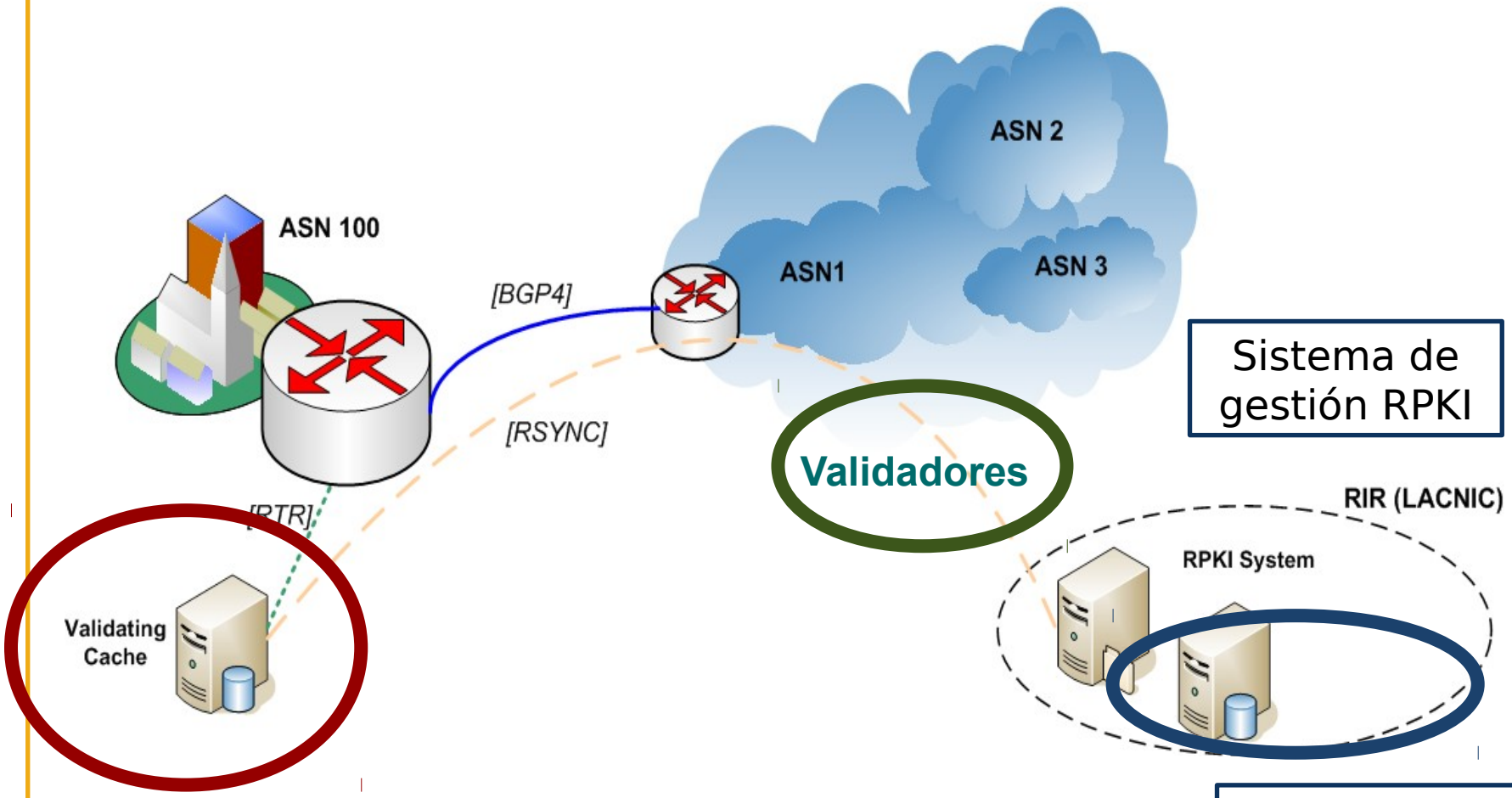
Seminario Virtual RPKI en practica (2-4)

Carlos Martínez
Gerardo Rada
LACNIC I+D

Arquitectura RPKI



Material Publico

- No posee información del sujeto
- BIT CA encendido
- Extensiones definidas en RFC 3779

Certificados X509v3

- Igual al de cualquier PKI
- Lista de los seriales asociados a los certificados revocados

