Ministerie van Economische Zaken

SAFEGUARDING THE .NL DOMAIN

Analysis and action

Bart Vastenburg (SIDN)
Thomas de Haan (Ministry of Economic Affairs, DG for Energy & Telecom)
Rick de Rooij (Verdonck, Klooster & Associates),

10 June 2008

current position	Definitive
version	1.0
internal review	Peter Hasperhoven (VKA), Antoin Verschuren (SIDN)

Contents

1 Introduction 3
- 1.1 Background 3
- 1.2 Purpose 3
- 1.3 Methodology 3
- 1.4 Structure of this report 4

2 The *.nl* delegation 5
- 2.1 Introduction 5
- 2.2 Current position 5
  - 2.2.1 Significance 5
- 2.3 Approach 6
- 2.4 Measures 8

3 Name Server Function (NSF) 9
- 3.1 Introduction 9
- 3.2 Current position 9
  - 3.2.1 Significance 9
  - 3.2.2 Concerns 9
- 3.3 Approach 11
- 3.4 Measures 11

4 Data entry function (DEF) 16
- 4.1 Introduction 16
- 4.2 Current position 16
  - 4.2.1 Significance 16
  - 4.2.2 Concerns 16
- 4.3 Approach 16
- 4.4 Measures 17

5 Registration policy 19
- 5.1 Introduction 19
- 5.2 Current position 19
  - 5.2.1 Significance 19
  - 5.2.2 Concerns 19
- 5.3 Approach 20
- 5.4 Measures 20

6 Intellectual property rights 22
6.1 Introduction 22
6.2 Current position 22
6.2.1 Significance 22
6.2.2 Concerns 22
6.3 Approach 23
6.4 Measures 23
6.4.1 Liability risk reduction 23
6.4.2 Safeguarding intellectual property rights 23

7 Conclusions 24
7.1 Stability 24
7.2 Redelegation 24
7.3 Division of the organisation 24
7.4 Organisational arrangements 25

8 Recommendations 26
8.1 Consultation 26
8.2 Consolidation of association with the Netherlands 26
8.3 Formal agreement 26
8.4 Business continuity 27
8.5 Last resort 27

Annex A: Summary of measures 28

Annex B: Last resort scenario 30

1 Introduction

1.1 Background

On 24 February 2005, the Minister of Economic Affairs, L.J. Brinkhorst, and the President of the Foundation for Internet Domain Registration in the Netherlands, C.M. Prins, signed a Statement of Intent[1]. This marked the start of a joint project to develop proposals regarding arrangements and further action aimed at assuring the continuity of the .nl domain[2] and ensuring the domain's continued association with the Netherlands. The Statement of Intent built upon a position paper drawn up by a joint SIDN-Ministry working group in October 2004. The position paper led to establishment of the project "Safeguarding the .nl Domain", of which this report is the outcome.

1.2 Purpose

The purpose of this document is to set out all the ways in which the .nl domain is or could be safeguarded, within the spheres of influence of the Dutch Government and SIDN. The project "Safeguarding .nl Domain" was set up to develop proposals regarding arrangements and further action aimed at assuring the continuity of the .nl domain under abnormal circumstances, formalising the relationship between SIDN and the Dutch state, and ensuring that the .nl domain continues to be associated with the Netherlands. The intention was that the proposals should address the concerns and risks identified in the position paper as not being covered by the existing legal or operational safeguards. Where safeguards that have yet to be implemented are concerned, this report may be regarded as a point of reference and a starting point for implementation.

1.3 Methodology

In the preparation of this document, it was decided that the stock list presented in the above-mentioned position paper should be used as the starting point for the project. Working from the position paper, including the stock list, a preliminary inventory was produced and the possible strategies categorised. SIDN and the Ministry of Economic Affairs worked closely together to detail these possible strategies and to define the associated courses of action.

---

[1] http://www.ez.nl/Onderwerpen/Elektronische_communicatie/Nummers_en_domeinnamen/Domeinnamen?rid=141845

[2] The .nl domain is a so-called country-code top-level domain (ccTLD).

Courses of action

The courses of action described in this document are aimed at the risks identified in the stock list, with the following three goals:

- **Removing** the risk by, for example, cutting off its source.
- **Avoiding** the risk by reducing the likelihood of manifestation.
- **Preventing** or **mitigating** the consequences of manifestation.

The selected measures are aimed first at removing the possible causes of an unstable phase, i.e. a phase in which the party currently responsible for the .nl top-level domain, SIDN, is no longer able to provide reliable services. Where the sources of risk cannot be removed, ways of reducing the likelihood of risk manifestation have been sought. Finally, attention has been given to ways of minimising the implications of the services that SIDN provides being compromised and subsequently restored, possibly through another organisational vehicle.

Measures aimed at the removal and avoidance of risk generally require implementation during the stable phase, as defined in the stock list. Measures whose object is management of the consequences of adverse events will normally belong to the unstable and transition phases.

1.4 Structure of this report

The structure of this document is based on the stock list. The stock list's subject areas are reflected in this document's section topics: the .nl delegation is dealt with in section 2, name server functions in section 3, the data entry function in section 4, registration policy in section 5 and intellectual property rights in section 6.

Each of these five sections is structured as follows: The first subsection contains a brief description of the topic. This is followed by a subsection outlining the current position, the importance of the topic, and the associated risks and concerns. In the third subsection, the preferred approach is defined in more general terms, before the corresponding measures are set out in the fourth subsection. In each section, there is also a table summarising all the relevant measures.

The final section contains the project team's conclusions and recommendations.

The report has two annexes. Annex A is a table summarising all the measures referred to in the report. Annex B describes a last resort scenario, in the context of which a number of powers are defined, which it is agreed the state should assume in the event of an unstable phase. The annex also specifies the circumstances under which an unstable phase may be deemed to exist and describes the escalation procedure to be followed if the parties disagree about the existence of an unstable phase.

2 The .nl delegation

2.1 Introduction

In the present context, delegation means control over the .nl top-level domain in the IANA root zone file.

2.2 Current position

Since 1986, the registration of.nl domain names and the provision of associated services have been undertaken in the Netherlands for the benefit of the local Internet community. Since 1996, these activities have been the responsibility of SIDN, and the Foundation has held the IANA delegation for the .nl top-level domain. Over time, the domain has grown considerably and the associated services have been expanded and professionalised.

2.2.1 Significance

There are two important issues associated with the delegation:

1. The existence and technical functionality of the .nl country-code top-level domain (ccTLD) within the domain name system
2. The identity of the delegation holder

For the continuity of the .nl domain, clarity and stability concerning the delegation holder is desirable.

Concerns

If the delegation were (temporarily) open, this would have an adverse effect on the stability of the .nl domain, undermining confidence in and the significance of the .nl zone. ICANN's redelegation process is politically driven to a considerable extent, and its outcome is not always predictable. This unpredictability is politically undesirable for the continuity of the .nl domain. The point should be made that we are not concerned here with revision of ICANN's redelegation procedure, as set out in ECP-1, but with preparedness for implementation of the process steps in the event of redelegation.

Risk profile (likelihood and impact of manifestation)

It is unlikely that government involvement in delegation of the .nl domain will ever be necessary in order to protect the Netherlands' general social and macroeconomic interests. ICP-1 clause f[3] specifies a small number of circumstances in which IANA would be entitled to review the .nl domain's delegation. Such a course of action would potentially give rise to financial and/or organisational problems, which could compromise SIDN's ability to manage the domain appropriately. The importance of the .nl domain is now such that, in exceptional circumstances, significant liabilities could arise, thus threatening SIDN's financial continuity. If the Foundation were ever to become insolvent, it might not be able to manage the domain in accordance with IANA

[3] ICP-1 clause f: *Revocation of TLD Delegation. In cases where there is misconduct, or violation of the policies set forth in this document and RFC 1591, or persistent, recurring problems with the proper operation of a domain, the IANA reserves the right to revoke and to redelegate a Top Level Domain to another manager.*

guidelines; this in turn could lead to the inception of a redelegation procedure by IANA. In the scenario described, other triggers could occur, such as acting against the interests of the local Internet community (LIC); cf Annex B.

