EPP keyrelay: solving the last obstacle for DNSSEC deployment

Antoin Verschuren
SIDN Labs
antoin.verschuren@sidn.nl

DNSSEC is the security extension to the Domain Name System (DNS), which is currently being rolled out in various places around the world, including the .nl domain. One last problem remains to be resolved: how do you transfer a DNSSEC domain from one DNS operator to another without interrupting DNSSEC security? As things stand, there is no straightforward answer, and this forms a significant obstacle to the further adoption of DNSSEC.

In this whitepaper we present our solution to the problem of secure transfers. At the heart of that solution is a 'key relay': a new concept, in which the registry acts as an intermediate for the transfer of public key material from the gaining to the loosing DNS operator. A mechanism of this kind is required because the loosing DNS operator needs the gaining DNS operator's key material for pre-publication. Our approach is independent both of the actors' business roles and of the communication protocols used; it is widely supported by .nl registrars and easy to implement. To realise the key relay mechanism we introduce a new EPP protocol command: EPP keyrelay.

I. Introduction

The Domain Name System (DNS) [1] is one of the internet's base protocols. It converts easily to remember names into the addresses of the computers on which applications are technically located. The DNS is used by almost all internet applications, making it critical to the working of the internet.

DNSSEC [2] is the security extension to the DNS. It ensures that DNS responses cannot be manipulated to divert users to another computer without them realising. DNSSEC therefore contributes directly to internet security and plays an important role in maximising user confidence in the internet. DNSSEC secures DNS responses by adding signatures generated using private keys. The signatures can be validated using public keys. A validated DNS response is described as 'secure'.

DNSSEC is currently being rolled out by various actors, including Google, Comcast and various country-code domains, such as .br (Brazil), .cz (Czech Republic) and .se (Sweden). In 2012, SIDN rolled out DNSSEC on a large scale: at the time of writing (July 2013 [3]) the .nl domain has more than 1.5 million domain names secured with DNSSEC. Indeed, .nl currently has more DNSSEC-secured domain names than any other TLD in the world. However, the domain's leading role in this field also means that it is the first to be significantly affected by an as yet unresolved problem: how to transfer a DNSSEC domain from one DNS operator to another. Having a lot of DNSSEC domains inevitably means that transfers of DNSSEC domains is relatively commonplace in .nl. During the experimental phase of DNSSEC deployment, it was still acceptable to briefly disable a domain name's DNSSEC protection while the infrastructure was updated. However, the future implementation of DNSSEC-based extensions, such as DANE [4], will make it necessary for domain names to permanently remain secure, even when the DNS infrastructure is being updated or a service provider is changed. If DNSSEC is temporarily disabled during a transfer, protocols such as DANE will not work and any service or website that depends on DANE will be temporarily unavailable.

Not being able to transfer a DNSSEC domain while keeping security intact, is therefore a significant obstacle to the further rollout of DNSSEC and thus to the further enhancement of internet security. In this whitepaper, we introduce our solution to the problem of secure transfers. At the heart of that solution is a 'key relay': a new concept, in which the registry acts as a central point for the transfer of key material from the gaining to the loosing DNS operator and thus facilitates to maintain security throughout the transfer process. Our approach has a number of unique advantages: it is independent both of the actors' business roles and of the communication protocols used; it is widely supported by .nl registrars and it is easy to implement. To make key relay possible at the protocol level, we are introducing a new command to the Extensible Provisioning Protocol (EPP) [5]: the EPP keyrelay command.

The remaining sections of this paper set out the pre-conditions for secure transfers (Section II) and how they apply to the transfer process (Section III). We then explain how we realised key relay (Section IV), and we conclude with a summary and future work (Section V).

II. The domain name industry

A. Domain transfers

Even without DNSSEC, transferring a domain to another DNS operator has always been problematic. When a service switches to another supplier, it is desirable that the two suppliers cooperate to make the transfer as smooth as possible for the end customer. In the case of a DNS transfer without DNSSEC, the loosing DNS operator should continue operating the name servers as secondary service for the relevant zone for some time, so that (a) querying name servers (resolvers) that reach the old authoritative name servers learn what the new authoritative name servers are and (b) the old name servers give the same responses as the new name servers. In the period immediately following a name server change, resolvers often continue to reach the old authoritative name servers for a while, because they have cached earlier responses of the NS RRset for the zone.

