this percentage will increase ahead, as a result of reduced license costs associated with the free alternatives and because software based on open source code is expected to become more frequently used among Swedish government agencies.

Most of the websites, 479 (71 percent), independently attached a cookie when visited. Of these 479, we also know that 297 use Google Analytics, which also requires that a third-party cookie be attached to count visitors.

In a remarkable number of cases, the visitor is redirected to an address other than the one that they specified through the use of redirects, which affects performance for the visitor to the website in question.

One change is that Latin-1 (ISO 8859-1) is making a strong recess, for the benefit of UTF-8, which means that an increasing number of websites are handling a strong rise in the number of scripts and characters used for content in the form of text.

8.4 Support for transport security (TLS/SSL)

Using certificates and the accompanying encryption keys, a web browser can establish secure, encrypted communication with the web server. For these purposes, TLS/SSL can also be used to establish a secure connection between a web browser and a website (https); refer to appendix 9.

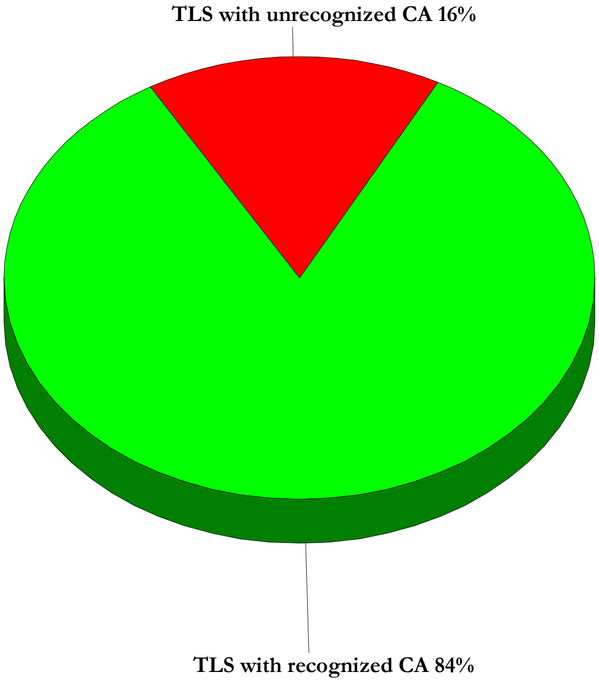
Accordingly, it is insufficient to just have a certificate issued for the domain or the web server. The certificate must also fulfill certain fundamental requirements that should be met by this type of security mechanism. For example, the certificate must be valid, it must use secure algorithms, the keys must be sufficiently long, and so on.

There are many reasons why certificates may be unreliable:

- The cryptographic algorithms used may be poor.
- The certificate may have been used before it is activated.
- The certificate may have been used after having expired.
- The domain for which the certificate was issued may not correspond to the domain for the site.
- The certificate may have been revoked.
- The certificate may be self signed.
- The issuer may not be an approved CA.
- The certificate chain may be incomplete.

In the 2007 study, only 25 percent of the web servers investigated had support for TLS/SSL, while the corresponding figure for 2008 was 75 percent. The studies cannot be compared from year to year, because we changed the method used to contact the web servers in 2009. As in last year, we only tested what response we received on an HTTP and HTTPS GET to the domain names in the test group with the "www." suffix. Some 227 of 670 domains, or 34 percent, returned a reasonable response to issues related to certificates.

Of these 227 domains, we were able to download completely correct certificates from 190 domains, or 84 percent, that were issued by a recognized CA. This is an increase of 6 percent on last year.



Among the 16 percent that have incorrect certificates, we found the following errors:

- 12 had certificates issued in the wrong host name.
- 10 had expired certificates.
- 9 had self-signed certificates.
- 3 had certificates signed by an unrecognized root CA.
- 2 had certificates whose cryptographic checksum was incorrect.
- 1 had a self-signed certificate between its own certificate and the root CA certificate.

