NLnet Labs

For an Open Internet

Lectori Salutem,

NLnet Labs is active in those areas where a long-breath can have a profound impact on the Internet societal value and 2012 was an interesting year in all areas on which NLnet Labs is active.

The world experienced a steady rise in the amount of DNSSEC deployment and the first innovations based on DNSSEC (DANE) got standardized. NLnet Labs is at the forefront of DNSSEC deployment, and the availability of NLnet Labs production grade tools and software continues to be a significant enabler for the improvement of the Internet's security. The combination of DNSSEC with DANE can potentially lead to a paradigm shift in the way the Internet Public Key Infrastructure is utilized and allows for increased trust in the Internet ecosystem.

World IPv6 Launch demonstrated that IPv6 is production prime-time and the IPv6 traffic levels are on the rise which is good news for an Internet that provides its societal and economic value by enabling innovation at the edges. IPv6 day also demonstrated that the collaborative nature of the Internet model of governance is key to its success.

That Internet model is not something we take for granted; NLnet Labs steps to the plate to defend it. Not only by providing technical innovations in areas where Internet as a global commons needs maintenance (DNS and Routing security), but also by providing technical expertise in the Internet Governance arena, for instance, through being the technical advisor to the Dutch delegation at WCIT 2012.

In the first half of this report I proudly present the results of our activities and in the second half of this report you can read that we would not have been able to do all this work without financial support.

In addition to the base subsidy from SIDN and the NLnet foundation we received generous donations from Afnic, Comcast, Cisco, and Verisign Inc.

We hope to welcome you to these ranks in the future[1]!

Olaf Kolkman,
Director NLnet Labs.

NLnet Labs

1 Contact info@NLnetLabs.nl for more information, or see http://www.nlnetlabs.nl/labs/contributors/

1 NLnet Labs, For an Open Internet

Mission

NLnet Labs' mission is:
To be a globally recognized technological innovation and expertise center for those technologies that turn a network of networks into an Open Internet for All.

All these terms are relevant:

- Global: even though NLnet Labs roots, location and name clearly relate to NL, The Netherlands, NLnet Labs is a global actor. We maintain an outward look, the Internet is a global facility.
- Technological innovation and expertise center: NLnet Labs wants its expertise to be rooted in technology, research and development. It wants to be *the* place where people turn to when they need expertise about Internet. It also wants to be a center, a place that people come to collaborate.
- Technologies that turn a network of networks into an Open Internet: the Internet is a collection of independent networks. NLnet Labs focuses at the technologies that are inter-domain. Technologies that are intra-domain such as those technologies to build data centers and enterprise networks may inform the work but will not define the major directions.
- An Open Internet for all: maintaining the Internet for all as a global commons is a guiding principle.

Guiding Principles for setting direction

The objectives of the NLnet Labs foundation are captured in its charter:

> *"[...] the foundation's object is to (further) develop and distribute on a non-profit basis Open Source Software (being software whose source code is freely available to third parties) and Open Standards (being standards developed based on a publicly accessible procedure and that may be used freely by all) for the Internet, and furthermore do all that is directly or indirectly connected thereto or conducive thereto, all this in the broadest sense."*

In addition to the chartered objectives, NLnet Labs takes into account the following guiding principles for setting direction (some of which are recognized from the mission statement):

1. Technological focus on an Open Internet: we focus on those technologies that are needed to turn a collection of individual networks into one Internet. Those technologies are not directly targeted to the users of one network but enhance quality, security, scalability, openness, transparency and the trust in the Internet for all of its users.
2. Applied research and development: we provide products, knowledge and results that need to be deployable or applicable on the *Internet of today*; the work takes place on the edge between academic research and industrial deployment.
3. Global commons: the work we do is targeted towards public good. Not necessarily places where economic benefit can be gained by working on the technology.
4. Long breath: some technologies will take years to catch on, those topics is where persistence and zeal needed.
5. Open ended innovation: success does not need to be defined at the start of the project, there should be time and space for ideas to mature, hence projects may fail.

NLnet Labs is globally recognized for its expertise in Internet system technology and architecture, in particular in DNS and DNSSEC. NLnet Labs' software is an important component of the Internet infrastructure. NLnet Labs plays a significant role in standards development. Dissemination of knowledge is realized through education and collaboration.

Stichting NLnet Labs was founded in 1999 by Stichting NLnet. The budget of NLnet Labs, a non-profit organization, is mainly based on a subsidy from Stichting NLnet and SIDN.

In sections 2, 3, 4, and 5 we describe our the Areas of Interest: DNSSEC, Routing and Addressing, IPv6, Outreach, and Research and Education respectively. In section 7 we give an outlook on NLnet Labs future activites, and section 8 contains our organizational and financial reports.

2 Area of Interest: DNS and DNSSEC

2.1 Introduction

Deployment of DNSSEC, a security extension to one of the protocols that is essential to the operation of the Internet, is the area where NLnet Labs makes the most significant difference.

We contribute to global deployment of DNSSEC by providing tools and software such as NSD, Unbound, ldns, Net::DNS, and OpenDNSSEC. Additionally, we contribute technical information, teach courses, and popularize the technology. The combination of solid engineering combined with spreading the word on the necessity of the technology is what we have come to call *evangineering*.

In addition to making an impact on the deployment of DNSSEC the software also serves an important roll in 'genetic diversity' of DNS implementations resulting in a higher resilience of one of the most critical Infrastructures needed to operate the Internet.

2.2 Software – Tools and Libraries

2.2.1 The Unbound Recursive Name Server

Description

Unbound is a reference implementation of a validating caching resolver with full DNSSEC support targeted at ISP and Enterprise environments.

Unbound is available at the dedicated website http://unbound.net, hosted and maintained by NLnet Labs.

NLnet Labs role and goal

With Unbound, NLnet Labs increases the resiliency of the global internet infrastructure by providing a telco-grade open source alternative for DNSSEC validating recursive name servers. By offering a BSD licensed high-quality piece of software we lower the barriers for embedding DNSSEC in commercial and open-source applications and devices.

2012 Results

In collaboration with VeriSign, NLnet Labs is implementing the IETF draft "Client subnet in DNS requests" in Unbound. The draft defines an EDNS0 extension with address information of the original query sender. This allows authorities to reply with an optimized answer for the client

network location. Most of the work is done in 2012 and the final result is expected Q2 of 2013. Multiple other parties expressed their interest for this feature on the unbound-user mailinglist.

Besides, we continued to provide support to the community whereby we made the software more stable and addressed a number of usability issues.

