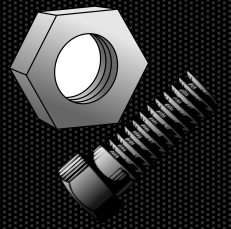
RPKI

Nuts & Bolts





Please let us know in the chatroom where you are joining us from

Your Presenters



Olatunde Awobuluyi

Trainer



Dev Jeenia

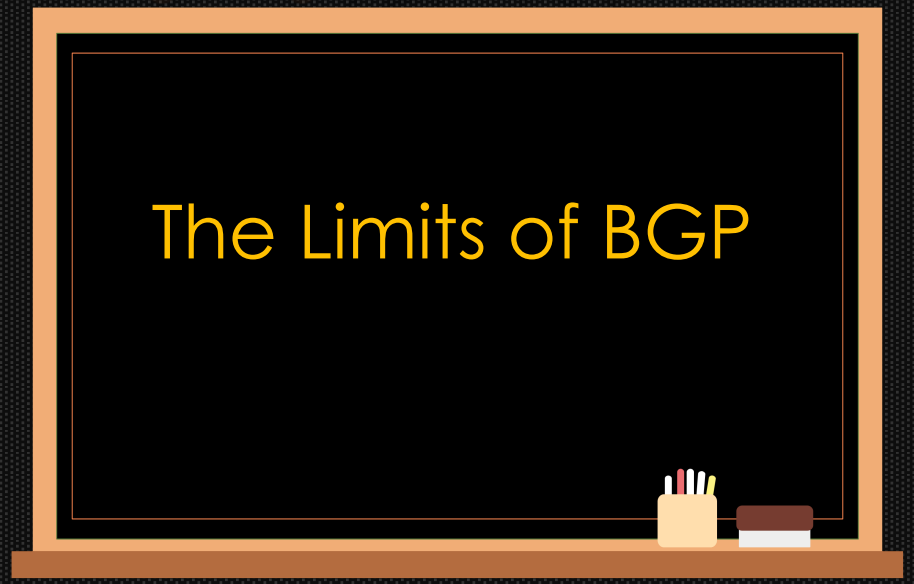
Senior IP Number Resource Analyst

AGENDA



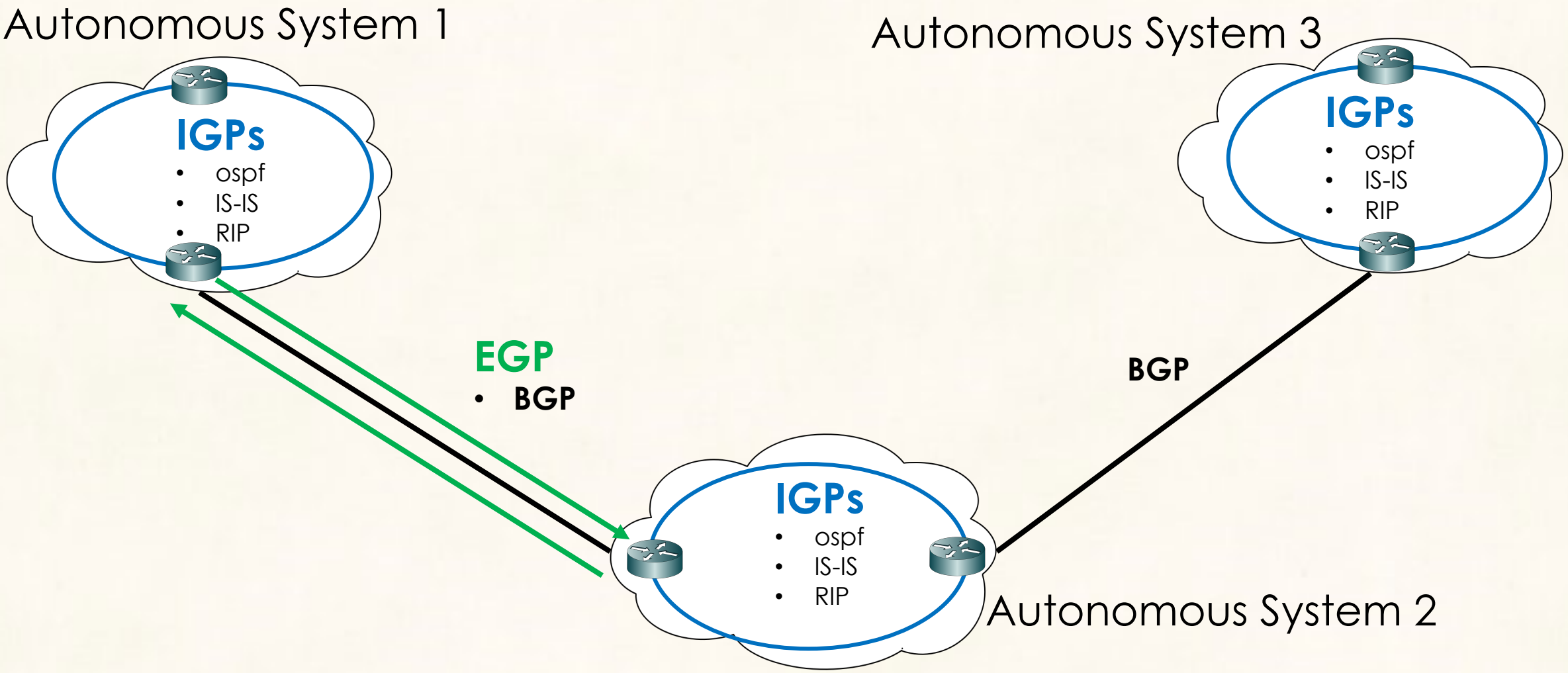
1. The Limits of BGP
2. Why the IRR alone is not Sufficient
3. How RPKI makes BGP more Secure
4. How to Create a ROA
5. Questions & Answers

AGENDA



1. The Limits of BGP
2. Why the IRR alone is not Sufficient
3. How RPKI makes BGP more Secure
4. How to Create a ROA
5. Questions & Answers

BGP: Inter-domain Routing



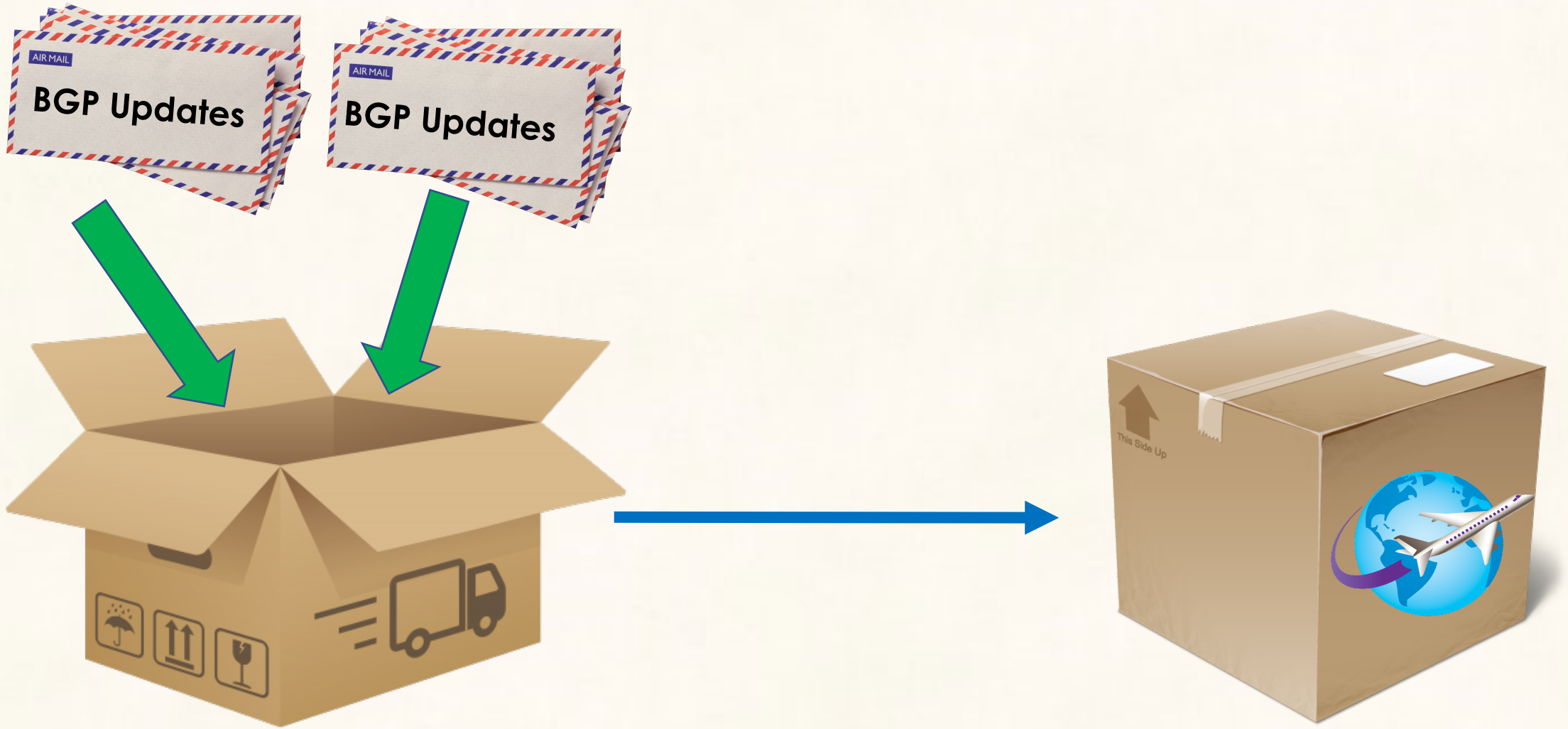
BGP: Rich Set of Path Attributes

- Origin
- AS_PATH
- Next-Hop

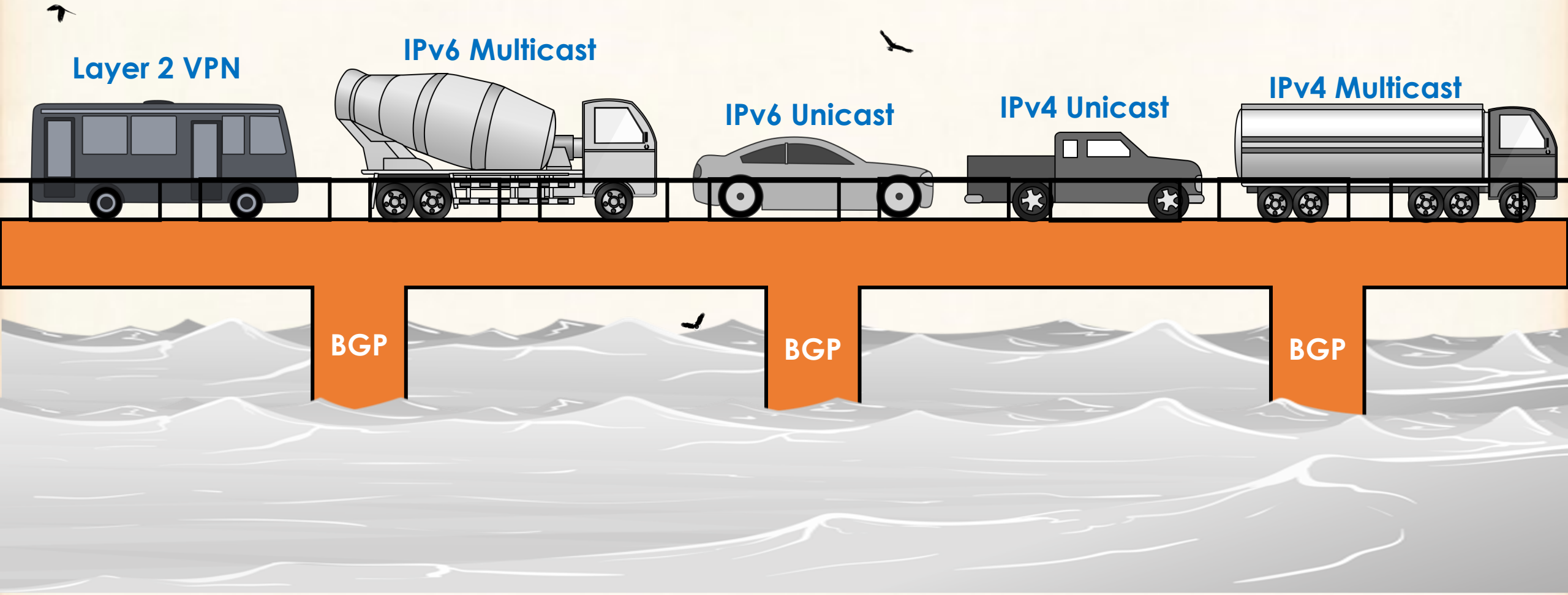


- Multi-exit discriminator
- Aggregator
- Community
- Local Preference
- Atomic Aggregate

BGP: Batched Updates



BGP: Multiprotocol Support



BGP Vulnerabilities

- TCP Related
- Route Leaks
- AS_PATH Spoofing
- Prefix Hijacking

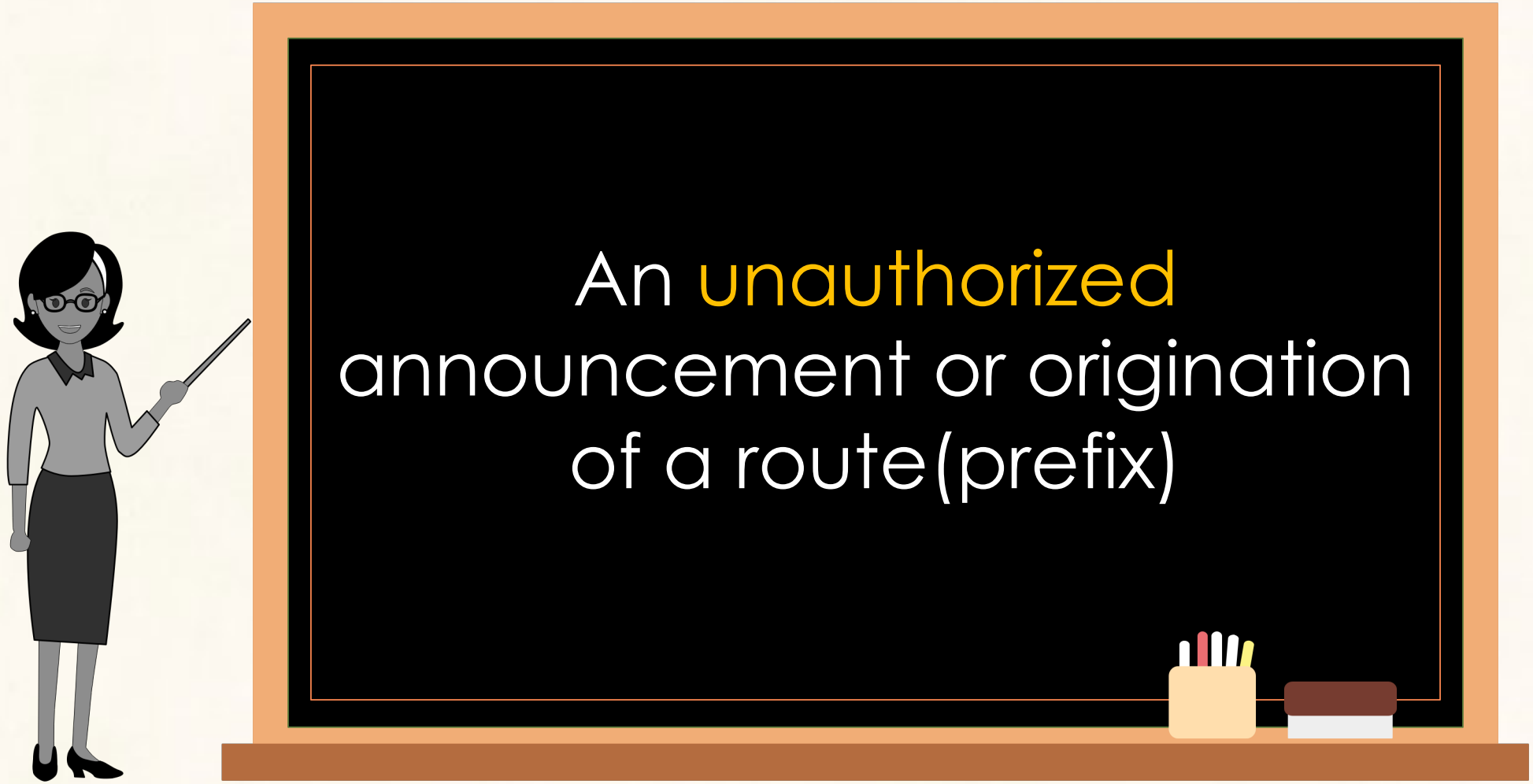


Latest BGP Hijack News Headlines

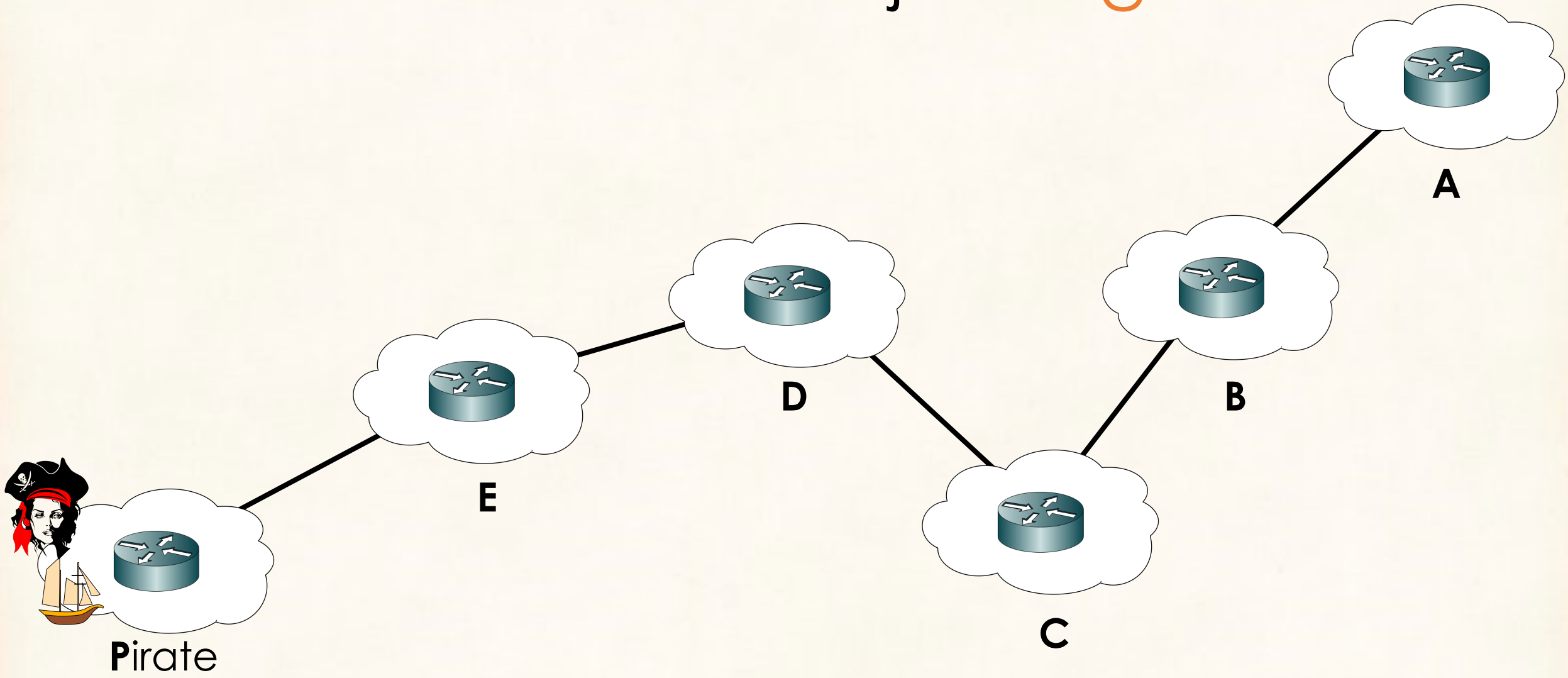


Please scan me!

