
2011 .se Health Status

Internet Reachability

Innehåll

1	Introduction.....	4
2	Summary	5
	2.1 About the survey group	5
	2.2 Reduction in the number of serious problems	5
	2.3 Differences compared with the 2010 survey	6
	2.4 Dominant players increase the risks.....	7
	2.5 Lack of competence among consultants and service providers	7
	2.6 Fewer nameservers with recursion activated	7
	2.7 Inadequate certificate management	7
3	Control points	8
4	Quality DNS service	10
5	Tests performed in 2011	12
6	Observations for 2011	13
	6.1 DNS tests – errors and warnings.....	13
	6.2 Most frequently occurring errors.....	14
	6.3 Comparison over time – defects and warnings.....	17
	6.4 Nameserver connections to the Internet.....	19
	6.5 Nameservers using IPv6	21
	6.6 Service providers offering nameserver hosting	22
	6.7 Nameservers with recursion activated.....	22
	6.8 Use of DNSSEC	24
	6.9 DNSSEC in other top-level domains	26
7	Key parameters for e-mail	27
	7.1 Transport layer security (TLS).....	27
	7.2 Location of e-mail servers	29
	7.3 Actions against spam	30
8	Key parameters for web servers	33
	8.1 Connection of web servers	33
	8.2 Software for web servers.....	33
	8.3 Additional interesting observations regarding web servers	34
	8.4 Support for transport security (TLS/SSL)	36
	8.5 Attacks against SSL	38
	8.6 Measures to counteract attacks against SSL	38

9	Comparison with the .se zone	40
	9.1 Distribution of errors and warnings.....	40
	9.2 Differences between the survey group and the comparative group	41
	9.3 Differences in the use of software for web servers.....	42
10	Advice and recommendations	44
	Appendix 1 - Abbreviations and glossary.....	46
	Appendix 2 - About DNS and the survey	48
	Appendix 3 - About DNSCheck test tool	51
	Appendix 4 - Industry standard for high-quality DNS service.....	52
	Appendix 5 – More information about DNSSEC	55
	Appendix 6 - Open recursive nameservers.....	59
	Appendix 7 - Action against spam	60
	Appendix 8 - Actions for transport security	61

1 Introduction

Another year has passed and it is time for the fifth report from .SE's survey on reachability online and .SE's health status by presenting the result from 2011.

This year's study is largely, though not completely, a follow-up of similar studies conducted in 2007 to 2010.

In purely statistical terms, the results in 2011 deviate somewhat from previous years due to the removal of one category, the OMX 30, and the addition of .SE's registrars, meaning .SE's resellers, and their domains as a new category. However, this has not resulted in any major fundamental differences.

The aim of the survey is to chart 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 a percentage of all .se domains.

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 status 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. In 2011, we implemented some technical improvements aimed at enhancing the performance of the tools that are used.

The Health status report is financed by .SE. The results of this year's survey have been analyzed and the report compiled by Anne-Marie Eklund Löwinder, Quality and Security Manager at .SE. Patrik Wallström, Project Manager at .SE, holds the operational responsibility for the tools that are used. Anders Örtengren, from Mistat AB, reviewed the statistical analysis.

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

2 Summary

Like the study conducted in earlier years, this year's study primarily focused on DNS quality. However, we have also studied some other key parameters, such as e-mail and web servers.

IPv6 and DNSSEC and their development are naturally key parameters, particularly as a result of the attention that both IPv6 and DNSSEC received in the Swedish government's recently launched strategy for the IT policy area "ICT for Everyone – a digital agenda for Sweden".¹

The survey was conducted in October 2011.

2.1 About the survey group

In the 2011 survey, the test encompassed a total of 912 domains distributed among 1,369 unique nameservers (both IPv4 and IPv6). The term "unique" is defined as servers with unique IP addresses. A nameserver with a service provider can host several domains. A list of the categories and the number of domains found in each category is presented in chapter 5.

A comparison was also conducted with a control group comprising 1 percent of the entire .se zone, meaning 10,991 randomly selected .se domains. The results from the comparison are presented in chapter 9.

To monitor the development from year to year, we generally try to limit ourselves to approximately the same survey group as used in previous years. However, in 2011 we decided to implement some changes, which resulted in an impression in this year's survey that does not entirely correspond to the impression from 2010.

For example, 670 domains were investigated in 2010, compared with 912 in 2011. The primary reason behind the increased number of domains is that we added the "Registrars" category, because we find it interesting to observe how well the players that often provide services to .se domain registrants correspond to what is considered standard in their own environment.

In addition, we have the traditional changes in other categories where operations have been discontinued, merged or added.

Previously, a domain could have been classified in several categories, primarily because we included the OMX-30 category, which in 2011 essentially only contained duplicates, meaning that the domains were also classified in another category. We do not believe that this category adds anything apart from the results of other categories, thus prompting its removal.

2.2 Reduction in the number of serious problems

In 2007, we conducted the first survey. The 2008 investigation gave us an indication that there had been some positive development in the area compared with 2007. When we began to see trends in 2009, we were able to confirm that the changes were negligible and that there were still major problems that we emphasized and for which we proposed solutions. These were sent to the

¹ <http://www.sweden.gov.se/content/1/c6/18/19/14/70f489cb.pdf>

Infrastructure Minister at the time. Unfortunately in 2010, we were unable to see any significant improvements.

However, the 2011 results are positive in several respects.

The total number of serious problems and warnings has declined. Some of this may be explained by changes in the survey group, although even if we examine the percentage of randomly selected domains from the .se zone that we used as a benchmark, the situation has improved dramatically since last year in terms of the percentage of serious problems, while the number of warnings increased somewhat in that category.

In last year's survey, two of the domains had such serious problems that they could not even be tested; they simply manage to "exist" somehow. According to our DNSCheck tests, they are not even included in the domain name system, yet their websites are nonetheless accessible. They are probably not accessible by e-mail. The domains are probably only used for online traffic and not for e-mail, which is probably the reason that the registrants have not noticed that they are experiencing reachability problems with the domains. It is nonetheless a unique phenomenon, which proves what we generally say about DNS; it is an extremely forgiving system and a number of incorrect actions can be performed without affecting its functionality.

2.3 Differences compared with the 2010 survey

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 and to assess whether or not it is possible to track the effects of some of the advice and recommendations that we communicate and if this has resulted in any corrective measures among the surveyed organizations.

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

In this case, we have independently defined what we consider high quality to be, but our definition is based on what is recommended as the international industry standard, also known as "best common practice". There is also reason to believe that the lack of knowledge materializes in the form of substandard quality in terms of maintenance and operational responsibility.

There are some differences in the basis for this year's survey in addition to certain changes among the survey-group categories. The randomly selected domains which we use to compare with the .se zone as a whole were compiled in a different manner than in 2010.

In the previous version of the tool, we could extract a list of an exact number of randomly selected domains. This year, the tool uses a different type of algorithm, which does not allow the exact number for the test group to be determined, but instead selects a share, in this case one percentage, which in the

actual process amounts to slightly more than 10,000 domains, or 10,991 to be exact.

2.4 Dominant players increase the risks

The array of service providers whose name servers are connected to the Internet declined further in 2011. The major Internet service providers are becoming increasingly large and the small service providers are fading. The risk associated with this is that if a single service provider dominates a certain category, an entire sector may be affected if the individual service provider experiences problems. Accordingly, it is important to maintain nameservers with several different service providers.

2.5 Lack of competence among consultants and service providers

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 pertains not only to design and implementation, but also 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 radically improved on earlier investigations. There is strong reason for operations to hone their procurement skills and impose relevant requirements on consultants, registrars and the suppliers who operate nameserver, e-mail and web services.

2.6 Fewer nameservers with recursion activated

Between 2007 and 2011, the percentage of nameservers with recursion activated declined sharply, from 40 to 11 percent. Since the last survey, we experienced a further 4-percent decline. We have a highly favorable view of this trend.

2.7 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 far better results, particularly concerning the use of valid, current certificates issued by reliable authorities.

In 2011, we have observed a number of serious attacks on certificate authorities (CAs), prompting a number of questions about the quality of the security of these authorities. This has also prompted web-browser suppliers to tighten the requirements that are imposed on CAs for inclusion in the lists of root CA certificates, which are included in every web browser.

3 Control points

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

- How does the organization manage its DNS? Who is responsible for DNS within the organization, what is its structure (in relation to what can be considered to be industry standard or Best Common Practice, BCP), what are the most serious deficiencies and in what categories do they most frequently occur?
- How does the organization manage its e-mail? Are the servers located in or outside Sweden? Is TLS/SSL (transport security) used?
- 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? How are server certificates obtained?
- Has IPv6 been implemented in the operation's IT environment?

The domains and nameservers of a large number of important organizations in society were tested: public service and state-owned companies; banks, insurance and finance companies; Internet service providers; municipalities; county councils; media companies and government authorities, including county administrative boards and universities and colleges, as well as .SE's registrars for a total of 912 domains. The allocation by category is presented in chapter 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, compared with what is considered standard practice.

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

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

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

By cultivating such strategic partners as the Swedish Post and Telecom Authority (PTS) and the Swedish Civil Contingencies Agency, .SE has helped enable municipalities to apply for grants to pursue projects to implement DNSSEC. These funds will be granted and available for use as of 2012. We recommend that government agencies and individuals in decision-making positions adopt our advice and recommendations and take the appropriate

actions to make improvements in the areas of DNS, DNSSEC and IPv6, as well as the protection of e-mail and web-server communications.

4 Quality DNS service

The domain name system (DNS) is one of the cornerstones of the Internet and is designed to simplify the process of addressing resources on the Internet.

.SE is responsible for Sweden's national top-level domain on the Internet, a task that is considered so socially critical that it is regulated by a specific law. Each Internet-connected unit has its own IP address, which, using DNS, can be connected to an address that is easier for people to handle, meaning a domain name.

We ensure that the more than one million domain names with the .se suffix can delegate the right resources online by maintaining a registry of said names, as well as routing queries and responses. This enables users to reach the correct Internet or e-mail server.

Round the clock, all year long, we ensure that DNS queries about .se domains are responded to on the Internet. .SE's nameservers respond to an average of 4,000 to 5,000 questions per second.

We have applied the below definitions of quality DNS service to the survey in 2011 and in previous years. High quality entails:

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

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

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

The 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 radically improved on earlier investigations. There is strong reason for operations to hone their

procurement skills and impose relevant requirements on consultants, registrars and the suppliers who pursue nameserver, e-mail and web services.

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

5 Tests performed in 2011

The tests performed in 2011 also naturally included the configuration of domains and the status of the nameservers that respond to queries about the domain, as well as some of what we consider to be the most important 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, for the survey group as a whole and by 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 912 domains and 1,369 unique nameservers. The test subjects were grouped into the following categories (the figures in parentheses pertain to the number of organizations that were included in each category last year):

- 60 public service and state-owned companies (40).
- 79 banks, financial institutions and insurance companies (67).
- 22 Internet service providers (ISPs) (20).
- 290 municipalities (290).
- 21 county councils (21).
- 34 media companies (24).
- 228 government agencies, including county administrative boards (excluding agencies under the Swedish Parliament) (201).
- 39 universities and colleges (35).
- 146 registrars (new).

We removed the OMX 30 list of 28 .se domains and introduced a new category for registrars, meaning .se domains resellers, which also often provide nameservers and other services for domain registrants.

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

Error: 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 reachability in DNS and other resources.