> In 2012, the Unbound versions 1.4.15 to 1.4.19 have been released.

Impact

Unbound is operated in most high availability and visibility environments that have chosen to be early innovative deployers of DNSSEC validation. Among those parties are SURFnet, Comcast, and T-Mobile and has contributed significantly to the acceptance of DNSSEC.

In 2012 various open-source OS vendors have started to consider to make Unbound a part of the core of their distributions[2].

2.2.2 DNSSEC-trigger: Validation for End Users

Description

One of the major hurdles in DNSSEC deployment is 'the last mile problem'; how to get validation information the application. There are roughly two approaches: bring validations as close to the applications as possible, or set up a trust relation with a validating recursive name server and have that machine do validation for you.

NLnet Labs Role and Goal

Labs provides running code to establish the feasibility and assesses the problems with bringing DNSSEC validation towards the user.

Our goal is to offer regular users seamless DNSSEC operation in all realistic operating environments e.g., in the presence of captive payment portals. We believe that the experience gained with this method crossing the last mile will be useful for other initiatives, such as the development of DNSSEC APIs.

2012 Results

DNSSEC-trigger is implemented in POSIX C and uses ldns, and Unbound code components.

> In 2012 we released DNSSEC-trigger versions 0.10 and 0.11

Impact

DNSSEC-trigger is generating useful experiences that feed back into our development efforts. It is recognized as a valuable tool to increase security and was nominated for the ISOC.NL awards 2012 in the category Security and Privacy. However, DNSSEC-trigger is not yet a tool that provides the usability for the common user.

---

2 At the moment of writing we are not aware of any final decisions. Sites like https://calomel.org/unbound_dns.html report:

```
In the future as BIND 10 is released it is expected that most open source operating
systems like OpenBSD and Ubuntu will migrate over to Unbound as their primary DNS
resolvers. BIND, also known as named, is getting extremely code bloated, slow and over
complicated. The other problem is that BIND is used for 70% of DNS servers leading to a
monoculture environment. If an attack or exploit comes out it is advantageous as the
attacker to go after the most used software. Unbound is an incredibly fast and secure DNS
name server which, due to its small size, can easily be code audited for security.
```

2.2.3 OpenDNSSEC: A DNSSEC Turnkey Solution

Description

OpenDNSSEC targets to be a generic turnkey solution for DNSSEC signing.

The project targets to be a drop-in solution for registries that maintain a few zones of considerable size as well as registrars and registrants that maintain a considerable amount of zones of little size.

OpenDNSSEC is a collaborative project, which NLnet Labs has joined in 2008. Two core modules, called the enforcer[3] and the signer engine are developed and maintained at NLnet Labs. the other parties in the consortium (IIS, Kirei, Nominet, SIDN, Sinodun, and SURFnet) are responsible for integration, testing, project management, training, etc.

OpenDNSSEC is distributed under a BSD license. For more information, see the website at http://www.OpenDNSSEC.org.

NLnet Labs role and goal

NLnet Labs goal is to lower the barriers to deployment of DNSSEC.

NLnet Labs brings relevant DNS expertise and code development to the project. In order to allow for trust in quality and continuity of the product, NLnet Labs commits to the long term maintenance and support of the two components.

2012 Results

NLnet Labs implemented an innovative state-based methodology as EnforcerNG, which will eventually succeed the current enforcer component of OpenDNSSEC in version 2.0 (in 2013) SURFnet contributed in design and implementation of the EnforcerNG by providing a developer until January 2012. EnforcerNG is more flexible and supports more kinds of rollovers (e.g. algorithm rollover, gracefully unsigning).

In 2012 the OpenDNSSEC team focused on releasing and maintaining version 1.4. The bulk of the work still required to release version 2.0 consists of testing and ensuring the two enforcers behave in similar ways.

The enforcer design that is being implemented for version 2.0 was submitted as a paper to *The SATIN2012 Conference*[4] and presented at *the IEPG meeting at IETF85*[5].

> Open DNSSEC Software Releases:
> Branch 1.3 Stable Releases: Version 1.3.9-1.3.12
> Branch 1.4: 1.3.0alpha3, beta1, and beta2
> Branch 2.0: Enforcer NG alpha-3 snapshot

Going forward, the main focus is making OpenDNSSEC more pluggable and scalable so that it is usable in more diverse operational environments, forward motion is accompanied by careful regression testing and maintaining compatibility.

3 The new generation Enforcer is developed and maintained by NLnet Labs, the original Enforcer was developed and maintained by Nominet
4 http://conferences.npl.co.uk/satin/papers/satin2012-Schaeffer.pdf
5 http://www.iepg.org/2012-11-ietf85/overeinder-iepg-ietf-85.pdf

Impact

OpenDNSSEC lowers the barrier to the deployment of DNSSEC, its availability has been contributing to positive decisions with respect to the deployment in several organizations, among which large TLDs.

Known users of OpenDNSSEC are SURFnet, CAcert, ICANN, as well as some top-level domain registries including .NL, .SE, .UK, .DK, .FI, .FR, and .LU.

2.2.4 NSD, NLnet Labs Authoritative Name Server

Description

The NLnet Labs Name Server Daemon (NSD) is an authoritative RFC compliant DNS name server. It was first conceived to allow for more genetic diversity for DNS server implementations used in the root-server system. NSD has been developed for operations in environments where speed, reliability, stability, and security are of high importance.

NLnet Labs commits to long term support of NSD. Not only will it announce the termination of support two years in advance, it also offers support contracts in three varieties.

Currently there are two versions of NSD: NSD3 and NSD4.

NLnet Labs' Role and Goal

With NSD NLnet Labs sets out to improve the Internet's critical infrastructures resiliency against critical bugs and lower the resistance and costs of deploying DNSSEC. With NSD we want to provide a fast, secure, inter-operable and telco-grade authoritative name server that typically is deployed as a secondary server in the DNS infrastructure.

2012 Results

NSD3

NSD3 is the production release version and can be found in almost all software repositories. NSD3 is in maintenance mode which means we concentrate on bug fixes and minor feature requests.

Unfortunately we had to deal with vulnarabilies that, under special circumstances, would allow a denial of service attack on a running nameserver[6]

> In 2012 we released NSD 3.2.10-3.2.14
> Two security related releases were:
> 3.2.12: VU#624931 CVE-2012-2978
> 3.2.13: VU#517036 CVE-2012-2979

NSD4

NSD4 development was a continuous activity throughout the year.