CRL

- CMS
- Información de ruteo
- Bloques Ips
- ASN único

ROAs

- CMS
- Listado del material firmado
- Hash y nombres de archivos

Manifiestos

Material Publico
Cert X509 v3

Emitido por Verisign

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            36:21:f4:76:13:c4:f4:c3:59:ea:95:83:f5:de:fa:b4
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=Terms of use at https://www.ver
isign.com/rpa (c)10, CN=VeriSign Class 3 International Server CA - G3
        Validity
            Not Before: Mar 28 00:00:00 2011 GMT
            Not After : Mar 27 23:59:59 2012 GMT
        Subject: C=US, ST=Florida, L=Miami, O=TODO1 Services Inc., OU=Technology, CN=www30.todo1.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:ca:d6:17:a2:ae:4b:f6:19:74:d9:b4:14:83:ba:
                    82:82:77:2e:c4:35:47:18:e5:af:ab:7c:f9:06:cd:
                    88:a6:2e:29:80:e5:b8:02:e7:c3:f9:39:1a:92:9f:
                    cc:ea:d1:bb:8f:5a:c9:af:02:16:38:e6:d6:cc:15:
                    21:1b:26:b7:63:a7:bd:5f:ed:be:b3:43:46:e9:8f:
                    4d:3a:1d:b7:0c:ca:b7:74:f5:3b:3e:68:d7:1a:4c:
                    74:6f:a0:fd:e5:a7:e3:03:91:f7:3f:15:bb:c3:f1:
                    7e:a0:61:81:7a:fd:27:6f:1a:a4:10:fe:49:c5:ab:
                    b3:10:b4:15:7e:f3:eb:9c:3d
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Key Usage:
                Digital Signature, Key Encipherment
            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://SVRIntl-G3-crl.verisign.com/SVRIntlG3.crl

            X509v3 Certificate Policies:
                Policy: 2.16.840.1.113733.1.7.23.3
                  CPS: https://www.verisign.com/rpa

            X509v3 Extended Key Usage:
                Netscape Server Gated Crypto, TLS Web Server Authentication, TLS Web Client Authentic
ation
            Authority Information Access:
                OCSP - URI:http://ocsp.verisign.com
                CA Issuers - URI:http://SVRIntl-G3-aia.verisign.com/SVRIntlG3.cer

            1.3.6.1.5.5.7.1.12:
                0`.^.\0Z0X0V..image/gif0!0.0...+......Kk.(.....R8.).K..!..0&.$http://logo.verisign.co
m/vslogo1.gif
    Signature Algorithm: sha1WithRSAEncryption
        08:c2:98:ef:17:11:d2:2d:2d:ed:74:23:98:69:e7:21:f9:92:
        bd:d0:52:47:96:6e:e3:96:35:7b:af:57:02:63:41:73:21:e5:
        12:88:8a:27:19:a8:5d:ae:2b:42:7c:3d:2e:ef:cc:7c:9b:0f:
        99:3d:82:4d:20:99:1d:a9:6f:6f:6a:b5:ef:2c:f1:cc:71:03:
```

Emitido por LACNIC

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 411423 (0x6471f)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN=QRonip0StN3-cpQwD-BsqEB-2I8
        Validity
            Not Before: Jan  7 16:48:15 2011 GMT
            Not After : Aug 22 05:00:00 2012 GMT
        Subject: CN=gjiKwYHjDnfxr4RAAyle259qbzU
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:9c:20:f9:00:57:d4:c3:54:0c:12:63:2f:ed:0c:
                    d6:09:46:6e:bf:af:df:b5:d8:02:3f:30:11:85:3d:
                    90:03:d1:86:22:90:30:4c:32:c5:f5:be:3f:63:ab:
                    ab:0d:14:2e:98:01:2f:b4:76:80:78:40:34:85:b1:
                    0f:b3:84:7b:93:df:35:92:e9:e1:09:80:5d:a0:27:
                    79:d0:1c:df:5b:f8:94:04:d9:82:71:ae:09:de:5d:
                    54:98:03:7c:66:d1:fd:ab:7c:f7:ba:b4:81:b0:f2:
                    77:0a:cb:29:46:d8:55:e5:c3:49:97:e7:18:13:7b:
                    30:17:32:e9:5d:63:fa:68:89:ae:63:97:5a:4c:63:
                    dd:79:e4:37:c4:19:6b:fc:84:ec:45:25:ed:61:12:
                    98:cb:09:46:2c:da:b2:3f:c0:a9:d6:aa:52:c4:ec:
                    a5:94:ba:7c:bc:3c:d0:fd:6c:d6:00:ec:19:a4:ab:
                    12:95:c3:9f:06:6c:af:3e:1a:c0:17:a1:3a:aa:d7:
                    bb:ca:a1:6c:2e:ae:cf:f3:68:fe:d4:dc:1c:78:96:
                    12:17:0b:e9:d2:39:6d:34:1b:89:7e:55:76:74:a7:
                    d0:1a:0c:68:1f:9b:3d:90:08:04:a3:93:2e:63:67:
                    b3:32:83:e9:72:e4:fa:8b:06:a0:79:d6:eb:5b:52:
                    b3:25
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                D1:4F:E0:62:F9:9A:DB:95:AB:0B:5B:0E:F3:DC:9E:DD:AA:EB:9A:30
            X509v3 Authority Key Identifier:
                keyid:81:18:43:75:41:AF:CD:C7:7D:93:14:B6:F2:37:1C:94:75:70:B4:A5

            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            Authority Information Access:
                CA Issuers - URI:rsync://repository.lacnic.net/rpki/lacnic/QRonip0StN3-cpQwD-BsqEB-2I8.
cer

            Subject Information Access:
                CA Repository - URI:rsync://repository.lacnic.net/rpki/hosted/440465ff-0035-4e16-bec1-8
e3e32e3499d/
                1.3.6.1.5.5.7.48.10 - URI:rsync://repository.lacnic.net/rpki/hosted/440465ff-0035-4e16-
bec1-8e3e32e3499d/gjiKwYHjDnfxr4RAAyle259qbzU.mft

            X509v3 CRL Distribution Points:
```