BGP: Prefix Hijacking



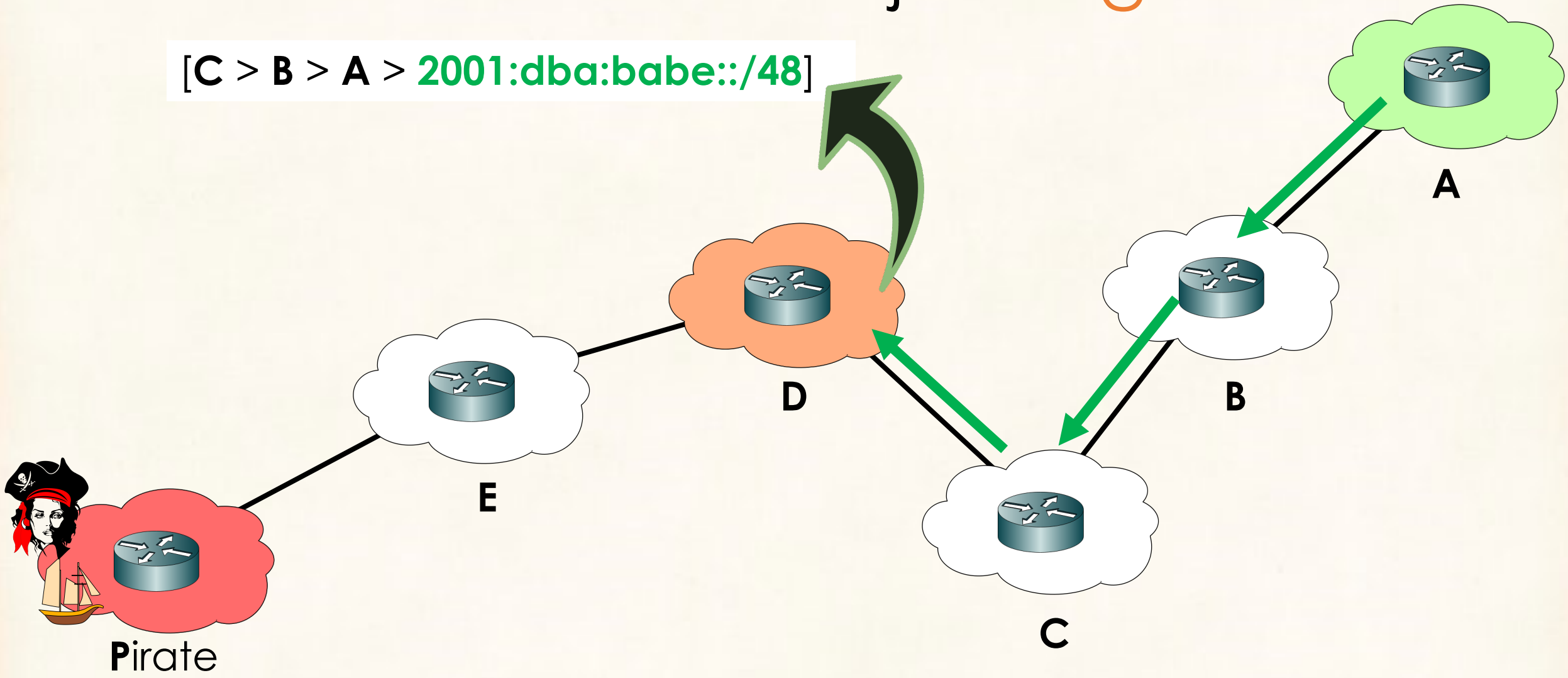
BGP: Prefix Hijacking



BGP: Prefix Hijacking

2001:dba:babe::/48

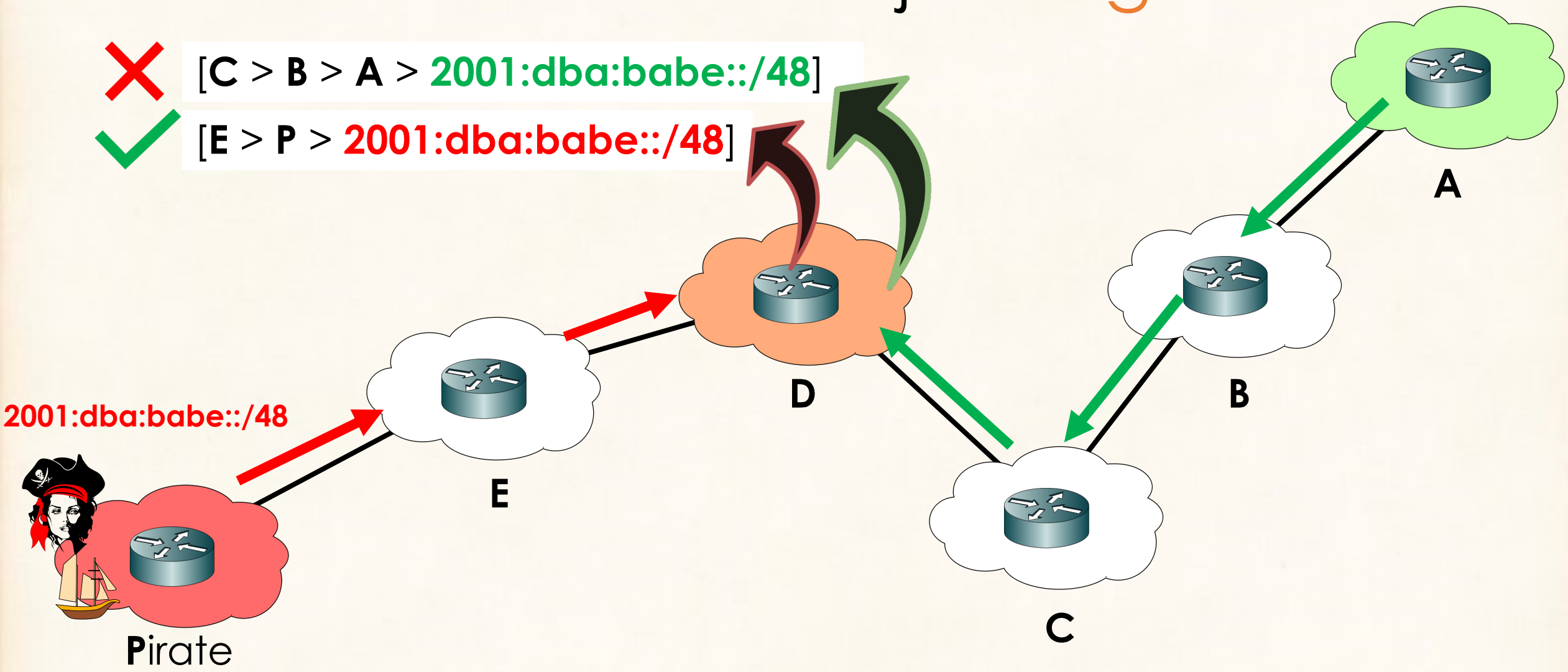
[C > B > A > 2001:dba:babe::/48]



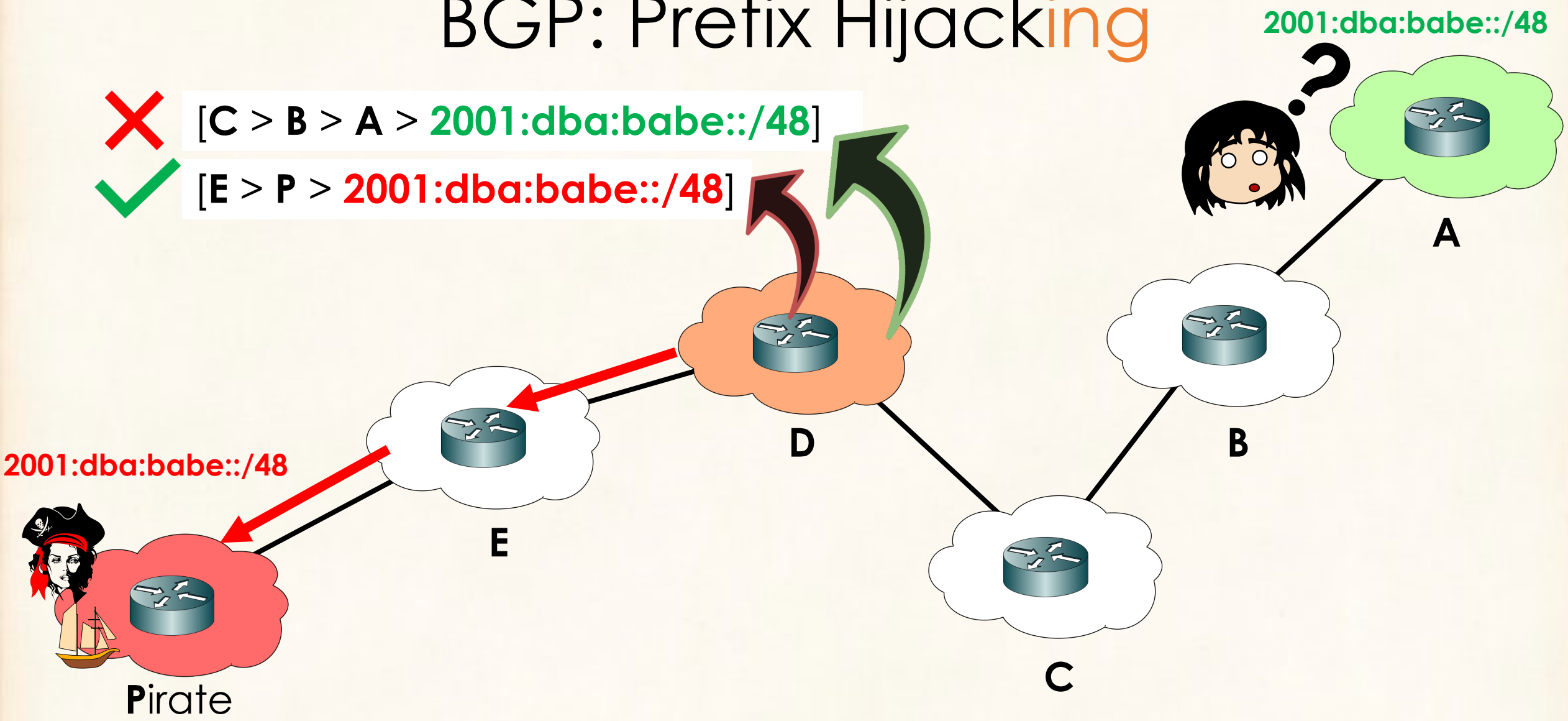
BGP: Prefix Hijacking

[C > B > A > 2001:dba:babe::/48]

[E > P > 2001:dba:babe::/48]



BGP: Prefix Hijacking



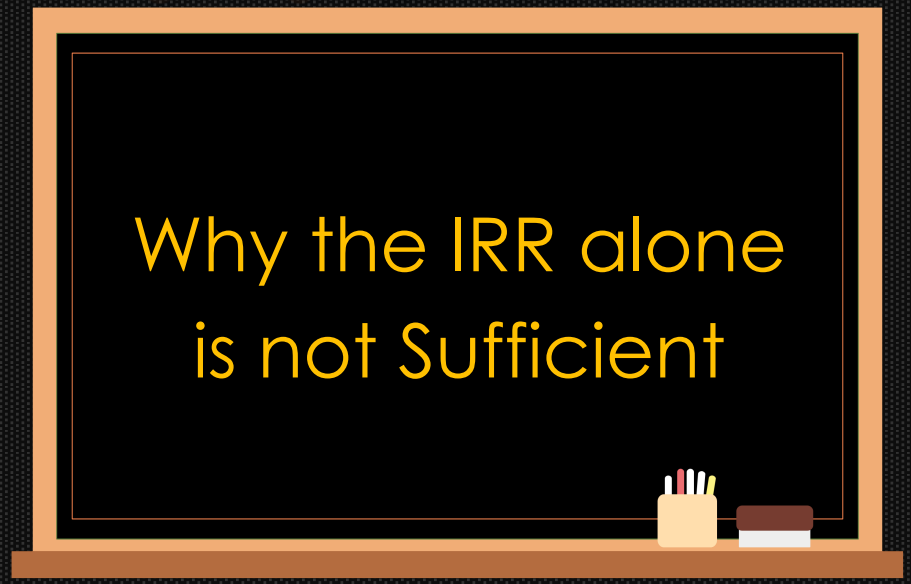
BGP: Origin Validation

Prevents redirection to an unauthorized party

Solution == "IRR/RPKI"

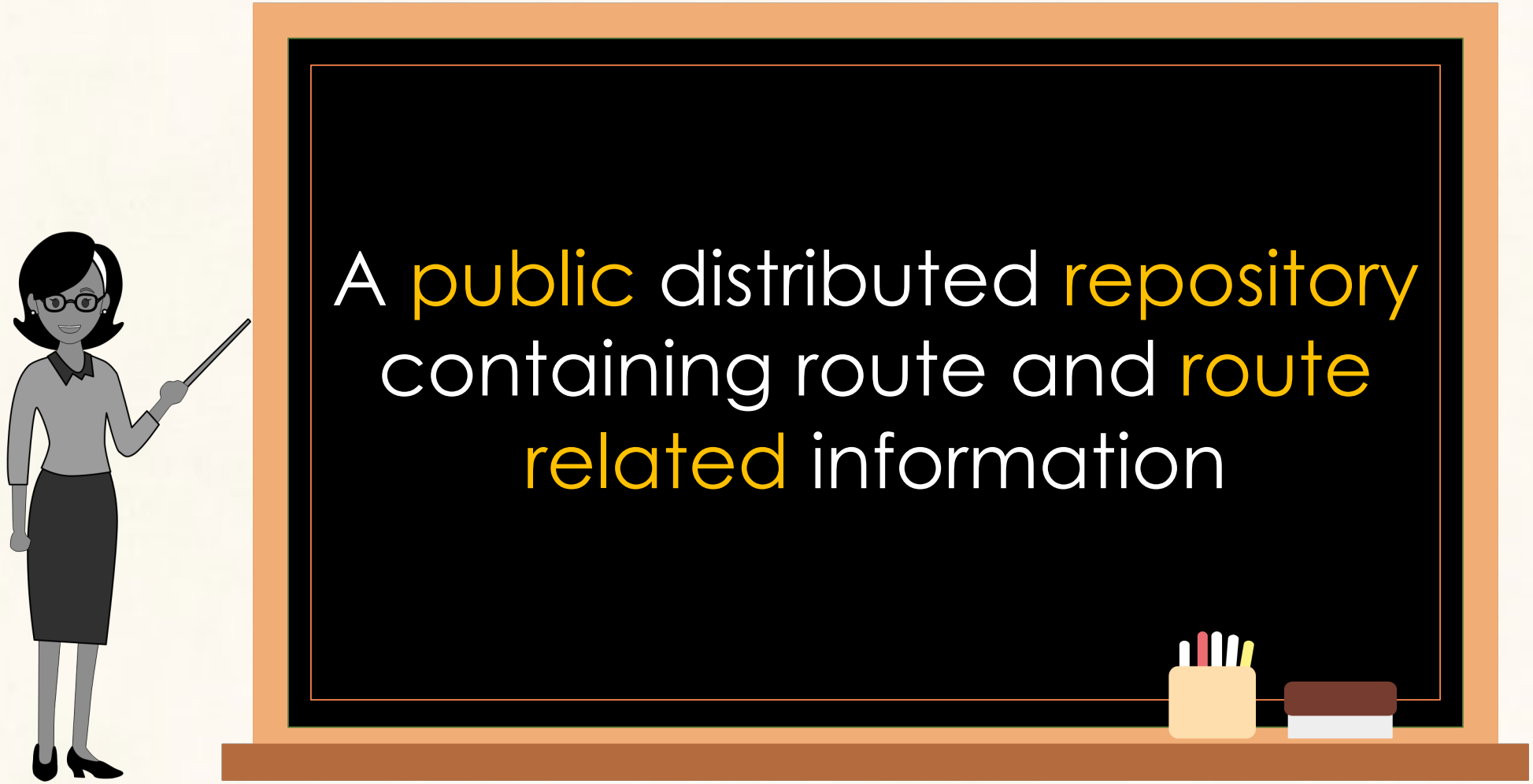


AGENDA

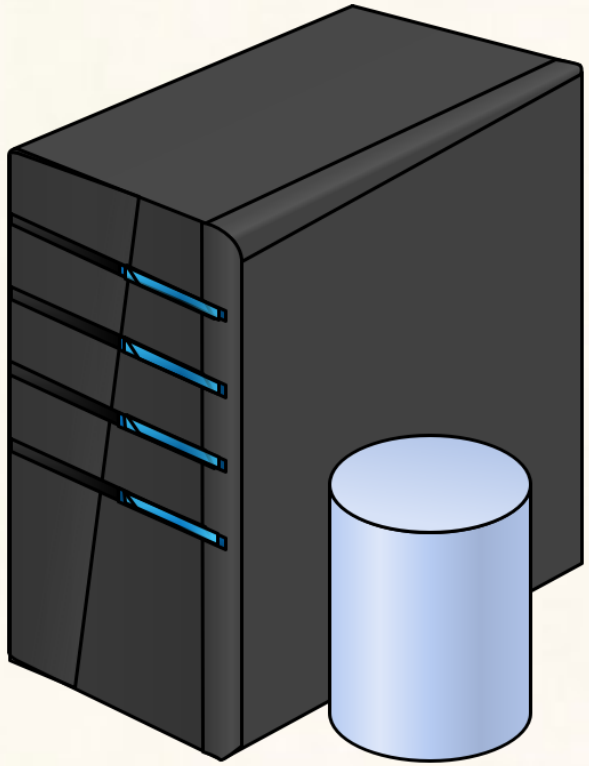


1. The Limits of BGP
2. Why the IRR alone is not Sufficient
3. How RPKI makes BGP more Secure
4. How to Create a ROA
5. Questions & Answers

Internet Routing Registry (IRR)



IRR: The Key Objects



IRR

route(6)

aut-num

set-objects

maintainer

IRR: aut-num Object

```
aut-num:        AS37288
as-name:        WACREN
descr:          AFRINIC MAIN AS (2 Byte)
status:         ASSIGNED
admin-c:        001-AFRINIC
tech-c:         WS14-AFRINIC
org:            ORG-WaCA1-AFRINIC
mnt-by:         AFRINIC-HM-MNT
notify:         hostmaster@afrinic.net 20210616
mp-export:      afi any.unicast to AS327992 announce ANY
mp-export:      afi any.unicast to AS37661 announce ANY
mp-import:      afi any.unicast from AS174 accept ANY
mp-import:      afi any.unicast from AS396390 accept ANY
changed:        james.chirwa@afrinic.net 20101129
changed:        hostmaster@afrinic.net 20131017
source:         AFRINIC
```