After prototyping and benchmarking alternative designs for memory performance tradeoffs we concluded that memory usage should remain at levels similar to NSD3. Still, redesign of internal data structures resulted in improved performance compared to NSD 4.

6 http://www.nlnetlabs.nl/publications/NSD_vulnerability_announcement.html

In 2012, we continued development of NSD4, which is aimed at providing support for environments that require dynamic provisioning of zones, as well as support for a high number of zones. End 2012 NSD4 was feature complete and saw two beta releases. A production release of NSD4 is expected mid 2013.

Response Rate Limiting

In 2012 we saw a rise in so called Reflector Attacks. Authoritative DNS servers are used to amplify DNS request with spoofed source addresses, causing *melt down* traffic to the direction of innocent victims. RRL on the authoritative name servers is one of the approaches to mitigate this effect. The RRL methodology has been designed by Vixie and Schryver[7]. In 2012 we made a start with implementing RRL for NSD3 and NSD4 resulting in a RRL code in production NSD3 in February 2013.

Impact

NSD clearly serves one of its design goals: to provide an alternative implementation of authoritative DNS servers in order to increase resiliency and stability of the global DNS infrastructure: NSD is currently used on critical elements of the Internet's Infrastructure. Among those elements are root servers such as the L and K root-servers and servers from several top-level domain registries such as .NL, .DE, .BR, .SE, and .UK.

NSD was the second implementation for which Response Rate Limiting (RRL) was available[8]. It allowed the DNS community to experiment with the approach and finesse the details of implementation. For 2013 we attracted students to perform modeling on long term success of the methodology.

2.2.5 The ldns Software Library

Description

Ldns is a C library aimed to simplify DNS programming. It allows developers to easily create fast production quality software conforming to current RFCs and Internet Drafts. The library originates from the drill tool, which was written to aid in DNSSEC debugging. Since drill needs a nearly complete DNS library to do its work, it was chosen to focus on the library itself, and make drill a part of that project. Ldns design is influenced by the Perl Net::DNS library.

2012 Results

In 2012 we adopted the unified BSD compatible build system (a solid base for potential inclusion in BSD operating systems), ECDSA support (RFC6605) and DANE support (RFC6698).

Thorough code analysis by our colleagues from CZ.NIC Labs and Paul Wouters, an established security specialist, has improved the reliability and maturity of the library.

In 2012 we also saw two emergency releases fixing breakage of existing ldns using software (Unbound and OpenDNSSEC respectively). To prevent this from recurring the build system has been adapted to not only do unit tests for ldns functionality, but also build and do unit tests for software depending on ldns; pyldns, Unbound and OpenDNSSEC currently.

In 2012 ldns saw five releases 1.6.12 t/m 1.6.16 (two emergency releases)

7 http://www.redbarn.org/dns/ratelimits

8 A description of the NLnet Labs implementation can be found at http://www.nlnetlabs.nl/blog/2012/10/11/nsd-ratelimit/

Ldns is often used to experiment and to have a reference implementation for new DNSSEC protocol extensions. In august 2012 the DNS-Based Authentication of Named Entities (DANE) draft became RFC6698. A tool providing the creation and verification of DANE resource records was provided in the ldns release thereafter.

Impact

Ldns offers the community library with up-to-date tools allowing for rapid development and prototyping: ldns is used by Unbound and OpenDNSSEC and in software not originating from NLnet Labs such as Phreebird, a DNSSEC supplementing DNS proxy from Dan Kaminsky; sshfp, a tool that generates DNS SSHFP records from SSH public keys from Paul Wouters and Chrisopher Olah.

Ldns-dane has already proven to be a valuable and reliable tool. It has withstand all corner cases that have come up since the introduction of DANE, and as such it aids in improving the technical specifications in the standardization process and the implementation of 3rd party software that utilizes DANE. It underlies SIDN's online DANE validator at http://check.sidnlabs.nl/dane/ .

2.2.6 The Perl Net::DNS and Net::DNS::SEC Libraries

Description

The maintenance responsibility for the Perl libraries Net::DNS and Net::DNS::SEC is a task that NLnet Labs started in 2005. NLnet Labs takes responsibility for review and coordination while development is done with and by community volunteers.

NLnet Labs Role and Goal

Labs provides a continuous and respected home and support for a seminal software library.

2012 Results

Groundwork for a new architecture has been gradually and incrementally introduced since 0.67 by Dick Franks, an active community member. With release 0.69 (and the quickly following 0.70 release) all pieces came together enabling internationalized domain name support and the enrichment of the text, mailbox and domain-name rdata fields. The new architecture also addressed some less visible improvements on the internal workings of Net::DNS (providing clearer separation of concerns and better protected module-interfaces.)

As a side effect of the architectural rework however, there were a bigger number of critical bugs then normally after release. Most notably SpamAssassin was affected in a way that prevented it from updating the rules database. Those incidents have resulted in the creation of a net-dns-users mailing-list. All (known) authors of software dependent on Net::DNS were informed about the mailing-list and it was received with much enthusiasm. We established a commitment to warn about and discuss release candidates on the mailing-list before actual release.

> In 2012 Net::DNS saw five releases 0.68 t/m 0.72.

Impact

Net::DNS is the de-facto library for DNS with Perl. It is in use by 80 other Perl packages from which some very popular, such as: Mail::DKIM, Mail::SPF and Mail::SpamAssassin. Tools popular in the DNS-community such as Verisign's YAZVS - Yet Another

Zone Validation Script, .SE's dnssec-monitor and fpdns, a tool that remotely determines DNS server versions from Jakob Schlyter depend on Net::DNS. "DNS and BIND" the reference work from Paul Albitz & Cricket Liu devotes a section on programming with Net::DNS.

2.2.7 Credns

Description

Credns (pronounce ˈkrē-dən(t)s[9]) is a software program aimed at fortifying DNSSEC system architectures by performing independent validation in the DNS notify/transfer-chain. Currently credns is a fork of the NSD_3_2 branch that has been extended with the possibility to assess zones (received or updated by AXFR or IXFR) by running an external verifier. Only zones that are deemed correct by the verifier will be notified to (public) slave servers and offered for transfer.

NLnet Labs Role and Goal

One of the barriers to DNSSEC deployment is the risk of introducing badly signed data. This tool aims to reduce those risks.

2012 Results

In 2011 at the request of RIPE, the development of a verifying DNS(SEc) proXY (dnssexy) was started. In 2012 we released the tool under the name Credns[10].