Material Publico Cert X509 v3

Emitido por Verisign

```
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=Terms of use at https://www.ver
isign.com/rpa (c)10, CN=VeriSign Class 3 International Server CA - G3
        Validity
            Not Before: Mar 28 00:00:00 2011 GMT
            Not After : Mar 27 23:59:59 2012 GMT
        Subject: C=US, ST=Florida, L=Miami, O=TODO1 Services Inc., OU=Technology, CN=www30.todo1.com
        Subject Public Key Info:
```

Emitido por LACNIC

```
            Serial Number: 411423 (0x6471f)
            Signature Algorithm: sha256WithRSAEncryption
            Issuer: CN=QRonip0StN3-cpQwD-BsqEB-2I8
            Validity
                Not Before: Jan  7 16:48:15 2011 GMT
                Not After : Aug 22 05:00:00 2012 GMT
            Subject: CN=gjiKwYHjDnfxr4RAAyle259qbzU
            Subject Public Key Info:
                Public Key Algorithm: rsaEncryption
```

Material Publico
Cert X509 v3

Emitido por Verisign

```
X509v3 extensions:
    X509v3 Basic Constraints:
        CA:FALSE
    X509v3 Key Usage:
        Digital Signature, Key Encipherment
    X509v3 CRL Distribution Points:
```

Emitido por LACNIC

```
X509v3 extensions:
    X509v3 Subject Key Identifier:
        D1:4F:E0:62:F9:9A:DB:95:AB:0B:5B:0E:F3:DC:9E:DD:AA:EB:9A:30
    X509v3 Authority Key Identifier:
        keyid:81:18:43:75:41:AF:CD:C7:7D:93:14:B6:F2:37:1C:94:75:70:B4:A5

    X509v3 Basic Constraints: critical
        CA:TRUE
    X509v3 Key Usage: critical
        Certificate Sign, CRL Sign
```

Material Publico
Cert X509 v3

Emitido por LACNIC

```
            Authority Information Access:
                CA Issuers - URI:rsync://repository.lacnic.net/rpki/lacnic/QRonip0StN3-cpQwD-BsqEB-2I8.
cer

            Subject Information Access:
                CA Repository - URI:rsync://repository.lacnic.net/rpki/hosted/440465ff-0035-4e16-bec1-8
e3e32e3499d/
                1.3.6.1.5.5.7.48.10 - URI:rsync://repository.lacnic.net/rpki/hosted/440465ff-0035-4e16-
bec1-8e3e32e3499d/gjiKwYHjDnfxr4RAAyle259qbzU.mft

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:rsync://repository.lacnic.net/rpki/hosted/12ab5638-2298-4687-a4b3-9888331a1104/QR
onip0StN3-cpQwD-BsqEB-2I8.crl

            X509v3 Certificate Policies: critical
                Policy: 1.3.6.1.5.5.7.14.2

            sbgp-ipAddrBlock: critical
                IPv4:
                  190.112.52.0/22

            sbgp-autonomousSysNum: critical
                Autonomous System Numbers:
                  52266

    Signature Algorithm: sha256WithRSAEncryption
        4e:9b:49:2b:5f:7f:21:97:ce:16:a8:5e:5b:6d:0c:99:a6:f7:
```