It is also possible that the domains lacking a correct certificate had more than one defect.

Of the websites investigated, we can confirm that 10 have certificates that are invalid because they were not renewed during the validity period. The worst-case example among these was a certificate issued for a Swedish mining company that had expired in July 2004, or six years and three months earlier. A Swedish municipality had a certificate that expired in December 2006. These certificates remain in use since they de facto return queries via https.

At the time of investigation, some of the municipalities had four days remaining until their certificates expired. All used the same service provider, and these municipalities also referred to certificates that were not even issued to them, but rather to an entirely different domain. When we conducted a new control after the validity period had expired, none of the certificates had been renewed.

Among the 190 domains that had approved certificates, we were only able to identify 27 addresses that used EV certificates (extended validation), which are a type of certificate that conveys increased visual support in web browsers to show that the certificate is approved and that the issuer has been reviewed more carefully than an ordinary server certificate.

A total of 181 websites accept encryption using weak algorithms and 19 websites used unsecured signature algorithms.

A couple of certificates were configured using relatively short RSA keys, 512 bits, while the most frequently used key lengths are currently 1,024 and 2,048 bits, respectively.

About 20 domains used what are known as wildcard certificates. A wildcard SSL certificate activates SSL encryption on several subdomains using a single certificate, provided that the domains are controlled by a single organization and have a single second-level domain. Some of the wildcard certificates that we examined were issued to a web-hosting service provider, which in turn used the wildcard to issue certificates for its own customers. Sharing certificates among domains is far from risk-free, in part because:

- If security at one server or subdomain has been compromised, there is a risk that all subdomains have also been compromised.
- If wildcard certificates must be replaced, all subdomains will also require new certificates.

The best solution to the problem is simply to use a unique certificate for each server instead of using wildcard certificates.

In other words, the handling of certificates in the test group's web environment was still of extremely poor quality in all respects as shown in the study. This type of encryption use has existed for some time and is apparently commonplace. Among the organizations included in the study, we had expected better results, primarily in terms of the use of valid, current certificates issued by credible issuers. In this part of the study, we want to mention that substandard use of web certificates undermines the credibility of this type of security solution.

Anything that results in a user having to click on icons that in practice mean "Yes, I know that this is incorrect, but let me proceed anyway", including self-signed certificates or certificates that are no longer valid, 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 complete 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, personal information, user information, payment information, credit card numbers, telephone numbers, etc. should use TLS/SSL with certificates issued by generally accepted certificate issuers, 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. In addition, they should consider:

Using the longest RSA keys possible.

Using EV certificates where justifiable.

Avoiding the use of wildcard certificates for web services, especially for 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.