22 June 2012, version 0.2.10 of credns was released.

Impact

The impact of Credns is low, we are not aware of widespread use.

2.3 DNS Communities and Community building

NLnet Labs Role and Goal

Participation and outreach in various communities helps us to disseminate our work and helps us to assimilate valuable input for our activities.

2012 Activities

DNSSEC Train the Trainer Training

In February two, two day courses commissioned by the Netwerk Gebruikersgroep Nederland (NGN) were given to teach DNSSEC to IT-trainers. A classroom setup hosted in the Amazon Elastic Compute Cloud has been developed and published for the trainers (and DNSSEC trainers in general) for use as practicum material in their own classrooms. Besides all material has been video taped and made available for the general public[11]. As a follow-up the NGN hosted trainings that were dedicated to Windows administrators.

Port Maintenance

We maintain the FreeBSD ports of software products we develop. This activity results in better portability and documentation. Besides it provides insight on the availability of, and dependencies

9 http://www.merriam-webster.com/dictionary/credence

10 , We changed the name because the name dnssexy was already in use by an excellent DNS blog aggregation site (dnssexy.net).

11 http://www.ngn.nl/nieuws/algemeen/dnssec-training-nu-op-video-beschikbaar and http://www.dns-school.org/

on a typical installation environment. We do not maintain ports and equivalent distribution mechanisms (such as RPM and DEB packages) for other operating systems.

3 Area of Interest: Routing and Addressing

The routing and addressing activities can be arranged in three sub-categories: BGP dynamics modeling and simulation, routing security, and multi-path networking (new activities are developed).

NLnet Labs Role and Goal

Routing and Addressing architecture, resiliency and security is an area in which NLnet Labs takes a global perspective with the interest of the global public and a sense of economic realities in mind. NLnet Labs identifies areas where the development of Open Source tools and specific expertise can improve security and resiliency with practical steps and takes a general interest in how the Internet's architecture can or should evolve while maintaining the Open nature that made it prosper.

2012 Results

BGP Dynamics Modeling and Simulation

In the past years, several MSc. students have worked on modeling and simulation of the (time) dynamical behavior of the BGP protocol. This has resulted in a simulation environment, and several use-case studies. See publication list of previous years for an overview of these.

In 2012 no new work was initiated on this topic.

Routing Security

The combined NLnet Labs and SURFnet pilot study on RPKI deployment in 2011 resulted in a presentation at the IETF 84 SIDR WG meeting[12]. Although an operational best practices document seemed relevant and important to the WG, it was, at the time, not clear if an RFC should be published eventually. The document serves as the basis for further collaboration with LACNIC and the ISOC Deploy 360 program.

Besides new routing security protocol definition and deployment, NLnet Labs also seeks opportunities to improve upon existing technology in routing security. In order to asses whether the improvement of tools would lead to a valuable security improvement of the global routing system we collaborated with ISOC's Andrei Robachevsky, talked to operators and network engineers and organized a BoF at RIPE64 in order to get more insight on the use of the Internet Routing Registries (IRR) and the existing toolset.

As a result it is clear that there are clear opportunities to improve the IRR toolset API and we build a network in the operator community that will help us to define requirements and can act as sound board when we progress with this work in 2013.

12 https://tools.ietf.org/agenda/84/slides/slides-84-sidr-4.pdf

Multi-Path Networking

In 2012, we started a collaboration with Ronald van der Pol on the subject of multi-path networking. With multi-path networking we consider layer 2, layer 4, and layer 7 networking protocols exploiting the availability of redundant alternative paths between two communicating endpoints. Existing protocols on layer 2 (data link) are TRILL and SPB, being already used in data centers. Layer 4 Multipath TCP is currently under development in the IETF, and a Linux and FreeBSD kernel implementations exist, but still in first deployment studies. Layer 7 multi-path BGP routing is mainly an academic exercise, and we have reported on a simulation study on this subject last year (2011).

In 2012 we considered the three layers where multi-path networking can be realized. This resulted in a in a SURFnet RoN project to study the availability and practical deployment barriers of multi-path networking (layer 2 and layer 4). The submitted SURFnet RoN project has been granted for 2013.

Impact

NLnet Labs has evolved to being a relevant specialist and managed to bridge and bring together operators and academics on this subject.

4 Area of Interest: IPv6

IPv4 depletion and IPv6 transition are topics that are of constant interest. Software developed by NLnet Labs has always supported IPv6 from its first design. Specific contributions are made mainly in the form of *evangineering*.

IPv6 Day Organization

Similar to last year's organization of IPv6 World Day, we joined forces with a number of institutes to organize a local instance of IPv6 World Launch Day in Amsterdam on June 6th, 2012. Instead of switching IPv6 connectivity on for one day only, the intention was that IPv6 connectivity stayed on after this date. About 250 participants attended various sessions on practical IPv6 deployment and usage, security, and business cases.[13]

NLnet Labs contributed to the success of the Dutch event.

NLNOG RING

The NLNOG RING is a resource sharing project initiated by the Dutch Network Operators Group based on mutual trust, aimed at enhancing operators debugging abilities by increasing the number of vantage points. Organizations join the RING by contributing a machine. Members have shell access to all contributed machines. Currently the RING consists of 214 nodes from 191 organizations in 39 countries.

In November NLnet Labs joined the NLNOG RING by dedicating a machine. To participate we also had to join the (IPv6) default free zone. We were assigned autonomous system (AS) number 199664 which has one Provider Independent IPv6 network assigned: 2001:67c:14c0::/48.

We expect our membership will result in improving our abilities to do network experiments because of the worldwide availability of vantage points and the relative freedom in usage they offer.

13 http://www.internetsociety.org/ipv6/results

5 Area or Interest: Knowledge, Outreach, and Participation

Description

NLnet Labs personnel actively participates on the tangent of technology, governance, and public interests. NLnet Labs volunteers its staff in various community supporting positions.

NLnet Labs Role and Goal

The Internet's technical architecture and the bottom-up nature of the Open Source and Open Standards development are key to the Internet's success. NLnet Labs believes that understanding of technology, and how that technology is operationally deployed, is key for successful Internet Governance and that understanding of public policy objectives is key for responsible engineering. NLnet Labs contributes resources to support the governance structures

2012 Results

As an established and trusted neutral entity NLnet Labs continues to advise and inform decision makers in the field of Internet Governance and Standardization: NLnet Labs is a protagonist in championing the values of Open Internet and Open Standards.