2.3 Approach

Where the .nl delegation is concerned, the best approach is the implementation of measures aimed at minimising the likelihood that redelegation will ever be necessary and at making the outcome of any redelegation process that might prove necessary more predictable. This can be achieved by increasing stability, consolidating the domain's association with the Netherlands and being prepared to intervene in any redelegation process that might prove necessary.

Increasing stability

Both SIDN and the local Internet community (including the Dutch government and the wider community) have an interest in the stability and continuity of services associated with the .nl top-level domain. All the parties concerned should therefore seek to minimise the risk of discontinuity. The Dutch government should contribute to action taken in this context.

One important thing that SIDN could do, would be to adopt a structure in which the .nl delegation is held by a distinct "guarantee foundation", which is isolated from the risks associated with commercial service operations. The government could also make a major contribution to the continuity of the .nl domain by acting as a financial guarantor for SIDN. A guarantee arrangement could be made, similar to that previously established in respect of KPN Telecoms' wire infrastructure.

Both measures have been carefully considered. SIDN has concluded that the cost and trouble associated with the division of its organisation are not (currently) justified by the potential benefits. Meanwhile, the Ministry of Economic Affairs has reached the conclusion that a financial guarantee is not appropriate at the present time. The Ministry regards the extension of a guarantee as an extreme measure, to be taken only if absolutely necessary. In view of SIDN's robust present position, the Ministry does not see any reason for a guarantee at this point in time.

Although it has been decided not to adopt the measures identified above, they are described in this report, because either or both could become desirable at some point in the future.

Consolidation of association with the Netherlands

In the Statement of Intent, SIDN and the Ministry expressed their mutual wish that .nl services should remain closely associated with the Netherlands and available to Dutch users. To this end, an undertaking was made that SIDN's .nl services would continue to be provided from within the Netherlands. The under lying principle, that control of a ccTLD is a national matter, is widely supported around the world. This principle is established within and referred to by various relevant international bodies[4] and formally included in the policies of certain countries[5]. The Dutch

[4] E.g. the GAC principles and guidelines for the delegation and administration of country-code top level domains, http://gac.icann.org/web/home/ccTLD_Principles.rtf

[5] The principle has a statutory basis in Switzerland, Norway, Finland and elsewhere; it is also included in the published policy of the US (see http://www.ntia.doc.gov/ntiahome/domainname/usdnsprinciples_06302005.htm).

government should consistently use its influence to promote this principle in international forums and should possibly enshrine it in public law. SIDN is to adhere to the principle in the context of its activities within ICANN, IANA, CCNSO and forums such as CENTR.
It is also important that Dutch law governs both SIDN's activities as the .nl delegation holder and its relationships with .nl registrars and registrants.
It must be recognised that the .nl Internet community includes registrants resident or based outside the Netherlands. SIDN's expectation is that the percentage of registrants that have direct ties with the Netherlands will continue to diminish over time. However, the majority are likely to remain associated with the country for the foreseeable future, making it important that the domain is governed by Dutch law.
It may nevertheless become commercially or operationally desirable for SIDN to seek working alliances with delegation holders in other countries.

Last resort

The Dutch government should also be prepared for the possibility that it might under certain circumstances need to involve itself in redefinition of SIDN's role in the event of redelegation of the .nl domain. To this end, the government and SIDN should jointly define trigger moments: circumstances under which an unstable situation and a transition phase may be deemed to exist. The action to be taken by the government under such circumstances should be outlined and made known to the relevant parties (LIC, ICANN/IANA), with a view to making the outcome more predictable, which would have continuity benefits, certainly from a political viewpoint. An outline of the redelegation process scenario, complete with trigger moment definitions, is presented in Annex B. The trigger moments can be used as a reference framework for the development of an early warning system, so that threats and possible substantial problems may be identified as early as possible (see below).

Consultation and early warning

Both parties stand to benefit from meeting once or twice a year to discuss the present situation with regard to the continuity of the .nl domain. The following items should also be addressed in the context of those discussions:

- SIDN's annual report
- DGET's annual report and work plan

It is also desirable that the respective contact persons have less formal and possibly more frequent talks regarding ongoing issues. Communication between the parties should feature an early warning system, in the context of which (1) SIDN should inform the government at the earliest possible stage about threats to and substantial potential problems for the .nl domain, and (2) the government should inform SIDN at the earliest possible stage about possible government intervention that is of particular relevance to the .nl domain.

2.4 Measures

The following table lists the measures that are relevant in relation to this topic. Each measure is briefly described, the responsible party is identified, the stock list phase is given, and details are provided of the intended effect, the time required and the estimated cost.

No.	Description	Who	Stock list	Result	Time	Cost
2.1	Create separate guarantee entity	SIDN	A.1 and A.2	Greater stability, but not currently practicable	N/a	N/a
2.2	Provide government guarantee	Government	A.1.2	Greater stability, but not currently practicable	N/a	N/a
2.3	Retain registered office in the Netherlands	SIDN	A.1.2 and E.1	Reinforcement of association between the .nl domain and the Netherlands; formal expression of support for the association in a joint statement	N/a	N/a
2.4	Ensure continued applicability of Dutch law	SIDN	A.1.2 and E.1	Reinforcement of association between the .nl domain and the Netherlands; formal expression of support for the association in a joint statement	N/a	N/a
2.5	Increase influence within ICANN	Government	A.1.3	Greater influence over any future redelegation process	Long term	-
2.6	Prepare and formally agree Accountability Framework with ICANN	SIDN	A.1.1	Greater stability	Implemented	Not yet known
2.7	Emphasise and formalise association between *.nl* and the Netherlands in dealings with ICANN	Government	A.3.1	Reinforcement of association between the .nl domain and the Netherlands	Long term	-
2.8	Prepare redelegation process scenario, complete with trigger moment definitions and summary procedural description	SIDN - Government	A.2.1 2, A.2.2 and A.2.4	Greater influence over any future redelegation process	Implemented except for outline procedure	Not yet known
2.9	Inform LIC and ICANN about the scenario	SIDN - Government	A.2.1	Acceptance of scenario as blueprint for any future redelegation	2-3 months	-

3 Name Server Function (NSF)

3.1 Introduction

The Name Server Function (NSF) is vital to the accessibility of the .nl domain. The NSF entails the translation of host and domain names into IP addresses, i.e. practical utilisation of the DNS information (DNS records) published by SIDN.

3.2 Current position

Distinction may be made between the role that ICANN/IANA plays (international dimension) and the role that SIDN plays (national dimension).

3.2.1 Significance

The NSF is the basis of all .nl services. Failure of the NSF would lead to the total inaccessibility of all services that rely on the .nl domain.

3.2.2 Concerns

The main reason for concern is that any failure of the NSF would have far-reaching consequences. The non-availability of all services that depend on the .nl domain would have very serious implications for the Dutch economy and for public order in the Netherlands.

International/Global NSF

There are currently thirteen authoritative root servers (see http://www.root-servers.org/), which are separately maintained by independent parties. Because the working of these servers is beyond the control of the project parties (and even beyond the control of ICANN), they are not considered in this report. The Accountability Framework agreed between SIDN and ICANN, which regulates the continuous availability of the .nl zone within the root, does fall within the scope of the report, however.

Local NSF

SIDN generates a new .nl zone file every day, which is propagated by the hidden primary server to seven authoritative .nl name servers, as illustrated below in

Figure 1 Technical infrastructure supporting the NSF.