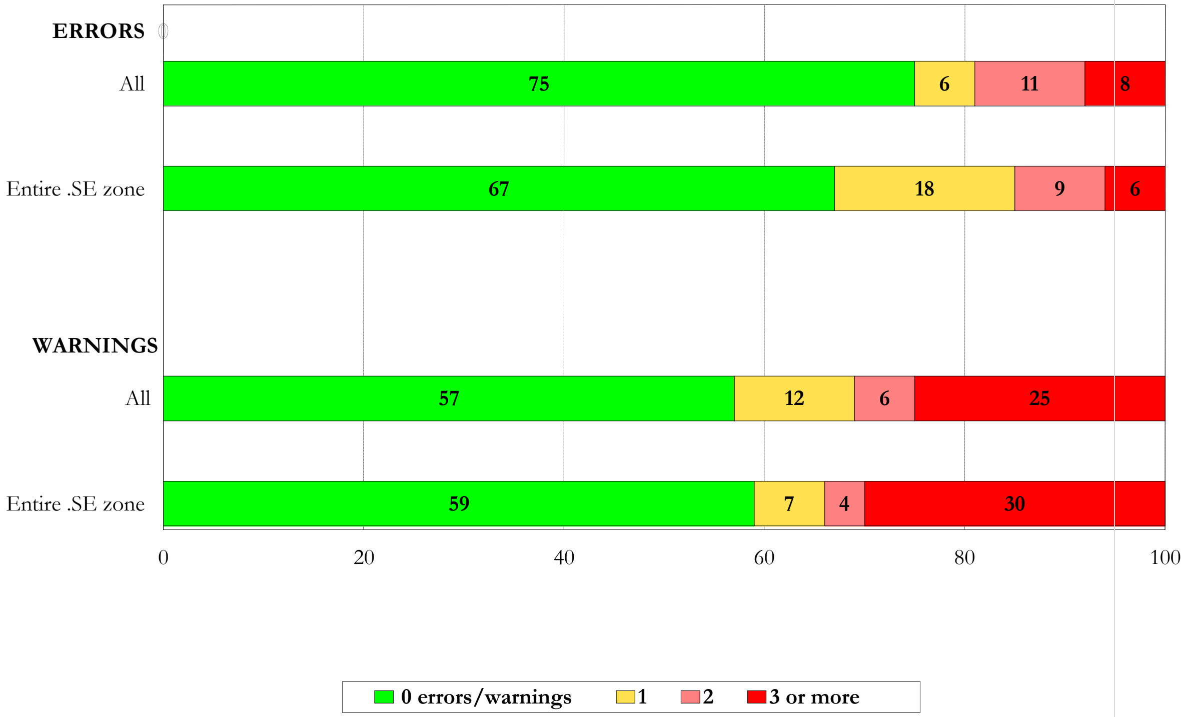
At http://www.ssllabs.com, those who use certificates to protect web services can check whether a website has adequate security in terms of SSL.

9 Comparison with the .se zone as a whole

In the 2010 study, we also examined a cross-section of randomly selected domains from the .se zone to assess whether our test group was better or worse than the .se zone as a whole. In the graphs below, “All” represents the current test group, while “Entire .se zone” represents the random selection of 10,000 domains from a version of the zone file dated October 7, 2010.

Above all, we examined the distribution of errors and warnings, and how the test group – which included several critical functions and organizations – compared with the .se zone as a whole.