Material Publico
CRL

```
Certificate Revocation List (CRL):
        Version 2 (0x1)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: /CN=QRonip0StN3-cpQwD-BsqEB-2I8
        Last Update: Mar 31 03:00:00 2011 GMT
        Next Update: Mar 31 15:00:00 2011 GMT
        CRL extensions:
            X509v3 Authority Key Identifier:
                keyid:81:18:43:75:41:AF:CD:C7:7D:93:14:B6:F2:37:1C:94:75:70:B4:A5

            X509v3 CRL Number:
                408
Revoked Certificates:
    Serial Number: 07A973
        Revocation Date: Jan 11 20:14:24 2011 GMT
    Serial Number: 1AA148
        Revocation Date: Mar 27 16:45:00 2011 GMT
    Serial Number: 1F8C0F
        Revocation Date: Mar 29 20:52:31 2011 GMT
    Signature Algorithm: sha256WithRSAEncryption
        4a:83:ef:78:76:48:18:1b:e4:43:bd:29:b1:91:9e:24:d8:12:
        c7:c1:12:76:e7:84:36:26:55:c6:e6:f0:fd:58:75:ab:68:54:
        56:3b:a5:96:4e:2b:d6:f9:ac:d6:c0:18:f3:f3:fc:c6:47:13:
        95:5c:27:7e:0b:95:bf:5e:f1:cc:0a:b8:4d:ee:f8:f7:6c:e0:
        d0:bc:73:7c:7a:e7:06:07:26:35:a0:2e:39:55:32:92:cf:c2:
        b2:6e:0f:5c:c5:0e:4b:d6:ad:52:26:47:54:ce:b8:34:ea:66:
        0e:ce:95:36:62:51:15:b2:1a:19:d3:0d:bc:e8:ca:3c:60:72:
        05:9e:d7:2e:ca:c7:88:88:1a:50:58:af:69:49:4e:f3:26:d0:
        2e:32:64:af:38:57:ad:91:47:4f:32:d3:56:80:e7:6b:81:b7:
        1c:99:29:b7:5c:bd:3a:96:72:3b:26:a4:6f:1d:dc:30:24:ec:
        56:e9:4b:b3:30:5b:e0:69:e2:0d:d2:27:e9:3c:cf:5f:ff:c8:
        4a:cd:96:02:82:f6:1f:ba:f0:f2:3b:37:ec:f1:5c:2e:69:4b:
        5a:9f:65:70:29:a0:36:21:e2:ae:98:a9:3b:38:6e:17:3a:2b:
        04:81:6a:b3:f4:fc:e6:a8:10:a3:b5:01:0b:fc:f7:c0:b9:e4:
        00:a0:de:06
```

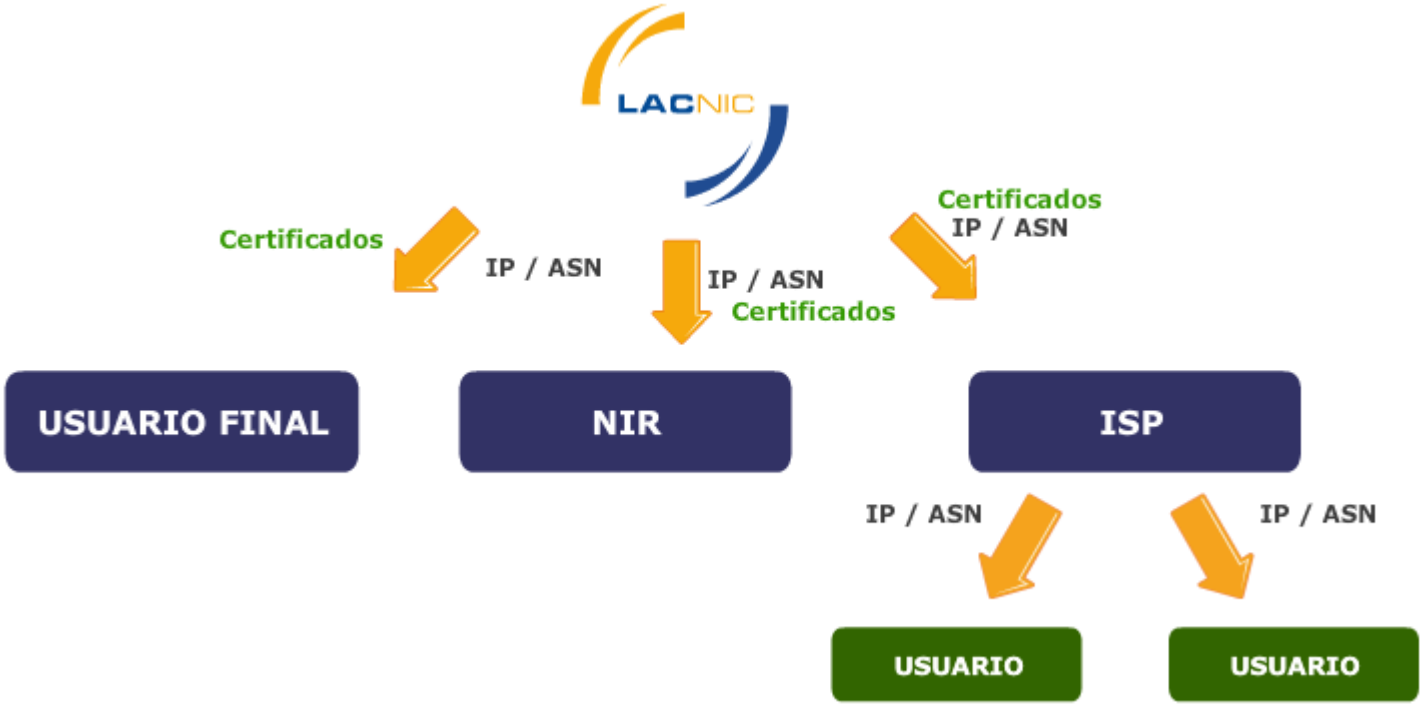
Material Publico
ROA

```
-------------------------
ROA Details
-------------------------
Origin ASN:        AS28001
Not valid Before:  2011-01-07 02:00:00
Not valid After:   2012-08-05 03:00:00
Trust Anchor:      repository.lacnic.net
Prefixes:          200.3.12.0/22 (max length /24)
                   2001:13c7:7012::/47 (max length /47)
                   200.7.86.0/23 (max length /24)
                   2001:13c7:7002::/48 (max length /48)
```