AS' Name



BGP Peering Polices of this Autonomous System

IRR: route Object

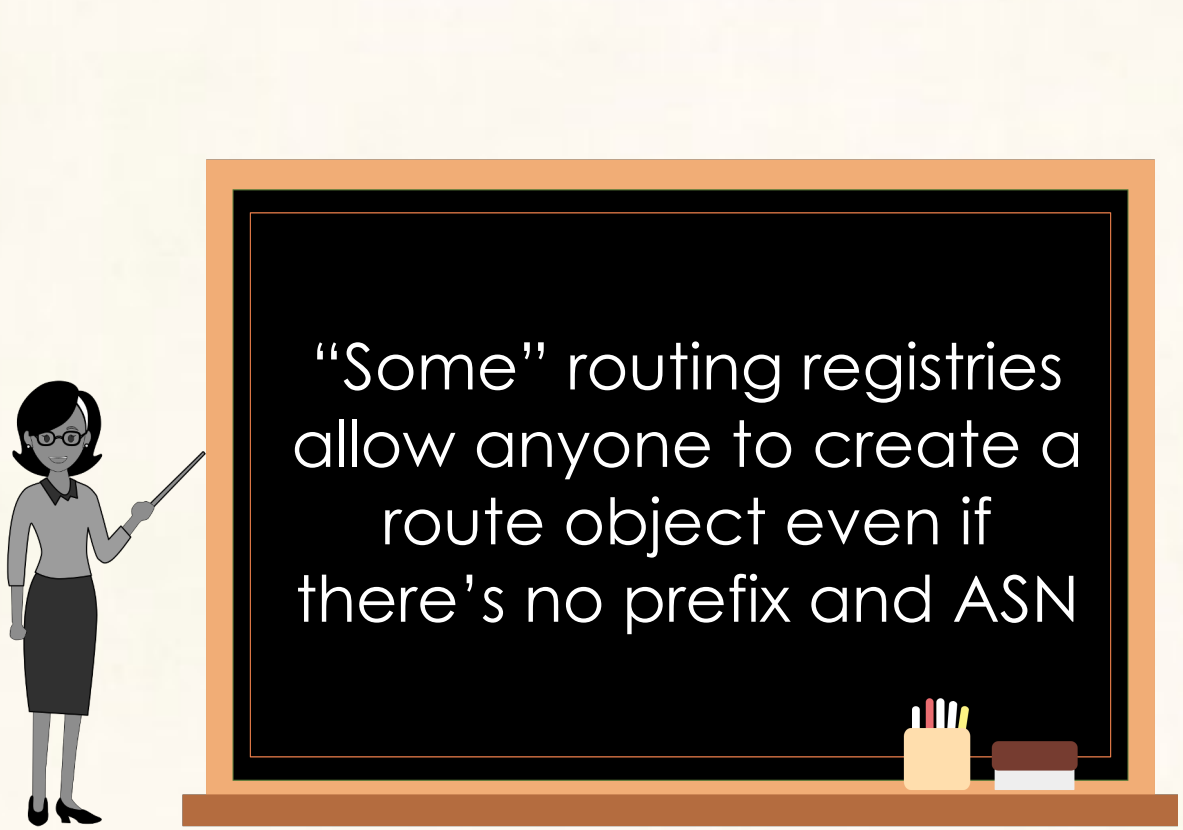
```
route6:         2001:43f8:92::/48
descr:          AFRINIC-CPT-OPS
origin:         AS37301
member-of:      rs-AFRINIC
mnt-by:         AFRINIC-IT-MNT
changed:        hudson@afrinic.net 20160928
source:         AFRINIC
```

Prefix announced in BGP

Specifies the AS that originates the route



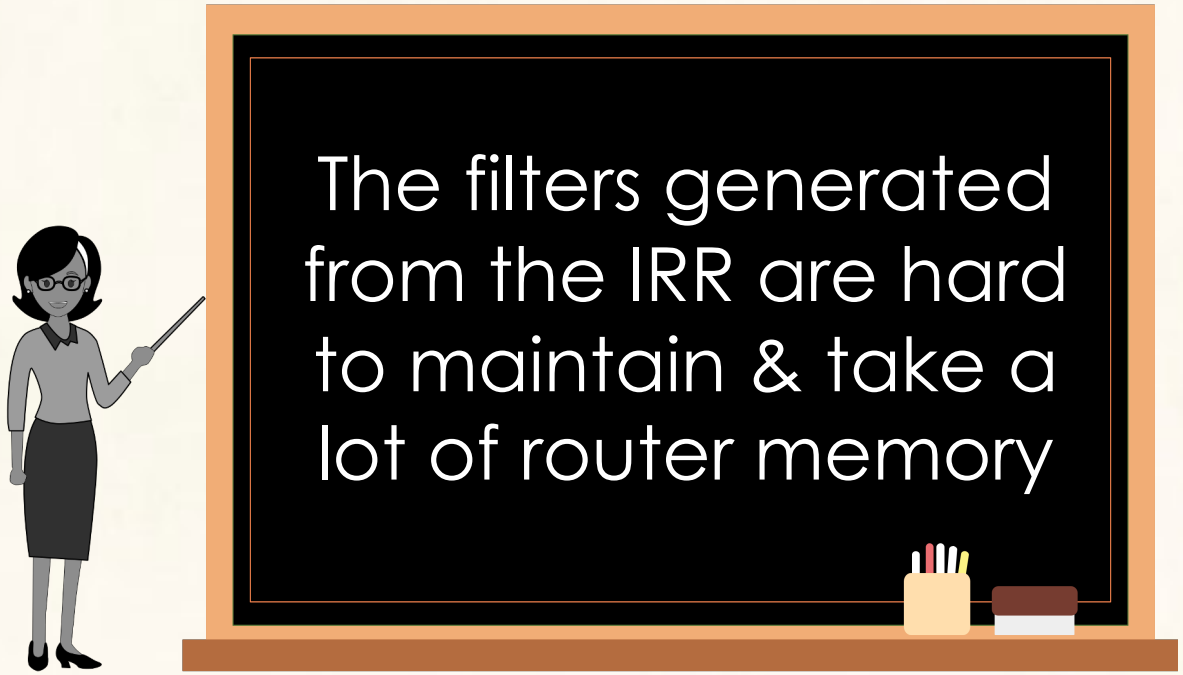
IRR Shortcomings: Vetting System

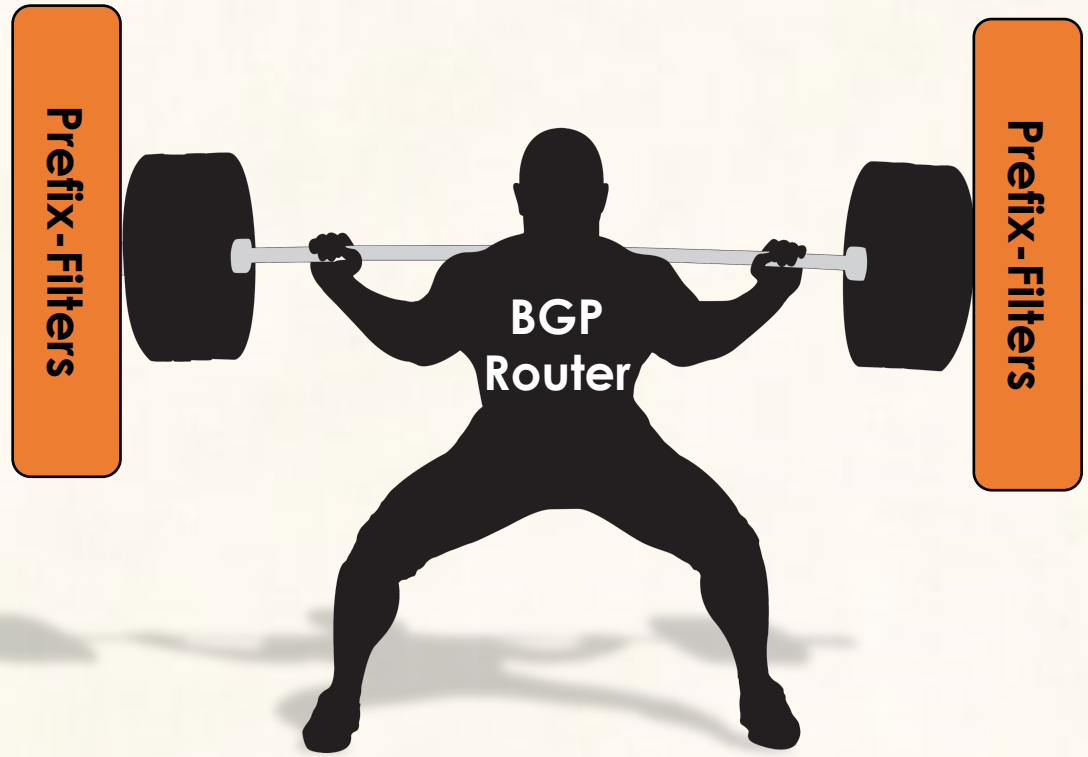




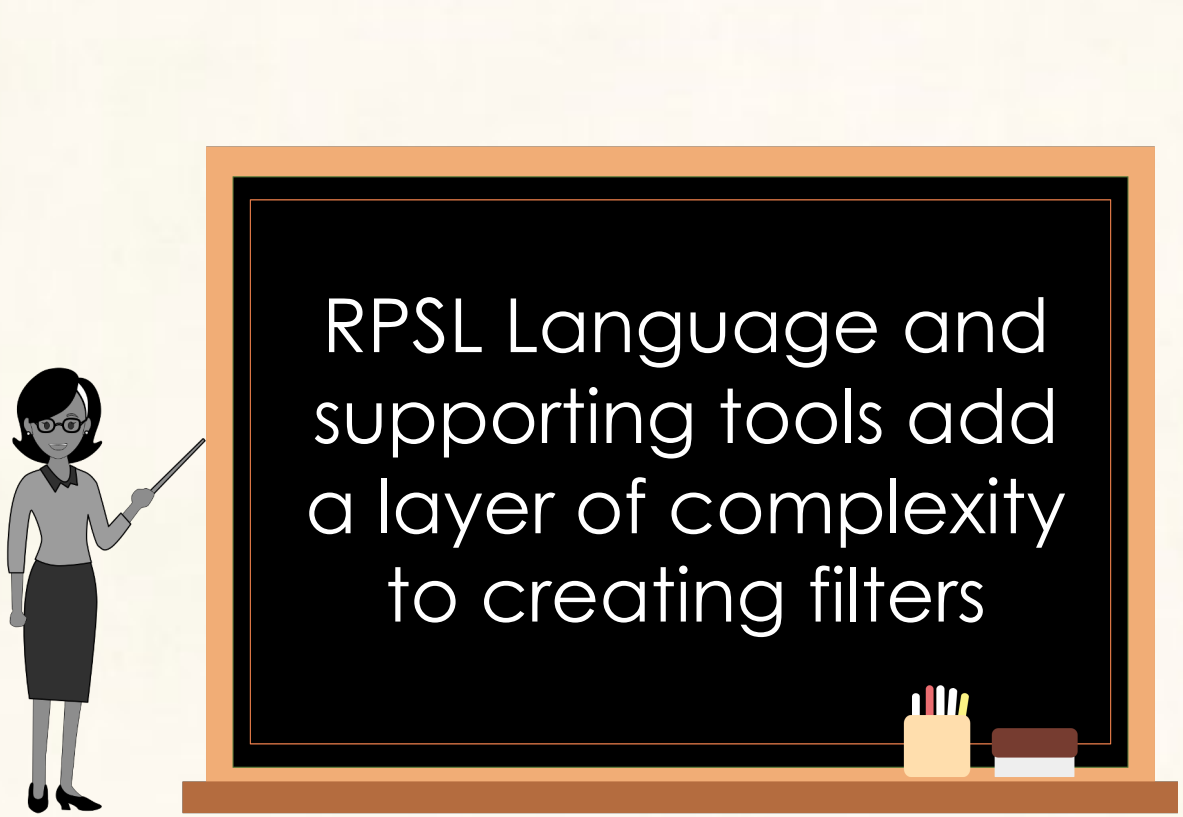
Routing Registry

IRR Shortcomings: Filter Management





IRR Shortcomings: Learning Curve





IRR: Summary

You shouldn't rely only on the IRR

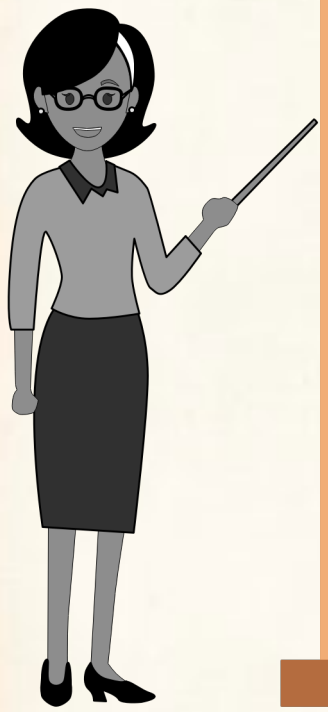


AGENDA

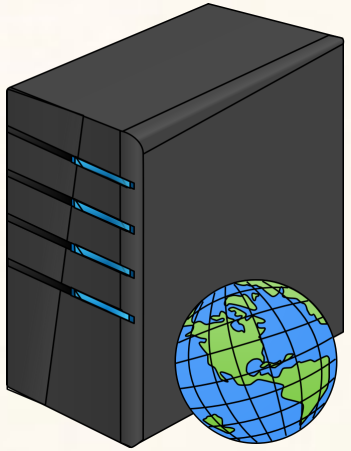
How RPKI makes BGP more Secure

1. The Limits of BGP
2. Why the IRR alone is not Sufficient
3. **How RPKI makes BGP more Secure**
4. **How to Create a ROA**
5. **Questions & Answers**

Public Key Infrastructure(PKI) Crash Course

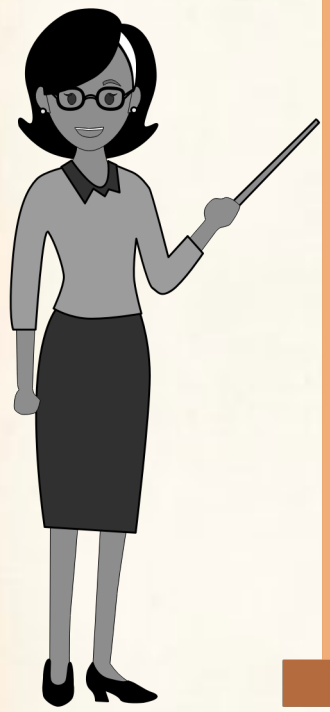


- PKI provides unique digital identities
- Uses Public Key Cryptography to achieve this

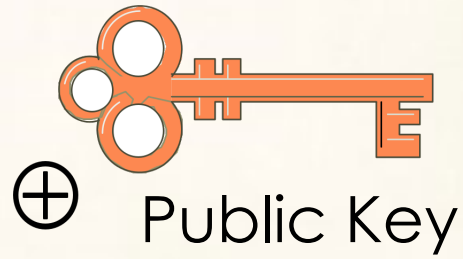


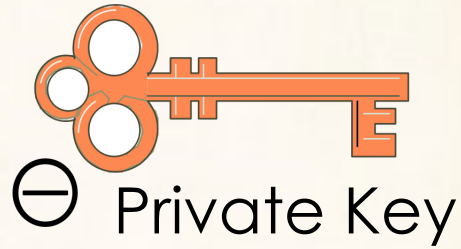
Web Server

PKI: Public & Private Keys

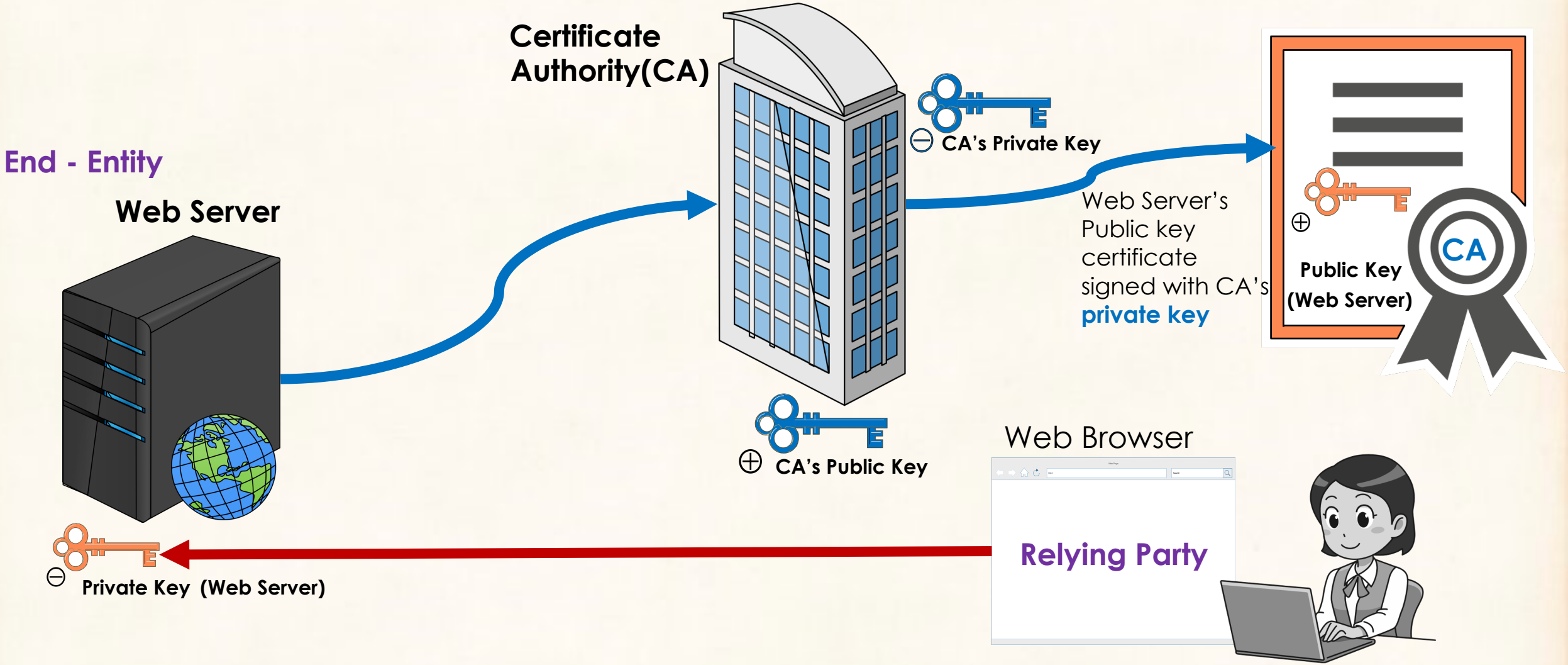


- Public keys are used for encrypting information and decrypting digital signatures created with a corresponding private key
- Private keys decrypt messages encrypted by a public key and encrypt or sign digital certificates