In practice, DNS without DNSSEC is very resilient and able to cope with many operational shortcomings. Consequently, even though many DNS operators are not as diligent as they might be in terms of cooperating when customers leave them, the customers are barely inconvenienced. The loosing operator abruptly drops its DNS service, and DNS without DNSSEC accepts any new response that the resolver receives from the new operator's name servers; the only impact is a small delay and extra DNS queries. Unfortunately, however, such a resolver will also accept a response from any name server operated by a man-in-the-middle.

With DNSSEC, things are clearly different. With DNSSEC, the 'chain of trust' must remain intact for a resolver to accept a DNS response [2]. Not just any response is accepted by a validating resolver to prevent man-in-the-middle attacks. So far, we only know of one solution to transfer a DNSSEC domain without breaking the chain of trust under any circumstances [6]. For this solution to work however, it is necessary for both DNS operators each having the other's public DNSSEC keys and cooperating to ensure that, during the transition period, a resolver will accept both responses from either the old or the new servers. In order to understand why such cooperation between operators is considered problematic, we shall first explain the various roles played by actors in the domain name registration model.

B. Roles in the domain name industry

In the years since the DNS was created, the way that domain names are managed has changed considerably. The technical model has remained fairly simple. There is a 'parent zone' and 'child zone' (see Figure 1). The parent zone is administered by a 'registry' and the child zone is administered by a 'registrant'.

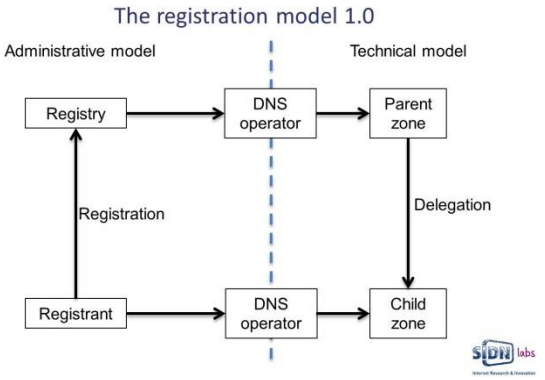

Figure 1. The traditional registration model

Administratively, however, increasing competition and commercialisation have led to the development of a complex matrix of actors, each seeking to play a part in the registration of domain names. Between the registry and the registrant, a variety of administrative intermediary roles have emerged, involving service providers such as registrars, resellers, third-party hosters and DNS operators (see Figure 2). Because a single actor will often perform several roles in the chain, discussions on this topic are often muddied by misunderstandings about what a role entails, and individual parties tend to be nervous about relinquishing responsibility and control, because that may imply losing business.

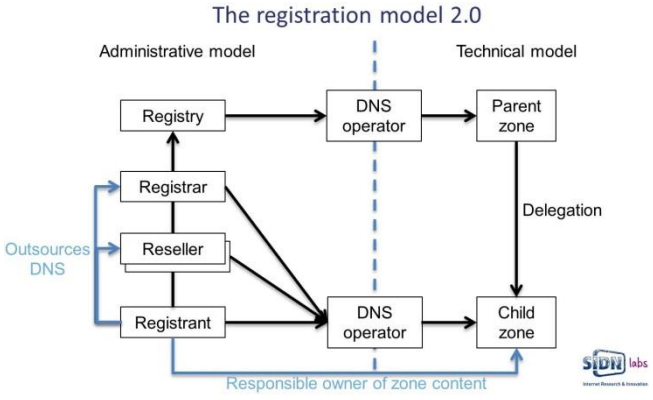

Figure 2. The modern registration model

An effective solution to the secure transfer problem therefore needs to address the cooperation issue and must work regardless of how the various roles are combined in practice and must make no assumptions about who fulfils what role. Any discussion of DNSSEC operator changes is complicated by the fact that the most important role in this process, that of the DNS operator maintaining the DNSSEC key material for the zone, is not properly recognised in the

context of the existing processes. In the past, it was automatically assumed that the registrant was also the DNS operator for the relevant child zone. However, that role is nowadays usually executed by a registrar, reseller, website hoster or another third party. Each of those actors is apt to regard the role of DNS operator as a natural part of their own activities, whereas the role is in fact outsourced by the registrant and it is therefore important that in the model the various roles remain distinct.

III. Secure transfer

A. Mechanism

For the secure transfer of a DNSSEC domain, each of the two DNS operators involved need to temporarily include the other's public Zone Signing Key (ZSK) in its own version of the zone [6]. The gaining operator can securely look up the loosing operator's ZSK in the DNS using DNSSEC. However, there is no secure channel for obtaining the gaining operator's ZSK. That is because the future zone has not yet been delegated, so there is as yet no chain of trust to validate a key obtained from the gaining operator's zone. Because there are very many DNS operators, putting them all in secure contact with each other would be unworkable.