The NSF could become unreliable or even completely non-functional under the following circumstances:

1. No .nl name server is reachable: If this were to happen, the .nl domain would be completely non-functional.

2. The zone file is corrupt and no longer reliable: If IP addresses listed in the zone file are incorrect, the relevant domain names will not be reachable. If the majority or all of the IP address associations were to become corrupted, the .nl zone would be completely inaccessible. The likelihood of comprehensive corruption of the .nl zone file is very small, but the potential impact is very great. By contrast, given the frequency with which amendments are made, the likelihood of isolated errors is quite great, but the impact of such errors will usually be minor. Nevertheless, an isolated error can have serious implications for an individual registrant, which could in turn lead to damages being claimed from SIDN.
3. The zone file is empty: Address translation is not possible and the .nl domain is unreachable. The likelihood of this happening is very small, but the potential impact is very great.
4. The zone file is no longer up to date or ceases to be updated: If the name servers are working from an outdated zone file, domain names whose translation has not been updated will be reachable only at their old IP addresses. Only a small proportion of the zone would be affected. The likelihood of such an eventuality is small, and its impact would be minor.

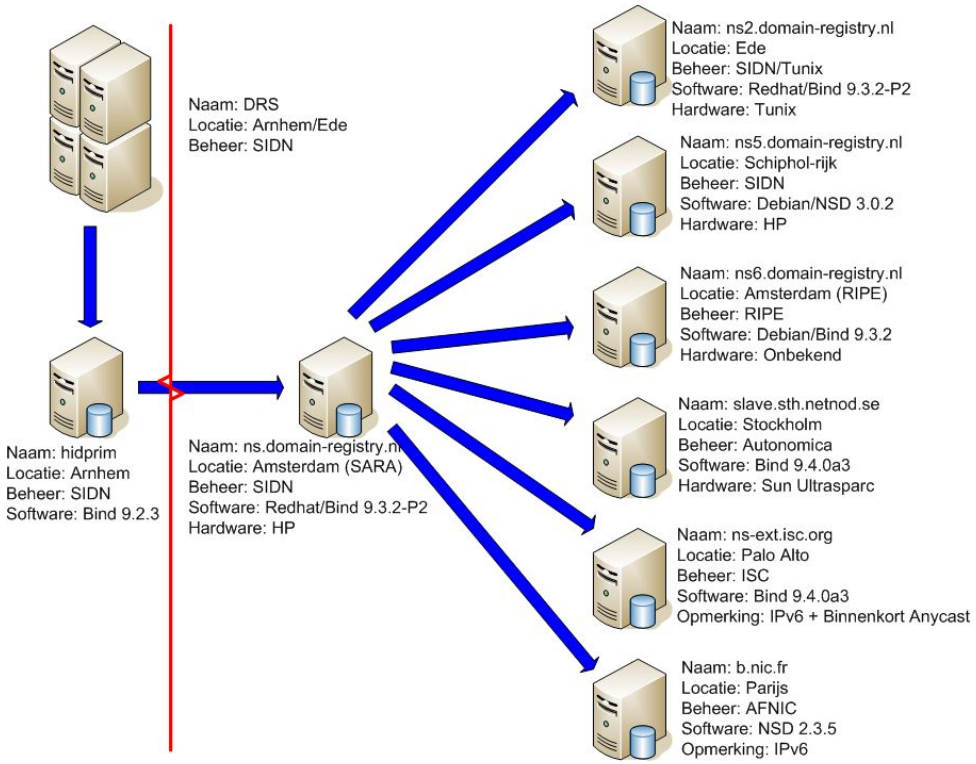

Figure 1 Technical infrastructure supporting the NSF

3.3 Approach

The body of measures has the following objectives:

1. Ensuring that withdrawal of the support operation, as currently provided by SIDN in its present form, does not lead to interruption of the NSF.
2. Achieving redundancy within technical name server infrastructure, in order to minimise the impact of technical NSF failures.
3. Providing physical and logical security in order to deter or counter attempts to sabotage the NSF, and to detect and rectify any damage that might nevertheless be done.
4. Introducing checks to the zone file generation and propagation procedures with a view to eliminating errors as far as possible, and detecting and correcting those that do nevertheless occur.
5. Investigating the vulnerability of the name server function.

The approach outlined above is intended to ensure that the NSF for the .nl domain is continuous, reliable, accurate and up-to-date, both when SIDN is operating normally and when it is not (i.e. during an unstable or transition phase). Each of the objectives set out above is considered more closely below.

3.4 Measures

Operational failure of SIDN

As indicated in section 2 (The .nl delegation), SIDN has considered the creation of separate legal entities to undertake risk-bearing operational activities and to hold the .nl delegation. The added stability created by such an arrangement could have benefits for the NSF as well. It may be worth establishing the extent to which organisational separation would allow the zone file to be made available for a reformed or successor organisation during any unstable or transition phase.

No.	Description	Who	Stock list	Result	Time	Cost
3.1	Secure NSF availability by organisational separation	SIDN	B.1 and B.2	Greater stability, but not currently practicable	N/a	N/a

Redundancy within the technical infrastructure

SIDN has also made contractual or less formal arrangements with a number of the parties regarding the hosting of secondary name servers. The parties in question[6] differ from one another in various respects, virtually eliminating the possibility of any single cause leading to the non-functionality of all .nl zone files.

- The parties are geographically well distributed: two in the Netherlands (Arnhem and Amsterdam), two elsewhere in Europe (Paris and Stockholm) and two in North America (Palo Alto and Washington).
- Some of the arrangements are commercial and some are peer-to-peer arrangements based on industry best practices. Arrangements of the latter kind are important because, in the event of SIDN's insolvency, the peer-to-peer partners would continue their services for the benefit of the Internet community, whereas commercial partners would withdraw their support. There will always be parties that are willing and able to support or take over the name server task at short notice, on a temporary or long-term basis. As a result, at least some of these services would even remain outside the reach of a receiver if SIDN were wound up.
- The various secondary name servers use different hardware configurations and operating systems. This minimises vulnerability to hardware-related problems, or to OS-specific virus attacks, resolver-related attacks and so forth.
- Separate backbones are employed, which again enhances resilience.
- The nature of the services is such that there is constant **public** monitoring. As a result, any problems come to light very quickly, enabling any recovery processes that may be required to be instigated promptly.

SIDN has also started to implement Anycast: a system whereby a globally dispersed cluster of nodes (servers) collectively function as a single logical domain name server. The great advantage of such an arrangement is that the cluster of nodes is much more resistant to large-scale DDOS attacks. The failure of one or more nodes results in the non-availability of the .nl domain only for the limited area served by the node(s) in question. The other nodes in the same cluster remain operational, as do the other DNS servers, so that the .nl domain remains accessible. This set-up has already shown its worth when some of the root servers recently came under attack, but there was no appreciable service degradation. The planned new structure is illustrated in
Figure 2 Planned technical infrastructure for the NSF.

[6] The parties that host *.nl* zone files are: AMS-IX (Sara in Amsterdam), SIDN (Schiphol-Rijk and Arnhem), RIPE (Amsterdam), AFNIC (Paris), ISOC USA (Palo Alto) and Netnod SE (Stockholm).