Kolkman stepped down member of the Internet Architecture Board in March 2011. However, as the IAB's IANA Evolution program-lead, Kolkman continued to contribute to the stewardship over the IANA functions for the Internet in general and the IETF in particular. In January Kolkman joined the Multi-Stakeholder Platform on ICT Standardisation[14] as a representative of the IETF.

At the ISOC Internet New Years Event 2012 Kolkman chaired the chairperson's debate.

During 2012, Akkerhuis contributed as a paid consultant to ICANN for 1.5 days per month. As part of this role he is a member of the ISO 3166 Maintenance Agency, ISO's focal point for country codes and a candidate to become a Liaison type D for ICANN for the Working Group 2 of Technical committee 46 - Information and documentation[15]. Akkerhuis also participated in various activities of the ICANN ccNSO such as the ccNSO Study Group on Use of Names for Countries and Territories[16], the IDN PDP Working Group[17], and the Framework of Interpretation Working Group[18].

Akkerhuis en Kolkman are arbitrators for the RIPE NCC Conflict Arbitration procedure.

Akkerhuis is a member of ICANN's security and stability advisory committee SSAC and the Dutch IPv6 Task Force.

End 2012 Akkerhuis serves, as payed consultant, on ICANN's Service Review Panel, for the initial evaluation of new gTLD registries.

---

14 An advisory Expert Group on all matters related to European ICT Standardisation and its effective implementation: - Advise the Commission on its ICT Standardisation workprogramme -Identify potential future ICT Standardisation needs - Advise the Commission on possible standardisation mandates - Advise the Commission on technical specifications in the field of ICT whith regard to its referencing in public procurement and policies - Advise the Commission on cooperation between standards developing organisations. http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=2758

15 http://www.iso.org/iso/iso_technical_committee?commid=48750

16 http://ccnso.icann.org/workinggroups/unctwg.htm

17 http://ccnso.icann.org/workinggroups/ipwg1.htm

18 http://ccnso.icann.org/workinggroups/foiwg.htm

Kolkman chairs the IETF working group on Web Extensible Internet Reregistration Data Service (WEIRDS).

NLnet Labs has observer status in the Council of European Top Level Domain Registries (CENTR), is a member of OARC, the DNS Operations, Analysis, and Research Center (OARC), and a member of the DNSSEC Industry coalition. NLnet Labs continued to participate in the DNSSEC deployment group, that strives to coordinate global DNSSEC deployment efforts and is hosted by ISOC's deploy 360 program.

Furthermore, NLnet Labs staff has actively participated or tracked the work in the BEHAVE, DANE, DNSEXT, DNSOP, ENUM, SHIM6, IDR, SIDR, and GROW working groups, within the IETF, and the Routing Research Group, both in email discussions and during meetings. NLnet Labs staff is also participating in the RIPE meetings.

Kolkman acted as expert witness after RIPE NCC filed a summons against the state of the Netherlands following a police order on 8 November 2011 to temporarily "lock" a set of specific registrations in the RIPE Database. The RIPE NCC filed this summons because it wanted the Dutch court to clarify what the RIPE NCC''s obligations are for such orders in future.[19]

Finally, Kolkman participated in WCIT 2012, an international treaty conference for renewing International Telecommunication Regulations, as technical advisor to the Dutch governmental delegation.

Impact

A better understanding with key decision makers and in key decision processes of the Internet Architecture and Governance principles.

6 Research and Education

NLnet Labs Role and Goal

One of NLnet Labs statutory methods to enable its goal is "*enabling talented software developers to develop, expand, maintain and make available Open Source Software and Open Standards for the Internet;*". We take pride,, honor and inspiration from training talents.

Over the years NLnet Labs has supervised talented students that found their way into the open-source, open standards, and Internet working communities. We maintain a page with our student alumni at https://www.nlnetlabs.nl/labs/alumni/.

6.1 2012 Results

6.1.1 Discovering Path MTU black holes on the Internet using RIPE Atlas (MSc. thesis)

In June and July NLnet Labs supervised a MSc. research project for the System and Network engineering master of the University of Amsterdam. The research was successfully performed by Maikel de Boer and Jeffrey Bosma, resulted in a MSc. thesis and was awarded a high grade.

The project concerned the quantification of fragment and ICMP dropping firewalls. The added value lied in the ability to perform experiments on a worldwide scale using a much larger number of vantage points (RIPE Atlas probes). Because of the large amount of vantage points, as well as the ability to retrieve important feedback from each vantage point, we were able to more accurately

19 http://www.ripe.net/internet-coordination/news/about-ripe-ncc-and-ripe/update-on-court-proceedings-between-ripe-ncc-and-state-of-the-netherlands

than before pinpoint where on the Internet PMTU black holes occur and determine the type of filtering.

PMTU black holes directly affect DNS performance. More specifically; fragment filtering firewalls might prevent resolvers from receiving large DNS answers which are common with DNSSEC. The research has inspired new research that seeks to explore possibilities to mitigate this issue which will be (and was) performed at NLnet Labs in 2013.

The research was presented by Maikel and Jeffrey at the Plenary session of the 65th RIPE conference in Amsterdam.

6.1.2 Resilient OpenDNSSEC

During an internship Aleksandar Kasabov, a master student from the University of Amsterdam wrote a paper on "Resilient OpenDNSSEC"[20] The paper explores error situations in securing DNS zones with OpenDNSSEC and how those can be avoided. The paper also makes recommendations for increasing the resilience level which OpenDNSSEC can offer against such situations.

20 http://www.nlnetlabs.nl/downloads/publications/Aleksandar-Kasabov-OpenDNSSEC.pdf

7 The Future

In this section we discuss the future areas of attention. In the section on Finances and Organization, we will be discussing the future of NLnet Lab's funding and possible organizational changes.

A major part of the NLnet budget has traditionally been provided by a subsidy from the NLnet Foundation. NLnet Labs had a subsidy contract that guaranteed the continued operation. Unfortunately the NLnet Foundation is not able to commit to subsidizing beyond end 2015. SIDN has committed a subsidy for the 2012-2016 (inclusive) period. There is uncertainty about the financial continuity beyond 2015-2016.

As of January 2013 Han Brouwers will join NLnet Labs. His assignment is to help to develop business and/or programs that will help sustainability of NLnet Labs on the long term. NLnet Labs seeks to increase its external funding by searching for other parties that are willing to subsidize NLnet Labs activities; engage in projects and contracts that fulfill NLnet Labs chartered (public-benefit) goals; maintain a body of support contracts. Besides we seek to incorporate elements of the operation that serve a for-profit function, such as certain consultancy assignments.