Graph 17: Number of errors and warnings

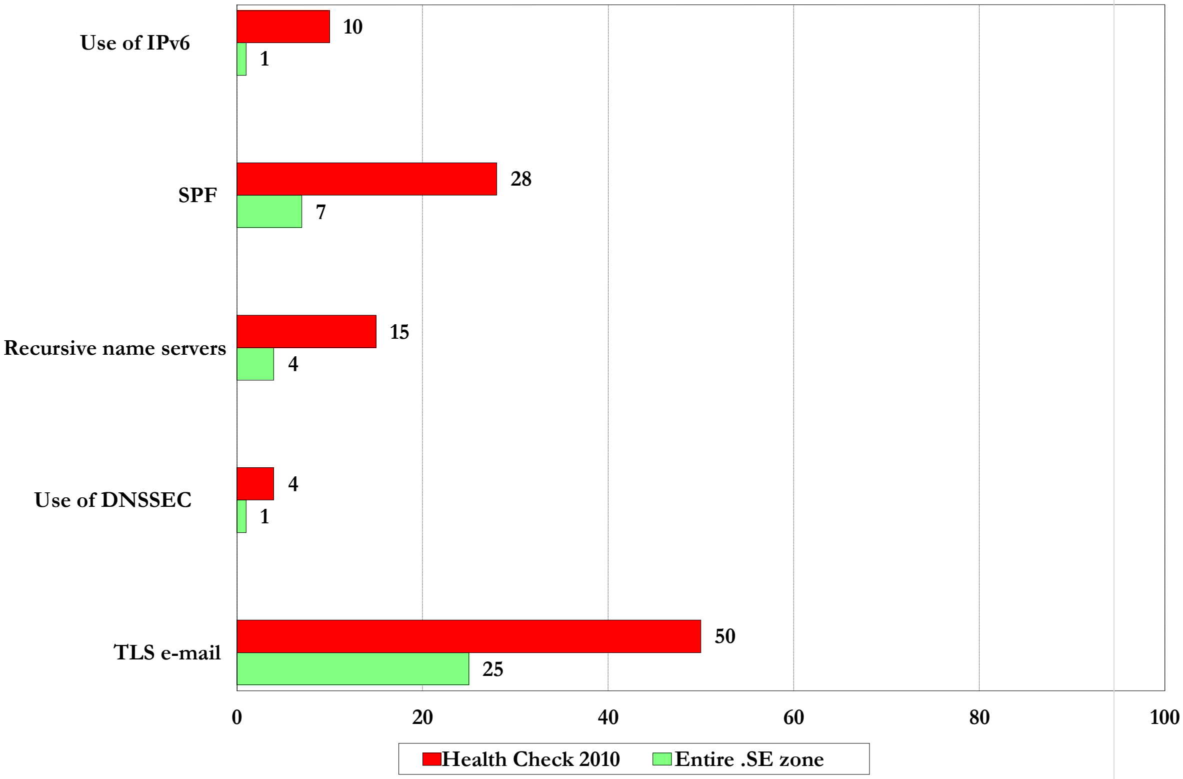


In 2010, there were more errors in our investigation group than in the .se zone as a whole, which is the opposite of last year. The number of warnings was approximately the same.

The major differences first become apparent when we examine the other specific areas we have reviewed more closely, apart from the parameters we associate with DNS quality in accordance with the definition in appendix 4. In the test group, the number of organizations using SPF is higher, as is the number of organizations using recursive name servers, the number using DNSSEC and the number protecting their e-mail with TLS. The conclusions that can be drawn from these results are not immediately apparent. Additional, more specific studies are required.

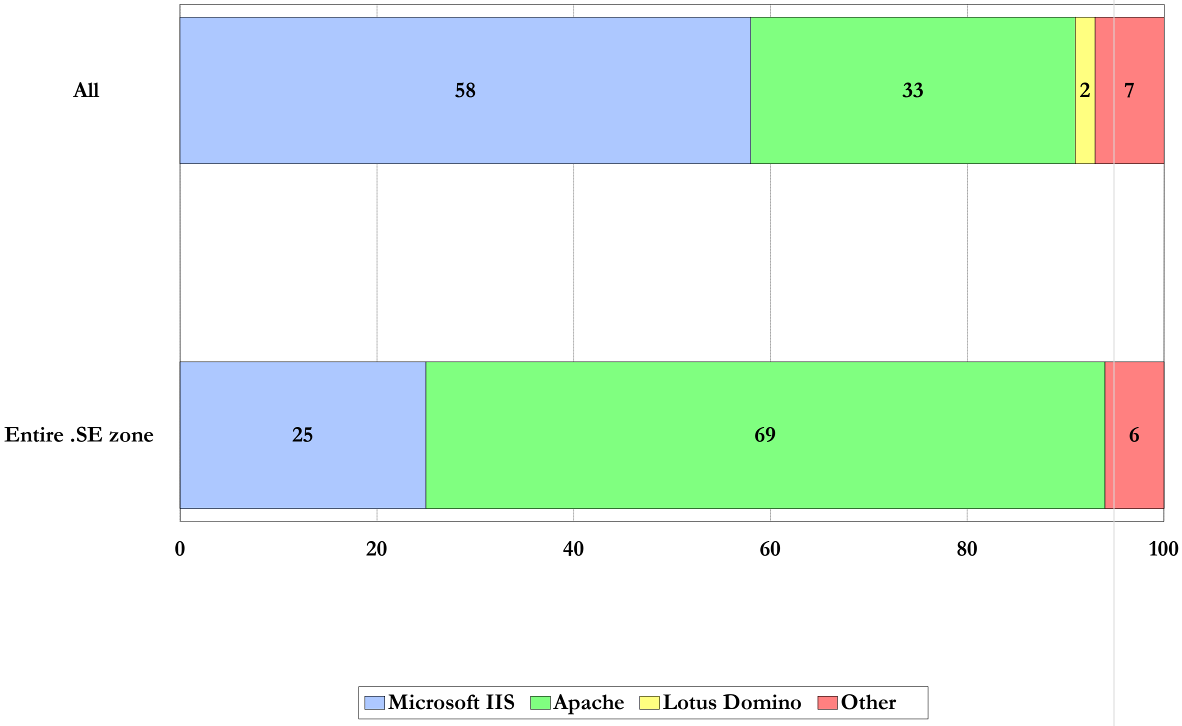
However, we can note, for example, that the number of organizations using IPv6 is much higher in the test group than in the .se zone as a whole. This is probably due in part to the results shown in Graph 8: that universities and colleges have made more progress than other organizations in the implementation of IPv6.