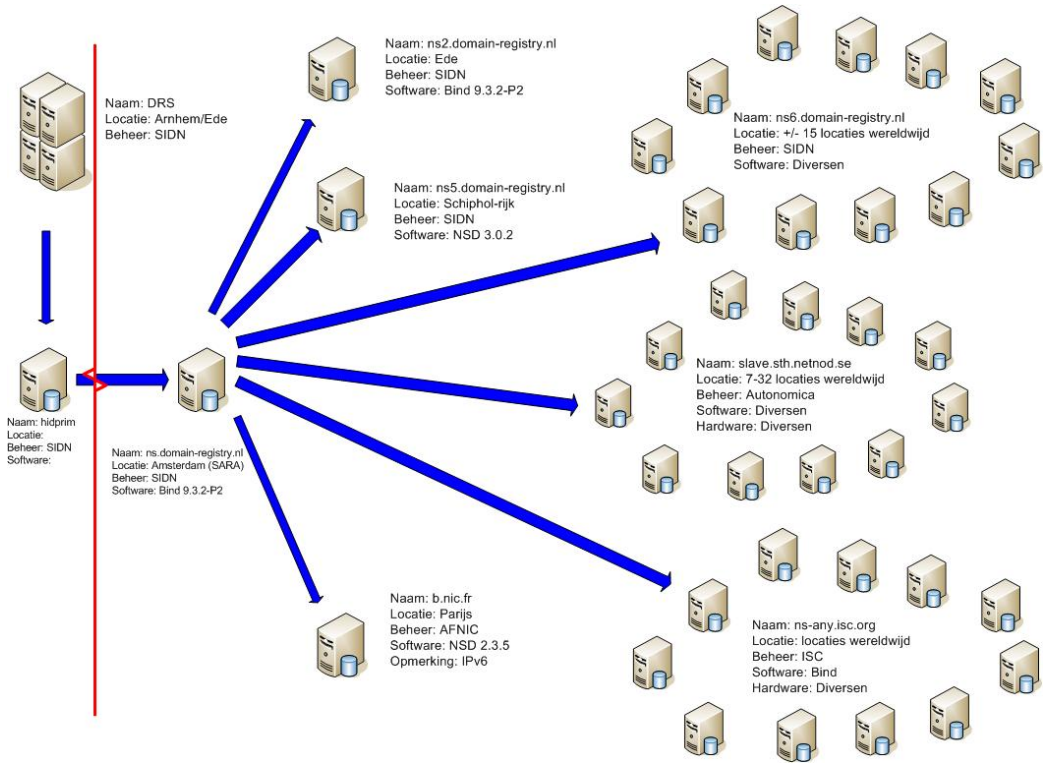

Figure 2 Planned technical infrastructure for the NSF

No.	Description	Who	Stock list	Result	Time	Cost
3.2	Ensure physical redundancy within the name server portfolio (particularly through Anycast implementation)	SIDN	C.2	Resilience	Implemented	- € 165k/yr
3.3	Ensure logical redundancy: support by dissimilar partners under dissimilar arrangements	SIDN	B.1	Resilience	Implemented	-
3.4	Use Anycast servers	SIDN	C.2	Resilience	Q4 2007	Not yet known

Security

The security arrangements for components under SIDN's control include the following:

- All SIDN servers, including the Domain Registration System (DRS) and the name servers are at high-availability locations with strict access controls.
- All SIDN servers are provided with state-of-the-art protection against Internet attacks.
- SIDN has set up a mirror site to minimise vulnerability.

No.	Description	Who	Stock list	Result	Time	Cost
3.5	Secure access for authorised registrars	SIDN	C.2	Security	Implemented	-
3.6	Secure physical access to SIDN server locations	SIDN	C.2	Security	Implemented	€ 25k
3.7	Provide logical security (firewalls etc)	SIDN	C.2	Security	Implemented	€ 30k and € 75k/yr
3.8	Set up mirror site	SIDN	C.2	Resilience	Implemented	N/a

Accuracy of the zone file

The final set of measures associated with the name server function is aimed at ensuring the accuracy of the data in the zone file. The measures in question are as follows:

- Each time that the zone file is generated, an integrity check is performed to ascertain whether the new file meets certain criteria: it must not be empty, it must be no more than x% modified, it must be no more than y% larger or smaller than the previous version, it must contain only syntactically correct addresses and so on.
- In the course of its operations, SIDN is constantly considering the desirability of broadening the integrity check. Wherever appropriate, criteria are added or refined.

No.	Description	Who	Stock list	Result	Time	Cost
3.9	Perform zone file integrity checks	SIDN	C.2	Integrity	Implemented	€ 4k
3.10	Broaden zone file integrity checks as appropriate	SIDN	C.2	Reliability	Continuous	-

Business continuity

As part of the project, a vulnerability analysis was performed. This involved determining which DNSs (or which clusters in an Anycast set-up) were and were not likely to remain in service if each of the potential threats identified were to materialise. The object of the exercise was to provide information that would enable SIDN to ensure that, in the event of any single threat[7] materialising, at least two servers would continue to function normally. The results are tabulated in annex B. It is desirable that the analysis should periodically be repeated.

With a view to assuring operational continuity, SIDN is also setting up an integrated (internal) business continuity process. This process provides ongoing protection for the continuity of the information supply by means of an integrated security strategy, covering all matters within SIDN's sphere of influence. Periodic vulnerability analyses are a feature of this strategy. In addition, the government (in conjunction with SIDN where possible) will investigate and develop a plan for the provision of additional support for the mitigation of risks and circumstances over which SIDN has no control.

[7] Individual threats have been assumed because, although it is theoretically possible for several simultaneous problems to cause the failure of all the DNS servers, this is not considered a realistic scenario.

No.	Description	Who	Stock list	Result	Time	Cost
3.11	Undertake vulnerability analysis and business intelligence management	SIDN	C.1.1	Reliability	Analysis implemented; BCM from 2008	€ 40k
3.12	Periodically repeat vulnerability analysis	SIDN	C.1.1	Reliability	Continuous	€ 17k

4 Data entry function (DEF)

4.1 Introduction

The .nl domain is a dynamic entity. Every day, new domain names are added, existing registrations are amended and unwanted ones are deleted. The data entry function (DEF) has been set up by SIDN to reliably receive, process and record register amendments.

4.2 Current position

SIDN has established a Domain Registration System (DRS), to which registrars have secure access in order to make authorised amendments. The DRS is the data source for daily generation of the .nl zone file.

4.2.1 Significance

Complete failure of the DEF would prevent the automated amendment of the data in the .nl zone file.[8] Although this would be inconvenient for any party with an interest is having an amendment made, it would not have major implications for the national economy. Indeed, even if the DEF were to fail permanently, no large-scale economic problems would result: existing, functional domain names would remain unaffected as long as the NSF remained operational. However, no new .nl domain names could be registered, and existing .nl registrations could not be modified. Parties wishing to register or transfer domain names would consequently use other TLDs, and the role of .nl would diminish.

4.2.2 Concerns

Neither temporary nor permanent failure of the DEF would be a macroeconomic disaster for the Netherlands. Such an event would nevertheless be politically undesirable, because it would undermine confidence in the .nl domain. The continuity of the DEF is therefore a business concern for SIDN and a socio-economic concern for the Dutch government.

4.3 Approach

The approach to assuring the continuity of the DEF is concerned primarily with technical and organisational matters:

- Increasing technical reliability through the redundancy of systems and connections
- Physical and logical access security
- Data backups and backup systems

The aims of the various measures are:

- To eliminate single points of failure (SPoF)
- To increase resilience to human error or deliberate action

[8] It is also possible to modify the zone file directly. However, modifications have to be made with great care; direct modification is not a normal operational procedure, but something to be done in exceptional circumstances.