Material Publico Manifiesto


```
Object Type: RPKI Manifest
Signing time: 2011-03-31T03:00:00.000Z
Version: 0
Number: 408
This update time: 2011-03-31T03:00:00.000Z
Next update time: 2011-03-31T15:00:00.000Z
Filenames and hashes:
    0rQTZEKcUjY9_FDjBuMtg4EkM9E.cer c22fe69ea7acf828b6f4caa80d1f67f34d021f916ffe258196644864b54d0dae
    7p_8kCrfr5ZjSkCpJRhyJUL8wX0.cer 3ee6adb8ddcbb1f4f42146f4705563d0a4adedbf408495284abe162172e42b14
    BkFqDshHyrPwlWOgK96s5cwa2Ec.cer 38bee6c253e2912e0c4197ff265e0c5f3df0b9d98f75871fdd19c2c52745614f
    L5cy4M4uz43_5oIbRx3dp_fetfA.cer 42f97d37dac19fe8030925c77995b703178ebf03bd69d171eb2cae5c80ba4357
    MfeOuduaM5NzCtAKgyimOo1wf_c.cer 265ee938e66ad899afd4808a0637de8c2e9c9a185045e31763ea86c578ed31c5
    QRonip0StN3-cpQwD-BsqEB-2I8.crl a15fedec44e195f330449a459ae1f510dd640af5be9b5122dc8f90b815e6aa4c
    c_bbNoefWlSSvaef2cr7ZcAxBsA.cer 25da0308f72a0fdd4b143f3189530c0819bcea81265ebfbcc28b7fbd5af8f8a9
    gjiKwYHjDnfxr4RAAyle259qbzU.cer cc6913fdbd8173540ccd3cebe1c29f139cff7e56d44e374f16ccfbdb8391c892
    o5nRW2KC14rVNShONYGJSUk0f6A.cer bf3164cf282b0d6978420a9e7a40803a40f9c70e609a00aa5c2b1d52a147c484
    suB60Qba6JzkDRhzj8Ddl3fdZlw.cer 063c97c72adea6972be2460dea4ccd62068003179cfa1ba14063fa64c6a494db
    uC3EYhxCe7-q8P-0EXkfaTaaG_U.cer 639d4d2ae64c3f9c04bfbf521aec53d49edba5ab49dc090c8392d1ae1290a85b
```