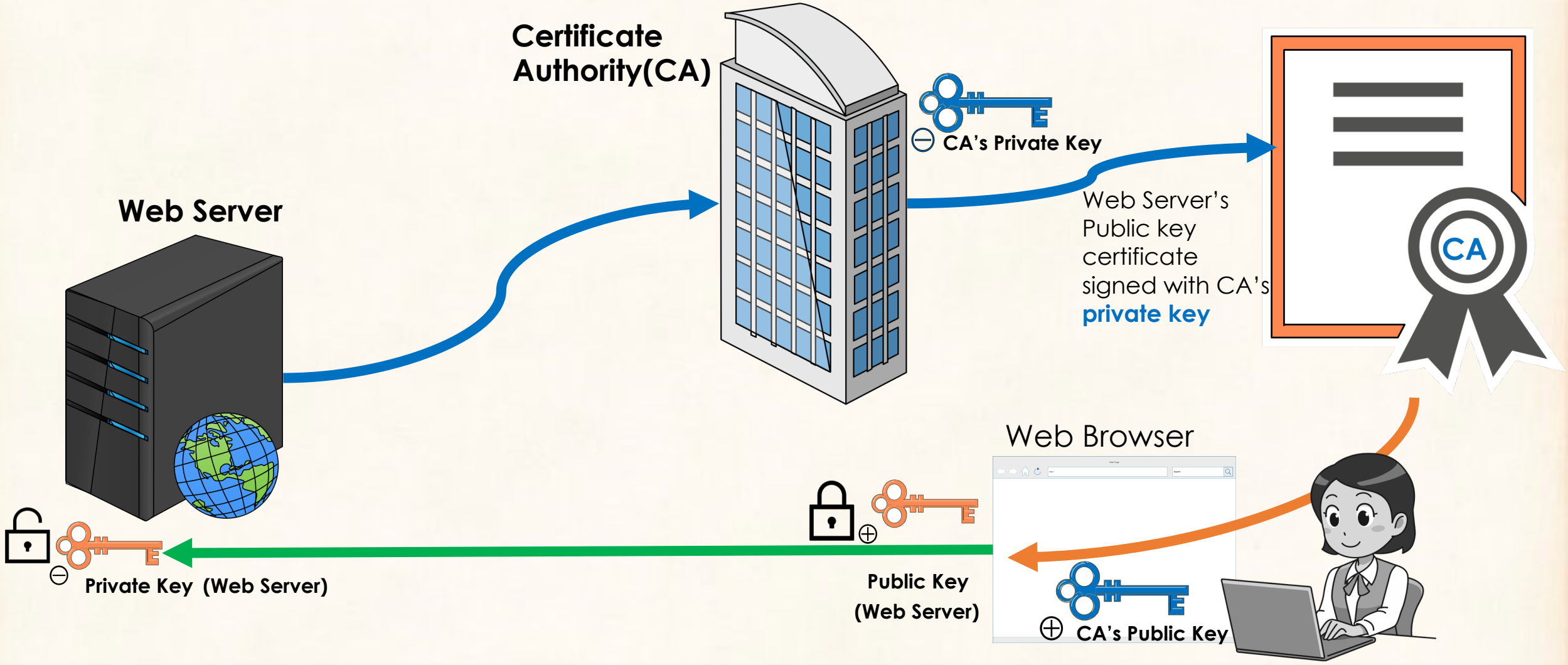




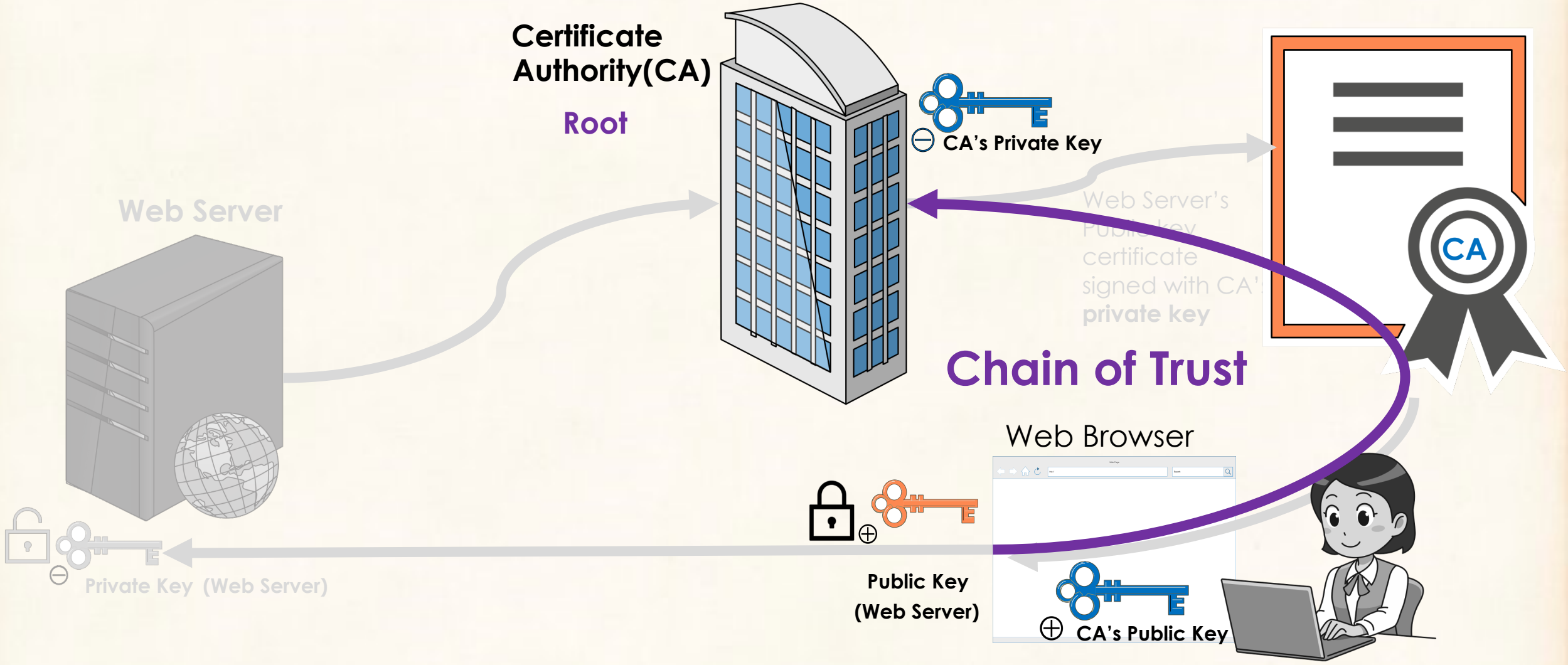
PKI: Asserting Identity (1)



PKI: Asserting Identity (2)



PKI: Asserting Identity (3)



Resource Public Key Infrastructure (RPKI)



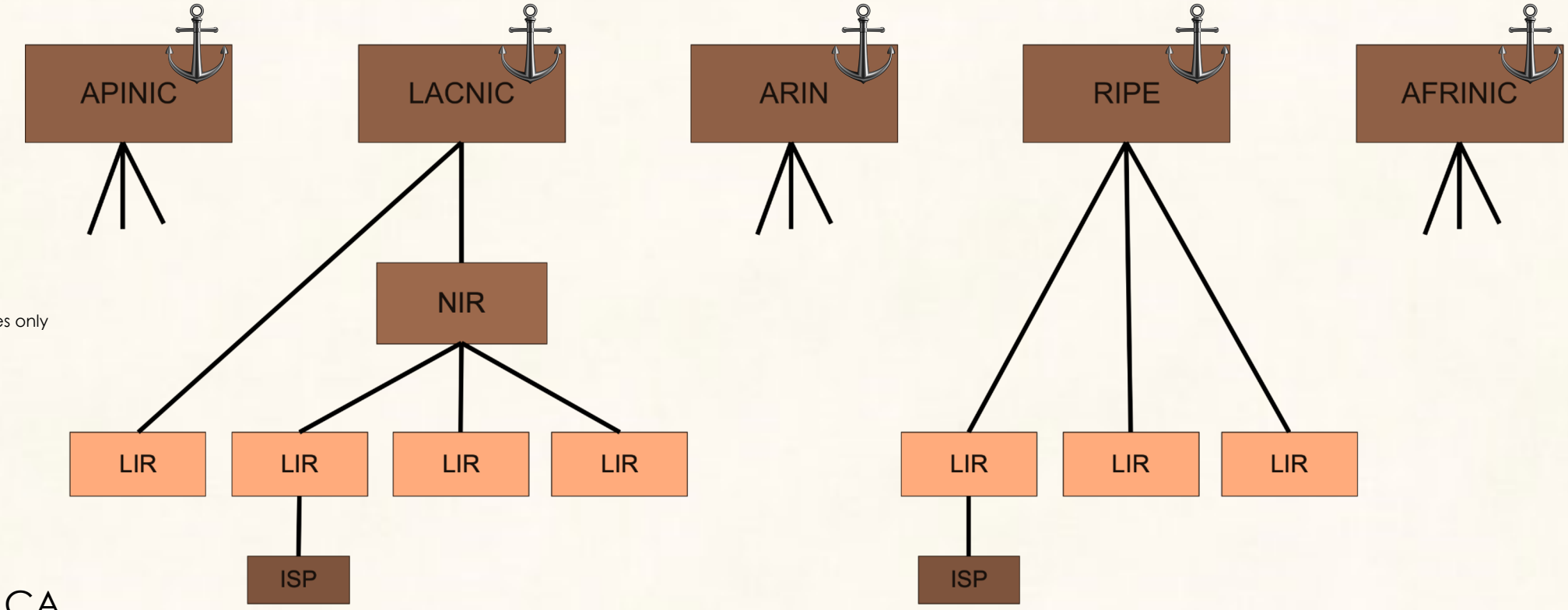
RIR Allocation/RPKI scheme

RIR Root CA

NIR Child CA
Some APNIC & LACNIC countries only

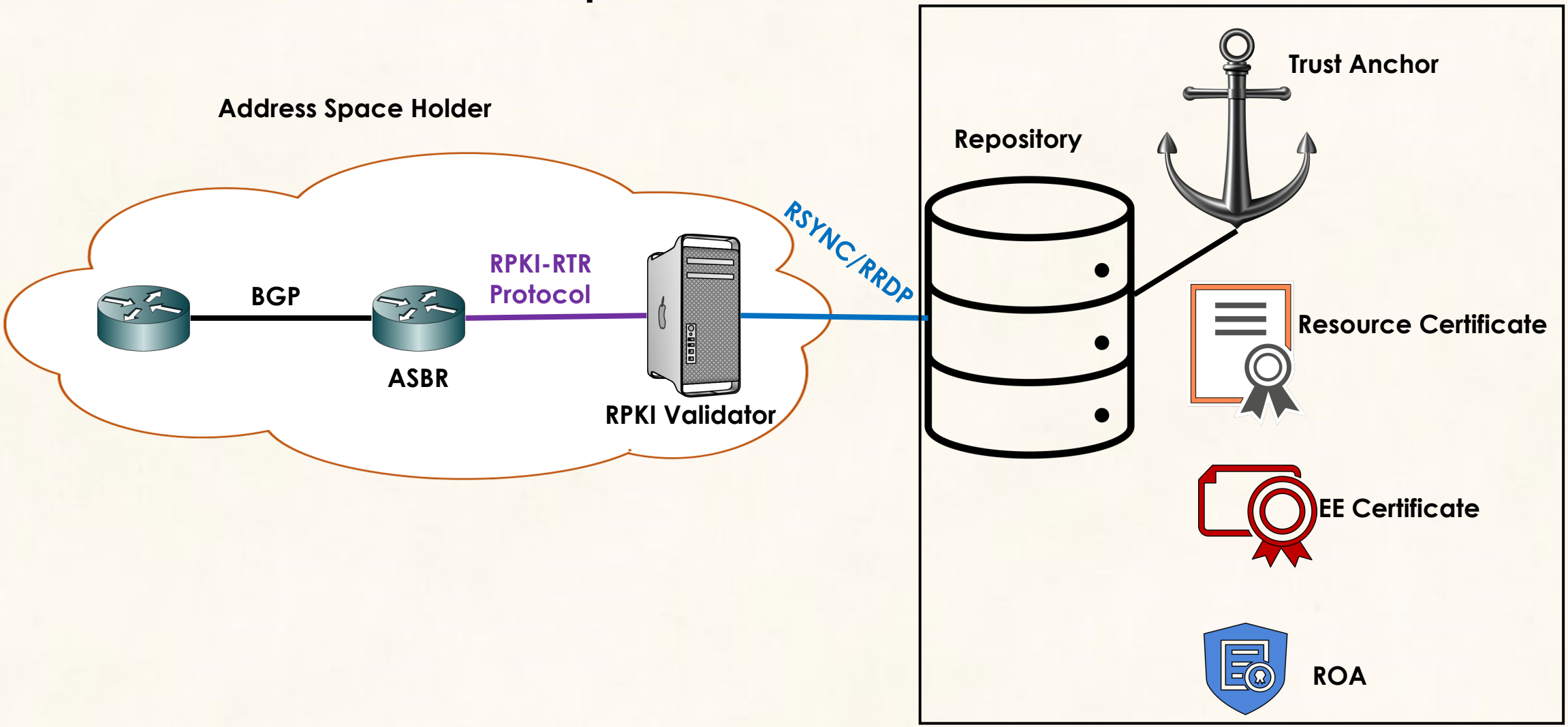
LIR Child CA

(Optional) ISP Child CA

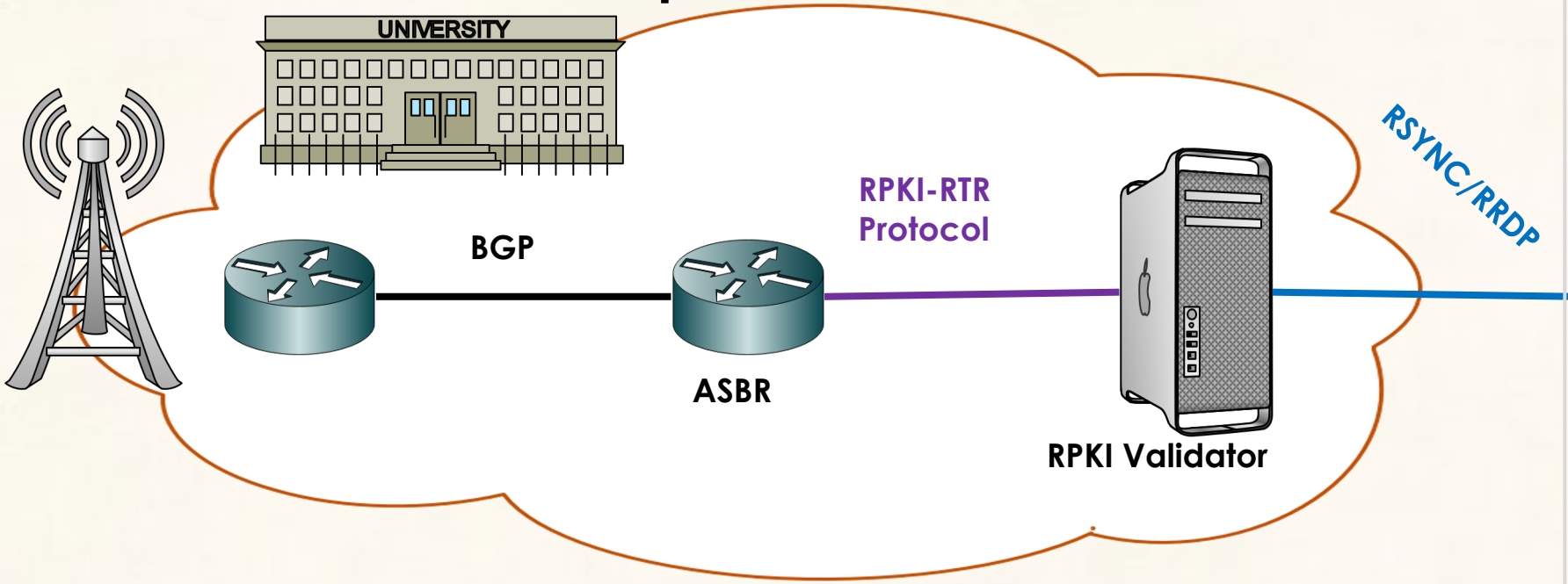


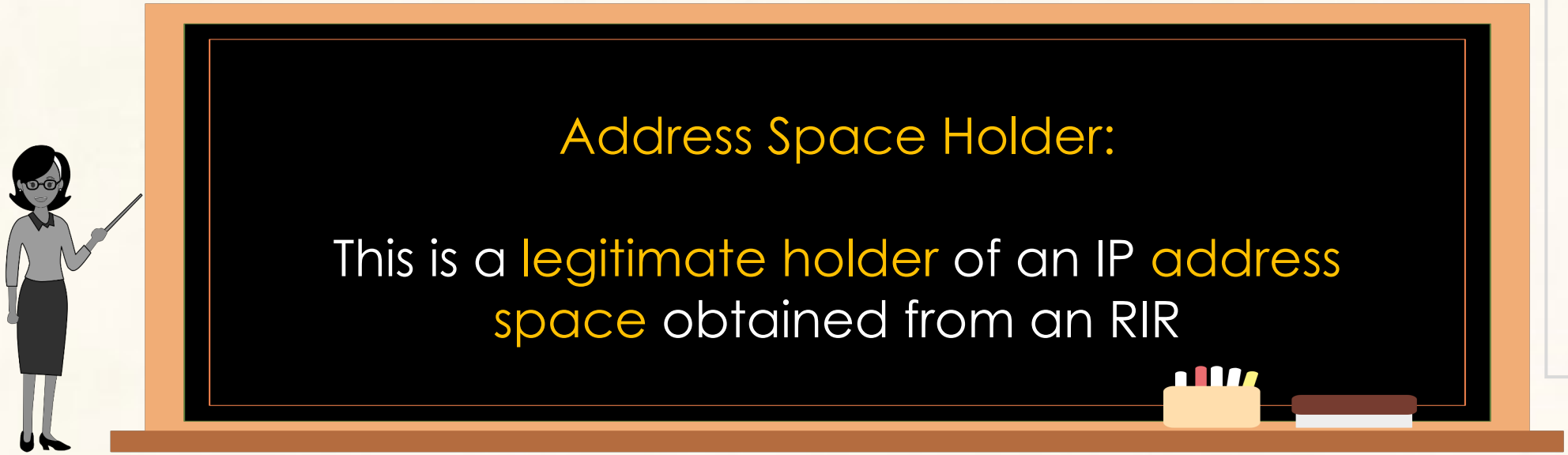
Adapted from The RPKI Documentation
(Nov 18, 2021)