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

6 Observations for 2011

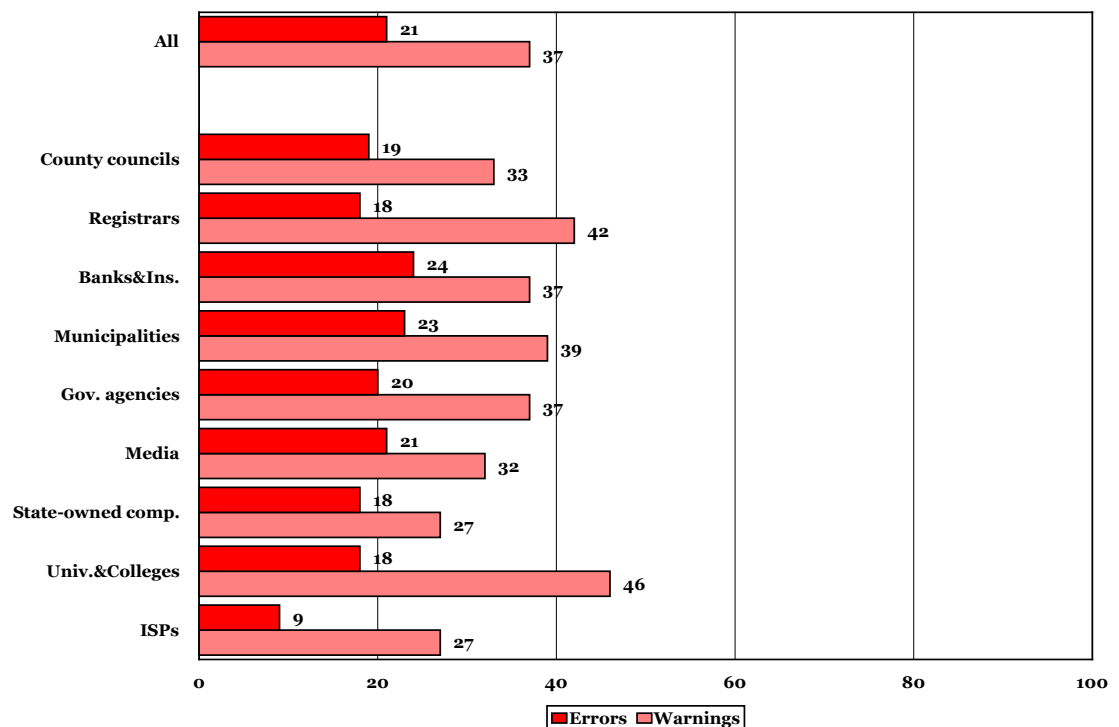
In 2007, we conducted the first survey to gain an impression of the status of the .se zone. The 2008 survey gave us an indication that some positive development had occurred in the area. When, in 2009, we began to see trends, we were able to confirm that the changes were negligible and that there were still major problems that we pointed out and for which we proposed solutions. In 2010, serious inadequacies remained and we were unable to observe any improvement, in fact, quite the opposite. Of the domains tested in 2010, 25 per cent had serious errors and 43 per cent had defects of a nature that resulted in a warning.

In 2011, the corresponding figures are: 21 percent with serious errors and 37 percent with errors of a nature that resulted in a warning. In other words, we observed a welcome improvement in the results.

6.1 DNS tests – errors 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 on the previous page shows the percentage of errors and warnings for all 912 domains in the survey group (referred to as “All”), and for each individual category. The bars of the graph should be read so that of the 912 organizations included in the study, 21 percent had serious errors and 37 percent had errors of a nature that generated a warning, down from last year’s survey.

For a more detailed description of the distribution of errors and warnings by category and year, refer to chapter 6.3.

6.2 Most frequently occurring errors

Among the domains and nameservers tested, the most common errors were:

- The nameserver did not respond to requests via the TCP (Transmission Control Protocol). This is probably because DNS server was not correctly set up or the firewall was incorrectly configured. It is a fairly common misconception that DNS does not need to communicate according to the TCP protocol (if it does not provide zone transmissions). However, TCP is usually 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 nameserver has insufficient current knowledge of DNS.
- The organization has an inconsistent nameserver structure (NS). The nameservers listed with NS records in a child zone differ from the information found in DNS in the parent zone and, accordingly, the nameservers cannot assume authoritative and proper responsibility for the domain. If the information is not consistent, the reachability 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 perform an update after a change was made.
 - 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 an error is that the redundancy that someone has tried to create essentially does not exist.
- The nameserver lacks EDNS support. This is an expansion of the DNS protocol to handle DNS responses that exceed the UDP protocol’s limit of 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.
- 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. Since a nameserver that responds to neither TCP nor UDP is probably not reachable at all, the error may be found

elsewhere, for example in the connection to the nameserver, or the server may not have a correctly stated IP address. Nameserver tests are now finalized in our survey 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 each domain so that temporary connection errors can be handled. If one of the servers or the connection to it were to stop functioning, services advertised by the nameserver would also be rendered unreachable. 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 notification).
- The DNS server is recursive. The DNS server responds to recursive orders from third parties (as in DNSCheck). It is very easy to abuse open recursive resolvers for distributed denial of service attacks (DDOS), since the use of a very small DNS query can create an amplification effect generating exponentially larger responses. False sender addresses can be generated using DNS, and those who want to attack a system create queries under a false sender address that produce large DNS responses that are sent to the presumed sender, which is in fact a third party whose services can more or less be blocked (refer to Appendix 6).
- The start of authority (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 nameserver receives the request, since the nameserver would then contain differing information on domains.

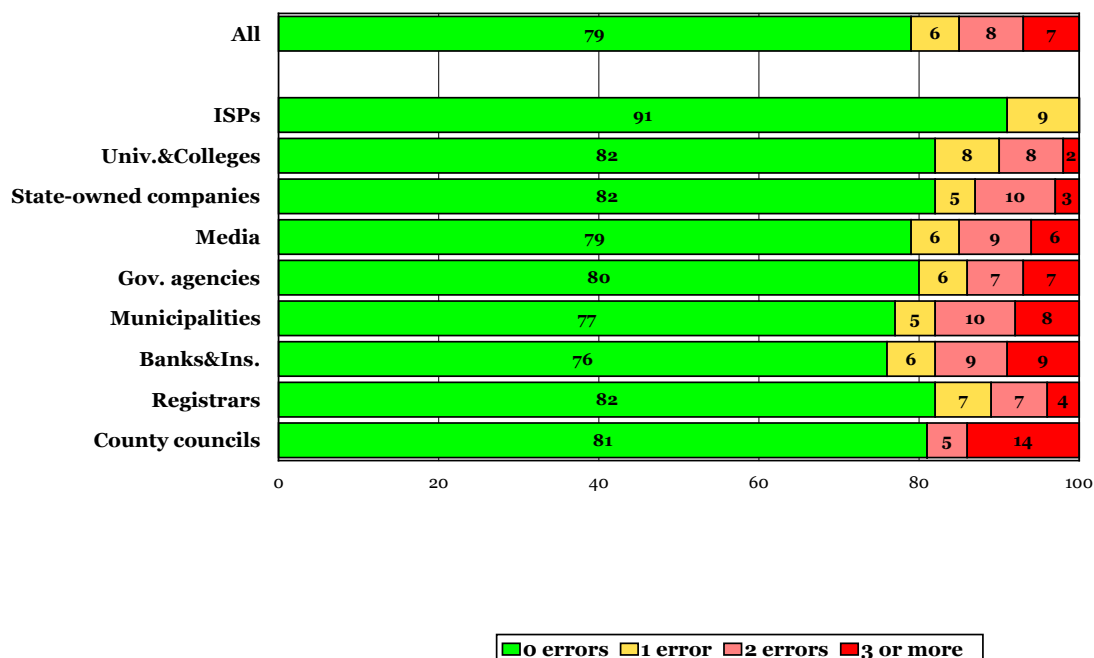
Incorrect configurations that are performed by a particular consultant at a number of organizations or by one of the major nameserver operators on a number of domains proliferate to all domains that said consultant/operator manages. If many domains are involved, this naturally has a substantial impact on the results of the survey, particularly if these incorrect configurations occur within a specific category.

It is worth noting that .SE's three largest registrars account for 50 percent of the market, while the seven largest commands 75 percent. Among the nameserver operators, the two largest have 36 percent of the market, while the five largest commands 50 percent. Also, among the nameserver operators, there are a vast number of very small players.

6.2.1 Number of errors per category

Naturally, there is a difference between whether a domain has one error or several errors which may also often interact. Accordingly, we have also examined the distribution of the number of errors in terms of quantity and by category.

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



The Internet service providers (ISP) category had the lowest percentage of errors in 2011 again, while the Banks and insurance company's category had the highest.

The poor result in the Universities and colleges category in 2010 was eventually explained. We contacted universities and colleges through the Swedish University Computer Network (SUNET), whose feedback explained that they had corrected most of the problems (they employed such tools as DNSCheck to identify the nature of the problem). Last year's poor results were primarily attributable to the TCP filter in the firewalls, but also the closing or reconfiguration of secondary nameservers without notifying the primary nameserver.

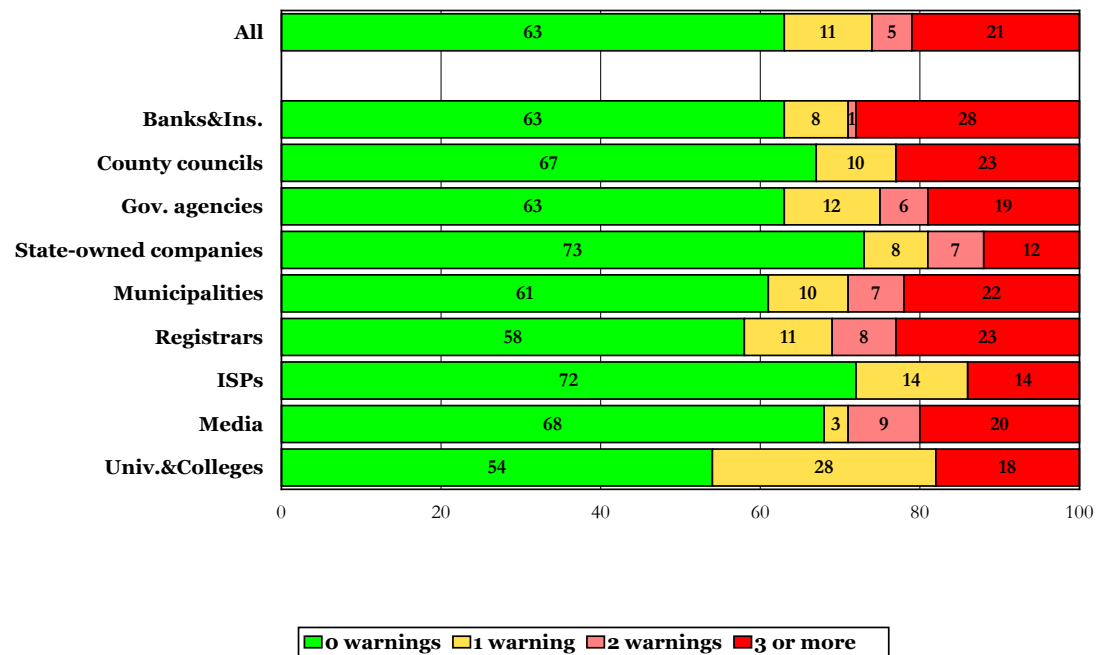
Once county councils have experienced one error, the errors appear to proliferate.

We are convinced that all categories should be able to reduce the level to less than 20 percent without any major effort. Getting below 15 percent errors requires slightly more effort than simply correcting basic hygiene factors.

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 following graph:

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



The Universities and colleges category had the highest percentage of warnings, followed by Registrars, Municipalities and Government agencies. However, Banks and insurance companies, as well as County councils, had very many warnings, meaning a high percentage of 3 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. In general it is also much more commonplace with warnings than errors. However, both errors and warnings have a negative impact on reachability.