The innovation that we are proposing is therefore to have DNS operators communicate the key via the channel that they already use to register domain names and to maintain their registrations: the administrative channel for communication with the registry. We will call this interaction a 'key relay': the key is 'relayed' by sending it to the registry. The registry passes the key on to the current registrar for the domain, which can make sure it ends up at the loosing DNS operator (see Figure 3).

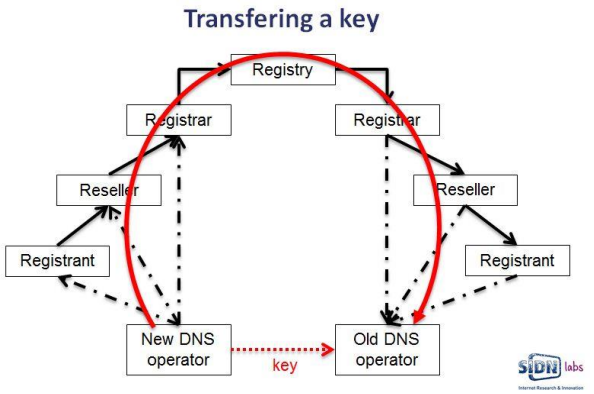

Figure 3. Sending the ZSK to the loosing DNS operator via the registry

The advantage of key relay is that it is a stateless mechanism, making it scalable, it's easy for the registry to realise and straightforward for registrars and resellers to automate (see Section IV.A). Furthermore, the registry or registrar can verify whether the key relay request has been authorised by the registrant, so that the loosing DNS operator can automatically include the key in the 'old' zone. Moreover, the process is agnostic to the different roles that may or may not be present in the chain, or who plays the role of DNS operator.

B. Stakeholder survey

In order arrive at a solution to the problem of DNSSEC operator changes that enjoyed widespread support, we undertook a survey amongst leading registrars, resellers, DNS experts and peer registries. We took note of all stakeholders' wishes and sought to address the risks that they foresaw.

Registries, for example, did not want the responsibility of monitoring difficult timers in their processes; nor were they happy with the idea of any given registrar being able to modify objects they did not own in the database. It was also important to the registries that registrants were free to choose their registrar and that it was always clear at any point who the current registrar of record was. For their part, the registrars and resellers were keen that everything could easily be automated, without manual checks. They also wanted to retain control in the event the loosing operator did not cooperate or to respond quickly enough. The DNS operators indicated that it was important to be sure that the addition of a key to the zone was done with the registrant's approval and to know how long a key should remain in the zone in case the transfer was ultimately aborted.

C. Overview of the secured domain name transfer process

Figure 4 shows that the process of transferring a DNSSEC domain involves a number of steps. Key relay is a self-contained step in the process, which could be used for other purposes as well in the future.

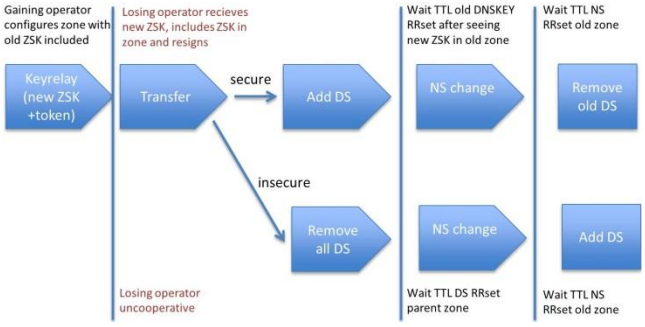

Figure 4. The DNSSEC operator change process

Once the key relay step is complete, the next steps in the process can be executed. These are all existing registry processes that do not change. The only thing that changes in the entire DNSSEC transfer process (in case the DNS operator maintaining the key material changes) is that it is preceded by the key being relayed from the gaining to the loosing DNS operator.

The remainder of the process is separate from the key relay because the timing of the remaining steps depends on various TTL settings, which allow the gaining registrar to retain control over the quality and speed of the transfer. Regardless of whether administrative control of a registration is transferred from one registrar to another, a key relay is only needed if there is a change in the DNS operator responsible for the DNSSEC key material. If there is no change of registrars, but only DNS operators change, the transfer step can be removed from the process.

If the loosing DNS operator cooperates, the 'secure path' is followed (upper path in Figure 4). However, the gaining registrar can always opt for the 'insecure path' and therefore retains control.