Components of RPKI

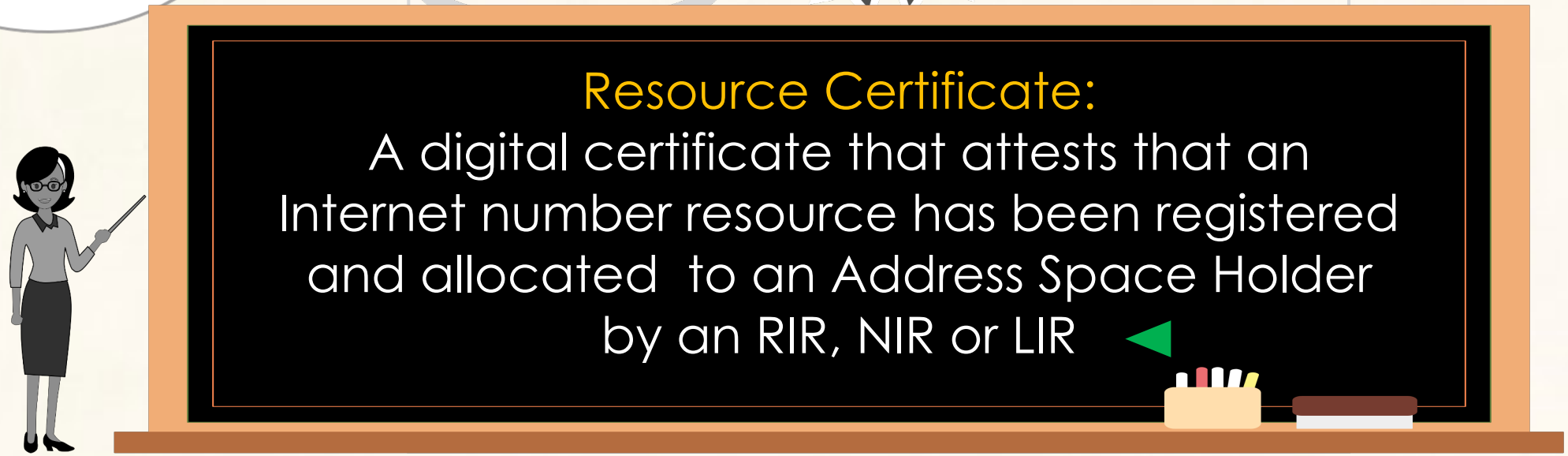


Address Space Holder





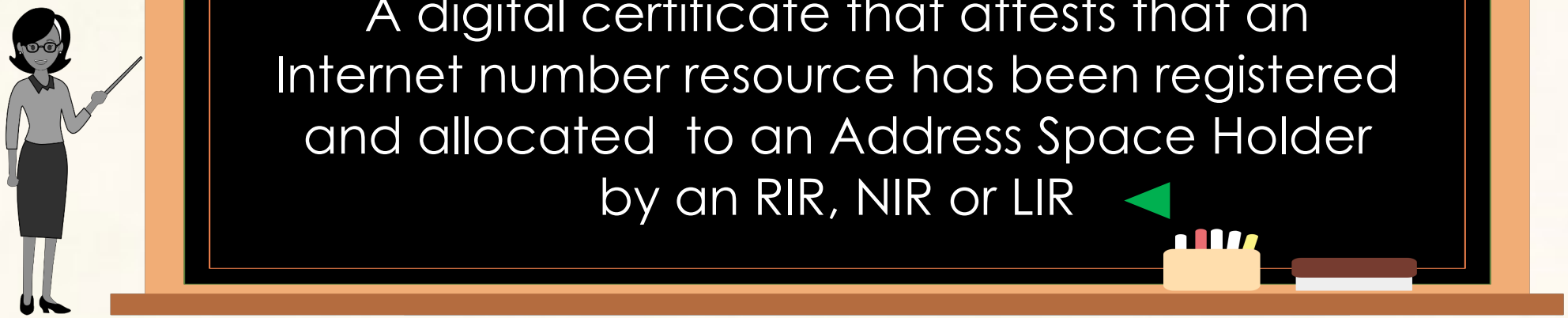
Field	Value
Version	3
Serial Number	13:D3
Issuer	/CN=AFRINIC/SN=2B57897A7CA964C3C8B7F7BDDAA7A4DA34A98F80
Subject	/CN=F3654F09AF/SN=D725C86FF27E2B008A97073E0D84CFF8946A40EA
Not Valid Before	Sep 22 2021 11:40:31 GMT
Not Valid After	Mar 31 2022 0:00:00 GMT
Subject Key Identifier	D7:25:C8:6F:F2:7E:2B:00:8A:97:07:3E:0D:84:CF:F8:94:6A:40:EA
Authority Key Identifier	2B:57:89:7A:7C:A9:64:C3:C8:B7:F7:BD:DA:A7:A4:DA:34:A9:8F:80
Authority Information Access	calssuers - rsync://rpki.afrinic.net/repository/04E8B0D80F4D11E0B657D8931367AE7D/afrinic-ca.cer
Subject Information Access	caRepository - rsync://rpki.afrinic.net/repository/member_repository/F3654F09/42C5BB7C50A111E5A6A4F444F8AEA228/ 1.3.6.1.5.5.7.48.13 - https://rrdp.afrinic.net/notification.xml
IPv4	105.179.32.0/19,
IPv6	2c0f:f2d8::/32,
ASNum	329727,
CRL Distribution Point	rsync://rpki.afrinic.net/repository/afrinic/K1eJenypZMPIt_e92qek2jSpj4A.crl
Policies	critical 1.3.6.1.5.5.7.14.2
Basic Constraints	critical TRUE
Key Usage	critical CRL Signing, Certificate Signing



Field	
Version	3
Serial Number	13:D3
Issuer	/CN=AFRINIC/SN=2B57897A7CA964C3C8B7F7BDDAA7A4DA34A98F80
Subject	/CN=F3654F09AF/SN=D725C86FF27E2B008A97073E0D84CFF8946A40EA
Not Valid Before	Sep 22 2021 11:40:31 GMT
Not Valid After	Mar 31 2022 0:00:00 GMT
Subject Key Identifier	D7:25:C8:6F:F2:7E:2B:00:8A:97:07:3E:0D:84:CF:F8:94:6A:40:EA
Authority Key Identifier	2B:57:89:7A:7C:A9:64:C3:C8:B7:F7:BD:DA:A7:A4:DA:34:A9:8F:80
Authority Information Access	calssuers - rsync://rpki.afrinic.net/repository/04E8B0D80F4D11E0B657D8931367AE7D/afrinic-ca.cer
Subject Information Access	caRepository - rsync://rpki.afrinic.net/repository/member_repository/F3654F09/42C5BB7C50A111E5A6A4F444F
IPv4	105.179.32.0/19,
IPv6	2c0f:f2d8::/32,
ASNum	329727,
CRL Distribution Point	rsync://rpki.afrinic.net/repository/afrinic/K1eJenypZMPIt_e92qek2jSpj4A.crl
Policies	critical 1.3.6.1.5.5.7.14.2
Basic Constraints	critical TRUE
Key Usage	critical CRL Signing, Certificate Signing

Resource Certificate:

1. **Issuer = AFRINIC**
2. **Subject = ASH-ISP**
3. **Address = 105.179.32.0/19**
4. **ASNum = 329727**
5. **Signature = +$£*&**

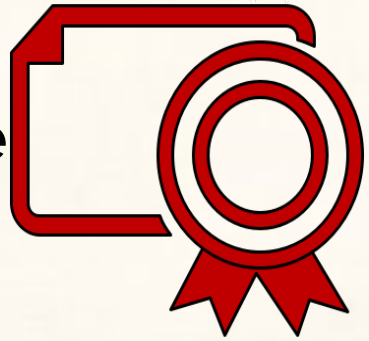








EE Certificate



EE Certificate:

1. **Issuer = ASH-ISP**
2. **Subject = ASH-ISP EE**
3. **Address = 105.179.32.0/19**
4. **Signature = $£%***

End-Entity Certificate:
These are certificates issued by an Address Space Holder with a valid resource certificate to delegate the authority attested by their allocation certificates



View ROA

Name:	RPKI_eCourse_ROA
Revoked:	No
As-number:	37455
Not Valid Before:	2021-09-22 12:55:53
Not Valid After:	2023-09-22 12:55:53
Product-url:	rsync://rpki7.staging.pkl.afrinic.net/repository/member_repository/F36AA8F8/C536754AA1BF11EBA67151B51D92ECD4/74F44BB61BA411ECAA7EAC1F7689C833.roa
IPv4 Prefixes:	80.67.128.0/20-21
Product-url:	rsync://rpki7.staging.pkl.afrinic.net/repository/member_repository/F36AA8F8/AD3219D6A1BF11EBB6E846B51D92ECD4/78B4A9F81BA411EC8F72B01F7689C833.roa
IPv6 Prefixes:	2c0f:f218::/32-36

Revoke

Back



View ROA

Name:	RPKI_eCourse_ROA
Revoked:	No
As-number:	37455
Not Valid Before:	2021-09-22 12:55:53
Not Valid After:	2023-09-22 12:55:53
Product-url:	rsync://rpki7.staging.pkl.afrinic.net/repository/member_repository/F36AA8F8/C536754AA1BF11EBA67151B51D92ECD4/74F44BB61BA411ECAA7EAC1F7689C833.roa
IPv4 Prefixes:	80.67.128.0/20-21
Product-url:	rsync://rpki7.staging.pkl.afrinic.net/repository/member_repository/F36AA8F8/AD3219D6A1BF11EBB6E846B51D92ECD4/78B4A9F81BA411EC8F72B01F7689C833.roa
IPv6 Prefixes:	2c0f:f218::/32-36

Revoke

Back



Route Origin Authorization(ROA):

An object digitally signed by an Address Space Holder stating that they have authorized an ASN to originate routes to one or more prefixes

View ROA

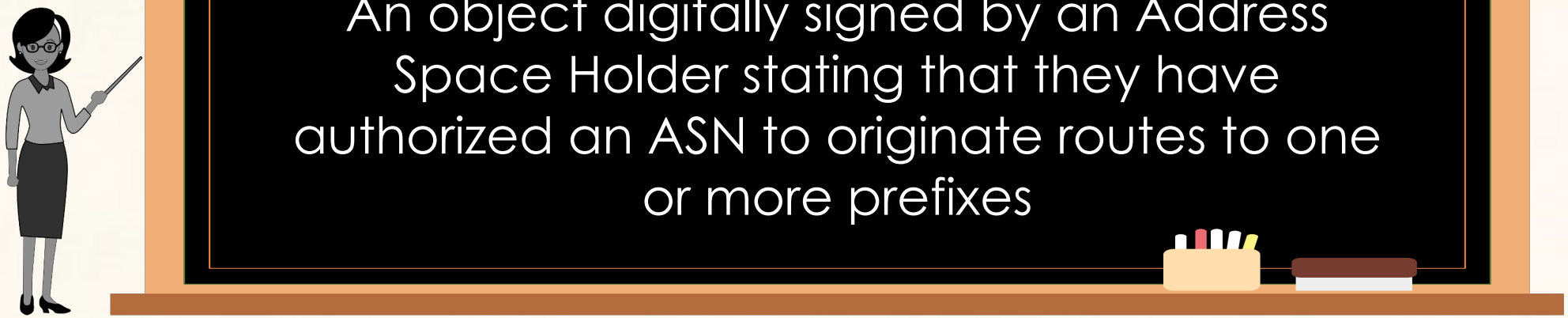
Name:	RPKI_eCourse_ROA
Revoked:	No
As-number:	37455
Not Valid Before:	2021-09-22 12:55:53
Not Valid After:	2023-09-22 12:55:53
Product-url:	rsync://rpki7.staging.pkl.afrinic.net/repository/member_repository/F36AA8F8/C536754AA1BF11EBA67151B51D92ECD4
IPv4 Prefixes:	80.67.128.0/20-21
Product-url:	rsync://rpki7.staging.pkl.afrinic.net/repository/member_repository/F36AA8F8/AD3219D6A1BF11EBB6E846B51D92ECD
IPv6 Prefixes:	2c0f:f218::/32-36

Revoke

Back

ROA:

1. **Issuer = ASH-ISP**
2. **Subject = ASH-ISP EE**
3. **ASN = 37455**
4. **Address = 105.179.32.0/19**
5. **MaxLen = 20**
6. **Signature = $£%***



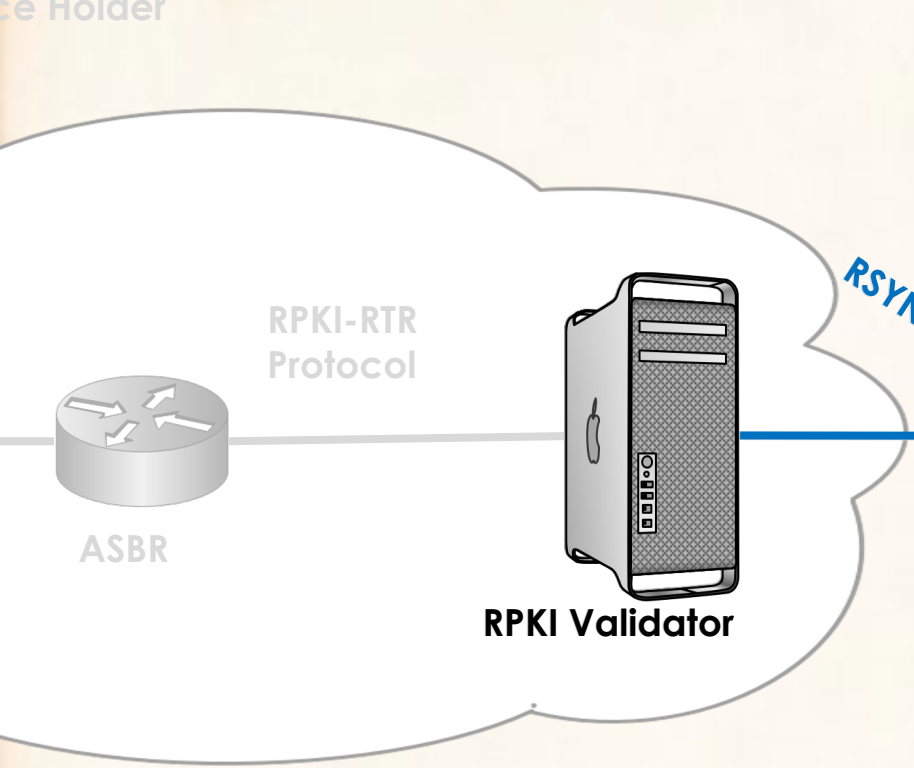
Trust Anchor Locator (TAL)



Trust Anchor







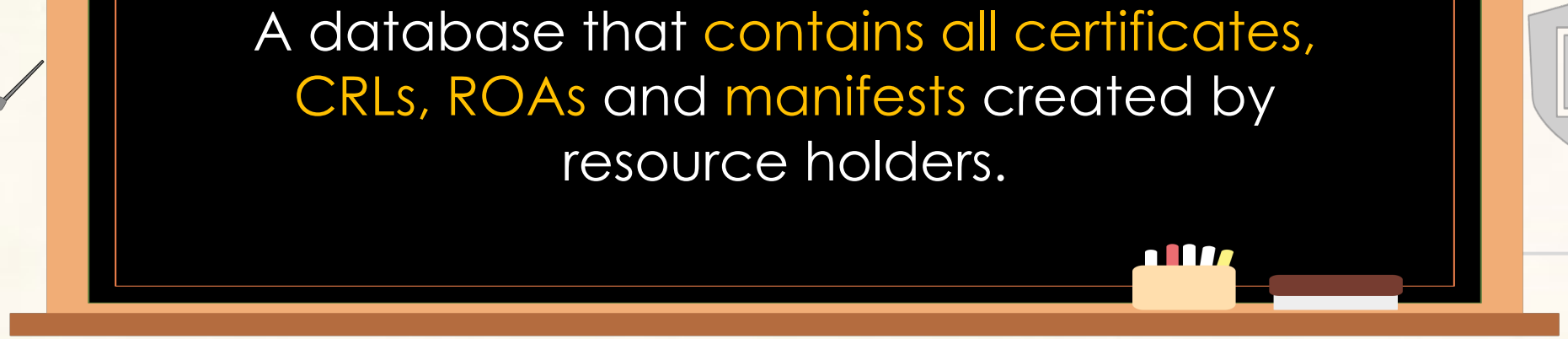
Repository



https://routinator.afrinic.net/ui/repositories

ROUTINATOR | Prefix Check | Metrics | Repositories

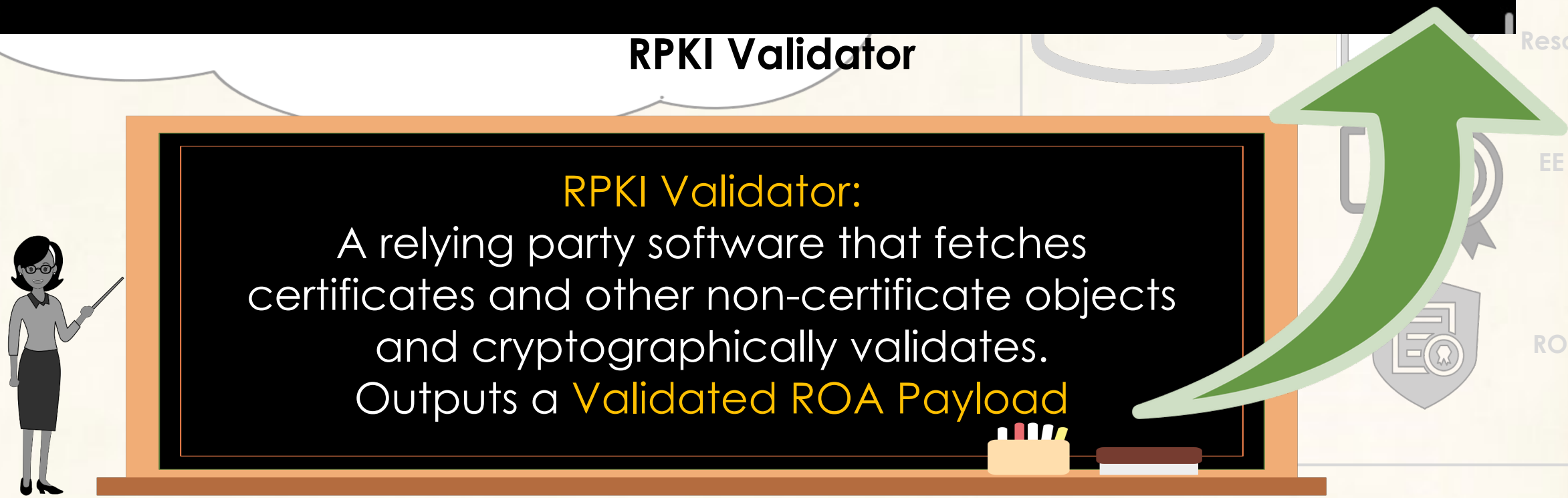
Repository	Type	Total VRPs	Unsafe VRPs
https://rrdp.afrinic.net/notification.xml	RRDP	4,137	3
https://rrdp.arin.net/notification.xml	RRDP	48,651	0
https://rrdp.apnic.net/notification.xml	RRDP	73,052	0
https://rrdp.lacnic.net/rrdp/notification.xml	RRDP	14,459	0
https://rrdp.ripe.net/notification.xml	RRDP	142,498	0





```
{
  "metadata": {
    "generated": 1633069313,
    "generatedTime": "2021-10-01T06:21:53Z"
  },
  "roas": [
    { "asn": "AS37708", "prefix": "2001:43f8:90::/48", "maxLength": 48, "ta": "afrinic" },
    { "asn": "AS37708", "prefix": "2001:43f8:92::/48", "maxLength": 48, "ta": "afrinic" },
    { "asn": "AS37708", "prefix": "196.1.0.0/24", "maxLength": 24, "ta": "afrinic" },
    { "asn": "AS37708", "prefix": "196.192.112.0/23", "maxLength": 24, "ta": "afrinic" }
  ]
}
```


RPKI Validator



Address Space Holder

Trust Anchor

Repository

RSYNC/RRDP

RPKI-RTR Protocol

BGP

ASBR

RPKI Validator

esource Certificate

EE Certificate

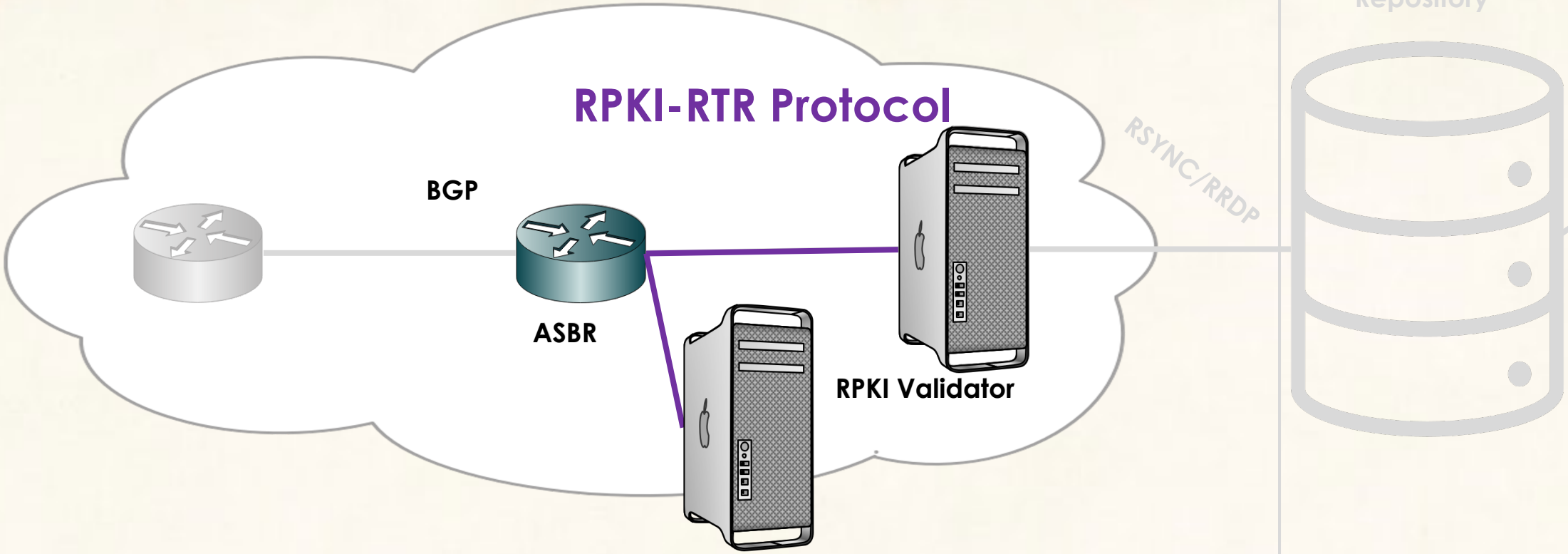
ROA



Access Protocols (RSYNC/RRDP)