- To facilitate service restoration following faults

4.4 Measures

Redundancy

The duplication of all critical systems and connections enables individual failures to be rectified without interrupting the DEF. Implementation of the following items is based on the redundancy principle:

- Connections between SIDN's production environment, the external (secondary) production environment and an external (backup) mirror location with transparent alternative routing
- Two physically separate production environments, as well as an emergency backup location with near-real-time mirroring of the servers and the database

In addition, a new version of the DRS (DRS 4) has been implemented, which is designed specifically for scalability. Additional processing and storage capacity can be added without having to close down the system. Hardware and software additions and changes can be prepared in an OTAP environment.[9]

No.	Description	Who	Stock list	Result	Time	Cost
4.1	Provide duplicate connection AMS-IX-SIDN	SIDN	D.1	Availability	Implemented	€ 12k and € 49k/yr
4.2	Provide redundant routing between production environments and mirror location	SIDN	D.1	Availability	Implemented	€ 17k and € 63k/yr
4.3	Provide mirror location	SIDN	D.1	Availability	Implemented	€ 300k
4.4	Ensure scalability of DRS	SIDN	D.1	Availability	Implemented	-
4.5	Provide OTAP environment for development and modifications	SIDN	D.1	Reliability	Implemented	€ 100k

Security

The physical security measures taken by SIDN include the introduction of access control based on the use of RFID passes. SIDN will in due course further tighten its physical security by the use of, for example, camera observation of vital components, a strict policy on the issue of passes, the screening of personnel and biometric access control.

In the interests of logical registrar security, SIDN works with web forms transmitted over a secure (https) connection. SIDN also takes all obvious ICT measures to secure its services. These measures are subject to regular testing, and the recommendations are acted upon. SIDN makes use of standard components and solutions in order to ensure the ready availability of protective

[9] OTAP is an acronym based on the Dutch for Development, Testing, Acceptance and Production. An OTAP environment is a separate environment. Consequently, operations do not need to be interrupted for the development of modifications, which can be thoroughly tested and accepted before implementation, in a testing and acceptance environment that is exactly like the operational environment.

resources. Because many of SIDN's ICT activities are organised in house, the organisation has considerable relevant know-how.

SIDN has also implemented various internal organisational measures. The Foundation's internal administrative organisation is described in an AO manual, which all personnel are obliged to adhere to. A number of vital service components are subject to explicit internal functional isolation, making it almost impossible for anyone with malicious intent to gain access to the entire process.
Finally, SIDN has a healthy financial basis, with sufficient working capital to sustain its service provision.

No.	Description	Who	Stock list	Result	Time	Cost
4.6	Provide physical security, using RFID passes for access control	SIDN	D.1	Security	Implemented	€ 55k
4.7	Provide physical security, based on biometric access control	SIDN	D.1	Security	Q4 2007	€ 25k
4.8	Implement camera observation	SIDN	D.1	Security	Q4 2007	€ 25k
4.9	Screen personnel	SIDN	D.1	Security	Q4 2007	€ 7k
4.10	Use https for data input by registrars	SIDN	D.1	Security	Implemented	-
4.11	Implement testing and screening measures	SIDN	D.1	Security	Implemented	-
4.12	Use standard components wherever possible	SIDN	D.1	Security	Implemented	-
4.13	Build up in-house know-how	SIDN	D.1	Security	Implemented	-
4.14	Oblige personnel to adhere to AO manual	SIDN	D.1	Security	Implemented	-
4.15	Implement explicit internal functional isolation	SIDN	D.1	Security	Implemented	-
4.16	Maintain healthy financial position	SIDN	A.1	Stability	Implemented	-

Data backups

All DEF data is stored in a central database, which is backed up to an external location every working day. The back-up and restore procedure is regularly tested.

No.	Description	Who	Stock list	Result	Time	Cost
4.17	Maintain central database	SIDN	D.1 and D.2	Reliability	Implemented	-
4.18	Back up database every working day	SIDN	D.2 and D.3	Reliability	Implemented	-
4.19	Regularly test back-up and restore procedure	SIDN	D.2 and D.3	Reliability	Implemented	-

5 Registration policy

5.1 Introduction

The registration policy has two components, which find expression in the following two questions:

1. What alphanumeric labels are suitable and acceptable for .nl domain name registration?
2. In the event of a dispute, who is the registrant entitled to .nl services?

The answers to these questions need to take account of the fact that the .nl domain is a ccTLD with close ties to the Netherlands, and should be consistent with the generally applicable ICANN guidelines.

5.2 Current position

The basis for .nl registration policy is formed by RFC 1591, which sets the ground rules for top-level domains. In addition to its general policy rules, RFC 1591 specifies that the local Internet community (LIC) should be consulted in connection with the development registration policy.

5.2.1 Significance

A good registration policy that is aligned with the LIC is based on familiarity and the consequent reliability for the Internet community. This promotes confidence and strengthens the position of the .nl domain.

5.2.2 Concerns

The client file of registered .nl domain names has considerable commercial value. There are concerns, particularly in political circles, that the party in possession of that file (which in the future might in principle be an organisation that succeeds SIDN or a buyer) could pursue a policy geared more to its own commercial interests than to the interests of the LIC, in particular those members of the LIC with close ties to the Netherlands. This could result in the .nl domain losing its significance and existing registrants incurring damages.

Although it is unlikely, if SIDN were ever to go into liquidation, a receiver could decide to sell the client database to the highest bidder. Alternatively, SIDN might conceivably adopt a policy geared to more commercial exploitation of the database.

At present, when disputes arise concerning .nl domain names, they are settled primarily on the basis of applicable Dutch law, because all contracts between SIDN and its registrars and registrants are governed by Dutch law.

5.3 Approach

The general approach is aimed at reinforcing the ties with the LIC as far as possible, both where name policy and dispute resolution are concerned. To this end, the LIC and the registrants are regularly consulted, and SIDN is under the independent watch of a Supervisory Board[10]. The makeup of this Board ensures that it has the experience, expertise and independence needed to fulfil its obligations to SIDN and to associated parties (including the members of the local Internet community), in accordance with the applicable legislation and regulations. Furthermore, SIDN is required – both by law and by its own constitution – to work within the Dutch regulatory system. As a result, the registration policy is clearly and firmly rooted in the Dutch Internet community and the Dutch regulatory regime.

5.4 Measures

Consultation with the LIC

ICANN's delegation of the .nl domain to SIDN is based partly on SIDN's acceptance of RFC 1591. SIDN is therefore publicly bound by RFC 1591. Furthermore, SIDN has put a number of organisational measures in place. The Foundation regularly consults its registrars and, on matters of general importance, initiates dialogue with the LIC as a whole (one example being the Domain Name Debate in 2006).

SIDN intends to document, publish and accord binding status to the process by which its .nl registration policy is formulated.

The composition of SIDN's Supervisory Board is intended to provide balance and a combination of experience, expertise and independence that will enable the Board to fulfil its obligations to SIDN and to associated parties (including the members of the local Internet community).

The applicability of Dutch law means that the judiciary can use the provisions of the Dutch Civil Code to ensure that SIDN's domain name policy is fair and reasonable. Domain name disputes between registrars can be referred to the courts or settled by means of a resolution procedure that is geared to the needs of the LIC. SIDN is obliged to respect court rulings and the outcomes of the arbitration process.

No.	Description	Who	Stock list	Result	Time	Cost
5.1	Publicly agree to be bound by RFC 1591	SIDN	E.1	Legal certainty	Implemented	-
5.2	Establish a Council of Registrars	SIDN	E.1	Legal certainty	Implemented	-
5.3	Pursue dialogue with the LIC (e.g. Domain Name Debate)	SIDN	E.4	Legal certainty	Implemented	-
5.4	Give binding status to registration policy development process	SIDN	E.4	Legal certainty	2008	-
5.5	Ensure that the Supervisory Board is balanced	SIDN	E.4	Legal certainty	Implemented	-
5.6	Ensure applicability of Dutch and European law	SIDN	E.1	Legal certainty	Implemented	-
5.7	Operate dispute resolution procedure for domain name disputes	SIDN	E.1 and E.4	Legal certainty	Implemented	-

[10] Constitutional title: Supervisory Board of SIDN.