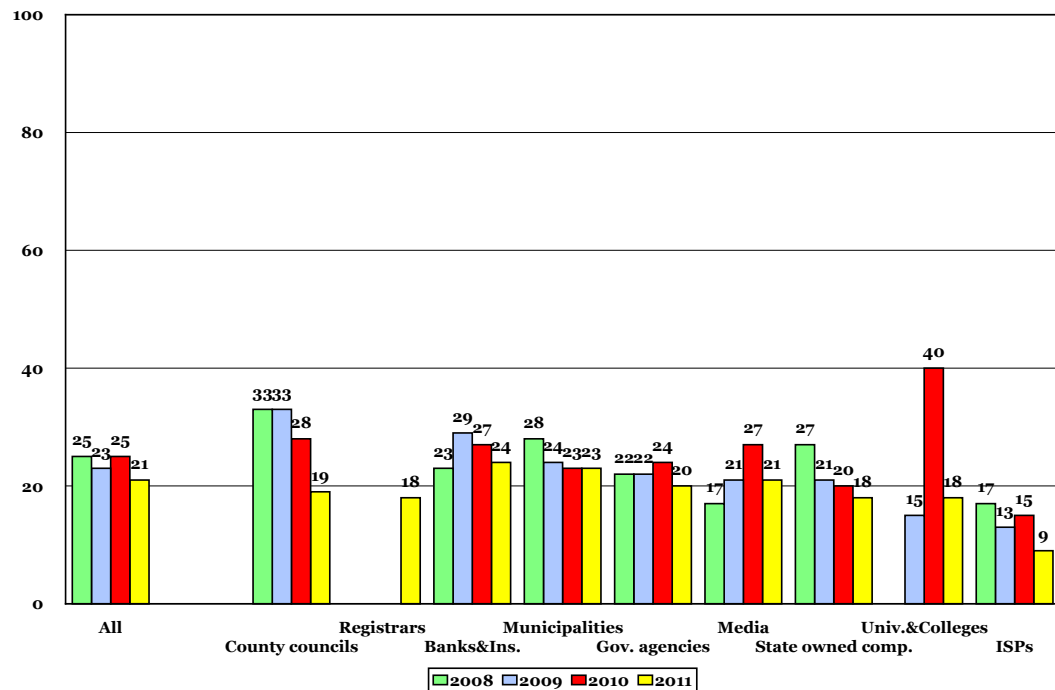
6.3 Comparison over time – defects and warnings

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 five years. Some categories were first

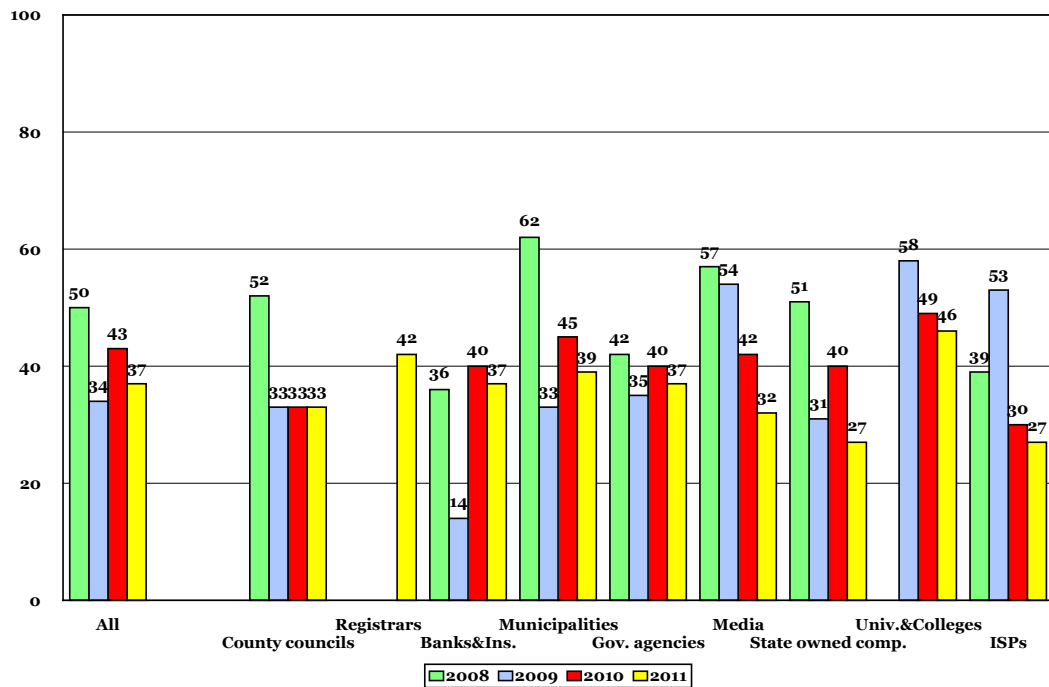
included in 2009 and we were thus only able to report results from the past three investigations for these categories. The Registrars category is new for 2011.

In the following graph, we compared the percentage of errors over time, from 2008 to 2011 (with the exception of Universities and colleges and Registrars, which were added in 2009 and 2010, respectively).

Graph 4: Number of errors over time



Graph 5: Number of warnings over time

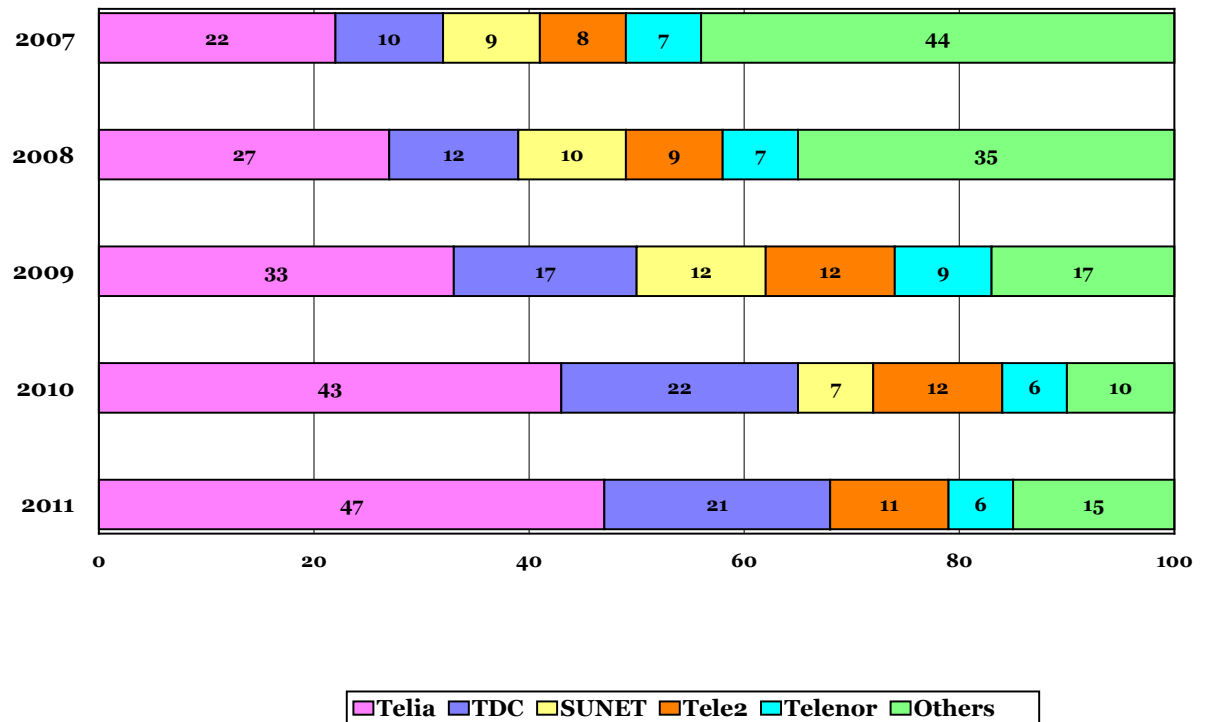


The situation for warnings remains unchanged for the County councils compared with 2010, while the number of warnings declined in all other categories included in the 2010 survey. For Registrars, warnings were generated among 42 percent of the test subjects.

6.4 Nameserver connections to the Internet

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

Graph 6: Allocation of ISPs – nameservers’ Internet connections



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

While the category *Others* rose somewhat in 2011, it has still fallen from 44 percent in 2007 to 15 percent this year. The *SUNET* category disappeared entirely, which probably explains the rise in the *Others* group.

We also observed an increase among the largest service providers. Here Telia in particular appears to increasingly dominant the market, increasing its share to 47 percent compared with 43 percent in 2010. TDC and Tele 2 lost market shares, while Telenor remained unchanged at 6 percent. In other words, the year-on-year changes were relatively extensive.

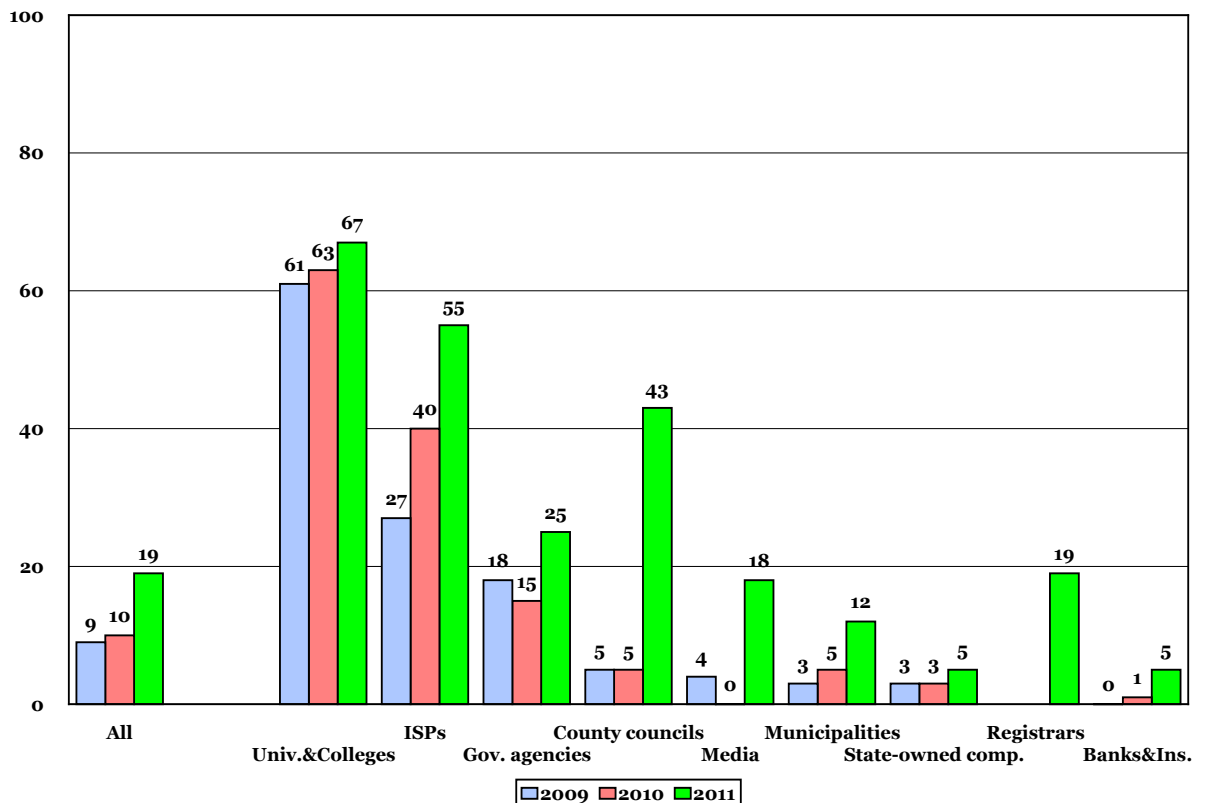
This means that the distribution of nameserver operation by various service providers continued to decline. The major Internet service providers are becoming increasingly large and the small service providers are fading. The risk associated with this is that if a single service provider dominates a certain category, an entire sector may be affected if the individual service provider experiences problems. In the case of Telia, we know that if said company were to experience problems, it would have major consequences in a number of areas.

It increases the redundancy if the nameservers are connected to various service providers.

6.5 Nameservers using IPv6

The trend of increased activity in the IPv6 area continued and rose sharply in 2011. Universities and colleges topped the statistics. The greatest improvement was made by the County councils, from 5 to 43 percent. Government agencies, Municipalities and Media also demonstrated a positive trend. The trend only seemed to be slower in the State-owned companies and Banks and insurance companies categories.

Graph 7: Percentage using nameservers accessible via IPv6



A total of 19 percent of the investigated domains have a nameserver that is reachable via IPv6, compared with 10 percent in 2010.

The lack of IPv4 addresses is already a fact and it is beyond high time to implement IPv6. It is important to understand that such a transition requires about 12-18 months of preparation and deployment.

Postponing the implementation of IPv6 is like postponing a visit to the dentist. Ultimately, you reach a point when you cannot wait any longer, it becomes expensive and painful. Everything that needs to be done urgently entails higher costs and poorer quality, which in turn leads to dissatisfied customers and users.

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 a section of

our website that is devoted to continuously reports on IPv6 in Sweden. These reports are available at <https://www.iis.se/en/internet-for-alla/ipv6>.