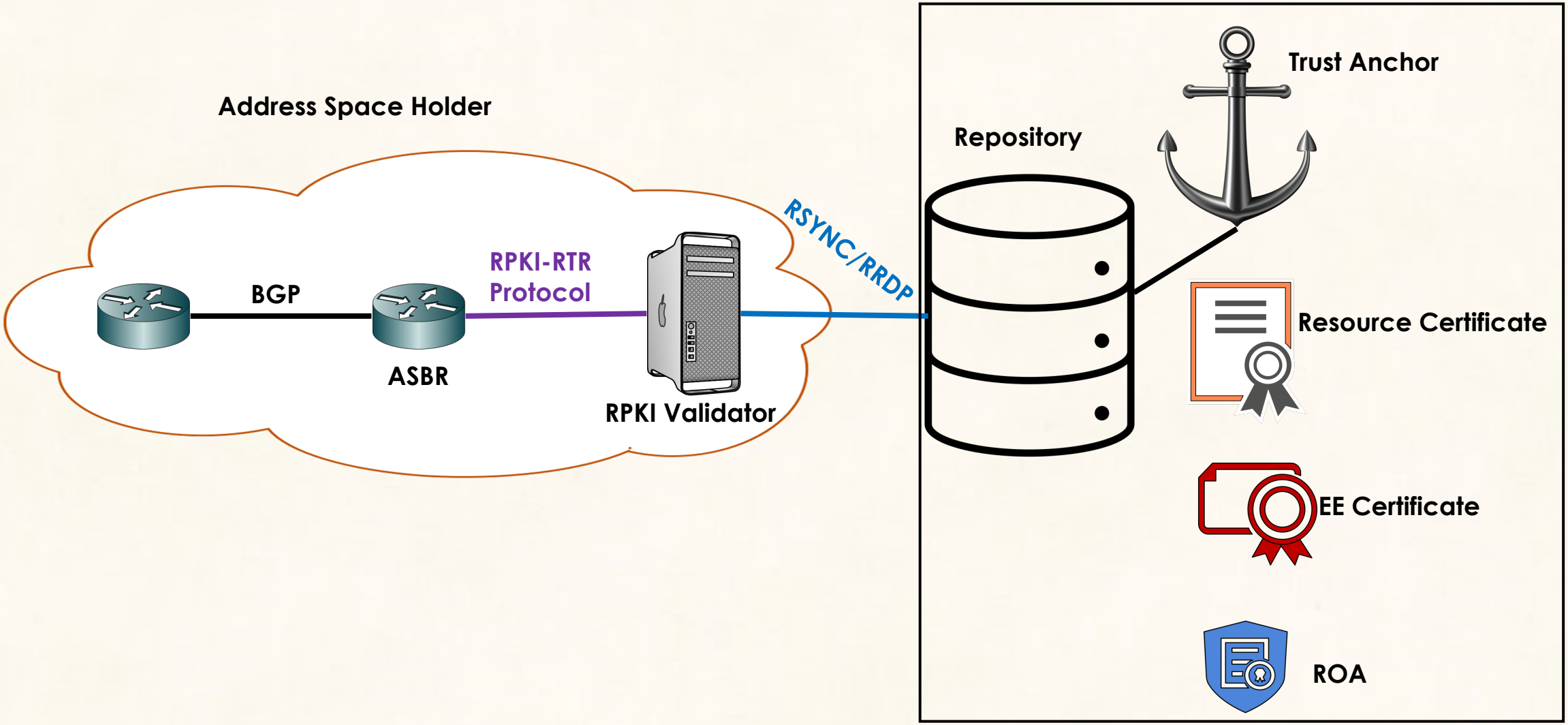
Used by repository operators to allow access to all participants in the RPKI to maintain their respective portions of the repository

RPKI-RTR Protocol

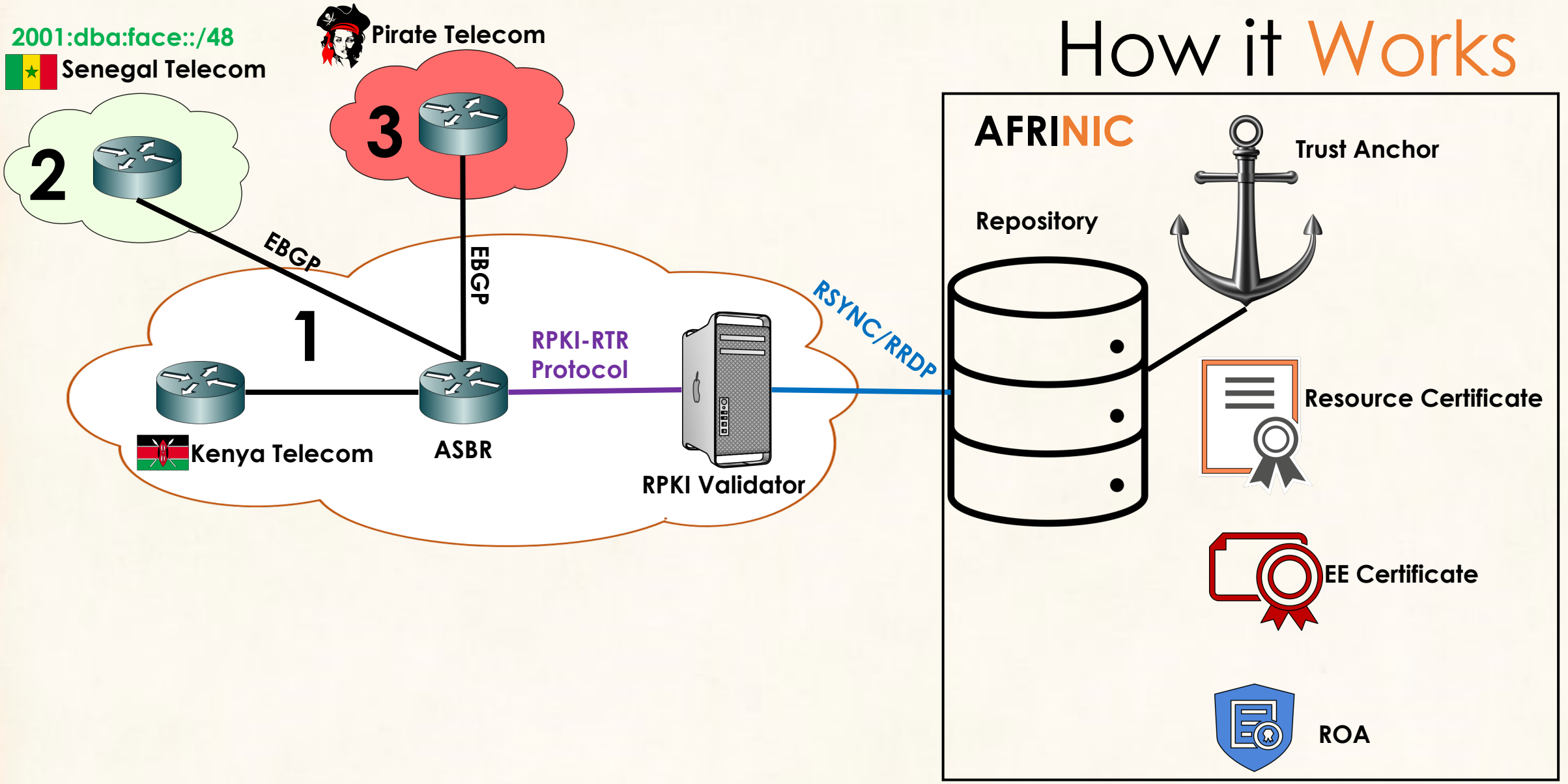


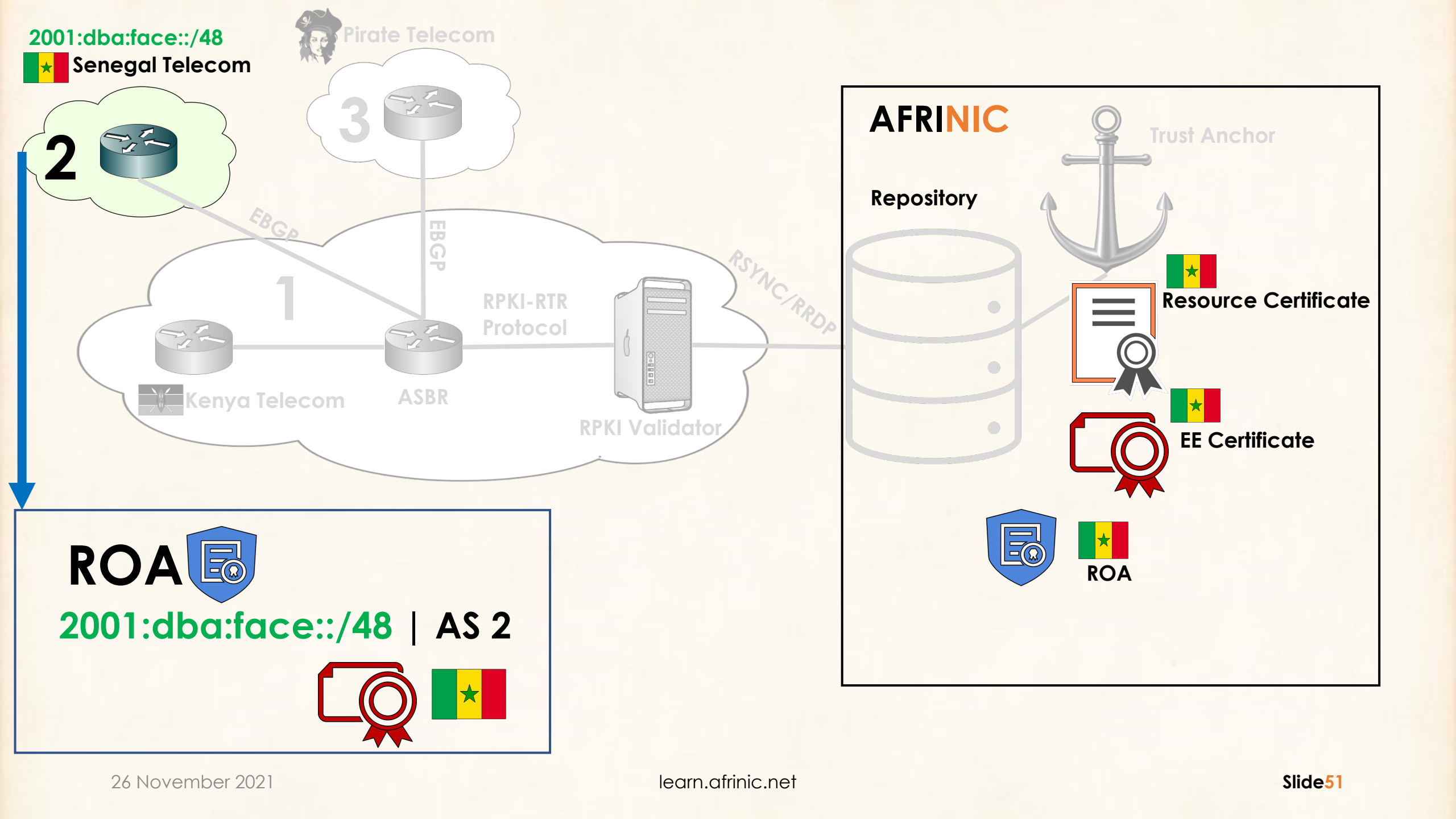
RPKI to Router Protocol:
A reliable communication protocol used to receive validated RPKI prefix origin data from a trusted cache (validated cache)

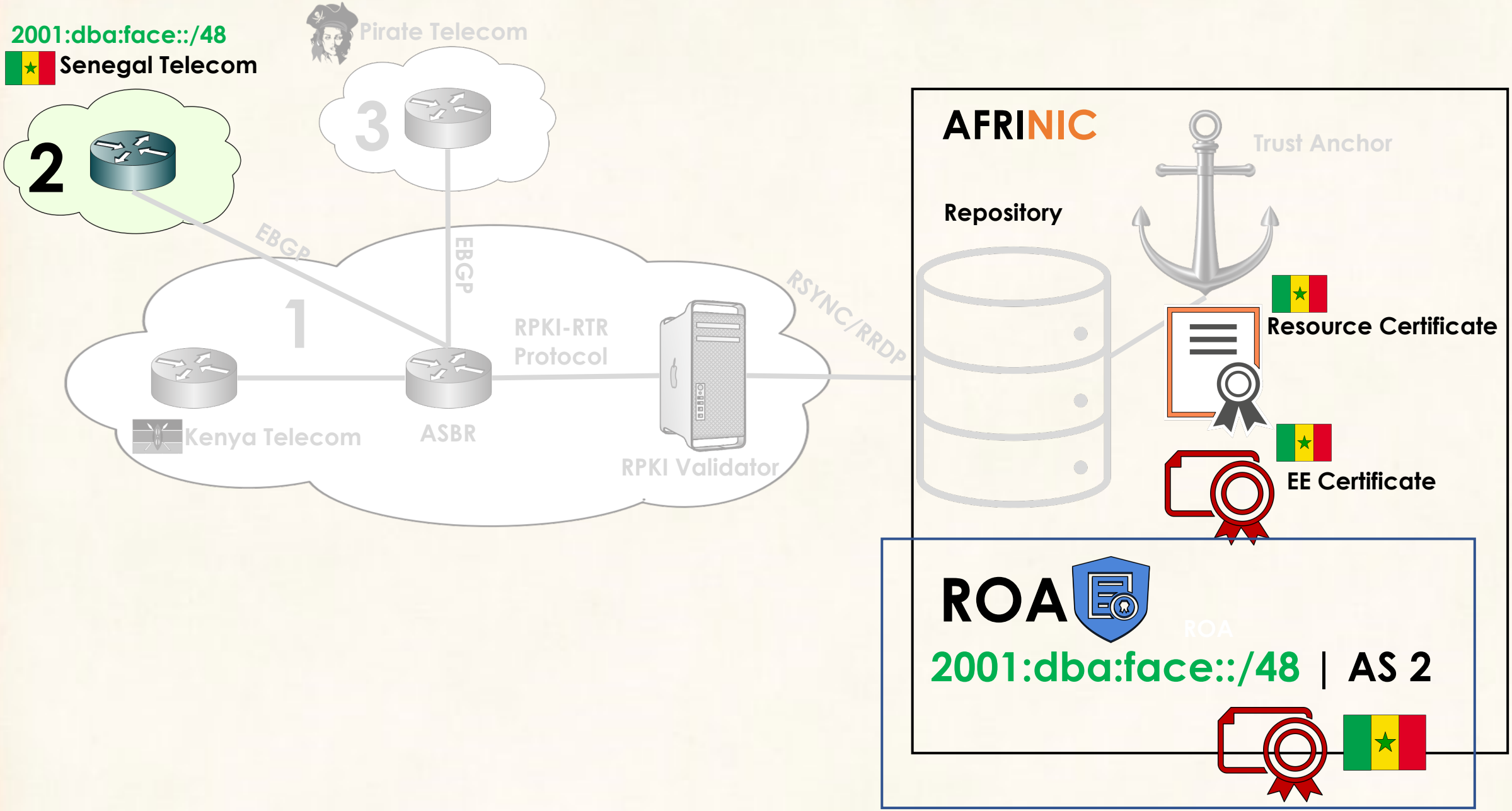
How it Works

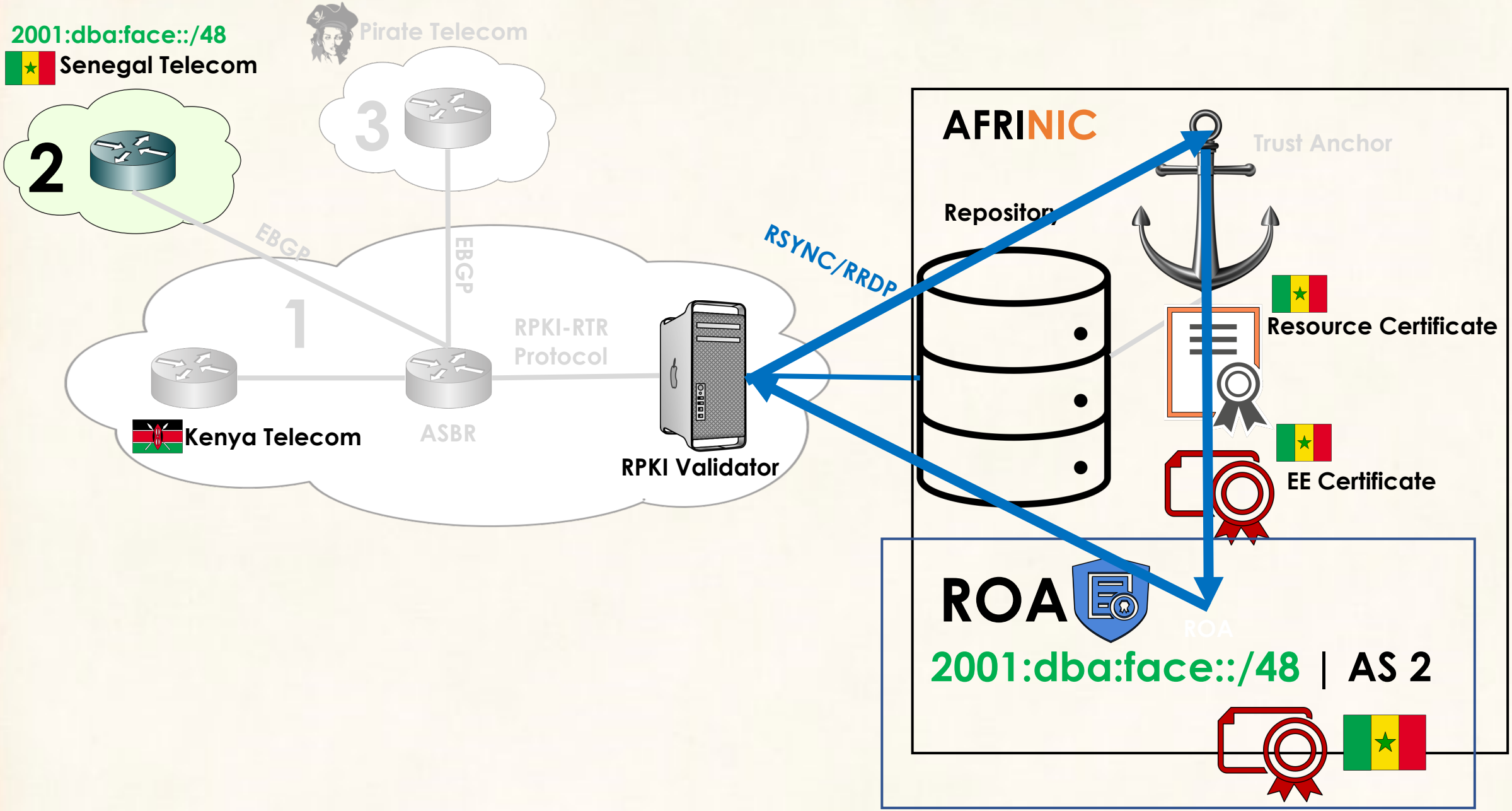

Address Space Holder
BGP
ASBR
RPKI-RTR
Protocol
RPKI Validator
RSYNC/RRDP
Repository
Trust Anchor
Resource Certificate
EE Certificate
ROA