6 Intellectual property rights

6.1 Introduction

The data entry function (EDF) and name server function (NSF) depend on two databases: the Domain Name Register (the database containing details of registered domain names and their registrants) and the .nl zone file. SIDN owns the intellectual property rights to both databases. The information in the databases is therefore the legal and commercial property of SIDN.

6.2 Current position

The current legal principle is that the intellectual property rights to a database are owned by the party that compiles the database. Intellectual property rights are tradable, so the rights to the two databases could theoretically be sold. It is desirable to define measures aimed at minimising the threat to the continuity of the .nl domain during any transitional or unstable phase that might result from exercise of the corresponding intellectual property rights.

6.2.1 Significance

As indicated in the sections on the DNS and DEF, continuity is advantageous to the provision of .nl services. A dispute concerning intellectual property rights could lead to temporary or longer-term interruption of the DEF and possibly even the NSF.

6.2.2 Concerns

The economic implications of difficulties in this field are limited, but the possibility of service discontinuity due to an intellectual property rights dispute is clearly a political concern.
In section 2 (The .nl delegation), it was suggested that division of the Foundation into an operating entity and a delegation-holding entity could resolve various potential problems. However, such a move would not provide adequate protection against the possibility of problems involving intellectual property rights. The reason being that the operating entity – as the party responsible for managing the databases – would in principle be the intellectual property rights holder. To get around this undesirable situation, additional measures would have to be taken to transfer those rights to another party (i.e. the rights-holding entity). Otherwise, if the operating entity (SIDN) were to go into liquidation, for example, the receiver would be at liberty to sell the databases to the highest bidder (although any such sale would not affect the .nl delegation).

6.3 Approach

The approach is focused on (1) reducing the liability risk and the consequent risk of insolvency and (2) safeguarding the intellectual property rights themselves.

6.4 Measures

6.4.1 Liability risk reduction

SIDN has already adopted a number of measures with a view to reducing the liability risk:

- The General Terms and Conditions include liability-limiting provisions that apply to all the Foundation's agreements with registrants and registrars.
- Liability insurance has been arranged.
- Several cases have come before the courts, in the context of which SIDN has deliberately put the resilience of its position to the test, and concluded that it is adequately protected.
- SIDN has built up a resistance capability.
- SIDN has significant liquid assets and a healthy cash flow, enabling it to meet significant claims if they should be made.

Furthermore, the legal principle of proportionality works to SIDN's advantage in this context, because, in the event of a registrant suffering major losses, any attempt to recover those losses from SIDN would be seen as out of proportion to the modest fees charged by SIDN for its services.

6.4.2 Safeguarding intellectual property rights

The one further measure that might be taken would be to use an escrow to secure any future delegation-holder's right to use the databases. The acceptability and practicability of this option need to be investigated. It should be noted that a receiver would be likely to want to keep the delegation and the intellectual property rights together, because the intellectual property rights will be worth more with the delegation than without it.

No.	Description	Who	Stock list	Result	Time	Cost
	Limit liability contractually	SIDN	C.1.2	Reduced liability risk	Implemented	-
6.2	Arrange liability insurance	SIDN	C.1.2	Reduced liability risk	Implemented	-
6.3	Build up jurisprudence	SIDN	C.1.2	Reduced liability risk	Implemented	-
6.4	Build up resistance capability	SIDN	C.1.2	Reduced liability impact	Implemented	-
6.5	Maintain healthy liquidity and cash flow	SIDN	C.1.2	Reduced liability impact	Implemented	-
6.6	Investigate legal validity of an escrow	SIDN	C.1.2	Secure intellectual property rights	3 months	Not yet known
6.7	Draw up and sign escrow	SIDN	C.1.2	Secure intellectual property rights	3 months	Not yet known

7 Conclusions

7.1 Stability

It has been established that the name server function is the critical feature of the .nl domain and of SIDN's .nl services. It is also apparent that there are only two possible threats to SIDN's .nl services. First, a technical threat brought about by a concerted system attack, focusing particularly on the name server function. Second, a financial claim for an amount that is too great for SIDN to meet. Adequate measures are currently in place or under development to assure the continuity of the .nl domain against both threats.

All things considered, it may be concluded that SIDN has succeeded in creating a very stable situation.

7.2 Redelegation

The redelegation procedure remains somewhat uncertain. However, the uncertainties can be minimised, if both the government and SIDN prepare for and endorse all the steps of the process that are under national control. Once this has been done, the national procedure should be made known to ICANN/IANA; these organisations should be informed that the Dutch government and SIDN intend to follow the procedure if it should ever prove necessary.

7.3 Division of the organisation

In the context of the study, it was observed that the division of SIDN into a risk-bearing operating entity and a low-risk delegation-holding entity could be advantageous as a means of further increasing stability and assuring continuity in the event of an unstable phase. It has nevertheless been concluded that, at the present time, these advantages are outweighed by the difficulties that such a move would entail.

The Dutch government could also contribute significantly to the continuity of the .nl domain by agreeing to act as a guarantor. This possibility has been investigated and it has been concluded that, under the present circumstances, such a move would not be justified.

7.4 Organisational arrangements

The Dutch government needs to be kept up to date regarding the development of risks to the .nl domain and regarding circumstances that could lead to an unstable situation. To this end, regular contact is desirable between the government (represented by the Ministry of Economic Affairs) and SIDN.

For its part, SIDN needs to be kept up to date regarding developments within government that could lead to the revision of regulations concerning, or with the potential to influence, the services associated with the .nl domain.

It is clear that the strength of the present position and the recognition of that position by the government have increased confidence on both sides. It is important that, going forward, the basis for that mutual confidence remains secure.

8 Recommendations

8.1 Consultation

Both parties stand to benefit from meeting once or twice a year to discuss the present situation with regard to the continuity of the .nl domain. The following items should also be addressed in the context of those discussions:

- SIDN's annual report
- DGET's annual report and work plan

It is also desirable that the respective contact persons have less formal and possibly more frequent talks regarding ongoing issues. Communication between the parties should feature an early warning system, in the context of which (1) SIDN should inform the government at the earliest possible stage about threats to and substantial potential problems for the .nl domain, and (2) the government should inform SIDN at the earliest possible stage about possible government intervention that is of particular relevance to the .nl domain.

8.2 Consolidation of association with the Netherlands

In the Statement of Intent, SIDN and the Ministry expressed their mutual wish that .nl services should remain closely associated with the Netherlands and available to Dutch users. To this end, an undertaking was made that SIDN's .nl services would continue to be provided from within the Netherlands. It is also important that Dutch law governs both SIDN's activities as the .nl delegation holder and its relationships with .nl registrars and registrants.

8.3 Formal agreement

With a view to easing the government's concerns, consideration should be given to formalising the arrangements made between the parties, e.g. through the conclusion of a covenant or other agreement. To this end, a mutually acceptable vehicle should be sought and its possible content explored.

In this context, it should be recognised that SIDN sees no reason to transfer any responsibilities to the government or to grant the government additional powers.

The government should also appreciate that even an arrangement covering the provision of extra information by SIDN raises certain questions, such as:

- What does the government intend to do with the information?
- What responsibilities does the government assume when it becomes a party to the information in question?

8.4 Business continuity

It is desirable that SIDN establishes and maintains a permanent business continuity process, which provides integrated information security. Periodic vulnerability analyses should be a feature of this process. If SIDN should encounter risks and circumstances that are beyond its sphere of influence, the government must be prepared to provide assistance, insofar as it is able.