NLnet Labs statutory goals are:

[…] to (further) develop and distribute on a non-profit basis Open Source Software (being software whose source code is freely available to third parties) and Open Standards (being standards developed based on a publicly accessible procedure and that may be used freely by all) for the Internet, and furthermore do all that is directly or indirectly connected thereto or conducive thereto, all this in the broadest sense.
The foundation attempts to realise its object by activities including, but not limited to, the following:

1. enabling talented software developers to develop, expand, maintain and make available Open Source Software and Open Standards for the Internet;
2. entering into collaborations of whatever kind with other developers in the area of developing projects as referred to in (a);
3. promoting a wide circulation of the developed standards or software;
4. making developers available to third parties for the development of (Open Standards for) specific Internet applications.

http://www.nlnetlabs.nl/labs/about/Statuten-20070322-eng.pdf

Details of how business development will be implemented and its relation to the strategic plan are being developed. NLnet Labs' mission and the guiding principles are *constants* within that context. The directions are the *variables* that are being reviewed. We talked about the mission and the guiding principles in the section 1, but as a quick recap:

The mission of NLnet Labs is:

To be a globally recognized technological innovation and expertise center for those technologies that turn a network of networks into an Open Internet for all.

The objectives of the NLnet Labs foundation are further captured in its statutes and the guiding principles are: Technological focus, applied R&D, Global Commons, long breath, and open ended innovation.

R&D Directions

The R&D directions are the variables, currently we are looking at logical extensions to the R&D work that NLnet currently undertakes.

- DNS: NLnet Labs intends to maintain the DNS area, whereby the focus will mainly be on enabling validation and bringing it closer to the end-user. Unbound plays a crucial role in those developments.
- Routing and Addressing: In addition we plan to strengthen our position with respect to Internet routing security, stability, and resilience. In 2013 we continue gathering requirements for a new routing toolset. Further, we've taken an interest in multi-path networking with a collaborative project with SURFnet in 2013 and start to explore software defined networking.
- A logical combination of the two fields is the area of content centric networking, a networking paradigm currently in vogue by academics.

These directions might be subject to change as the strategic plan is being reviewed (a milestone for 2013).

The NLnet Labs offices are located in Matrix II at the Amsterdam Science Park

NLnet Labs Board in 2012	name	function	end of term
	Frances Brazier	secretary	December 28, 2014
	Roelof Meijer	member	May 31, 2015
	Wytze van der Raay	treasurer	December 28, 2013
	Leo Willems	chair	February 1, 2013
	Ted Lindgreen	member	January 31, 2015
	Frans Kollee	member	May 31, 2012

8 NLnet Labs organization and finance

8.1 Board

Stichting NLnet Labs was founded on 29 December 1999 by Stichting NLnet. Its board consists of three to five members with staggered terms. The board's composition and most recent rotation schedule is shown in the tables. In May 2013 Roelof Meijer replaced Frans Kollee as board member.

Six board meetings took place in the year 2012. Olaf Kolkman participated in the board meetings in his role of Director of NLnet Labs.

Director and Board Member Additional Functions in 2012						
Frances Brazier	**Frans Kollee**	**Ted Lindgreen**	**Roelof Meijer**	**Wytze van der Raay**	**Leo Willems**	**Olaf Kolkman**
- Professor Engineering Systems Foundations at *the Technische Universiteit Delft (TU Delft)* - Vice-chair of the board of *Landelijk Netwerk Vrouwelijke Hoog leraren (LNVH)*	- Senior security consultant Madison Gurkha	none	- CEO of *SIDN* - Participant in *Platform Internet Veiligheid* - Participant in *Programmaraad Digivaardig & Digiveilig* - Chair *Digiveilig* - Member of the Council of the Board of *PI Lab* - Council member of *the ICANN ccNSO* - Participant in the *IGF* - Member of the advisory council of *Dutch ISOC Chapter*	- Team leader *CAcert critical system administrators* - Administrator, *Stichting Wereldwinkel Doorn*	- Owner TUNIX Digital Security. Member of the board of *Stichting IT Projecten (StitPro)*.	*See page 22*

Board members do not receive any compensation for their board work. If necessary, expenses may be reimbursed (€326 for 2012). The table below shows the additional functions held by board members and director of Stichting NLnet Labs.

8.2 Staff

NLnet Labs employed seven people in 2012: Jaap Akkerhuis, Olaf Kolkman (director), Wouter Wijngaards, Benno Overeinder, Matthijs Mekking, Willem Toorop, and Yuri Schaeffer. The director of Stichting NLnet Labs is responsible for the daily management of all activities of the laboratory, including development of strategies and plans for new activities.

Finances are administered by Patricia Otter of the Stichting NLnet.

8.3 Offices

NLnet Labs resided at the Amsterdam Science Park ever since its incubation in 1999. Its offices are located in the Matrix II building.

8.4 Finances

Stichting NLnet Labs primarily finances its projects and activities from grants obtained from two organizations:

1. Stichting NLnet:
   The long term financial commitment of NLnet towards NLnet labs has been codified in a subsidy contract since 2007. In 2010 NLnet Labs was given notice that because of uncertainty of available funding, that contract is terminated as of Jan 1, 2016.
2. SIDN, the Internet domain registry for the Netherlands: A subsidy contract between SIDN and NLnet Labs provides for structural financing for the period Jan 1, 2012 – December 31, 2016.

A second means of income are subsidies and donations by other parties. NLnet Labs has developed a sponsor agreement. For 2012, we would like to acknowledge AFNIC, Comcast, and Verisign for their generous support.

In addition, income may be obtained by providing Open Source Internet based consultancy and/or programming services to third parties. Unbound and NSD support contracts were sources of additional income in 2012 in the latter category.