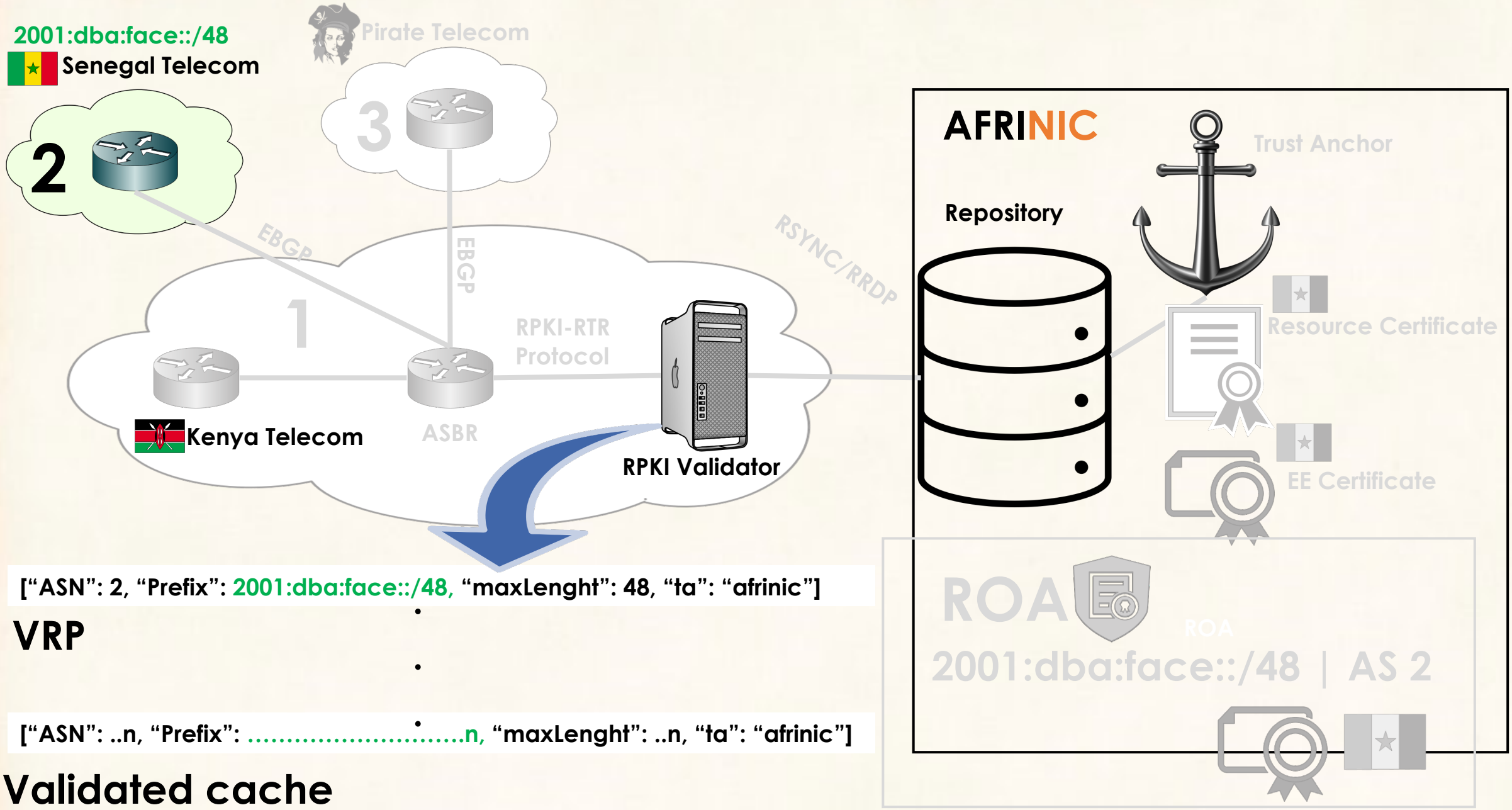
How it Works


2001:dba:face::/48
Senegal Telecom
Pirate Telecom
2
3
1
EBGP
EBGP
RPKI-RTR
Protocol
RSYNC/RRDP
Kenya Telecom
ASBR
RPKI Validator
AFRINIC
Repository
Trust Anchor
Resource Certificate
EE Certificate
ROA


2001:dba:face::/48
Senegal Telecom
Pirate Telecom
3
2
1
EBGP
EBGP
RPKI-RTR
Protocol
RSYNC/RRDP
Kenya Telecom
ASBR
RPKI Validator
AFRINIC
Trust Anchor
Repository
Resource Certificate
EE Certificate
ROA
ROA
2001:dba:face::/48 | AS 2


2001:dba:face::/48
Senegal Telecom
Pirate Telecom
3
2
1
EBGP
EBGP
RPKI-RTR
Protocol
RSYNC/RRDP
Kenya Telecom
ASBR
RPKI Validator
AFRINIC
Trust Anchor
Repository
Resource Certificate
EE Certificate
ROA
2001:dba:face::/48 | AS 2


2001:dba:face::/48
Senegal Telecom
Pirate Telecom
3
2
1
EBGP
EBGP
RPKI-RTR
Protocol
Kenya Telecom
ASBR
RPKI Validator
RSYNC/RRDP
AFRINIC
Trust Anchor
Repository
Resource Certificate
EE Certificate
ROA
2001:dba:face::/48 | AS 2

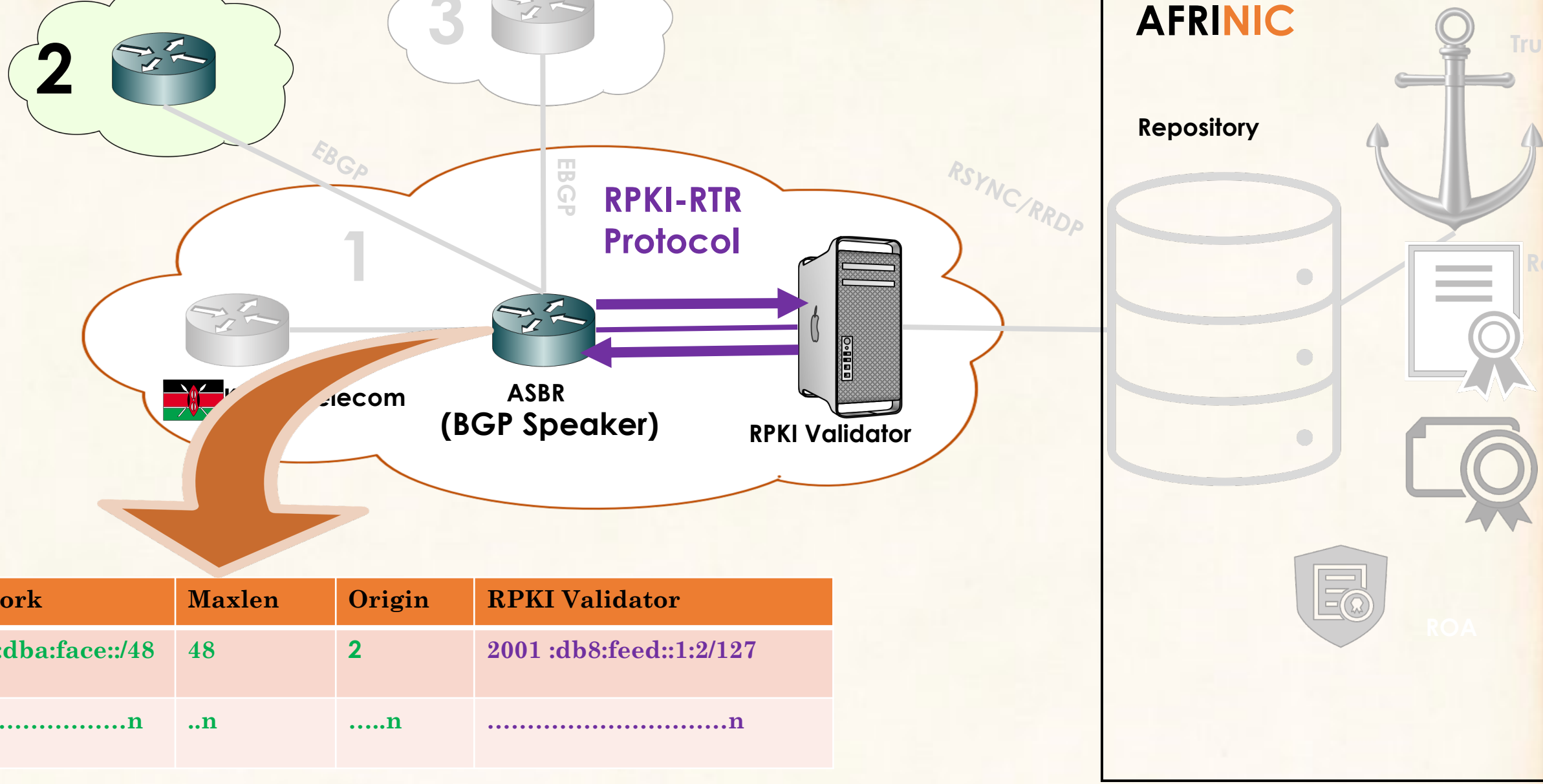


["ASN": 2, "Prefix": 2001:dba:face::/48, "maxLenght": 48, "ta": "afrinic"]

VRP

["ASN": ..n, "Prefix": .....n, "maxLenght": ..n, "ta": "afrinic"]

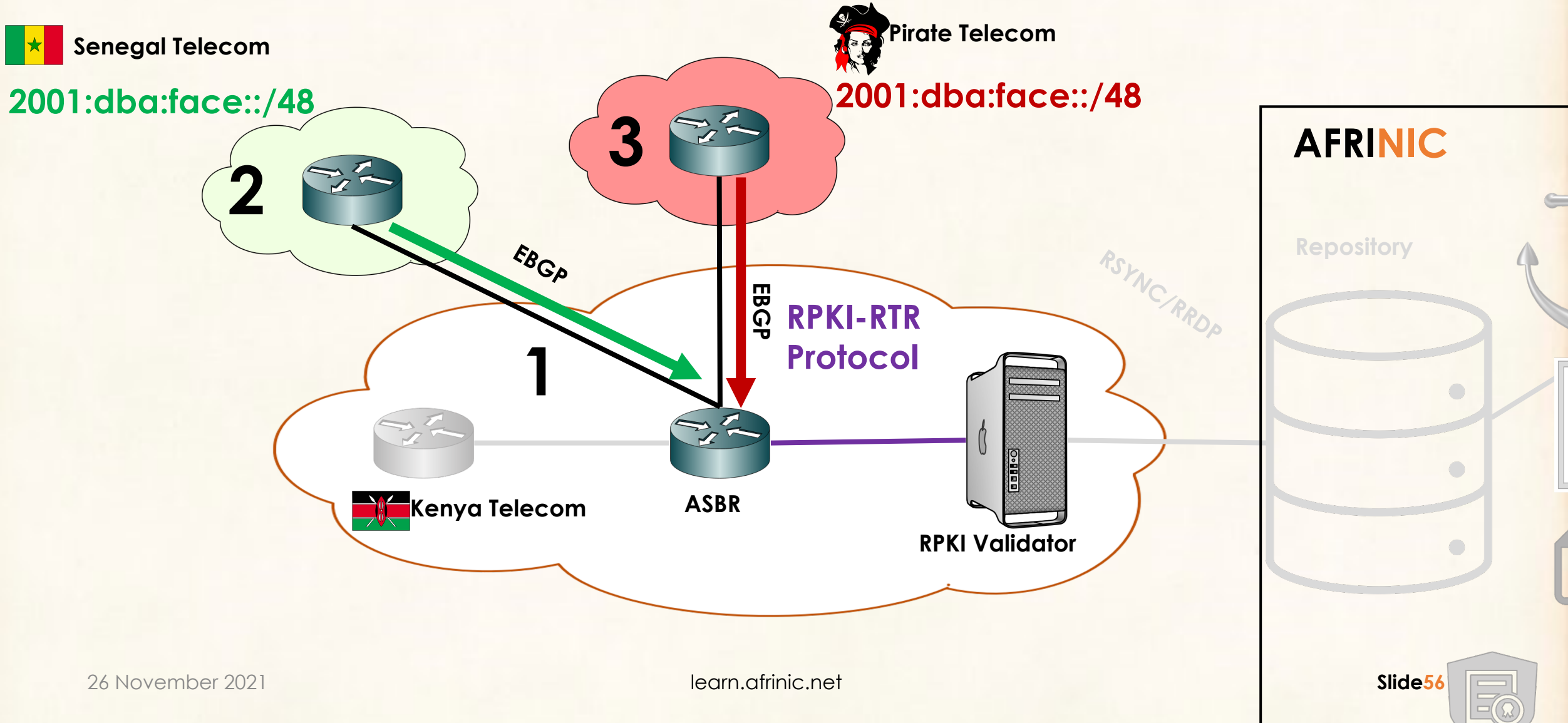
Validated cache



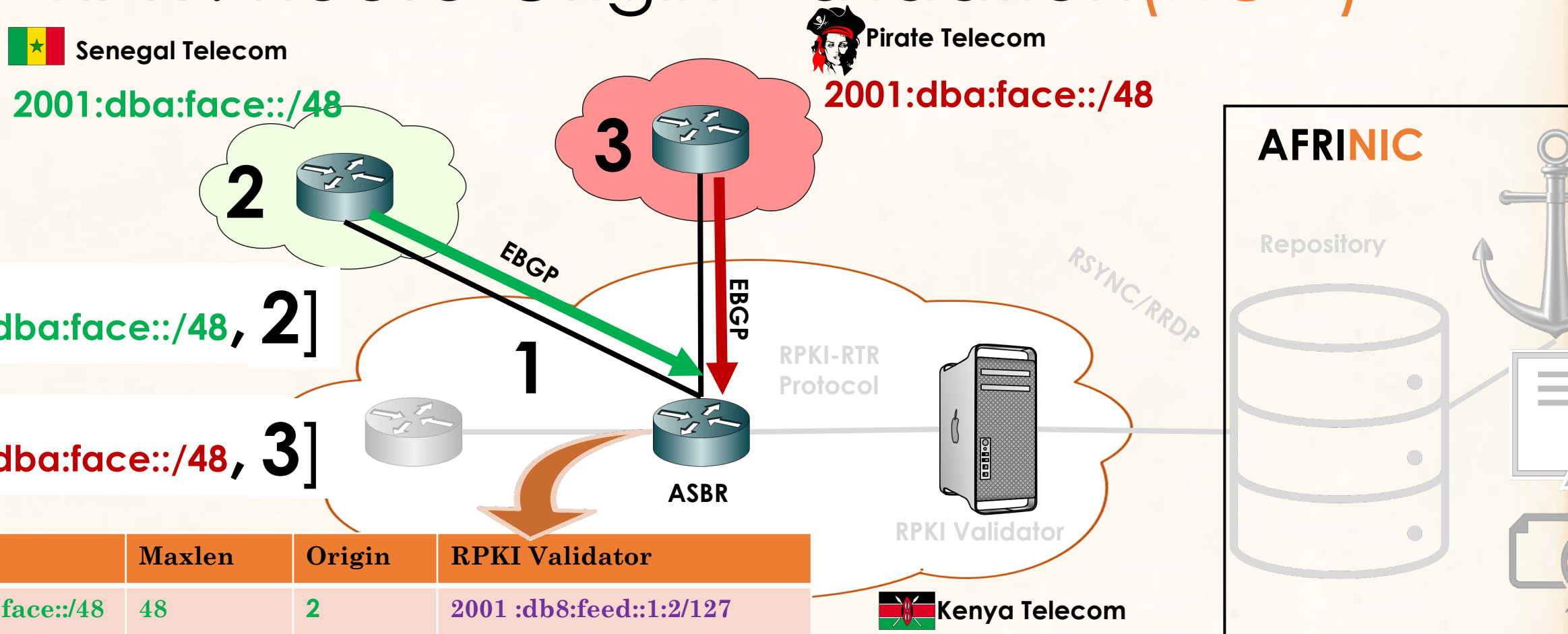
Network	Maxlen	Origin	RPKI Validator
2001 :dba:face::/48	48	2	2001 :db8:feed::1:2/127
……n	..n	…..n	……n

BGP-RPKI Table

RPKI: Route Origin Validation(ROV)



RPKI: Route Origin Validation(ROV)

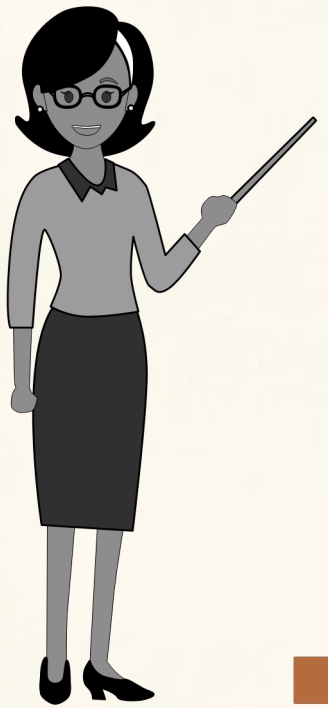


[2001:dba:face::/48, 2]

[2001:dba:face::/48, 3]