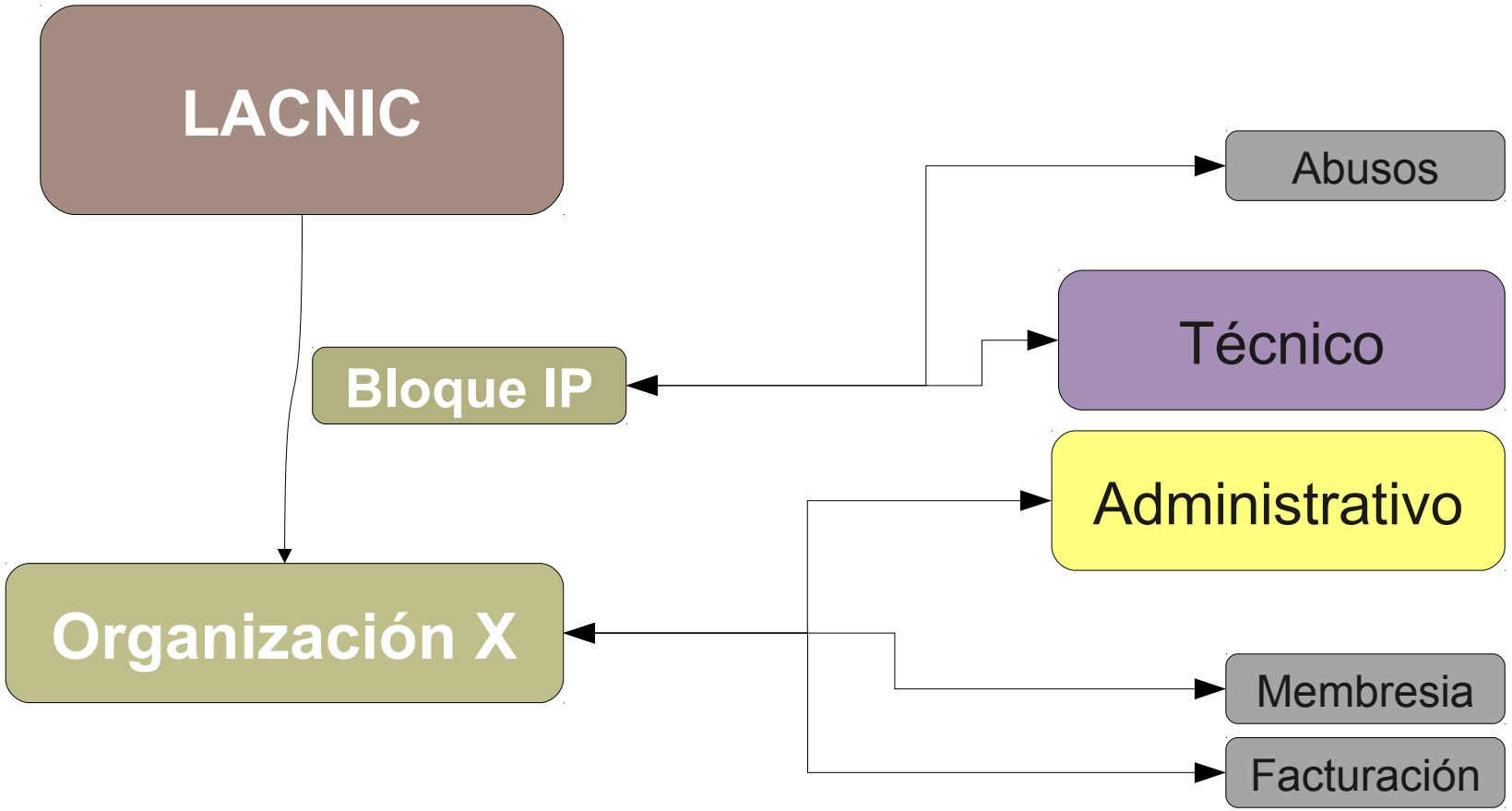
Asignación de recursos y Emisión de certificados