Graph 18: Use of IPv6



The same explanation probably applies for the major difference between which software is used for web servers; in the test group, Microsoft IIS dominates, while the trend in the .se zone as a whole resembles that seen in the rest of the world in that Apache is the dominant software. Systems that feature public procurement and framework agreements contribute to a homogenization of the IT environments of public administrations, which may not always be optimal.

Graph 19: Software for web servers



10 Advice and recommendations

After carrying out a new round of tests with relatively similar results to those performed in 2009 (which were somewhat poor), we see a much stronger need for greater coordination of various stakeholders in order to improve security on the Swedish part of the Internet. In particular, we see opportunities for extensive efficiency gains and cost savings.

Primarily, organizations in public administration must be able to agree on recommendations and a plan of action for the implementation of some important activities:

- Critical resources in Sweden should have name servers that are connected to several service providers simultaneously; for example with the use of Anycast technology. At a central level, someone must establish a definition of 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.
- A common function for public administration should be established for virus scanning and clearing of spam, 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 mean that government authority information would not leave the country.
- Issue guidelines on what is acceptable in terms of managing spam and virus scanning in public administrations. It should be unacceptable for Swedish government authorities and municipalities to send their e-mail abroad, at least not without the establishment of relevant, uniform requirements for transport security and encryption.
- Issue recommendations stating that e-mail servers for critical operations at Swedish government authorities and utilities should be physically located in Sweden to protect the traceability of information sent between government authorities 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 security.
- Make all services available with 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 issuers and maintain control of their validity.
- Introduce DNSSEC for domains in public administration.

For public administrations, it should be possible to address several of these activities in the framework of the e-Government Delegation’s task. In addition to the above activities, further actions should be taken, including at the service provider level, to strengthen Internet infrastructure. Primarily, these actions are the responsibility of the Swedish Post and Telecom Agency, as the supervising authority, and relate to setting requirements for the service providers.

Appendix 1 – Abbreviations and glossary

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

BCP Best Common Practice.

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

DKIM Domain Keys Identified Mail. DKIM makes it possible for 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 *name servers* are to respond to requests for a certain *domain*.

DNSSEC Secure DNS. DNSSEC is an internationally standardized expansion 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 name 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 held by a certain *registrant* after allocation.

IP address Numerical address that is allocated to each computer that will be reachable over the Internet.

Name server A computer with programs that store and/or distribute *zones*, and that receives and responds to domain-name requests.

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

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

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).

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 *name servers*.

Zone file A data file with the information required about a *zone* so that it is possible to use addressing with *DNS*.

Appendix 2 – About DNS and the study

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 studies of earlier years convinces us at .SE that the study is valuable and we will continue to conduct it. The study is being conducted for the fourth time this year. It is part of a long-term focus area called the Health of the Internet in Sweden.