The government also charged the Swedish Post and Telecom Agency (PTS) with describing how to implement IPv6 at the government agency level in terms of accessibility, security and financial aspects. The description is aimed at serving as a support platform for government agencies, municipalities and other organizations in the public sector in their implementation of IPv6. The PTS applied the experiences that the agency gained during the implementation of IPv6 in parts of its own IT environment during spring 2010. Under the assignment, PTS also performed an impact analysis of the implementation of IPv6 as the sole protocol, but also in coexistence with IPv4. The report was recently published and is available for reading (in Swedish) at [http://www.pts.se/upload/Rapporter/Internet/2011/2011-18 Att infora internetprotokollet IPv6.pdf](http://www.pts.se/upload/Rapporter/Internet/2011/2011-18_Att_infora_internetprotokollet_IPv6.pdf).

6.6 Service providers offering nameserver hosting

Normally, a registrar is also responsible for the operation of nameservers for a domain. As previously mentioned, the seven largest registrars manage 75 percent of the domains in the .se zone. Serious incorrect configurations by the registrars who also operate nameservers on behalf of their customers would probably become extremely noticeable.

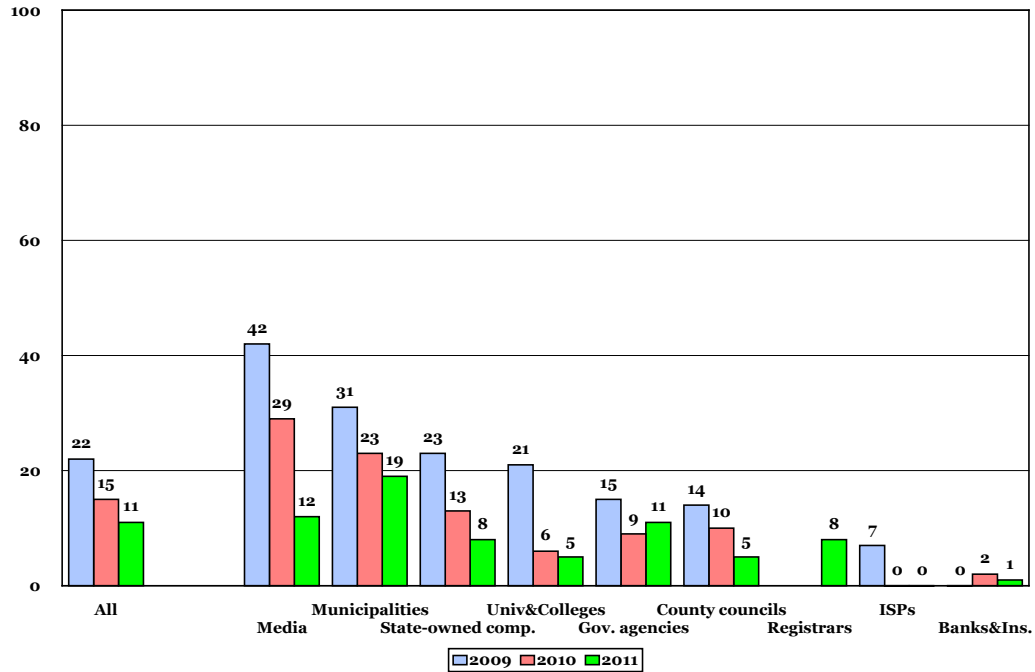
6.7 Nameservers with recursion activated

As we have reiterated each year, open recursive nameservers have a very limited number of legitimate areas of application and may be abused in conjunction with denial-of-service attacks, for example. 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 nameservers open for recursion declined even further in 2011 and is currently down to 11 percent, compared with 15 percent in 2010. This is excellent considering the risks involved.

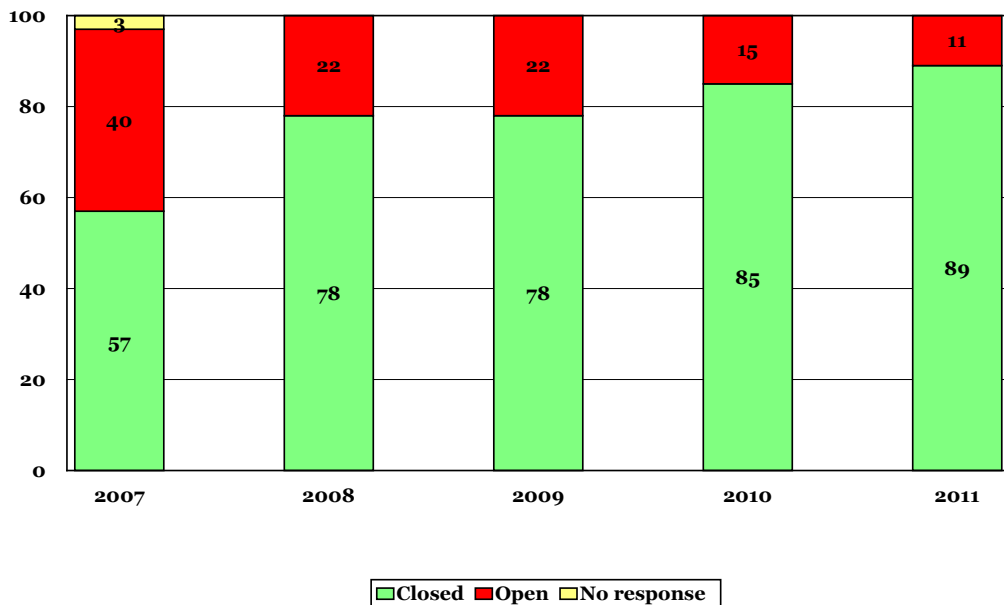
This most frequently occurred in the Municipalities (19 percent), as indicated in the graph below.

Graph 8: Nameservers with recursion activated per category



The improvement in results shown in the graph is attributable in part to nameservers now being delivered with recursion inactivated as the default setting. We also believe that those responsible for DNS infrastructure have become more proficient at implementing a separation between authoritative nameservers (those that actually respond to queries) and resolvers (those that simply mediate queries and responses).

Graph 9: Nameservers with recursion activated, 2007-2011



Between 2007 and 2011, the proportion of nameservers with recursion activated declined sharply, from 40 to 11 percent. Since the last investigation, there was a decline of a further 4 percent. We are very pleased with this trend.

6.8 Use of DNSSEC

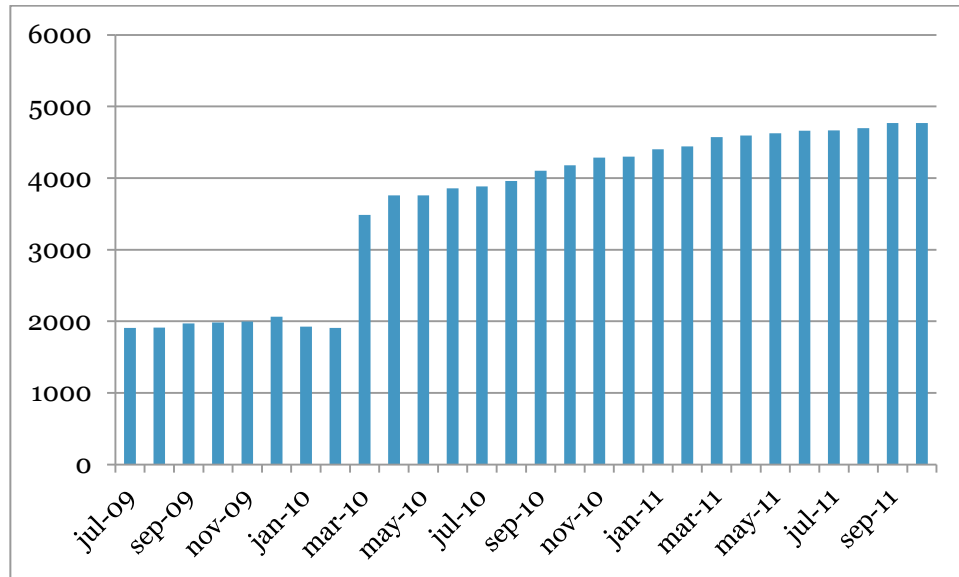
DNSSEC protects Internet users from forged or manipulated DNS information, for example, what is known as DNS cache poisoning. Responses to DNS queries that are protected using DNSSEC are assigned a digital signature, the verification of which ensures that DNS information has not been tampered with on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

As usual, the number of domains in the .se zone that are signed using DNSSEC is reported separately.

6.8.1 How widespread is the use of DNSSEC?

Among the domains in the 2011 survey group, 6.69 percent, or 61 domains, were signed using DNSSEC. Municipalities, government agencies, county councils and ISPs are the primary organizations that have begun to implement the safer technology. As a comparison, it can be noted that in the entire .se-zone, only 0.45 percent of the total number of domains are signed. We noted some growth, although far from the rate that we would have wanted. The following graph shows the growth of DNSSEC-signed domains throughout the .se zone, and not solely the comparative group.

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



Source: .SE's website

<https://www.iis.se/en/domaner/statistik/tillvaxt?chart=per-type>

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

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

In partnership with the Swedish Civil Contingencies Agency (MSB), the PTS and the Swedish Association of Local Authorities and Regions (SALAR), .SE has made preparations to enable the municipalities to apply for funds from Appropriation bill 2:4 Crisis Contingencies. In 2012, the MSB has prioritized reinforcement measures to facilitate secure resolution of Internet addresses, which is conducted via the domain name system. Among other remarks, MSB says that “it is vital that domains for public websites are signed using DNSSEC.” During autumn 2011, municipalities have been free to apply for funds. We are very hopeful that this will generate results in 2012.

One year ago, 15 municipalities had signed their domains and in October 2011, that figure was 24. In other words, slow progress has been made.

It is important to recruit the right skills when implementing DNSSEC. Fatal mistakes can be made, for example, assigning the signatures a certain lifetime without the renewal of which the domains cease to function. We have seen examples of organizations that have signatures with a lifetime of less than a week and other parameters that greatly hamper an organization's ability to react and repair. This means measures must be in place to handle various types of disruptions in the system relatively quickly, which could pose a problem during vacation periods, holidays or longer weekends, for example, unless maintenance measures are in place, round the clock, every day of the week, all year round.

Tools are available to assist in the administration of DNSSEC keys and the signing of zone files for a domain.

Another rumor spread by half-baked consultants to municipalities is that the management of DNSSEC requires at least a half-time position. The truth is that using modern tools, the impact on operations is relatively minor. Some consultants also seem to believe that Windows 2008 R2 is compatible with DNSSEC, which is also false.

In other words, it is important to use the right consultants and at the present, not that many consultants have been involved in practical implementation generating solid experience. Although judging by the limited number of signed domains, not many have tried either, without having sufficient knowledge and thus not been able to destroy anything.

6.9 DNSSEC in other top-level domains

The proliferation of DNSSEC has gained momentum among other top-level domains worldwide, particularly after the signing of the root zone, which took place last year. Of all 310 top-level domains that are announced in the root zone, 83 are signed using DNSSEC and 76 of these have published information about their keys in the root zone.

Current statistics are available at
http://stats.research.icann.org/dns/tld_report/
More information on DNSSEC is available in Appendix 5.