8.5 Last resort

The criteria and (escalation) processes described in Annex B are intended as a clear statement of the action that may be expected of the parties in emergency situations where the continuity of the .nl domain is under serious general threat. To make any government intervention and its outcome more predictable, the steps of the process that are under national control should be planned on a contingency basis. The defined national process steps should be translated into English and presented to ICANN/IANA as a statement of the policy that the Netherlands would wish to follow if redelegation should ever prove necessary.

Annex A: Summary of measures

The following table lists all the measures referred to in this report. Each measure is briefly described, the responsible party is identified, the corresponding stock list number is given, and details are provided of the intended effect, the likely implementation date or current position and the estimated cost (where available).

No.	Description	Who	Stock list	Result	Time	Cost
2.1	Create separate guarantee entity	SIDN	A.1 and A.2	Greater stability, but not currently practicable	N/a	N/a
2.2	Provide government guarantee	Government	A.1.2	Greater stability, but not currently practicable	N/a	N/a
2.3	Retain registered office in the Netherlands	SIDN	A.1.2 and E.1	Reinforcement of association between the .nl domain and the Netherlands; formal expression of support for the association in a joint statement	N/a	N/a
2.4	Ensure continued applicability of Dutch law	SIDN	A.1.2 and E.1	Reinforcement of association between the .nl domain and the Netherlands; formal expression of support for the association in a joint statement	N/a	N/a
2.5	Increase influence within ICANN	Government	A.1.3	Greater influence over any future redelegation process	Long term	-
2.6	Prepare and formally agree Accountability Framework with ICANN	SIDN	A.1.1	Greater stability	Implemented	Not yet known
2.7	Emphasise and formalise association between .nl and the Netherlands in dealings with ICANN	Government	A.3.1	Reinforcement of association between the .nl domain and the Netherlands	Long term	-
2.8	Prepare and agree redelegation process scenario, complete with trigger moment definitions and summary procedural description	SIDN - Government	A.2.1 2, A.2.2 and A.2.4	Greater influence over any future redelegation process	Implemented except for outline procedure	Not yet known
2.9	Inform LIC and ICANN about the scenario	SIDN - Government	A.2.1	Acceptance of scenario as blueprint for any future redelegation	2-3 months	-
3.1	Secure zone file availability by organisational separation	SIDN	B.1 and B.2	Greater stability, but not currently practicable	N/a	N/a
3.2	Ensure physical redundancy within the name server portfolio (particularly through Anycast implementation)	SIDN	C.2	Resilience	Implemented	- € 165k/yr
3.3	Ensure logical redundancy: support by dissimilar partners under dissimilar arrangements	SIDN	B.1	Resilience	Implemented	-
3.4	Use Anycast servers	SIDN	C.2	Resilience	Q4 2007	Not yet known
3.5	Secure access for authorised registrars	SIDN	C.2	Security	Implemented	-
3.6	Secure physical access to SIDN server locations	SIDN	C.2	Security	Implemented	€ 25k
3.7	Provide logical security (firewalls etc)	SIDN	C.2	Security	Implemented	€ 30k and € 75k/yr
3.8	Set up mirror site	SIDN	C.2	Resilience	Implemented	N/a
3.9	Perform zone file integrity checks	SIDN	C.2	Integrity	Implemented	€ 4k
3.10	Broaden zone file integrity checks as appropriate	SIDN	C.2	Reliability	Continuous	-
3.11	Undertake vulnerability analysis (Business Continuity Management)	SIDN	C.1.1	Reliability	Implemented	€ 40k
3.12	Periodically repeat vulnerability analysis	SIDN	C.1.1	Reliability	Continuous	€ 17k

No.	Description	Who	Stock list	Result	Time	Cost
4.1	Provide duplicate connection AMS-IX-SIDN	SIDN	D.1	Availability	Implemented	€ 12k and € 49k/yr
4.2	Provide redundant routing between production environments and mirror location	SIDN	D.1	Availability	Implemented	€ 17k and € 63k/yr
4.3	Mirror location	SIDN	D.1	Availability	Implemented	€ 300k
4.4	Ensure scalability of DRS	SIDN	D.1	Availability	Implemented	-
4.5	Provide OTAP environment for development and modifications	SIDN	D.1	Reliability	Implemented	€ 100k
4.6	Provide physical security, using RFID passes for access control	SIDN	D.1	Security	Implemented	€ 55k
4.7	Provide physical security, based on biometric access control	SIDN	D.1	Security	Q4 2007	€ 25k
4.8	Implement camera observation	SIDN	D.1	Security	Q4 2007	€ 25k
4.9	Screen personnel	SIDN	D.1	Security	Q4 2007	€ 7k
4.10	Use of https for data input by registrars	SIDN	D.1	Security	Implemented	-
4.11	Implement testing and screening measures	SIDN	D.1	Security	Implemented	-
4.12	Use standard components wherever possible	SIDN	D.1	Security	Implemented	-
4.13	Build up in-house know-how	SIDN	D.1	Security	Implemented	-
4.14	Oblige personnel to adhere to AO manual	SIDN	D.1	Security	Implemented	-
4.15	Implement explicit internal functional isolation	SIDN	D.1	Security	Implemented	-
4.16	Maintain healthy financial position	SIDN	A.1	Stability	Implemented	-
4.17	Maintain central database	SIDN	D.1 and D.2	Reliability	Implemented	-
4.18	Back up database every working day	SIDN	D.2 and D.3	Reliability	Implemented	-
4.19	Regularly test back-up and restore procedure	SIDN	D.2 and D.3	Reliability	Implemented	-
5.1	Publicly agree to be bound by RFC 1591	SIDN	E.1	Legal certainty	Implemented	-
5.2	Establish a Council of Registrars	SIDN	E.1	Legal certainty	Implemented	-
5.3	Pursue dialogue with the LIC (e.g. Domain Name Debate)	SIDN	E.4	Legal certainty	Implemented	-
5.4	Give binding status to registration policy development process	SIDN	E.4	Legal certainty	2008	-
5.5	Ensure that the Supervisory Board is balanced	SIDN	E.4	Legal certainty	Implemented	-
5.6	Ensure applicability of Dutch and European law	SIDN	E.1	Legal certainty	Implemented	-
5.7	Operate dispute resolution procedure for domain name disputes	SIDN	E.1 and E.4	Legal certainty	Implemented	-
6.1	Limit liability contractually	SIDN	C.1.2	Reduced liability risk	Implemented	-
6.2	Arrange liability insurance	SIDN	C.1.2	Reduced liability risk	Implemented	-
6.3	Build up jurisprudence	SIDN	C.1.2	Reduced liability risk	Implemented	-
6.4	Build up resistance capability	SIDN	C.1.2	Reduced liability impact	Implemented	-
6.5	Maintain healthy liquidity and cash flow	SIDN	C.1.2	Reduced liability impact	Implemented	-
6.6	Investigate legal validity of an escrow	SIDN	C.1.2	Secure intellectual property rights	3 months	Not yet known
6.7	Draw up and sign escrow	SIDN	C.1.2	Secure intellectual property rights	3 months	Not yet known

Annex B: Last resort scenario

Introduction

At the project steering committee meeting on 23 August 2006, it was decided that the government and SIDN should jointly draw up a description of the course that any future redelegation process should ideally take. This annex is the implementation of the passage of the Statement of Intent regarding the detailing of additional measures/arrangements regarding (re)delegation during any unstable phase (stock list A2) or transition phase (stock list A.3) that might occur, and the passage regarding transfer of the name server function (stock list B and C). If SIDN and the Ministry of Economic Affairs are able to agree on the process description, details of the proposed procedure may be submitted to ICANN.

Purpose

By defining this procedure, the Dutch government and SIDN hope to minimise the disruption to .nl services likely to occur if it should ever prove necessary to redelegate the .nl domain; in doing so, it is not the intention to give additional powers to the Dutch government, which would be potentially disruptive to SIDN's services.