.SE has been responsible for the operation and administration of all name servers 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 the 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 top-level domains. The DNS is somewhat of an unknown system that has existed for more than 25 years. Throughout the years, the 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, the DNS has become increasingly important to the existence of functioning communication between Internet users worldwide, and this requires that all areas of the 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 forged. 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 to DNS have been developed and been designated DNSSEC (DNS Security Extensions). With DNSSEC, the domain name system is secured from abuse by the responses to DNS lookups being signed cryptographically. The validation of signatures can ensure that the responses really come from the right source and have not been tampered with 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 the Swedish top-level domain – is the reason why our tests focus specifically on the quality of DNS.

IPv6

For computers and other equipment to be able to communicate with one another over the Internet, they must use a common communication architecture. This means that they must use the same structure rules for communication, or the same protocol. The common 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, that is, the unique number series that identify each unit connected to the Internet, are a 32 bits long number. This means that for IPv4, there can only be slightly more than four billion unique IP addresses. Every day, as more and more people worldwide gain access to Internet connections, we are approaching a point where a shortage of Internet addresses will arise.

The solution for this shortage of addresses is to introduce a new version of the IP protocol, IPv6, with 128-bit addresses. With IPv6, there will be enough addresses for the foreseeable future. A rich supply of IP addresses will also facilitate access to applications that would otherwise be difficult to realize in practice, such as intelligent homes in which all technological equipment is connected with a single specific IP address. We have therefore taken a closer look at the current extent of IPv6.

Services for e-mail and the Internet

At .SE, we are also interested in looking more closely at how organizations handle their communication otherwise, mainly in terms of security, availability and robustness for the most common services like electronic mail and web communication. We continuously work on further development of the measurement tool to be able to study more details, particularly with regard to parameters that concern web applications, but also concerning e-mail use. The MailCheck tool, the latest addition under development, is a beta version that can be used. MailCheck aims to improve the quality of e-mail-related services in general by pointing out possible configuration problems, weaknesses in software and breaches of standards for both system administrators and end-users.

Appendix 3 – About the 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 people control, measure and, it is hoped, 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 the DNS from its root (.) via the TLD (top-level domain – for example, .se) up to the name servers 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/.

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.

.SE has further developed the DNSCheck tool so that it is also possible to carry out 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 example if a domain registrant plans to move a domain from one name server operator to another. For instance, let us say that the domain example.se is to be moved from the name server "ns.nic.se" to the name server "ns.iis.se". In this case, an undelegated domain test can be carried out on the domain (example.se) using the name server 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, defects 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 name servers

Recommendation: DNS data for a zone should be located on at least two separate name servers. For reasons of availability, these name servers 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 name servers should exist for each underlying domain. They should be listed as NS entries 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 name servers stops working.

Consequence: When the sole server or sole service provider experiences a disruption, the 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 name server operator.

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

Recommendation: All of the NS entries 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 entries are used in the overlying zone to transfer responsibility for (delegate) a certain domain to other servers. According to the 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 entries 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 name servers listed with NS entries 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 entries for the subdomain. This applies to all servers listed in the underlying zone's DNS for the domain in question.

Consequence: The DNS usually functions even if this defect exists. However, a defect existing in a zone indicates weaknesses in the procedures of the party responsible for the content of the domain's DNS.

4. Serial numbers for zone files

Recommendation: All name servers listed with NS entries in the delegated zone shall respond with the same serial number in the SOA entry for the domain.

Explanation: The serial number in the SOA entry 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 stands for Start of Authority.

Consequence: If the name servers 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 entry must be reachable.

Explanation: The SOA entry 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 having 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 the DNS due to an individual domain.

6. Reachability

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

Explanation: The NS entries for a domain comprise the list of the computers that function as name servers for the domain. All listed servers must be reachable via the Internet at all of the addresses listed in the corresponding address entries in the 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. Many 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 any effect.

