

European Union's Horizon 2020 Programme
European Commission
Directorate General for Communications Networks, Content and Technology
eInfrastructure



Magic

Middleware for collaborative Applications
and Global virtual Communities

Deliverable D4.3

Three (newly delegated countries or already members) participants that secured the country code prefix ENUM zone with DNSSec

Periodical Progress Report

MAGIC Deliverable: 4.3 Three (newly delegated countries or already members) participants that secured the country code prefix ENUM zone with DNSSec

Document Full Name	D4.3 Three (newly delegated countries or already members) participants that secured the country code prefix ENUM zone with DNSSec
Date	30-11-2016
Activity	Agreements for real time communications
Lead Partner	RENATA®
Document status	Final
Classification Attribute	Public
Document link	

Abstract: This report explains the countries that implemented DNSsec for its NRENum.NET service. The DNSsec allows to secure the domain name system zone to avoid possible attacks.



COPYRIGHT NOTICE

Copyright © Members of the MAGIC Project, Dec 2016.

MAGIC (Middleware for collaborative Applications and Global vIrtual Communities – Project number: 654225) is a project co-funded by the European Commission within the Horizon 2020 Programme (H2020), Directorate General for Communications Networks, Content and Technology - eInfrastructure. MAGIC began on 1st May 2015 and will run for 24 months.

For more information on MAGIC, its partners and contributors please see <http://www.magic-project.eu>.

You are permitted to copy and distribute, for non-profit purposes, verbatim copies of this document containing this copyright notice. This includes the right to copy this document in whole or in part, but without modification, into other documents if you attach the following reference to the copied elements: "Copyright © Members of the MAGIC Project, 2015".

Using this document in a way and/or for purposes not foreseen in the paragraph above, requires the prior written permission of the copyright holders.

The information contained in this document represents the views of the copyright holders as of the date such views were published.

THE INFORMATION CONTAINED IN THIS DOCUMENT IS PROVIDED BY THE COPYRIGHT HOLDERS "AS IT IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE MEMBERS OF THE MAGIC COLLABORATION, INCLUDING THE COPYRIGHT HOLDERS, OR THE EUROPEAN COMMISSION BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THE INFORMATION CONTAINED IN THIS DOCUMENT, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.



This project is co-funded by the Horizon 2020
Framework Programme of the European Union



A project implemented by RedCLARA



DELIVERABLE ROUTE

	Name	Member/Activity	Date	Responsible
From	Gustavo García	RedCLARA	30-9-2016	RENATA
Revised by				
Revised by				
Revised by				
Revised by				
Revised by				
Revised by				
Approved by	Florencio Utreras	RedCLARA/CEO	12-12-2016	RENATA





TABLE OF CONTENTS

COPYRIGHT NOTICE.....	3
DELIVERABLE ROUTE.....	4
1. Introduction.....	6
2. Glossary.....	6
3. References.....	6
4. DNSsec implementation procedure.....	7
5. Nrens that implemented dnssec.....	7
6. conclusions.....	8
7. Document Amendment Procedure.....	9





1. INTRODUCTION

One of the defined work package goals was that NRENs implement the DNSsec for its NRENum.NET servers. DNSsec is a technology that add security certificates so they can validate the authenticity of the name system information. DNSsec does not encrypt information, it just allow to sign the answers from the DNS server on domain A, so the receiving party in domain B can validate that the responding party is valid. This allows to avoid various DNS security attacks that allow hackers to poison DNS caches so they return incorrect IP addresses or still data from the end users. The DNSsec implementation was a well received strategy among the implementing NRENs, and this report shows how many of them implemented.

2. GLOSSARY

DNS	Domain Name System
EC	European Commission
EU	European Union
EU-LAC	Europe, Latin America and the Caribbean
E.164	ITU Recommendation for telephone numbering format
ENUM	E.164 number mapping using DNS service
NRENum.NET	ENUM service run by GÉANT
NREN	National Research and Education Network

3. REFERENCES

- [R1] MAGIC Website <http://www.magic-project.eu>
- [R2] NRENum.net Website <https://nrenum.net>





4. DNSSEC IMPLEMENTATION PROCEDURE

The DNSsec implementation carried out by the organizations on this report, is compound of three main steps:

- a) Installation and setup of the secure DNS software
- b) Generation of the zone certificates
- c) Register the domain certificates on the domain registrar organization.

The installation of the secure DNS software is done using standard Linux tools, and it is documented on the NRENum.NET manual developed in the MAGIC project:

http://clara.fun-campus.net/courses/course-v1:MAGIC+NRENUMen+2016_T4/about

The generation of the zone certificates, also known as zone signing usually involves the creation of certificates (private and public keys) for the server. On the OpenDNSsec solution, the step will be something like:

```
softhsm --init-token --slot 0 --label "OpenDNSSEC"
```

The next step, will be to use the public key to sign the zone. The step will be something like:

```
ods-signer sign 7.5.redclara.net
```

Once the zone is signed, there is a hash string that must be send to the NRENum.NET tree managers in order to associate it with the specific zone. This is an administrative step, and can be included in the zone delegation form.

5. NRENS THAT IMPLEMENTED DNSSEC

The following NRENS implemented DNSsec within the MAGIC WP4 scope of work:

	Country	DNSsec implementation date
CESNET	Czech Republic (+420)	Dec 2, 2015
RAAP	Perú (+51)	Dec 12, 2015
RENATA	Colombia (+57)	January 21, 2016
RAICES	El Salvador (+503)	April 25, 2016
CEDIA	Ecuador (+593)	July 26, 2016





All implementations were validated and registered with the NRENum.NET service. Each of them received a confirmation email like the following:

----- Forwarded Message -----

Subject: [discussion] Welcome Czech Republic to NRENum.net (+420) + DNSSEC!!
Date: Wed, 2 Dec 2015 23:00:48 +0100
From: MÉSZÁROS Mihály <misi@niiif.hu>
To: discussion@nrenum.net
CC: delegations@nrenum.net <delegations@nrenum.net>, Jan Ruzicka <janru@cesnet.cz>, Peter Szegedi <peter.szegedi@geant.org>

Welcome CESNET, Czech Republic to NRENum.net!

@Jan Thank you very much for your cooperation!

Country code +420 is now officially delegated to CESNET!

Please add at least few NAPTR records to your new 0.2.4.nrenum.net zone (if it is not done already) to make it fully functional, and get on the crawler list <https://crawler.nrenum.net/>

I am very happy to announce that zone 0.2.4.nrenum.net is already using DNSSEC!

Nice job & Many thanks to Jan!

If You are not yet subscribed, then I strongly suggest to subscribe to discussion@nrenum.net list, to keep you up to date with nrenum.net, keep you informed about any further changes.

@Péter Please update the nrenum.net wiki, map etc. according the change.

Thanks in advance,
Misi

6. CONCLUSIONS

The working group can said that NRENum.NET sale is harder than DNSsec. In some of the cases, the NRENs just required the recommendation and the goal set, and they went into the implementation by them self. Advertising and proper communication the new entering countries could encourage and promote the adoption in others. The MAGIC project members will continue the effort to engage partners in the DNSsec implementation path.



This project is co-funded by the Horizon 2020
Framework Programme of the European Union



A project implemented by RedCLARA



7. DOCUMENT AMENDMENT PROCEDURE

Requests for amendments to this document must be made to the author, Gustavo García, WP4 – RedCLARA, gustavo.garcia@redclara.net, and copied to the Management of the MAGIC project.



This project is co-funded by the Horizon 2020
Framework Programme of the European Union



A project implemented by RedCLARA