One point to note is that, if a domain is secured with DNSSEC prior to a transfer, the number of steps that the transfer entails is the same, whether the secure path or the insecure path is followed. An interval between the individual steps is required because it takes time for an established chain of trust to be updated or removed in the caches of all resolvers. Without any intervals, the domain would be regarded as bogus by validating resolvers, rendering it non-functional. This is also why a transfer of a DNSSEC domain always involves more steps than the transfer of a domain without DNSSEC. Not only the delegation must be updated in the caches, but also the existing chain of trust must be renewed.

IV. KEY RELAY

A. Execution

Key relay execution involves two subprocesses:

1. From gaining DNS operator to the registry:
   You receive a key relay request from a subordinate actor (compare Figure 3). For example, you are a reseller and you receive a key relay request from a registrant. You then forward it to the future superordinate actor. In our example, that means to your registrar. Each actor follows suit until the request reaches the registry. A key relay request must be accompanied by the authorisation token provided by the current registrant. With this token, the registry or loosing registrar can validate that the request has been authorised by the existing registrant.
2. From the registry to the loosing DNS operator:
   You receive a key relay request from a superordinate actor, which you forward to the subordinate actor on the loosing side (the actor with current responsibility on the loosing side). Each actor follows suit until the request reaches the loosing DNS operator. That operator knows that the request has been authorised by the existing registrant, because the registry or registrar has validated the authorisation token. The loosing DNS operator can therefore immediately add the key to the current zone for the domain.

Both steps are still viable, even if the registrar (or another actor) remains the same, or if, for example, the chain does not include a reseller. Furthermore, it makes no difference which actor plays the role of DNS operator. At least one actor in the chain should know who performs the DNS operator role; otherwise the domain could never have been delegated.

The process can be completely automated, providing all actors have their administration and provisioning in order. The communication between the registrars and registry usually takes place through EPP messages, but communication between other actors in the chain (DNS operator, registrant, reseller) usually not. However, it makes no difference to the model what protocol the communication uses, providing that the channel used is at least as secure as the one used to register or maintain the domain. This makes the key relay concept generally applicable.

The process is also straightforward for the registry. The registry receives a key relay request from a random registrar. Upon receipt, the registry may validate the registrant's authorisation token provided in the key relay request, and then queries the registry database to find the current registrar of record for the domain specified in the request. The key relay request is then forwarded straight to that registrar. That is all that happens. No changes are made to the database and there is no need to monitor a state or timer. The registry merely facilitates the communication between the registrars.

B. EPP keyrelay command

As indicated above, administrative communication between registry and registrars usually takes place through the provisioning protocol EPP [5]. Therefore, to realise the key relay mechanism within the registry, we have formulated a new EPP command: EPP keyrelay [7].

The EPP keyrelay command contains various familiar fields, plus fields providing the following information:

- The domain name
- The public key to be relayed
- The current registrant's authorisation token
- How long the key should remain in the old zone
- The registrar submitting the key relay request

That information is submitted to the registry by the gaining registrar in the EPP keyrelay command. The registry relays the unaltered information by placing a message in the EPP message queue of the current registrar of record for the domain in question.

Most EPP commands relate to the modification of objects in the registry database by the existing registrar of record for a domain. Only the registrar appointed by the registrant is entitled to modify the registry data for a given domain. EPP also recognises a transfer command (for changing the registrar responsible for a domain name), which also modifies an object in the database, but may be submitted to the registry by any given registrar. Because any registrar may initiate a transfer, the command has to include an authorisation token obtained by the registrant from the current registrar of record, so that the registry can verify that the initiating registrar is acting on the registrant's behalf.

The EPP keyrelay command is similar to the transfer command, but serves to initiate a change of the DNS operator for a domain, and not always a change of registrar. Like a transfer command, it may be submitted to the registry by any registrar, but it does not result in modification of any objects in the database. What it does do is trigger an action, usually for another actor than the registrar submitting the command. To make sure that that action is not triggered abusively, the key relay command, like the transfer command, must include an authorisation token provided by the registrant

The EPP keyrelay command that we are proposing is therefore not only a new command, but also a new command category. At present, the EPP protocol recognises three categories of commands: session management commands, query commands and object transform commands [5]. The EPP keyrelay command cannot be placed in any of those categories; it is best described as a 'communication command'.