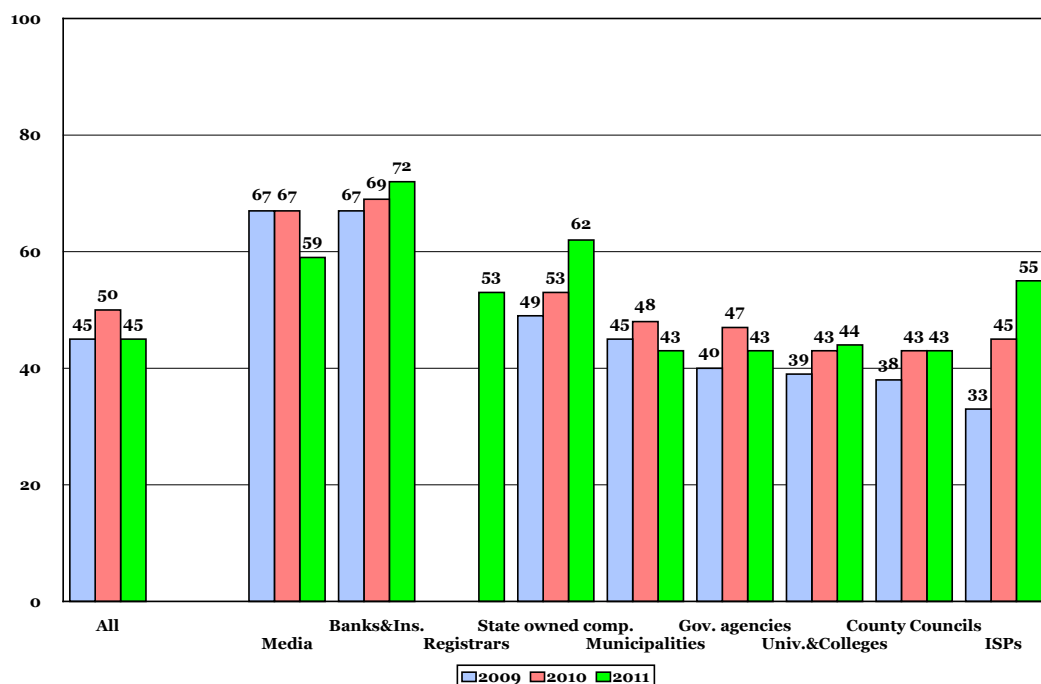
7 Key parameters for e-mail

7.1 Transport layer security (TLS)

To ensure the secure exchange of information between e-mail servers, these communications should be protected during transit. Transport layer security, or TLS, is an open standard for the secure exchange of encrypted information between computer systems. TLS is an improvement on version 3 of the SSL protocol and is governed by the IETF. In addition to confidentiality (encryption), TLS offers correctness (data integrity), and also authenticity protection (source protection), depending on its use. TLS/SSL can, among other things, be used for transfer of electronic mail (SMTP).

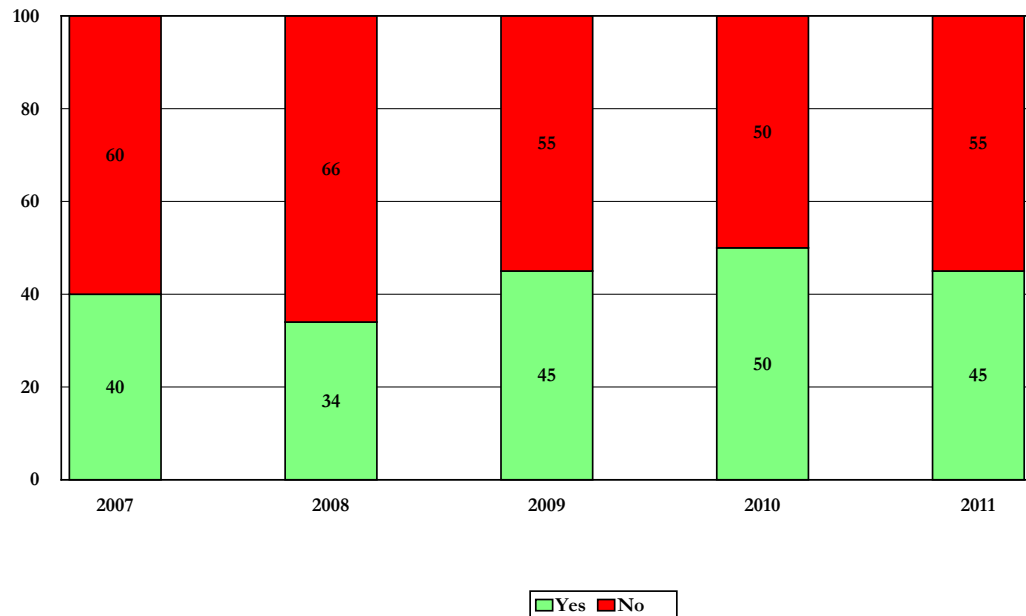
Of the organizations investigated in 2011, only 45 percent supported TLS/SSL on their e-mail servers. This is an overall decline on last year (50), and means that there has certainly not been an increase in the number of people taking sufficient actions to protect their e-mail traffic against eavesdropping, although the changed survey groups have impacted the scenario somewhat. The figures have risen in certain categories, while declining in others. However, all software now has built-in support for this, and it is not difficult to implement. For more information, see Appendix 9.

Graph 11: E-mail servers offering support for TLS



The use of StartTLS has increased in the Banks and insurance companies, State-owned companies, Universities and colleges and ISP categories, while remaining unchanged in the County councils category and declining in the Media, Municipalities and Government agencies categories. In the Registrars category, only 53 percent use StartTLS. The decline in the Media, Municipalities and Government agencies categories is particularly interesting in light of the crucial informant protection law, meaning the importance of protecting informants who provide journalists with information. Unfortunately, we do not have any information as to the reasons behind this. The graph below shows the trend in the past five years.

Graph 12: E-mail servers with support for TLS, 2007-2011

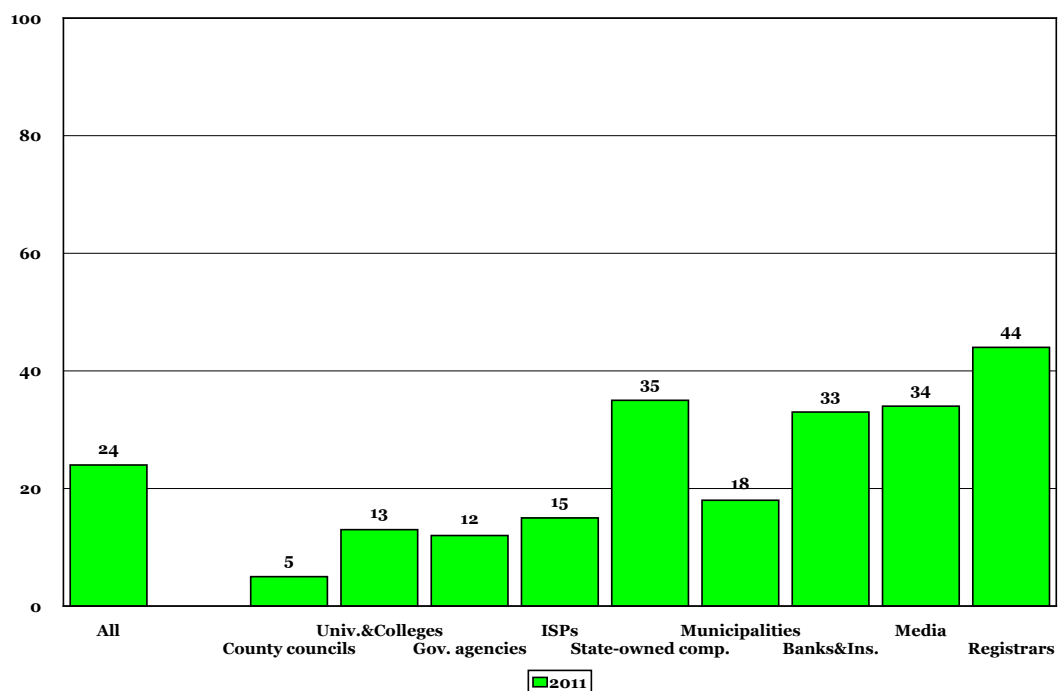


7.2 Location of e-mail servers

Since a greater percentage of e-mail servers used IPv6 addresses in 2011, and because we are unable to accurately determine where these are located pursuant to the method that was used in previous years, we have now opted to report results only for the servers that use IPv4 addresses.

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

Graph 13: Percentage of organizations with e-mail servers abroad



In the 2011 survey, a total of 19.5 percent of domains have nameservers, e-mail servers or web servers with IPv6 addresses.

In the Registrars category, part of the reason that so many organizations have servers abroad is that a full 46 of the 146 accredited registrars are players with operations in a country other than Sweden.

Another aspect that differentiates this year's survey from last year's is that registrars operate a significant number of e-mail servers because they often deliver e-mail as a service to others. This means that the percentage values for e-mail servers in Sweden has changed radically, since twice as many servers were included in the survey in 2011 (1,856) compared with 2010 (940).

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

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. In the case of the media, this also applies to e-mail communications between the informant and the journalists. Since communications are often unprotected (see section 7.1), this entails an unnecessary risk for the exposure of sensitive information.

In conclusion, we can state that organizations still seem to frequently send their e-mail abroad to be filtered from spam and viruses.

At the same time, we know that less than half of the organizations investigated use encryption for transport security of their e-mail. Only 45 percent of the domains investigated support 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 aims of this part of the study is to show that there could be consequences for e-mail sent from Swedish companies and organizations when Sweden begins applying 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 not only Swedish but also foreign intelligence services can eavesdrop on the traffic without major difficulty. 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 any impact analyses.

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. Among the solutions are DKIM and SPF or a combination of the two, which are based on some form of authentication of the sender at the server and domain level.

7.3.1 DKIM

DomainKeys Identified Mail (DKIM) is a technology 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 unfortunately impossible to precisely determine whether or not a domain uses DKIM. We are

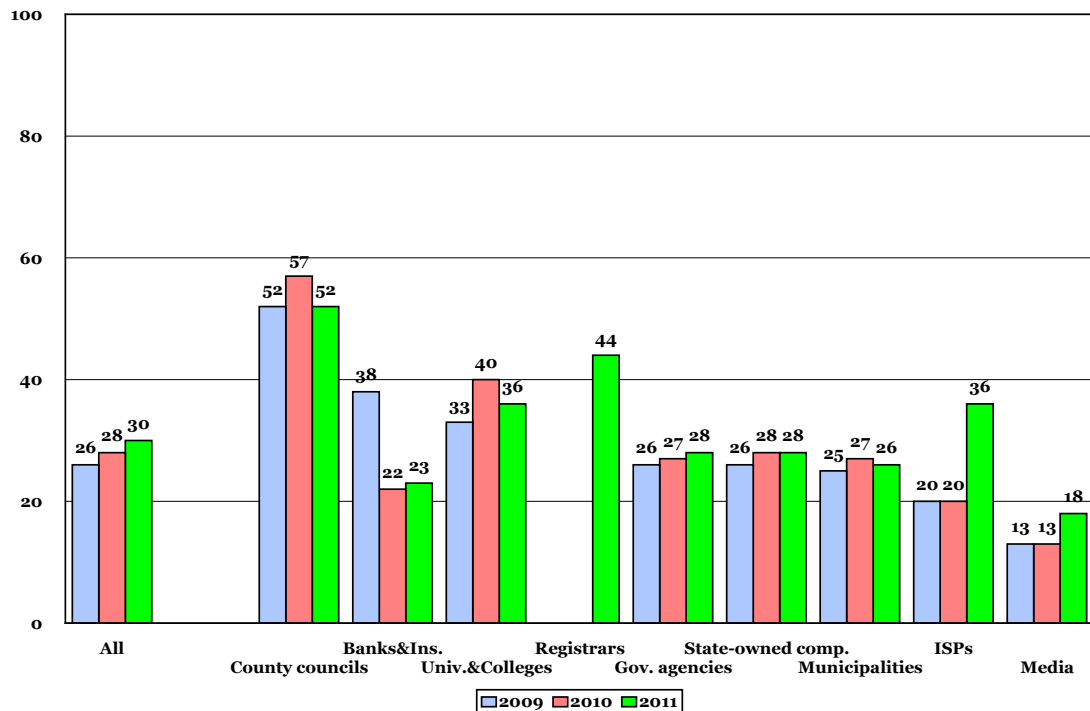
currently unable to report the results on the expansion of DKIM since it is impossible to exactly determine the existence of DKIM for a domain before the use of author domain signing practices (ADSP) becomes more commonplace (see Appendix 8). DKIM itself does not protect against spam unless it is combined with an ADSP policy. The current use of ADSP is essentially nonexistent. We will probably report on the existence of ADSP in future surveys. The presence of ADSP can be measured since it is published in DNS.

7.3.2 SPF

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

In the current measurement, we only examined whether the domain has a published SPF entry or not. We did not perform an assessment of the other content.

Graph 14: Use of SPF



We noted a moderate although increased use of SPF in this year's survey, from 28 percent in 2010 to 30 percent in 2011. County councils declined somewhat, from 57 percent to 52 percent, although they remain the top users. Use among ISPs rose relatively sharply from 20 percent to 36 percent and among registrars, 44 percent uses SPF. Banks and insurance companies, Government agencies, State-owned companies and Municipalities were essentially unchanged compared with 2010.

8 Key parameters for web servers

A number of organizations currently provide information and services via web interfaces and many organizations are entirely dependent on their web interfaces working and being accessible for their customers, business partners and the public at large. Increased use also imposes stricter requirements on accessibility and reachability.