In recent years, all the new threats against DNSs have led to DNSSEC becoming increasingly relevant to organizations. The most known and most important threats to a DNS include cache poisoning and pharming. Pharming means that someone directs the actual content of a DNS to incorrect servers. In practical terms, this means that an web address, such as that of an Internet bank, can be redirected to a completely different server, but for the visitor, the address field continues to appear to be the correct server.

Cache poisoning means that a situation is created – either by launching an attack or unintentionally – that provides a name server with DNS data that does not come from an authoritative source. One of the most recent examples of this was the much-discussed Kaminsky bug in 2008.

Accordingly, there is no doubt that the DNS 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 top-level domain to sign its zone with DNSSEC. In 2007, we were also the first to offer a commercial DNSSEC service to our domain holders. We currently have some 20 resellers (registrars) that offer DNSSEC.

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 source and that the content is not tampered with during transmission. 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 the 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 the DNS comes from the correct source and whether it has been manipulated en route. Thus, it is difficult to forge 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) and pharming (redirecting a DNS query to the wrong computer) and other similar attacks against the 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 both 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 entries in the DNS.

.SE will still sign .SE's zone file, but 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 level domains, which are *trust anchors* for underlying domains. With the root signed, they only need to keep track of the root key. Modern standards also offer simpler handlings of key roll-overs and new tools have been developed to make it easier (refer to Open DNSSEC below).

For further information on .SE's DNSSEC service, see http://www.iis.se/en/domaner/dnssec.

At the following website, .SE provides additional information on DNS vulnerabilities: http://www.thekaminskybug.se.

The website's functions include allowing users to check whether the resolver they are using is vulnerable to the Kaminsky bug and whether DNSSEC is used for a domain.

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

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 stay abreast of developments in the field.

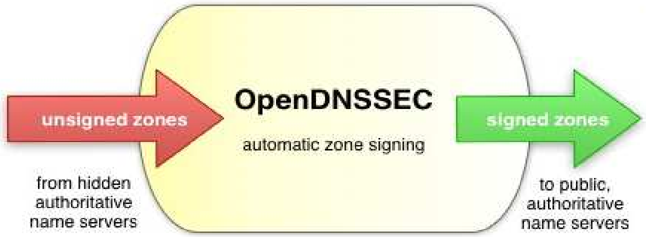
Development project – OpenDNSSEC

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-ready program, or a tool for facilitating the implementation and use of DNSSEC. OpenDNSSEC secures the DNS information the moment before it is published on an authoritative name server. OpenDNSSEC takes an unsigned zone file, adds signatures and other items for DNSSEC and sends the file on to the authoritative name servers 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.


unsigned zones
from hidden authoritative name servers
OpenDNSSEC
automatic zone signing
signed zones
to public, authoritative name servers

OpenDNSSEC is being developed in the framework of collaboration between .SE, Nominet, NLNet Labs, SIDN, SURFnet, Kirei and John Dickinson. Further 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 name server** not only responds to queries about DNS entries for which it itself is responsible, but also goes further and asks other name servers 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 name server** 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 name server by allowing these parties to submit queries that will result in unusually large responses (Amplification Attacks). 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 name servers, but the fact that service providers do not filter traffic by source addresses. If they did, open recursive resolvers might not be considered a problem. Since such filtering is relatively difficult and costly to implement, we need to attempt to limit the damage caused by DDOS attacks in the meantime until the service providers have managed to solve the fundamental problem. We consider closing a recursive resolver to be a worthwhile and simple task for many organizations, since it will help ease problems arising from DDOS attacks.

Pointers for further information

The following links provide high-quality, informative material about DDOS and open recursive name servers.

Secure Domain Name System (DNS) Deployment Guide
http://csrc.nist.gov/publications/drafts/800-81-rev1/nist_draft_sp800-81r1-round2.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's functions.
http://oldwww.isc.org/index.pl?/sw/bind/arm95/index.php

Appendix 7 - Ipv6

Today's Internet is dominated by IPv4 (IP version 4), which was developed as early as 1981.