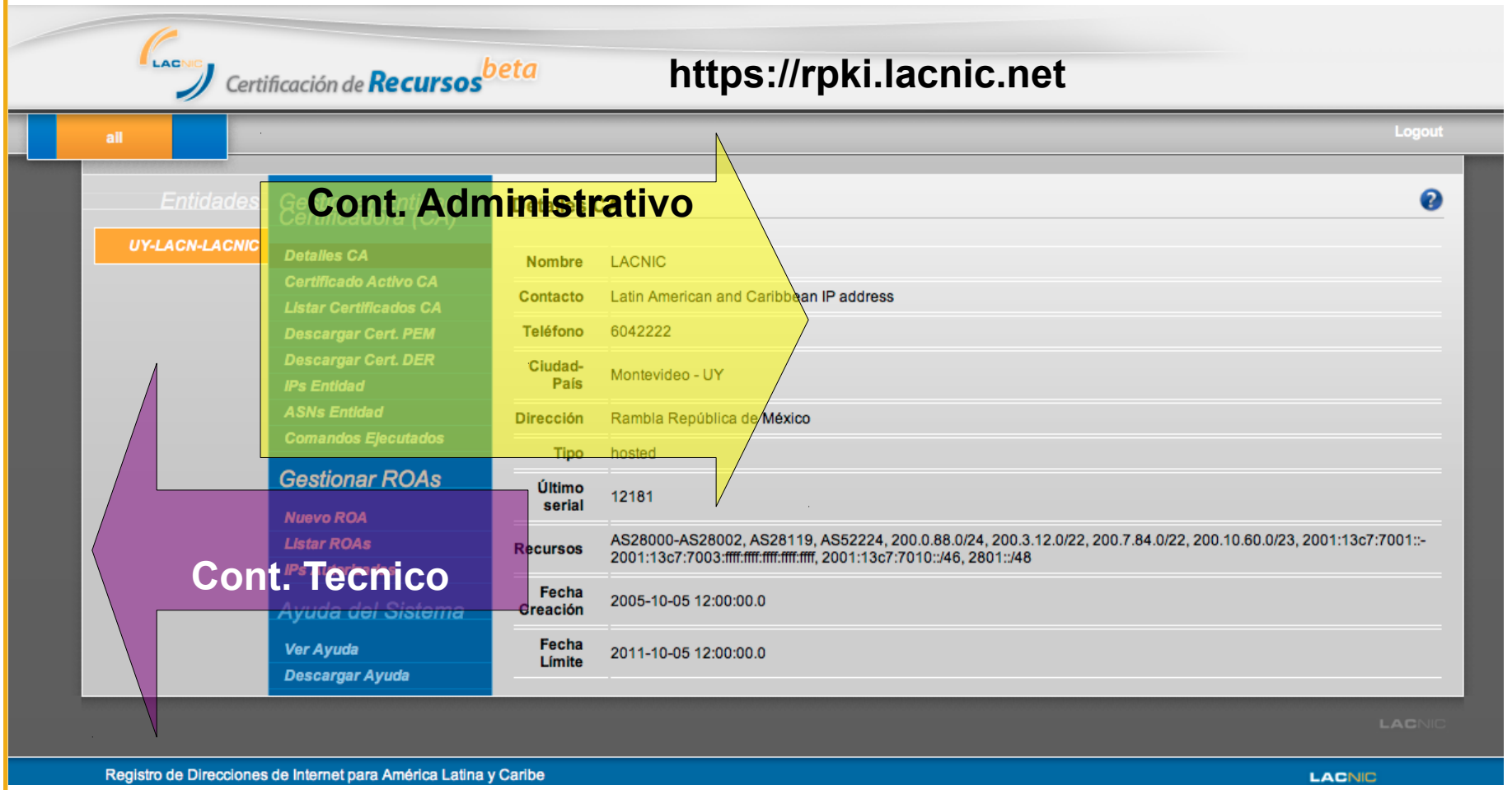
Sistema RPKI-LACNIC
Funciones

- https://rpki.lacnic.net
- Organizaciones asociadas a LACNIC -(MX y BR)
- Gestión del Material
- Gestión del repositorio
- Multilenguaje
- Roles

Sistema RPKI-LACNIC
Roles



Sistema RPKI-LACNIC Apariencia y Roles



Contacto Administrativo

```
gerardo@Gerardo-Desktop:~$ whois -h whois.lacnic.net UY-LACN-LACNIC
 % LACNIC resource: whois.lacnic.net


% Copyright LACNIC lacnic.net
%  The data below is provided for information purposes
%  and to assist persons in obtaining information about or
%  related to AS and IP numbers registrations
%  By submitting a whois query, you agree to use this data
%  only for lawful purposes.
%  2011-09-05 17:41:34 (BRT -03:00)

owner:       LACNIC - Latin American and Caribbean IP address
ownerid:     UY-LACN-LACNIC
responsible: Raul Echeberria
address:     Rambla Rep�blica de M�xico, 6125,
address:     11400 - Montevideo -
country:     UY
phone:       +598 2 6042222 []
owner-c:     AIL
created:     20051005
changed:     20101209

nic-hdl:     AIL
person:      Arturo Servin
e-mail:      ipadmin@LACNIC.NET
address:     Rambla Rep. Mexico, 6125,
address:     11600 - Montevideo -
country:     UY
phone:       +598 2 6042222 []
created:     20080125
changed:     20110512

aut-num:     28000
aut-num:     28001
aut-num:     28002
aut-num:     28119
aut-num:     52224
inetnum:     200.0.88/24
inetnum:     200.3.12/22
inetnum:     200.7.84/23
inetnum:     200.7.86/23
inetnum:     200.10.60/23
```