Actions can be taken to increase redundancy also for web services. It may be a good idea to consider this if any critical functions are provided via web services and non-functionality of the service would prompt a strong reaction from users.

Increased accessibility is a key component, and equally important is security in terms of protection of information (confidentiality), which we will focus on in the rest of this section.

In addition to traditional web services, web technology is increasingly used for M2M communications (machine-to-machine), meaning web services. These services also require secure communications in the form of transport protection, protection against repeated attacks, the authentication of servers and authentication of the client side.

Web technology is often used in what are known as apps, since they communicate with server functions. Even those who developed the apps often do not know whether these use SSL/TLS. Tests using protocol analyzers have demonstrated that several popular apps send information in plain text.

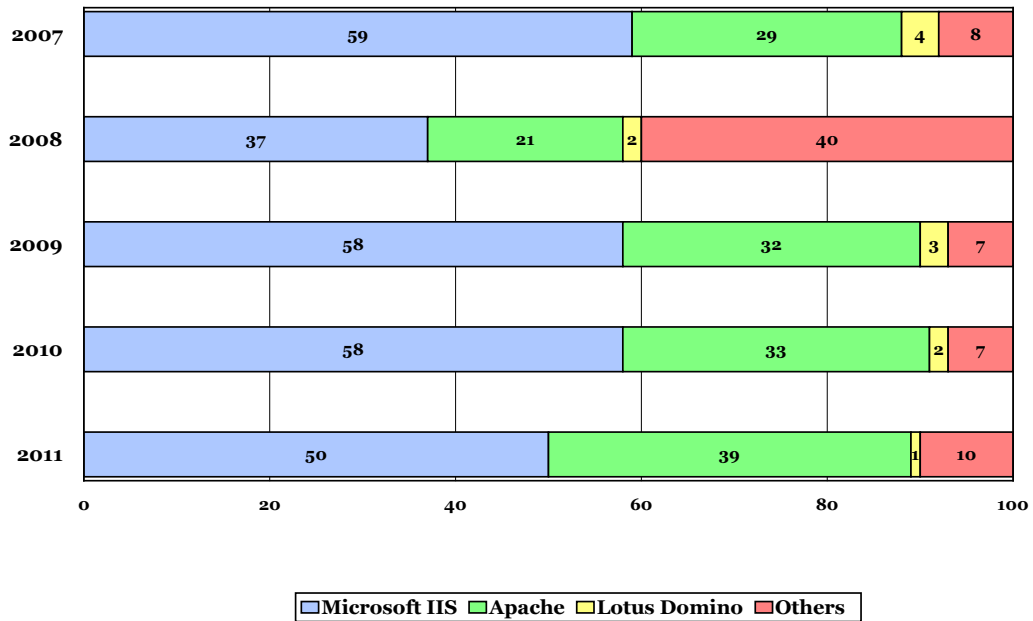
8.1 Connection of web servers

If all of an organization's nameservers are connected to a single Internet service provider, and if the web server is also connected to the same provider, there will be major problems if said service provider experiences reachability problems. This would not only affect the nameservers, but also the web servers, thus rendering the system unreachable. An organization should have at least one more nameserver located with another service provider, and consider establishing a backup or secondary site somewhere to achieve the greatest possible redundancy.

8.2 Software for web servers

As usual, we examined which web server software was used in the organizations investigated. Microsoft Internet Information Server (Microsoft IIS) and Apache were still the clearly dominant software.

Graph 15: Software used for web servers



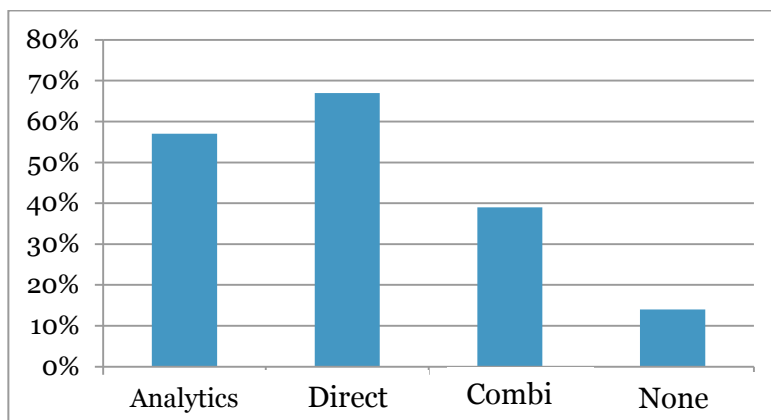
8.3 Additional interesting observations regarding web servers

For the second consecutive year, we have checked a number of parameters that are of particular interest for web applications.

8.3.1 Cookies

On July 1, 2011, the Swedish Electronic Communications Act (2003:389) was amended. A result of this amendment was that everyone who actively visits a website may have to consent to the website using what are known as cookies.

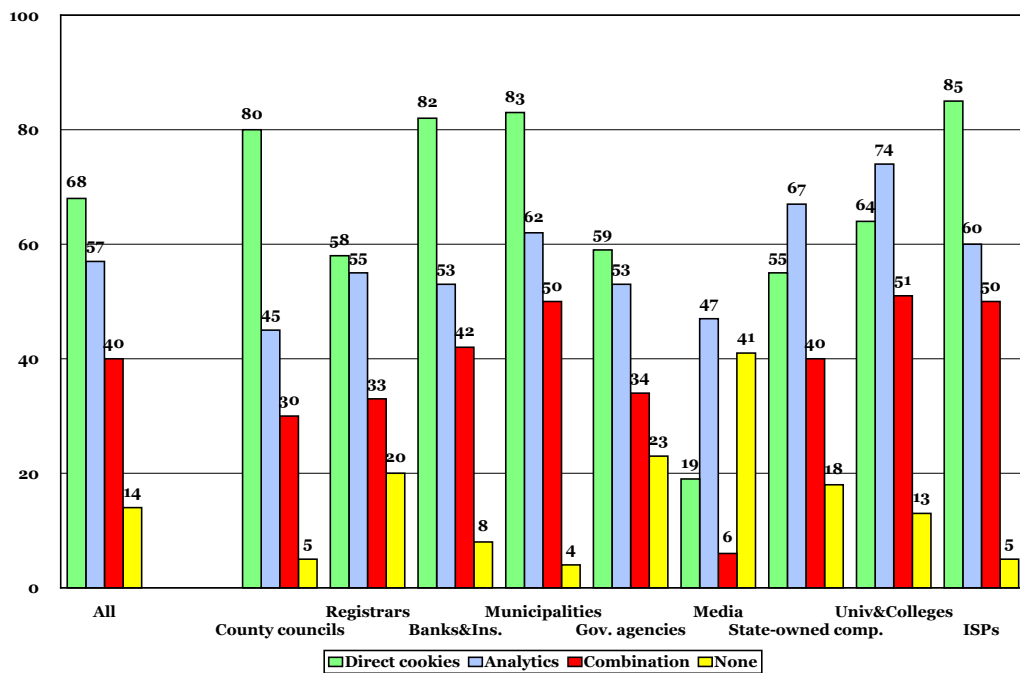
Graph 16: Cookies



Of the 912 domains in the survey group, these tests were conducted on 904. A significant share (44 percent) of the surveyed websites uses Google Analytics and thus attaches third-party cookies to collect visitor statistics, which is an increase from last year. It is important to know that regardless of the organization’s cookie policy, Google Analytics attaches cookies without first requesting permission.

A total of 612 of the 904 websites of the surveyed domains, or 67 percent, independently attach cookies. Nearly 40 percent use a combination of both Google Analytics and direct cookies. In this context, the term “None” means that neither Google Analytics nor direct cookies are used, although this does not preclude the use of other third-party resources that attach cookies.

Graph 17: Cookies by type and category



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

A potentially more in-depth project from .SE’s perspective in this area could be to survey how many websites are trying to comply with the law and actually requesting active consent from users.

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

Sharing visitor statistics with Google Analytics also enables Google to draw its own conclusions of visitor traffic to the websites of Swedish government agencies, for example. Google may also choose to perform cross-references to examine which of the visitors to an agency's website also visit another agency's website, for example. Prior to selecting a tool to assess visitor statistics, it is important to perform a consequence analysis that takes into consideration where and with whom the information is stored.

8.3.2 Publication system

The EPiServer system remains by far the most popular publishing system (CMS) used by the organizations included in the survey. We did not note any tangible increase in the use of alternatives based on open source code. Last year, we assumed that this percentage would probably rise, as a result of reduced license costs from the free alternatives and because the software based on open source code could be expected to become more commonplace among Swedish government agencies. However, as it turns out, we were unable to note such a trend, at least not to date.

A possible explanation may be that replacing CMS is an extensive effort, meaning that functionality, not license costs, is the governing factor.

8.4 Support for transport security (TLS/SSL)

TLS/SSL is the technology that protects online traffic against eavesdropping and that enables a user to trust that he/she is communicating with the right organization when, for example, performing banking transactions online. A more detailed description is available in chapter 7.1.

Using certificates and the accompanying encryption keys, a web browser can establish secure, encrypted communication with the web server. As with e-mail, 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 have a certificate issued for the domain or the web server. The certificate must also be seen as reliable by fulfilling certain fundamental requirements that should be imposed on this type of security mechanism. For example, the certificate must be issued by a reliable certificate authority, be valid, it must use secure algorithms, the keys must be sufficiently long, and so on.

There are some reasons why certificates may occasionally be unreliable:

- The certificate may have been used before becoming valid.
- 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 website.
- The certificate may have been revoked (blocked).

- The certificate may be self signed.
- The issuer may not be a well-known CA.
- The certificate may be deemed unreliable.
- The certificate chain may be incomplete.

Measuring the existence and quality of certificates is not entirely easy, and we are testing various approaches to identify a solid method of measurement. Accordingly, our approach in 2011 was not identical to our approach in 2010, which is why the comparisons between the figures in 2010 and those from 2011 are not always relevant, although we have reported them in brief below.

In 2010, some 227 of 670 domains, or 34 percent, returned a relevant response to queries related to certificates. Of these 227 domains, we were able to download completely correct certificates from 190 domains that were issued by a recognized CA, or 84 percent. This was an increase of 6 percent since 2009.

In 2011, we received a response from 175 domains with certificates of the 912 tested, or 19 percent, which is a decline. Of these, 16 failed entirely (they received the lowest grade – F – on a six-point scale of A-F). Some 46 certificate maintained a top level of quality and received an A. The grading process is detailed in:

https://www.ssllabs.com/downloads/SSL_Server_Rating_Guide_2009.pdf

The most frequently observed defects among the tested domains were:

- The use of certificates issued under the wrong host name.
- The use of expired certificates.
- The use of self-signed certificates.
- The use of certificates signed by an unknown root CA.
- The use of certificates with incorrect electronic signature.

It is also commonplace for domains lacking a correct certificate to have more than one defect.

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 fairly 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 being forced to click on popups 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 with username and password, 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 EV certificates where warranted.
- Avoiding the use of wildcard certificates for web services, especially for subcontracted operation of web hosting or cloud services, where organizations do not control their own key material and certificates.
- Using hardware support to save private keys for sensitive web servers.

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

8.5 Attacks against SSL

During the year, there have been several highly serious attacks against several major certificate authorities, and there is reason to wonder how reliable the SSL system is and what can be done about the existing problems.

We are discussing security here. Certificate management of the CAs that were attacked during the year has been highly varied, and some of the affected CAs acted slowly and inadequately.

In this context, we want to remind you that the certificate warnings are not to be ignored but taken under very serious consideration (see Appendix 8). It is important to monitor the https connection and try to ensure that it is authentic. We also recommend examining the certificate more closely.

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

8.6 Measures to counteract attacks against SSL

Many people are considering solutions and one of the more interesting initiatives that we have seen is made by the IETF task force known as DNS-based Authentication of Named Entities (DANE), which can be expected to be completed soon. Under DANE, certificates are stored in DNS so that they can be verified using DNSSEC. The approach supplements the CA's signatures by also verifying the certificate through DNS. This helps reinforce the quality of the certificate and thus also its reliability. Moreover, it enables users to forego the traditional CAs and rely solely on DNS if they only want to verify the domain name and not the legal entity behind a service.