IP addresses, the unique series of numbers that identify each connected unit on the Internet, comprise 32 bits. Accordingly, with IPv4, only a total of slightly more than four billion unique IP addresses can exist. As the world becomes more connected, the consequence will simply be a lack of addresses on the Internet.

The solution to the problem of a lack of addresses is to implement a new version of the protocol, IPv6, with 128-bits 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. With IPv6, IP addresses will be 128 bits long instead of 32, meaning that the total number of possible addresses will be almost unlimited.

With IPv4, not even one IP address is available for every person in the world. With IPv6, every living individual could each have 5 x 10^{28} IP addresses. This means that each of us could have 50,000,000,000,000,000,000,000,000,000 of our own IP addresses at our disposal. An ample supply of IP addresses would also open the way for applications that would otherwise be difficult to implement in practice, such as the Internet of Things and intelligent homes.

Appendix 8 - Action against spam

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, that is to say that the sender uses an address other than his or her own as the sender address. Read more about SPF at http://www.openspf.org.

SPF gives the domain registrant the option of publishing rules in the 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 the 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 sorting it as spam. The SPF standard does not define what will happen to messages that do not meet the SPF validation criteria.

DKIM

Another method for preventing this phenomenon is Domain Keys Identified Mail (DKIM). 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 by using 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. 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.

Further information on the DKIM standard is available at http://www.dkim.org.

Appendix 9 - Action for transport security

Electronic mail

E-mail is most commonly transmitted in cleartext and is, accordingly, 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.

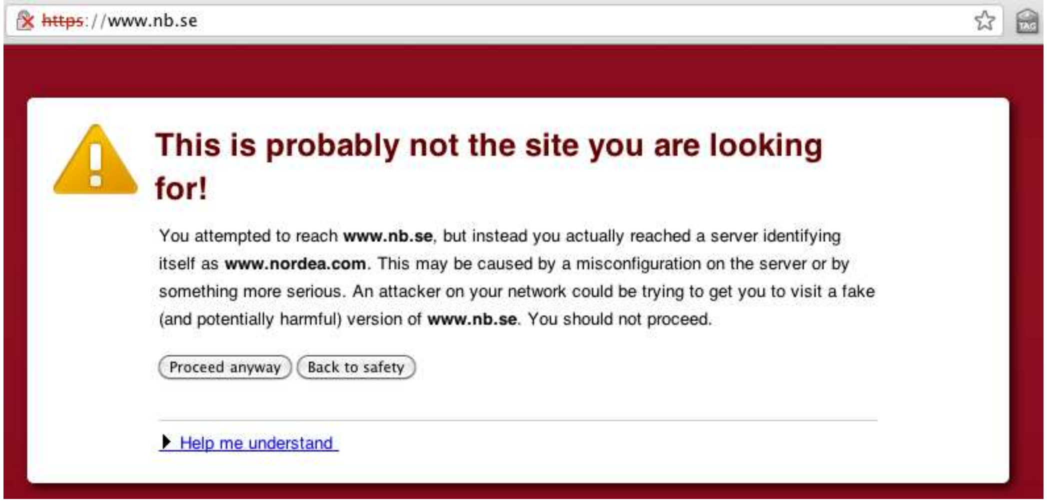
Additional protection is required if the sender wants to send an e-mail that nobody else can read, not even those responsible for the e-mail system (or those who "work at the post office"). In these cases, the entire letter can be encrypted by "gluing the envelope shut and sending it by registered letter", 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 Google Chrome.



~~https~~://www.nb.se

This is probably not the site you are looking for!

You attempted to reach **www.nb.se**, but instead you actually reached a server identifying itself as **www.nordea.com**. This may be caused by a misconfiguration on the server or by something more serious. An attacker on your network could be trying to get you to visit a fake (and potentially harmful) version of **www.nb.se**. You should not proceed.