Phases

In line with the stock list, the procedure recognises three phases: the stable phase (1), in which the registry is functioning normally and no abnormal circumstances exist; the unstable phase (2), in which the registry is no longer functional or not functioning adequately; and the transition phase (3), in which the delegation is transferred to another registry. In practice, each phase would succeed the next without clear demarcation. The parties may disagree as to whether transition from one phase to the next has taken place, even where the situation appears unambiguous to an individual party.

Trigger moments

In order to reduce ambiguity regarding the commencement of an unstable phase, a number of trigger moments have been defined. Trigger moments are junctures characterised by events that both SIDN and the Ministry regard as marking a transition from stability to instability. The Dutch government is not entitled to initiate a procedure intended to lead to redelegation of the .nl domain unless and until these trigger moments should occur. The trigger moments have NO third-party implications.

All the following criteria must be met before a trigger moment may be deemed to have been reached:

- Serious macroeconomic damage associated with the provision of services to the LIC is occurring or very likely to occur.
- The prevailing circumstances are not of a transient nature.
- The situation cannot be corrected within a time-scale that is sufficiently short to prevent serious or irreversible damage to the provision of services to the LIC.

Furthermore, one of the following conditions must be met:

- The registry is to some degree responsible for or culpable in relation to the prevailing situation.
- The failing(s) of the registry is/are to some degree systemic, not incidental.

A trigger moment is a juncture characterised by the existence of several simultaneous circumstances,[11] which are directly relevant to SIDN's core activities i.e. fulfilment of the .nl name server function (NSF), the .nl data entry function (DEF) and the .nl registration policy.

Examples of trigger moments:

1. The registry is the subject of a (final) court winding up order or a legally valid application for such an order from the lawful director, leading to the prolonged or permanent suspension of .nl services to the local Internet community, or making such a suspension probable.
2. A (final) court order is issued, granting the registry protection against its creditors, or a legally valid application for such an order is made by the lawful director, leading to the prolonged or permanent suspension of .nl services to the local Internet community, or making such a suspension probable.
3. The registry goes into liquidation, or nearly all of its core activities are affected by liquidation.
4. All or nearly all of the registry's .nl core activities are discontinued.
5. The registry's registered office is moved abroad, leading to prolonged or permanent unlawful encumbrance or suspension of the .nl services to those members of the local Internet community that have close ties with the Netherlands.
6. There are demonstrable and prolonged structural organisational technical and/or operational shortcomings in the provision of services to its registrants by SIDN (as referred to in ICP-1), and these shortcomings are culpable and not attributable to force majeure. (In this context, 'prolonged' means continuing for several months.)
7. SIDN is guilty of criminal or persistent unlawful activities that are directly relevant to and have a negative influence on its registry function or the performance of that function.
8. SIDN's entire Executive Board and entire Supervisory Board resign or abdicate their duty, leading to the prolonged or permanent suspension of .nl services to the local Internet community, or making such a suspension probable.
9. The registry consistently fails to adhere to generally accepted principles of good governance, or the principles of reasonableness and fairness, with the result that the interests of registrars and registrants are seriously threatened.

[11] It is questionable, however, to what extent every one of the circumstances need exist. The parties will work together to more precisely specify what is required for a trigger moment to be deemed to have been reached.

Escalation

Escalation is appropriate only if a trigger moment is deemed to have been reached. If the Dutch government and SIDN disagree as to whether this is the case, they will hold proper discussions in search of consensus. If and insofar as it is considered desirable, the parties may seek consensus through mediation. If consensus cannot be reached by these means, either or both of the parties may refer the matter to a competent court for a ruling.

Therefore, in any situation where there is disagreement as to the initiation of a redelegation procedure, the following steps will be taken (where steps 2 and 3 are concerned, if and insofar as the preceding step has not resulted in resolution):

1. Internal escalation to the Ministry's DG and SIDN's Executive Board
2. Consideration of the merits of seeking resolution through mediation
3. Referral to a competent court for a ruling

Steps

As soon as it is ascertained that a trigger moment has been reached, an unstable situation is deemed to exist. In an unstable situation, the Dutch government has the option of implementing the steps outlined below. The government may elect to implement measures with a view to enabling a running start, thus removing the need for redelegation:

1. Obtain reassurance with regard to the safeguarding of the stability and continuity of the .nl zone through proper fulfilment of the registry's NSF obligations.

If adequate reassurance cannot be obtained, the Dutch government may implement the following steps if there is an acute need to temporarily relieve SIDN of control of the .nl domain:

1. Inform the interested parties regarding the situation that has arisen. In this context, the interested parties are ICANN, IANA, the LIC, interested departments and agencies of the Dutch government, the managers of the secondary .nl name servers and the .nl registrars.
2. Seek a caretaker to take over the activities that are threatened by the unstable situation (which will depend on the causes, nature and extent of the instability). In preparation for this step, a contingency plan and associated arrangements must be drawn up, dealing with continuity and the transfer of the registry function in the unstable and transition phases.

In preparation for the ultimate and definitive redelegation of the .nl domain, the Dutch government will also implement the following steps, in parallel to those described above, and independently of any temporary caretaker arrangements:

1. Inform the interested parties regarding the situation that has arisen. In this context, the interested parties are ICANN, IANA, the LIC, interested departments and agencies of the Dutch government, the managers of the secondary .nl name servers and the .nl registrars.
2. Instigate a call for candidates in order to identify organisations interested in taking over as the .nl registry.
3. Organise a (pre)selection process to identify the most suitable candidate to take over as the .nl registry; assess the acceptability of the selected party to the .nl registrar community, to the user community, to the government and to other relevant parties.

4. Propose the selected candidate to ICANN/IANA.
5. ICANN/IANA will then make the delegation.
6. Assurance by ICANN/IANA.

NB: steps 4, 5, 6 need to be worked out in more detail at a later stage.

Contingency plan and arrangements for transfer of the registry function

If, in response to a trigger moment, as defined in this report, the Dutch government should decide to intervene in the delegation of the .nl top-level domain, it should do so on the basis of a detailed contingency plan.
This plan will be formulated by the Ministry; SIDN will cooperate with its formulation and make expertise available, if asked to do so. The Ministry may also seek the advice of third parties with relevant expertise, but will not do so until it has concluded reasonable discussions with SIDN. The Ministry will clear its contingency plan with ICANN.

The contingency plan will detail the procedure to be followed for the purpose of redelegation, and will address at least the following matters:

- The Dutch government will involve SIDN and, where possible and appropriate, ICANN in specification of the manner in which the following will be handled:
  1. Transfer of the name server function
  2. Transfer of the authority to make name server changes with IANA in respect of the .nl domain
  3. Transfer of the .nl zone to the proposed or new registry entity
  4. Availability of the registration details for the proposed or new registry entity

- Organisation of the LIC in relation to the redelegation process. The contingency plan must specify how the LIC is to be quickly mobilised for the redelegation process, in order that the process may be implemented swiftly and effectively.

- The conditions under which the government will support a prospective registry's candidacy for the .nl delegation.

Responsibilities

The redelegation will be effected by ICANN. Although technical implementation of the redelegation will be in the hands of ICANN/IANA, operation of the .nl domain is regarded as a national matter, since the domain's local Internet community is predominantly resident or based in the Netherlands. The underlying rationale is based on the GAC principle of subsidiarity. Consequently, it is important that the Dutch government properly prepares any redelegation that might prove necessary, in order that everything proceeds as quickly and smoothly as possible and in order that ICANN/IANA are able to simply endorse and act upon the national choice of registry after performing the necessary technical checks (RFC).

Responsibility for registry nomination and selection generally lies with the LIC. The government is part of that community and, as guardian of the general interests of Dutch society, has responsibility for initiating and supervising the process.

* * *