8.5 Fiscal Status

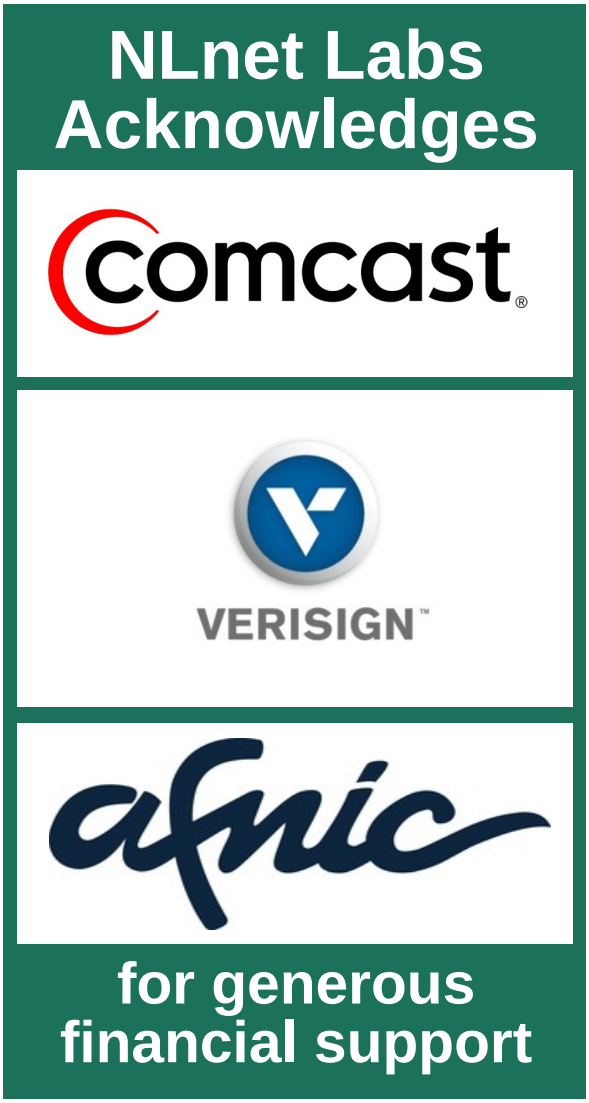
On 20 September 2007, NLnet Labs has been recognized as an institution with general benefit objectives, “Algemeen Nut Beogende Instelling (ANBI)”. This status has become relevant under new regulations that are effective as of January 1, 2008.

8.5.1 Income in 2012

At the end of 2011, a budget was drawn up for the expected staffing level and activities of NLnet Labs during the year 2012, with a total of € 646,320. Based on this budget and the expected consultancy income, grants were requested from SIDN and Stichting NLnet for € 300,000 and 236,520 respectively. Both sponsors allocated these funds for 2012, to be received by NLnet Labs on a quarterly basis, € 134,130 per quarter. By the end of 2012 it became obvious that the requested budget would be more than needed to cover 2012’s costs. This was mainly due to unforeseen consultancy and subsidy income. At the end of the year, € 115,000 subsidy could thus be returned to NLnet. The net result is that during 2012, Stichting NLnet Labs received a total of €300,000 from SIDN, € 121,520 from Stichting NLnet and a total of € 82,121 in donations (from Verisign, Comcast and AFNIC).

The total income for consultancy and support in 2012 came to € 132.658. These funds came from: the consultancy contract with ICANN (mostly ISO3660 related work); our participation in an ICANN evaluation panel in the context of the new gTLD program; the collaboration with SURFnet on RPKI that is structured as a consultancy project; the support contracts for NSD and Unbound; and finally, a compensation for the bandwidth used by the secondary server for .PT.

The only other significant source of income during 2012 was interest derived from a savings account used to deposit funds temporarily. This amounted to € 3,755



8.5.2 Expenditure in 2012

The major expenditure categories of NLnet Labs in 2012 are staff (total of 7 persons), travel and housing. Contributing to € 600,350 out of a total of € 637,845 of total costs.

Over 2013 NLnet Labs had a positive result of € 2208. The financial reserve at the start of 2013 is € 69,743

The NLnet Labs books have been audited and approved by Koningsbos Accountants BV from Amsterdam in May 2013.

8.5.3 Budget for 2013

The 2013 budget has been drawn up in October 2012. Based on having 6.7 FTE we have budgeted a total expenditure of 692k€

Income				
	2011 actual (€)	2012 actual (€)	2012 budget (k€)	2013 budget (k€)
NLnet Subsidy	447,000	121,520	237	286
SIDN Subsidy		300,000	300	286
Other Donations	92,306	82,121	27	27
Consultancy Income	19,250	56,796	16	17
NSD & Unbound Support	66,456	74,435	64	74
Interest Income	2,480	3,754	2	2
Other	2,250	1,425	0	0
Total	629,743	640,053	646	692

Expenditure				
	2011 actual (€)	2012 actual (€)	2012 budget (k€)	2013 Budget (k€)
Staff	506,490	516.926	515	547
Housing	36,225	37,840	38	40
Travel	52,385	54,964	48	52
Depreciation	2,899	2,232	4	4
Other costs	31,722	25,883	41	49
Total	629,398	637,845	646	692

NLnet Labs expects to receive about 17k€ from consulting activities, 27k€ though donations, and 74k€ from support contracts.

On January 20, 2012 Stichting SIDN signed a five year contractual commitment to subsidize 50% of the expenditure needed to execute our chartered activities. SIDN and NLnet will jointly cover 572k€ in four quarterly grants of 143k€.

8.5.4 Financial Outlook

In December 2010, Stichting NLnet has formally announced that it will terminate its subsidy contract by January 1, 2016, due to an expected lack of funds by that time. Director and board have started an effort to identify new sponsors and other sources of income with the goal of establishing a solid base for continued existence of NLnet Labs beyond the expiration of this subsidy contract.

In January 2013 Han Brouwers joined NLnet Labs as business developer. Stichting NLnet has committed to subsidize this initiative[21].

21 The Business Development is not part of our 2013 budget.

9 Publications, Presentations, Reports, and Presence

RFCs

- RFC6781: **DNSSEC Operational Practices, Version 2**, O Kolkman, W. Mekking and R.Gieben, December 2012, http://www.rfc-editor.org/rfc/rfc6781.txt
- RFC6672: **DNAME Redirection in the DNS**, S. Rose & W. Wijngaards, June 2012, http://www.rfc-editor.org/rfc/rfc6672.txt
- RFC6635: **RFC Editor Model (Version 2)**, O. Kolkman & J. Halpern, June 2012,http://www.rfc-editor.org/rfc/rfc6635.txt
- RFC6605: **Elliptic Curve Digital Signature Algorithm (DSA) for DNSSEC**, P.Hoffman & W.C.A. Wijngaards, April 2012, http://www.rfc-editor.org/rfc/rfc6605.txt

Conference Papers

- **Flexible and Robust Key Rollover in DNSSEC**, Yuri Schaeffer, Benno Overeinder and Matthijs Mekking, SATIN, March 2012, https://www.nlnetlabs.nl/downloads/publications/satin2012-Schaeffer.pdf

Technical Publications and Reports

- **Authenticated Denial of Existence in the DNS, Version 2** , Miek Gieben, Matthijs Mekking, https://www.sidn.nl/fileadmin/docs/PDF-files_UK/wp-2011-0x01-v2.pdf

Thesis and Student Reports

- **Resilient OpenDNSSEC** (MSc. Thesis), Alexandar Kosabov, University of Amsterdam, August 2012, http://www.nlnetlabs.nl/downloads/publications/Aleksandar-Kasabov-OpenDNSSEC.pdf
- **Discovering Path MTU Black Holes on the Internet Using the RIPE Atlas** (MSc. Thesis),Maikel de Boer and Jeffrey Bosma, University of Amsterdam, July 2012, http://www.nlnetlabs.nl/downloads/publications/pmtu-black-holes-msc-thesis.pdf

Work in progress

In this section we present Internet Drafts with NLnet Labs' authors or editors on which work has actively been done. The latest version published in 2012 is referenced.