In some cases, the key relay process will not ultimately be followed by the transfer of the zone, or that a transfer will be subsequently reversed by the registrant. Furthermore, some DNS operators will wish to oversee the process closely and, where critical domain names are concerned, perform manual progress checks. As a result, the process will take longer with some operators compared to others. Therefore, to ensure that, following automated addition to the zone managed by the loosing operator, keys are neither removed from the 'old' zone too soon nor left there too long, the gaining operator may specify in a key relay request how long the key should remain in the old zone. After elapse of the specified period, the loosing operator may safely remove the key from the zone if the zone transfer does not conclude after all.

When we surveyed our stakeholders, operators indicated to us that they would like to know who had submitted a key relay request, so that, if technical flaws were found in the key material or if other technical issues arose, the loosing operator would be able to contact the gaining operator. The final feature of the EPP key relay command is therefore the ID of the registrar that submitted the command at the registry.

Making the EPP keyrelay command a self-contained command, rather than developing a complex combined operator change plus domain transfer process, avoids the need to change any other EPP commands. It also means that the EPP keyrelay command may be used in the context of other processes in the future that require the exchange of key material.

C. Implementation in DRS

As the registry for .nl, SIDN has already implemented the proposed solution in its own Domain Registration System (DRS). By facilitating the DNSSEC operator change process, we have removed a significant obstacle to DNSSEC adoption and contributed to the security of the .nl zone.

Implementation in SIDN's registration system was relatively straightforward, because the EPP keyrelay command does not modify the database. It did not require the creation of any new tables or the revision of existing tables. EPP keyrelay simply involves a database query and the whole process is external to the database. Furthermore, EPP keyrelay is a facilitating command. There is no obligation to relay a key via the registry. If DNS operators wish to communicate with each other directly, they remain free to do so.

Most .nl registrars that support DNSSEC have indicated that they intend to adopt our new secure transfer method as soon as EPP keyrelay is standardised by the IETF. Their motivation is that, without such a process, not only are existing customers compromised in their ability to securely transfer domain names elsewhere, but also new customers are compromised in their ability to securely transfer in domain names. The appearance on the horizon of applications such as DANE [4] makes smooth transfers all the more important and market players wish to support their customers in that regard.

V. Conclusions and plans for further work

This whitepaper sets out our solution for DNSSEC operator changes, the last remaining problem with provisioning DNSSEC. The innovative aspect of the solution is the concept of a 'key relay', which uses the registry as central trust anchor to facilitate secure communication of the public ZSK from the gaining to the loosing DNS operator. Our approach is independent both of the actors' business roles and of the communication protocols used; it is widely supported by .nl registrars and it is easy to implement. We therefore believe that key relay is the ideal mechanism for effecting DNSSEC operator changes and that it therefore removes the final obstacle to the further rollout of DNSSEC.

We have submitted the key relay process and the associated EPP syntax to the IETF as an internet draft [7] and are working with the internet community to secure RFC status for our proposed methodology. Both feedback and simple expressions of support are welcome using the IETF's public provreg mailing list [8] where EPP extensions are being discussed. The initial response to the draft has been very positive.

Future work on the increased adoption of DNSSEC on the authoritative side consists of policy development and marketing. Some registries, including New Zealand's country-code registry, have decided to oblige registrars by policy to cooperate with the transfer of DNSSEC-signed domains. On the technical side, SIDN still needs to implement the key relay process in its registration system's web interface, thus complementing the EPP interface implementation. Furthermore, more ISPs need to be persuaded to support DNSSEC validation, so that DNSSEC is actually available to end users and thus contributes to internet security in practice.

Acknowledgements

Thanks are due to Miek Gieben, Marc Groeneweg, Rik Ribbers, Marco Davids and Cristian Hesselman.

References

[1] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

[2] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, "Resource Records for the DNS Security Extensions", RFC 4034, "Protocol Modifications for the DNS Security Extensions", RFC 4035, March 2005.

[3] https://www.sidn.nl/kennisbank/statistieken/

[4] Hoffman, P., and J. Schlyter, "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA", RFC 6698, August 2012.

[5] Hollenbeck, S., "Extensible Provisioning Protocol (EPP)", STD 69, RFC 5730, August 2009.

[6] Koch, P., Sanz M. and A.L.J. Verschuren, "Changing DNS Operators for DNSSEC signed Zones", draft-koch-dnsop-dnssec-operator-change-05 (work in progress), July 2013.

[7] Gieben, R., Groeneweg, M., Ribbers, R., and A.L.J. Verschuren "Key Relay Mapping for the Extensible Provisioning Protocol" draft-gieben-epp-keyrelay-03 (work in progress), July 2013.

[8] PROVREG mailing list, https://www.ietf.org/mailman/listinfo/provreg