Another relatively standard variety of attacks against websites that use SSL involves various types of downgrade attacks. This means that the user is tricked

into using a simpler form of encryption, or no encryption at all, to communicate with the website. In this case, not even a valid website certificate is needed to effectively perform what is known as a man-in-the-middle-attack. IETF is working on the development of HTTP Strict Transport Security (HSTS), which forces the web browser to run SSL on the website, regardless of other commands. HSTS remembers whether a website that has been visited before has used SSL and forces communications to the same level during recurrent visits.

The Chrome web browser includes a number of extensions, including *certificate pinning*², which is the feature that revealed this year's CA attack on DigiNotar. Other Chrome extensions include *HTTPS-preloading*³, which means that websites are preprogrammed to always use SSL.

A plugin is also available for Mozilla Firefox and other web browsers for enhanced certificate management, such as *HTTPSEverywhere*⁴, which was co-developed by Electronic Frontier Foundation (EFF) and the Tor project.

Another Swedish survey⁵ of certificate use during the year was conducted by Romab. Romab examined the use of certificates for Alexa top 100 companies, Swedish media sites, Alexa top 100 international media, Swedish trade unions and Swedish political parties. Even though these are not the same survey group that we focused on in our tests, the results are interesting to read for those who want to take a closer look at the quality, use and management of certificates.

.SE intends to conduct an extended survey of the quality and use of certificates in the .se zone during 2012.

² <http://www.imperialviolet.org/2011/05/04/pinning.html>

³ <http://dev.chromium.org/sts>

⁴ <https://www.eff.org/https-everywhere>

⁵ <https://www.romab.com/swess/>

9 Comparison with the entire .se zone

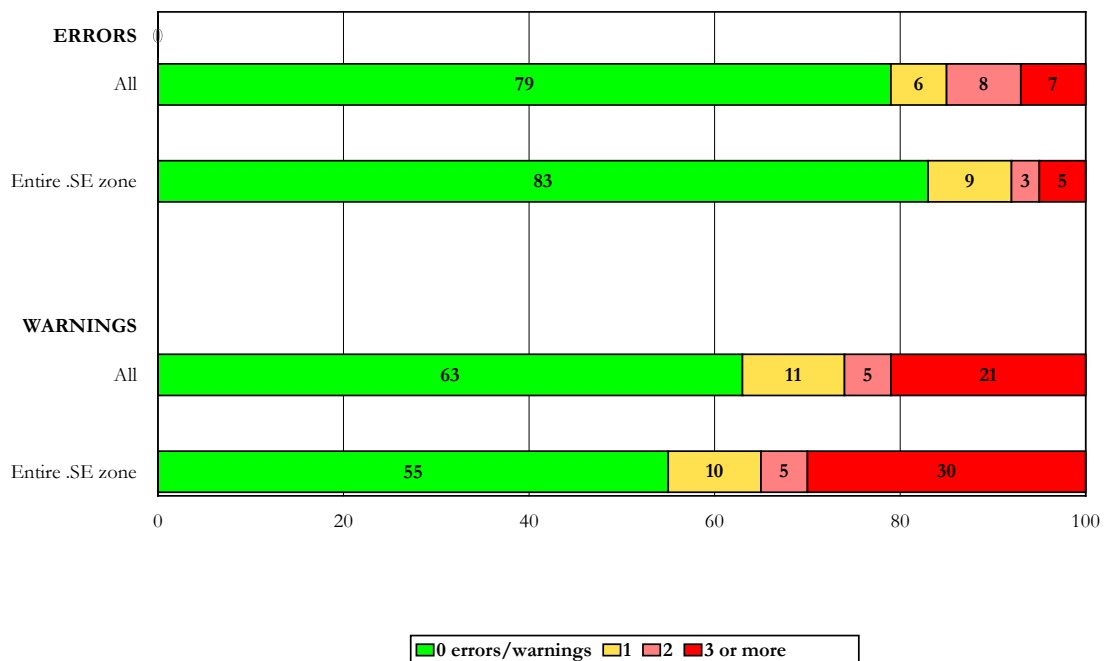
In the 2011 survey, we also examined a cross-section of randomly selected domains from the .se zone to assess whether our test group was better or worse than the .se zone as a whole.

In the graphs below, “All” represents the current test group, while “Entire .se zone” represents the random selection of 10,991 domains from a version of the zone file dated October 31, 2011.

9.1 Distribution of errors and warnings

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

Graph 18: Number of errors and warnings



In 2011, there were more errors in our survey group than in the comparative group for the .se zone as a whole, which is in line with last year. However, there were fewer warnings in our survey group than in the comparative group.

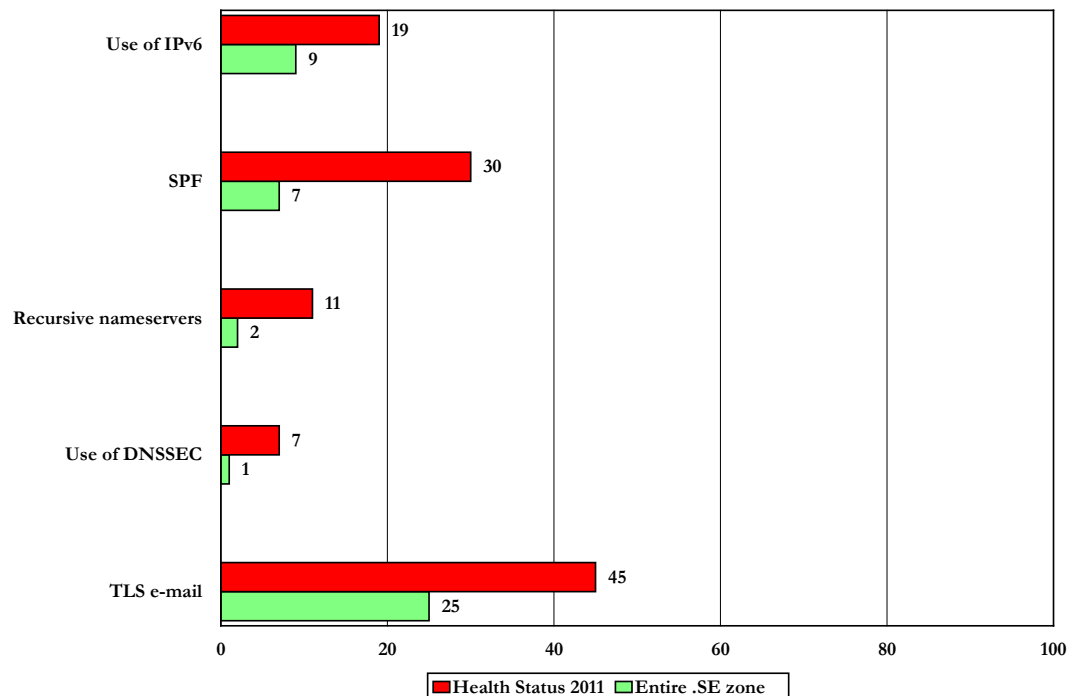
9.2 Differences between the survey group and the comparative group

The major differences first become apparent when we examine the specific areas we have reviewed more closely, such as the parameters we associate with DNS quality in accordance with the definition in Appendix 4. There were more incorrect delegations in the comparative group for the .se zone as a whole than in the survey group and more organizations that were dependent on just one nameserver. Meanwhile, there were more organizations in the survey group that had open recursive nameservers (11 percent compared with 2.4 percent in the comparative group).

In the survey group, more organizations had implemented IPv6 (19.5 percent compared with 9 percent in the comparative group), far more are using DNSSEC (6.6 percent compared with 0.5 percent in the comparative group for the .se zone as a whole) and more are protecting their e-mail using TLS. In 2012, we will conduct some more detailed surveys for various limited areas.

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

Graph 19: Comparison between the survey group and the .se zone

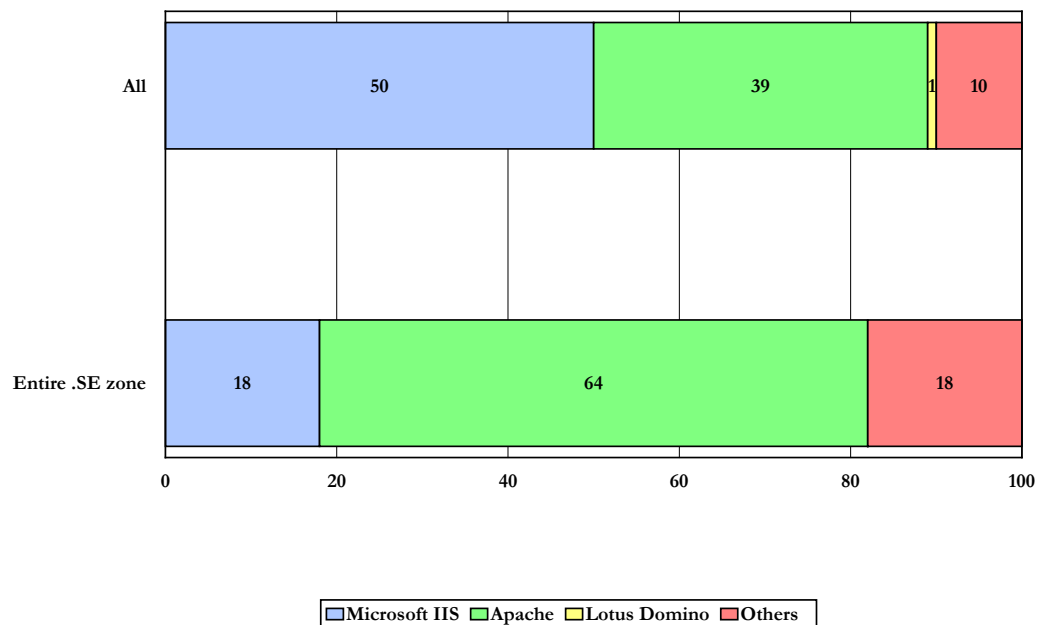


9.3 Differences in the use of software for web servers

The difference between which software is used for web servers, whereby Microsoft IIS dominates the test group and the .se zone as a whole resembles that seen in the rest of the world, where Apache is the dominant software, remained the same as in 2010. Microsoft IIS lost some ground to Apache and other software.

Lotus Domino declined further, from 2 percent in 2010 to 1 percent in 2011, while the category Other increased.

Graph 20: Software for web servers

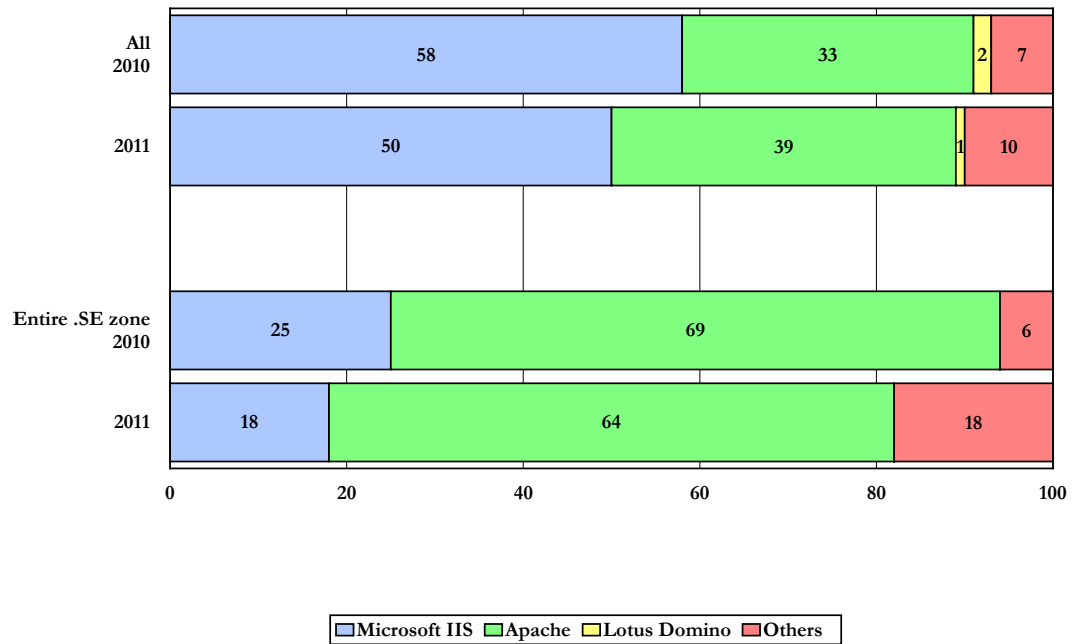


In Graph 21, we performed the same comparison, but for 2010 and 2011. In this comparison, we can state that Microsoft IIS lost ground both in the survey group and in the comparative group. However, it maintained very strong ground in the survey group.