- **Architectural Considerations on Application Features in the DNS**, Peterson, Kolkman, Tschofenig, and Aboba, http://tools.ietf.org/html/draft-iab-dns-applications-06
- **Principles for Unicode Code Point Inclusion in Labels in the DNS**, A. Sullivan, D. Thaler, J. Klensin, and O. Kolkman, http://tools.ietf.org/html/draft-iab-dns-zone-codepoint-pples-01
- **Technical Considerations for Internet Service Blocking and Filtering**, R. Barnes, A. Cooper, and O. Kolkman, http://tools.ietf.org/html/draft-iab-filtering-considerations-01

Conferences and other contributions

ISOC Internet New Years Event 2012, 12 January 2012, Amsterdam, The Netherlands

- Attended by NLnet Labs staff
- chairperson's debate chaird by Kolkman

Cisco SP Security Forum, Februari 2012, Amsterdam, The Netherlands

- Kolkman presented an update on DNSSEC deployment Status

Netwerk Gebruikersgroep Nederland (NGN), 9-10, 16-17 february 2012, de Meern, The Netherlands

- Kolkman (lecturer), Toorop (amanuensis), DNSSEC Train the Trainer Training

Satin 2012, March 2012, Oxford, Great Brittain,

- Scheaffer presented on Flexible and Robust Key Rollover in DNSSEC

ENISA Workshop on Resilient Internet Connections, March 2012, Amsterdam

- Kolkman and Overeinder participated

GUUG Frühjahrsfachgespräch 2012, 2 March 2012, München, Germany

- Mekking presented OpenDNSSEC

IETF 83, March 2012, Paris, France

- Akkerhuis, Kolkman, Mekking, and Overeinder participated

RIPE64, 16-20 April 2012, Ljubljana, Slovenia,

- Toorop, dnssexy, a verifying DNS(SEc) proXY
- Attended by Akkerhuis, Kolkman, Overeinder, Toorop

INET 2012, April 2012, Geneva, Swiss

- Kolkman partcipated in a round table on *Innovation on the Internet*

ISO TC46, May 2012, Berlin Germany

- Akkerhuis participated in WG2 and the ISO 3166 maintenance committee as ICANN liaison

CENTR Jamboree (Tech26, RD4, Secur1), Frankfurt am Main, DE, June 4-6

- Attended by Mekking.

ICANN 44, 24-29 june 2012, Prague, Czech Republic

- Akkerhuis and Kolkman participated

DNS Benchmarking Session, Amsterdam, NL, July 10-11

- NLnet Labs hosted a session between developers of Bind10, YADIFA, Knot and NSD. Mekking attended.

IETF 84, July 2012, Vancouver, Canada

- Akkerhuis, Kolkman, Mekking, and Overeinder participated
- Mekking attended a meeting between OpenDNSSEC and CIRA to aid their DNSSEC deployment.
- Overeinder IEPG 84 presentation on Discovering Path MTU black holes uing RIPE Atlas

S**oftware Freedom Day**, 13 September 2012, Amsterdam, The Netherlands

- Kolkman presentation: “Open...”

RIPE65, 24-28 September 2012, Amsterdam, The Netherlands,

- de Boer and Bosma, Discovering Path MTU black holes in the Internet using RIPE Atlas
- Overeinder and Homburg, MAT WG meeting presentation Measuring and Analysis Methodologies with RIPE Atlas Infrastructure
- Attended by Akkerhuis, de Boer, Bosma, Kolkman, Mekking, Overeinder, Schaeffer, Toorop

OpenDNSSEC Developers Meeting, Amsterdam, NL, September 21

- NLnet Labs hosted the OpenDNSSEC Developers Meeting. Mekking attended.

CENTR Tech27, Amsterdam, NL, September 23

- Attended by Mekking.
- Mekking was a panelist in the discussion panel on DNS rate limiting.

DENIC 2012 Conference, 25 sep 2012,

- Wijngaards presented on NSD

SURFnet Relatiedagen, October 2012, Noordwijk
Overeinder participated

Security Congress CPI, 10 October 2012, Bunnik, The Netherlands

- Kolkman presentation: “Dane, DNSSEC, & Diginotar”

IPv6 Launch Day, 6 June 2012, Amsterdam

- Overeinder in organizing committee
- Kolkman chair & opening plenary session

ECP Congress, 15 November 2012

- Kolkman presentation: “Innovation at the Waist”

IETF 85, November 2012, Atlanta, GA

- Akkerhuis, Kolkman, and Overeinder participated
- Overeinder IEPG 85 presentation on Flexible and Robus Key Rollover in DNSSEC

15 Jaar ISOC.NL, 22 November 2012, Amsterdam, The Netherlands

- Kolkman presentation: “Innovation at the Waist”

ICLN 11th Annual Conference: Combating Cybercrime, Den Haag, NL, December 13

- Akkerhuis, Mekking, and Overeinder participated

NLnet Labs staff responsibilities

- Akkerhuis:
  - ICANN representative in the ISO 3166 Maintenance Agency
  - RIPE Arbiter
  - Member of the ccNSO study group on Use of Names for Countries
- Kolkman:
  - Chair of the IETF WEIRDS working group
  - Member of the IAB internationalization and IANA evolution, ITU-T Coordination, and RFC Oversight Programs
  - IAB/IETF representative in the EU Multi-Stakeholder Platform on ICT Standardization
  - RIPE Arbiter
- Overeinder:
  - Member of the RIPE Program Committee

Stichting NLnet Labs
Science Park 400, 1098 XH Amsterdam
e-mail: labs@nlnetlabs.nl, *web*: http://www.nlnetlabs.nl/