Contacto Técnico

```
gerardo@Gerardo-Desktop:~$ whois -h whois.lacnic.net 200.7.84/24
 % LACNIC resource: whois.lacnic.net


% Copyright LACNIC lacnic.net
%  The data below is provided for information purposes
%  and to assist persons in obtaining information about or
%  related to AS and IP numbers registrations
%  By submitting a whois query, you agree to use this data
%  only for lawful purposes.
%  2011-09-05 17:38:56 (BRT -03:00)

inetnum:     200.7.84/23
status:      assigned
owner:       LACNIC - Latin American and Caribbean IP address
ownerid:     UY-LACN-LACNIC
responsible: Raul Echeberria
address:     Rambla Rep□blica de M□xico, 6125,
address:     11400 - Montevideo -
country:     UY
phone:       +598 2 6042222 []
owner-c:     AIL
tech-c:      AIL
abuse-c:     ABL2
inetrev:     200.7.84/23
nserver:     NS.LACNIC.NET.UY
nsstat:      20110901 AA
nslastaa:    20110901
nserver:     NS2.LACNIC.NET
nsstat:      20110901 AA
nslastaa:    20110901
nserver:     NS.LACNIC.NET
nsstat:      20110901 AA
nslastaa:    20110901
created:     20080125
changed:     20080827

nic-hdl:     ABL2
person:      Abuse LACNIC
e-mail:      ipabuse@LACNIC.NET
address:     Rambla Rep. Mexico, 6125,
address:     11600 - Montevideo -
country:     UY
```

Antes de comenzar con los ejercicios
¿Preguntas?

Ejercicio 1

Identificar los roles técnicos y administrativos para una organización asociada a LACNIC

Son los campos "owner-c" y "tech-c" de la consulta WHOIS
whois -h whois.lacnic.net PAIS-ORGID-LACNIC
whois por direccion IP
whois en la página de LACNIC

Ejercicio 2

Crear un certificado utilizando el sistema DEMO de LACNIC

Crear un ROA que incluya IPv4 utilizando en el sistema DEMO de LACNIC

Crear un ROA que incluya IPv4 e IPv6 utilizando el sistema DEMO de LACNIC

http://rpkidemo.labs.lacnic.net

Ejercicio 3

Generar el repositorio del sistema DEMO de LACNIC

Descargar repositorio del sistema DEMO de LACNIC

rsync -av rsync://rpki-demo-vm/rpkidemo ./repo-rpkidemo

http://rpkidemo.labs.lacnic.net

Ejercicio 4

Visualizar el material generado anteriormente con la herramienta de RIPE (Certificados, ROAs, CRL y manifiestos)

$BASE/bin/certification-validator --print -f ./lacnic/LACNIC_RTA_RPKIDEMO.cer

Ejercicio 5

Visualizar el material generado anteriormente con openssl (Certificados y CRL)

```
/opt/openssl-rpki/bin/openssl x509 -in
./repo-rpkidemo/hosted/8d09585d-7fd6-
48c0-be43-435b2df77311/QP7wZ_PxYnOqRQcjjPza4jeeAR0.cer
-noout -purpose -text -inform DER
```

Ejercicio 6

Crear el Trust Anchor Locator (rpki-demo.tal)

Encontrar TAL

http://www.ripe.net/lir-services/resource-management/certification/trust-anchor-locators

http://www.labs.lacnic.net/drupal/rpki

Descargar make-tal

http://subvert-rpki.hactrn.net/rcynic/make-tal.sh

Para hacer el TAL:

sh make-tal.sh

rsync://repository.lacnic.net/rpki/lacnic/RTA_LACNIC_RPKI.cer > lacnic.tal

Ejercicio 7

Validar el repositorio utilizando el .TAL creado anteriormente

```
/opt/rpki-validator/bin/certification-validator -t ./lacnic.tal -o repo-lacnic
-r lacnic-roas.csv
```

Ejercicio 8

Realizar consultas a whois.bgpmon.net

Anuncio valido:

whois -h whois.bgpmon.net “ --roa 27725 200.55.152.0”

Anuncio invalido:

whois -h whois.bgpmon.net “ --roa 6057 200.55.152.0”

Generico

whois -h whois.bgpmon.net “ 200.55.152.0”

Ejercicio 9

Ver validaciones de UPDATE BGP en sistemas operativos experimentales

Algunas referencias

Para ver de nuevo este seminario
http://eventos.lacnic.net/evra/publico?la=sp&id=190366&cod=info

Estadísticas sobre este seminario
http://eventos.lacnic.net/evra/publico?la=&id=190366&cod=estadisticas

Próximo seminario RPKI en LACNIC
http://eventos.lacnic.net/evra/publico?la=&id=190368&cod=info

¡Gracias!

gerardo @ lacnic.net

dario @ lacnic.net

carlos @ lacnic.net