The Other category rose even further for the comparative group and was three times larger in 2011 than in 2010. This indicates that other software is available that is also gaining in popularity.

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

Graph 21: Software for web servers – changes over time



10 Advice and recommendations

After performing yet another round of tests with relatively positive results compared with 2010, we still see a strong need for greater coordination of various stakeholders in order to improve security and reachability on the Swedish part of the Internet and, not least, potential for major gains in efficiency-enhancements and cost savings. In particular, we see opportunities for extensive efficiency gains and cost savings. In this area, we hope that the government's digital agenda will have a positive impact on developments.

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

- Critical resources in Sweden should have nameservers that are connected to several service providers simultaneously; for example with the use of Anycast technology. 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 points where these could be connected as an extra measure to create redundancy. Such a function could be regulated by agreement.
- Implement joint procurement functions for virus checking and spam filtering, subject to the requirement that the servers be located in Sweden. This would be more efficient and probably save resources and make it easier to conduct audits. It would also mean that sensitive government authority information would not leave the country.
- Issue guidelines on what is acceptable in terms of managing spam and virus filtering in public administrations. It should be unacceptable for Swedish government authorities and municipalities to send their e-mail abroad, at least not without imposing relevant, uniform requirements for transport 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 over IPv6 and promptly establish plans for a systematic transition to IPv6 in the entire public administration. This process itself is an operation lasting 12-18 months.
- Protect web servers with certificates issued by generally accepted certificate authorities and maintain control of their validity. A Swedish authority of this nature would be preferable.

- Introduce DNSSEC for domains in public administration.

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.

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

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

Appendix 1 - Abbreviations and glossary

ADSP	Author Domain Signing Practices are used to detect unauthorized removal of the signature in DKIM.
Child zone	The underlying <i>zone</i> – for example, .example.se is the child zone of the parent zone .se.
BCP	Best Common Practice, industry standard.
DKIM	Domain Keys Identified Mail. DKIM enables e-mail servers to send and receive electronically signed e-mail.
DNS	Domain Name System. An international, hierarchically designed, distributed database that is used to find information about allocated <i>domain names</i> 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 <i>Registry</i> that states which <i>nameservers</i> are to respond to requests for a certain <i>domain</i> .
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 <i>Nameserver</i> .
Domain	The designation of a level in the domain name system.
Domain name	A unique name, comprising parts of a name, in which a domain at a lower level in the domain name system, comes before a higher level domain. A registered <i>domain name</i> is a <i>domain name</i> that is allocated to a certain <i>registrant</i> .
Parent zone	The overlying <i>zone</i> – for example, .se is the parent zone of example.se. See also <i>Child zone</i> .
IP address	Numerical address that is allocated to each computer that will be reachable over the Internet. Available as IPv4 and IPv6 addresses.
Nameserver	A computer with programs that store and/or distribute <i>zones</i> , and that receives and responds to domain name requests.
Nameserver operator	An operator that provides a <i>DNS function</i> to Internet users.
Resolver	The software that translates names to <i>IP addresses</i> 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 hierarchy. A <i>zone</i> comprises a cohesive part of the domain name tree that is administered by an organization and stored on its <i>nameservers</i> .
Zone file	A data file containing the information required about a <i>zone</i> that enables the use of <i>DNS</i> addressing.

Appendix 2 - About DNS and the survey

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

The considerable interest shown in the results of the 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 fifth consecutive year. It is part of a long-term project called the Health Status Project.

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

DNSSEC

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

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

.SE’s launch of 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 crucial reason why our tests focus specifically on the quality of DNS.

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

IPv6

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

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

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

IPv4 addresses were officially exhausted as early as in February 2010. Accordingly, we also examined the current expansion of IPv6 in Sweden in greater detail.

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

Services for e-mail and the Internet

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

improve the quality of e-mail-related services in general by pointing out possible configuration problems, weaknesses in software and deviations from standards for both system administrators and end-users.

Appendix 3 - About DNSCheck test tool

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

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

Other tools being used include Page analyzer and Whatweb. Page analyzer measures performance and performance affecting parameters, such as the number of external resources loaded and the sizes of the resources. Whatweb analyzes web technology.

Appendix 4 - Industry standard for high-quality DNS service

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

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

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

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

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

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

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

Explanation: NS records are used in the overlying zone to transfer responsibility for (delegate) a certain domain to other servers. According to DNS documentation, this list of computers should also be found in the zone file that "receives" the responsibility and that contains other data about the zone. The lists must be kept synchronized so that all NS 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 nameservers 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: DNS usually functions even if this error exists. However, the existence of this error in a zone indicates inadequate administrative procedures of the party responsible for the content of the domain’s DNS.

4. Serial numbers for zone files

Recommendation: All nameservers listed with NS 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 is the acronym for Start of Authority.

Consequence: If the nameservers are not synchronized and do not have the same version of the zone file, the entity submitting a query about a domain risks not receiving a response. Reachability 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 DNS due to an individual domain.

6. Reachability

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

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

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

Appendix 5 – More information about DNSSEC

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

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

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

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

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

Accordingly, there is no doubt that 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 national top-level domain to sign its zone with DNSSEC and in 2007, we were also the first to offer DNSSEC to our domain holders. We currently have some 30 resellers (registrars) that offer DNSSEC.

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

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



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

What DNSSEC protects against

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

For ordinary users, DNSSEC reduces the risk of being defrauded, for example, when conducting bank transactions or shopping on the Internet, since it is easier for the user to determine whether he or she is really connected to the correct bank or store and not to an impostor.

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

What DNSSEC does not protect against

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

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

.SE's role in DNSSEC

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

underlying zones. This is comparable with the management of NS records in DNS.

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

Further information on .SE's DNSSEC service is available at <https://www.iis.se/en/domaner/dnssec>.

.SE provides additional information on DNS vulnerabilities at <https://www.iis.se/en/domaner/dnssec/kaminskybuggen> The website's features include a link to a movie that demonstrates how an attack is carried out and the ability to test whether the resolver being used is vulnerable to the Kaminsky bug.

<http://www.youtube.com/watch?v=29IhLOhnclY>

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 DNSSEC Deployment Initiative is distributed regularly at:

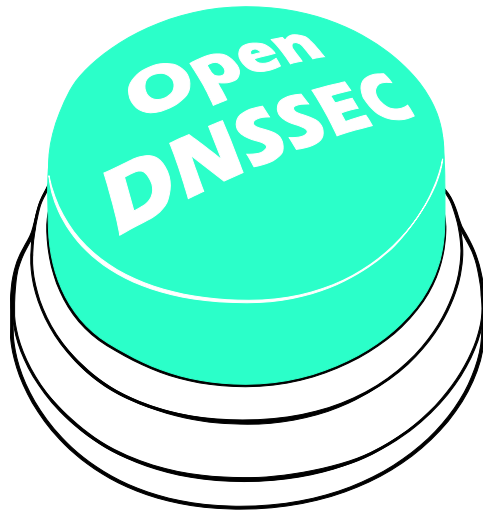
<http://www.dnssec-deployment.org/>

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

OpenDNSSEC

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

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



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

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



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

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

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

Appendix 6 - Open recursive nameservers

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

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

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

Pointers to further information

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

Secure Domain Name System (DNS) Deployment Guide

<http://csrc.nist.gov/publications/nistpubs/800-81r1/sp-800-81r1.pdf>

DNS Amplification attacks

An excellent description of how these attacks occur and what they entail.

<http://www.isotf.org/news/DNS-Amplification-Attacks.pdf>

Official advice from the US CERT

The Continuing Denial of Service Threat Posed by DNS Recursion

http://www.us-cert.gov/reading_room/DNS-recursion033006.pdf

ISC BIND. Here you can find source codes and binaries for BIND and links to highly interesting and useful information.

<https://www.isc.org/downloads/all/>

BIND 9 Administrator Reference Manual.

Includes examples of configuration, practical tips and detailed descriptions of BIND functions.

<http://oldwww.isc.org/index.pl?/sw/bind/arm95/index.php>

Appendix 7 - Action against spam

DKIM

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

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

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

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

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

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

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

SPF

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

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

Based on this information, the receiving server can determine the fate of the message, such as refusing to accept the message or sorting it as spam. The SPF standard does not define what will happen to messages that do not meet the SPF validation criteria.

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

Appendix 8 - Actions for transport security

Electronic mail

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

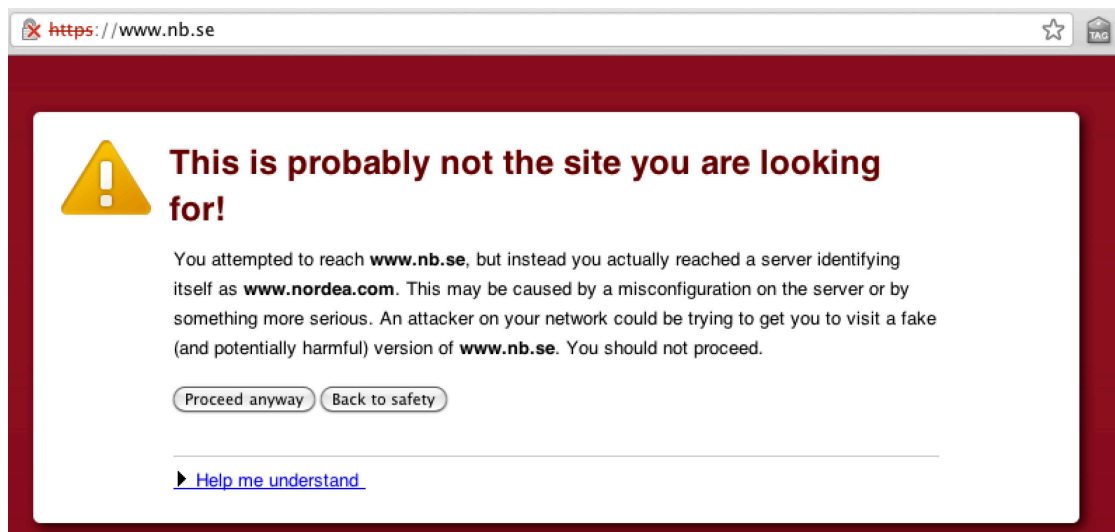
Additional protection is required if the sender wants to send e-mail that nobody else can read, not even those responsible for the e-mail system (or those who “work at the post office”). In these cases, the entire letter can be encrypted by “gluing the envelope shut and sending it by registered letter,”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

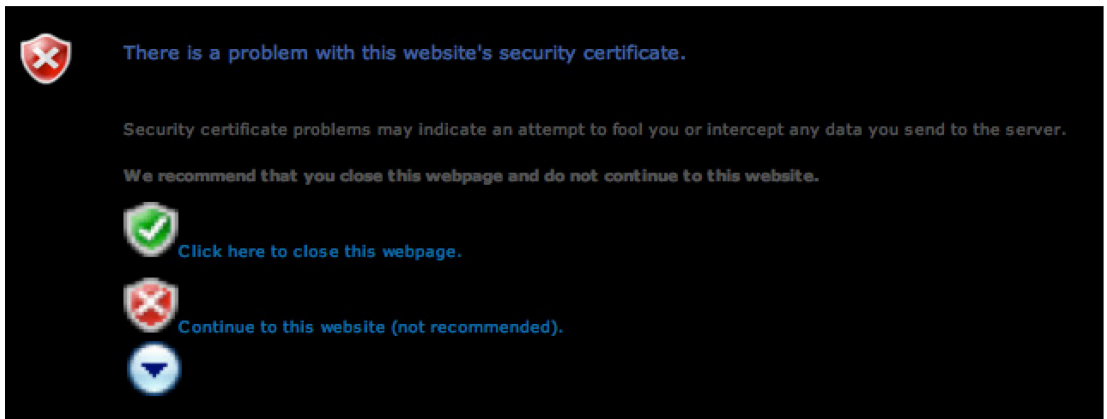
Web traffic


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

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

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







 **There is a problem with this website's security certificate.**

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

 [Click here to close this webpage.](#)

 [Continue to this website \(not recommended\).](#)