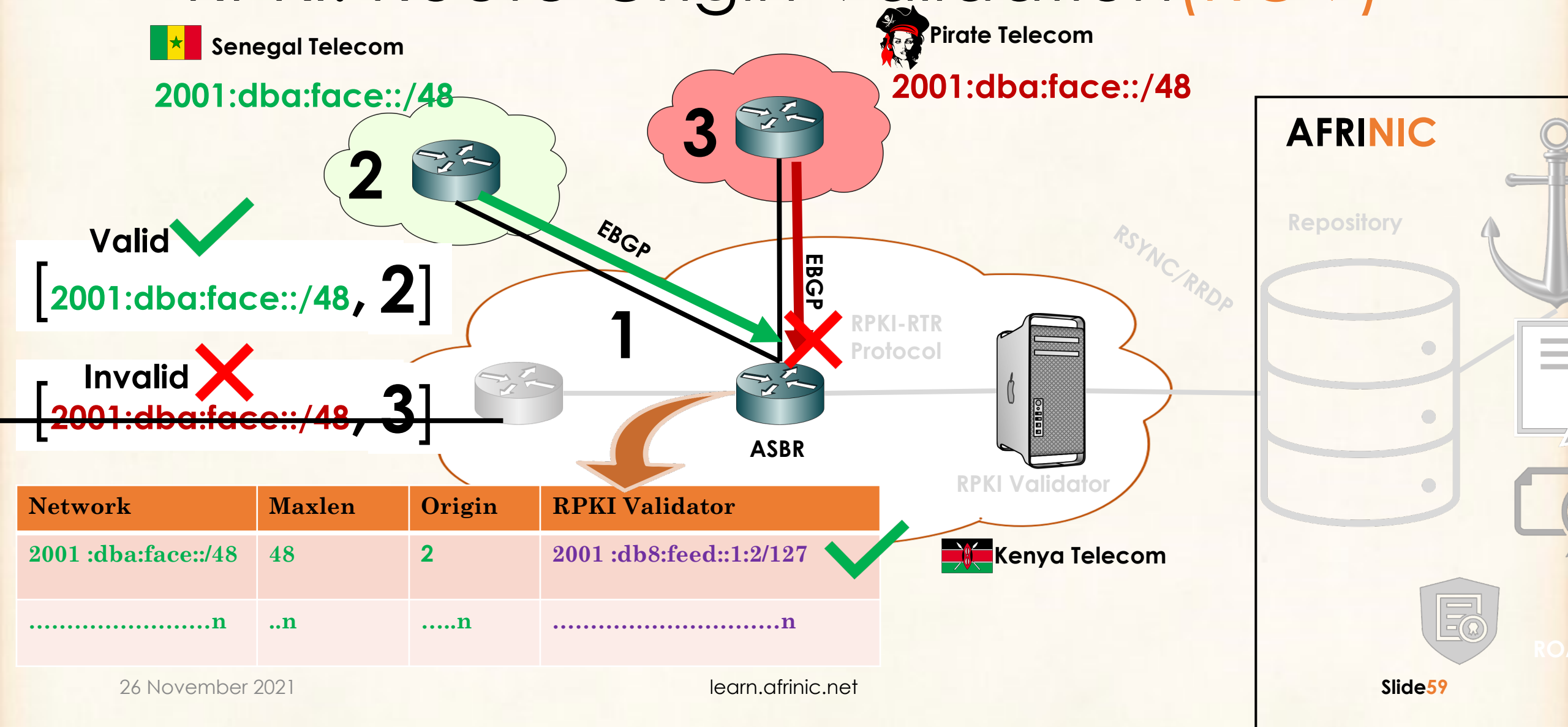
Network	Maxlen	Origin	RPKI Validator
2001 :dba:face::/48	48	2	2001 :db8:feed::1:2/127
……n	..n	…..n	……n

RPKI: ROV States



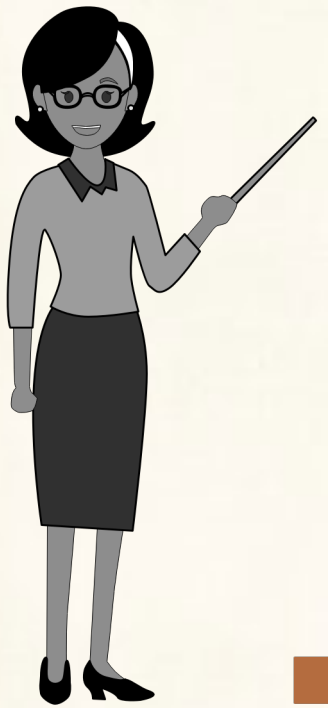
- Valid: Prefix covered by at least one VRP
- Invalid: Prefix announced from an unauthorized AS or a more specific announcement is made
- Not Found: Prefix not covered or partially covered by a VRP

RPKI: Route Origin Validation(ROV)



Network	Maxlen	Origin	RPKI Validator
2001 :dba:face::/48	48	2	2001 :db8:feed::1:2/127
……n	..n	…..n	……n

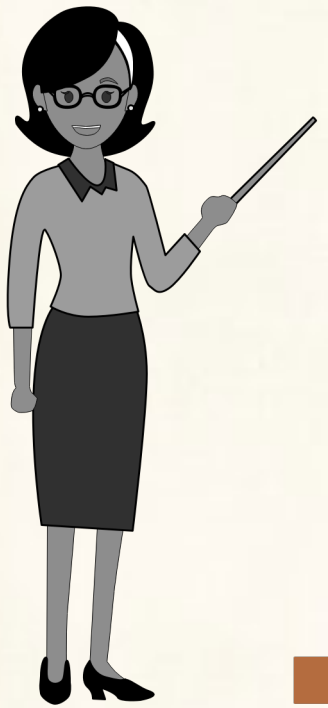
RPKI: Implementation Models



There are 2 types of RPKI Implementation Models. These are:

- **Hosted RPKI**
- **Delegated RPKI**

RPKI: Hosted Implementation



- Certificates and ROAs are published in repositories hosted by an RIR/NIR/LIR
- Users create and maintain ROAs through a portal
- This is the only implementation currently offered by AFRINIC

RPKI: Hosted RPKI



Address Space Holder

BGP

ASBR

RPKI-RTR Protocol

RPKI Validator

RSYNC/RRDP

Repository

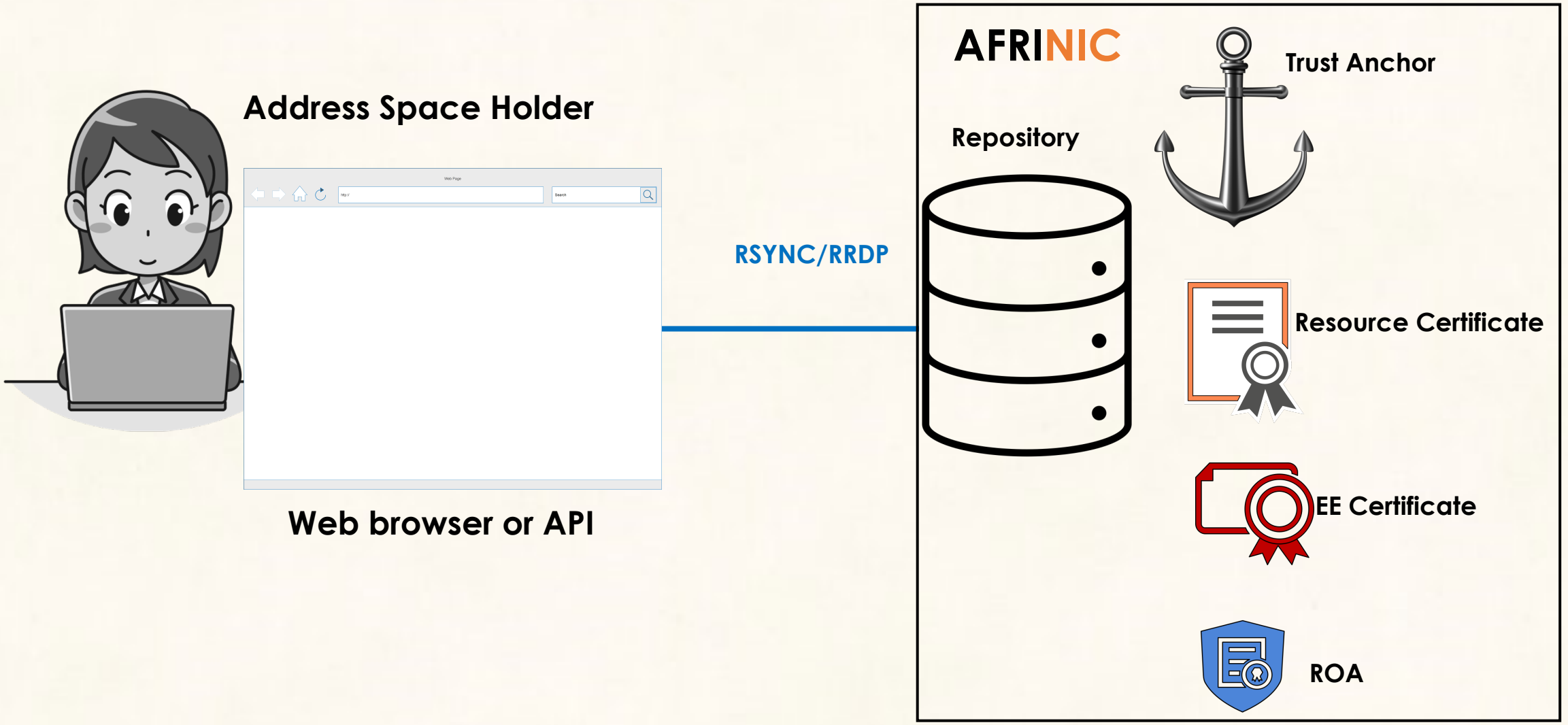
Trust Anchor

Resource Certificate

EE Certificate

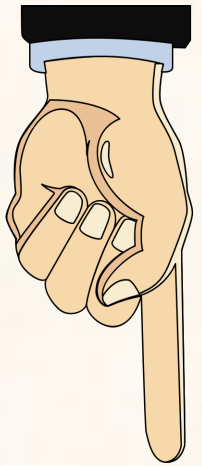
ROA

RPKI: Hosted RPKI



Hosted RPKI: Low Entry Barrier (+1)







Hosted RPKI: Gain operational XP (+1)



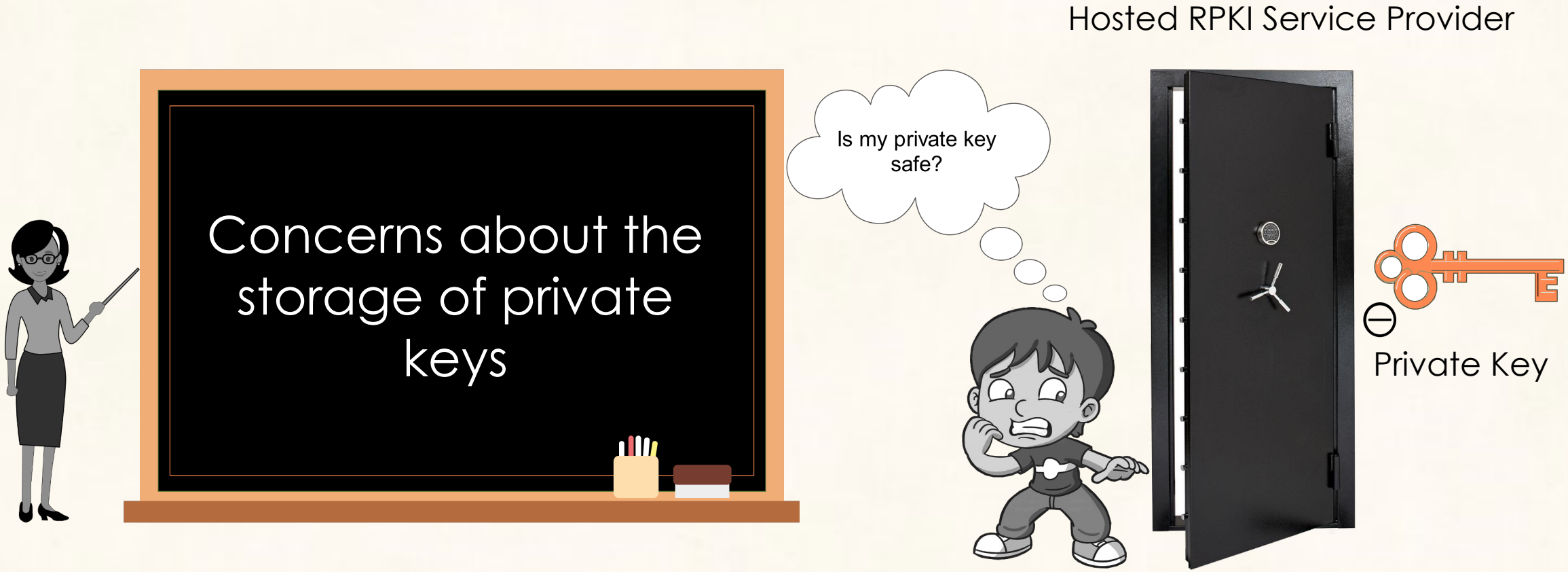


Hosted RPKI: Outages (-1)

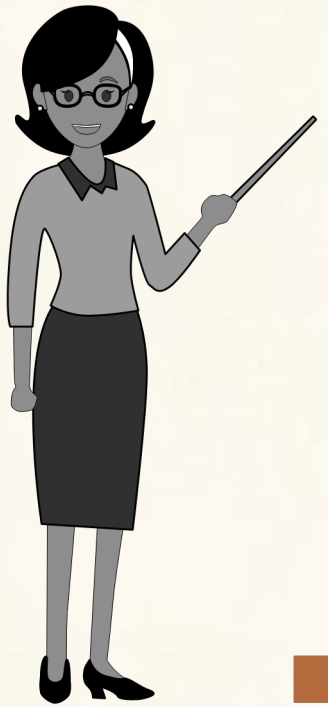




Hosted RPKI: Private Key Storage (-1)



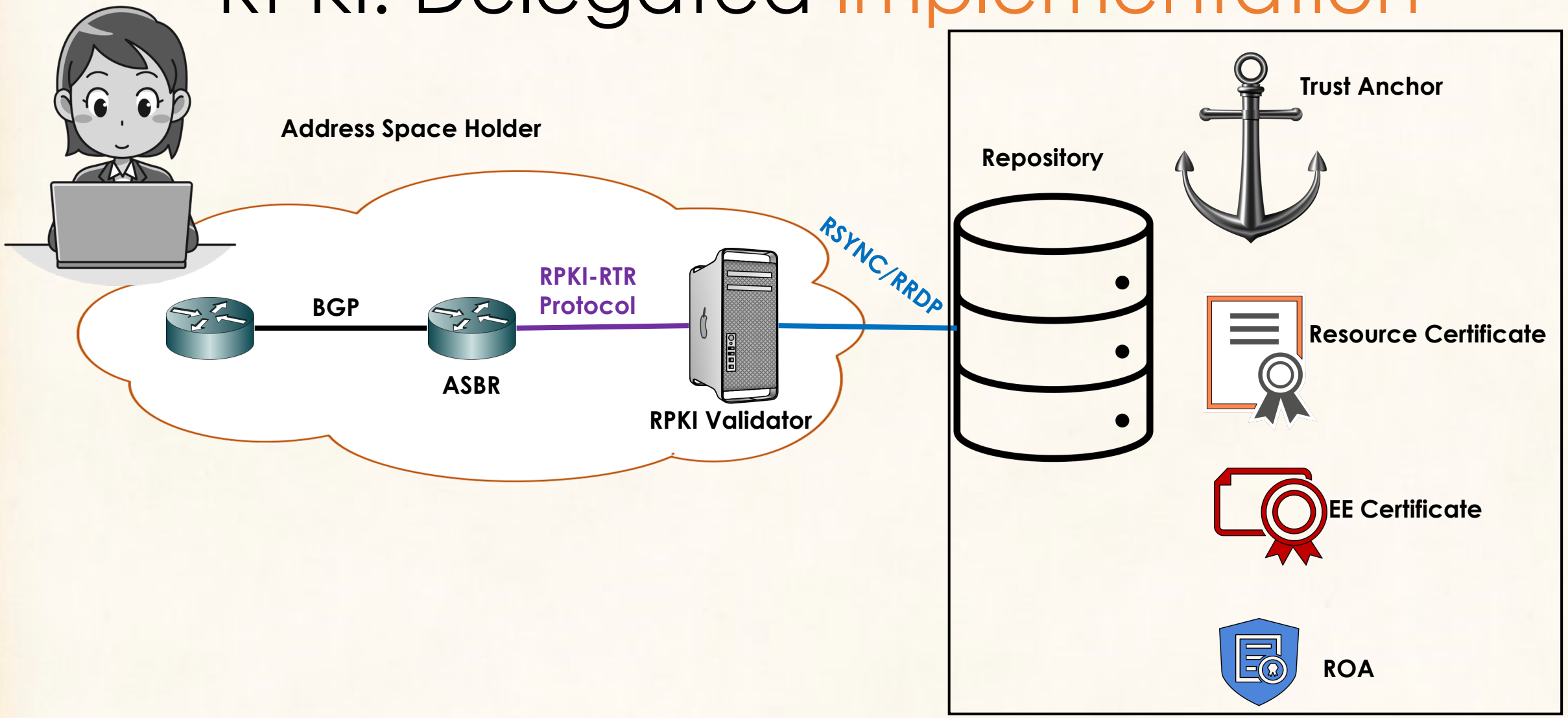
RPKI: Delegated Implementation



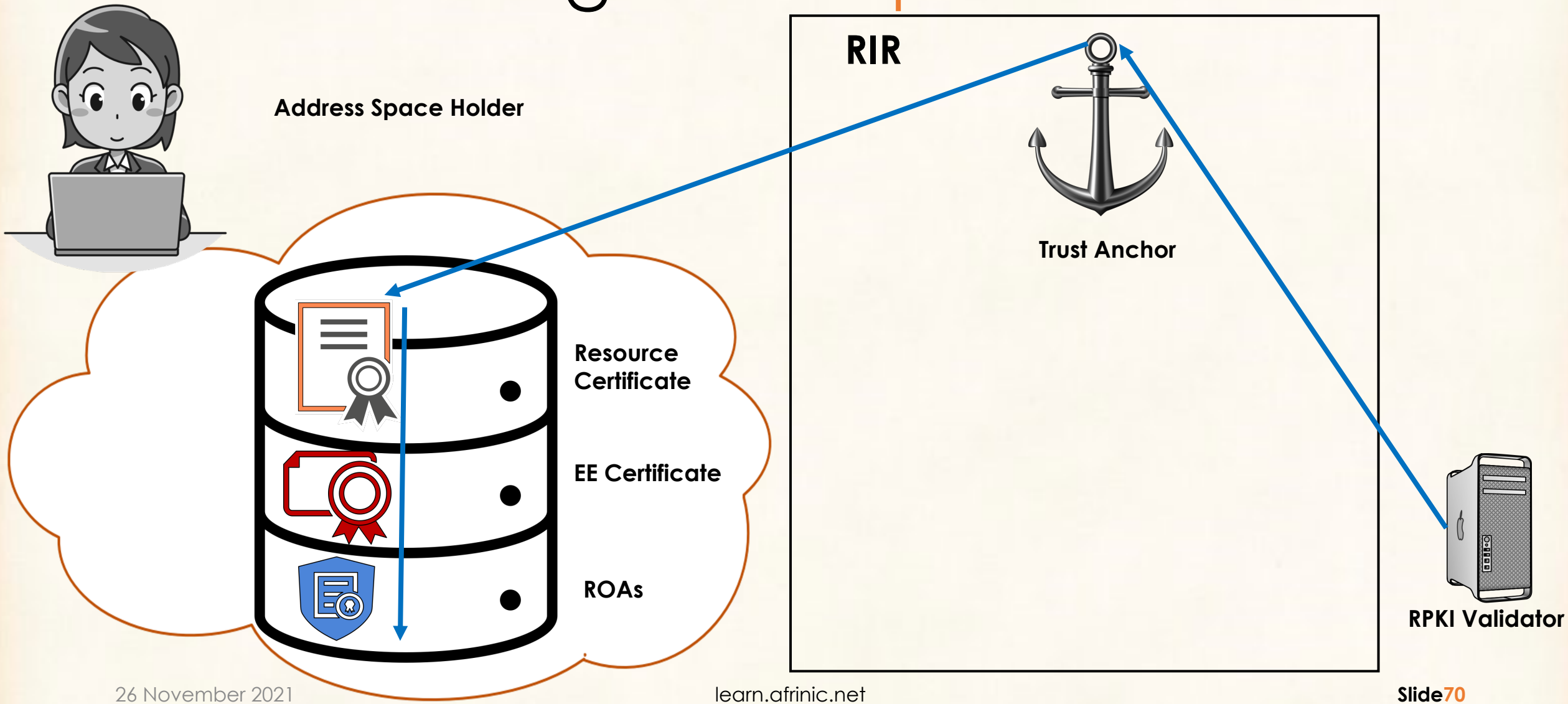
In this implementation:

- You run your CA as a child of the RIR
- You publish signed objects or contract a third party to carry out this function

RPKI: Delegated Implementation

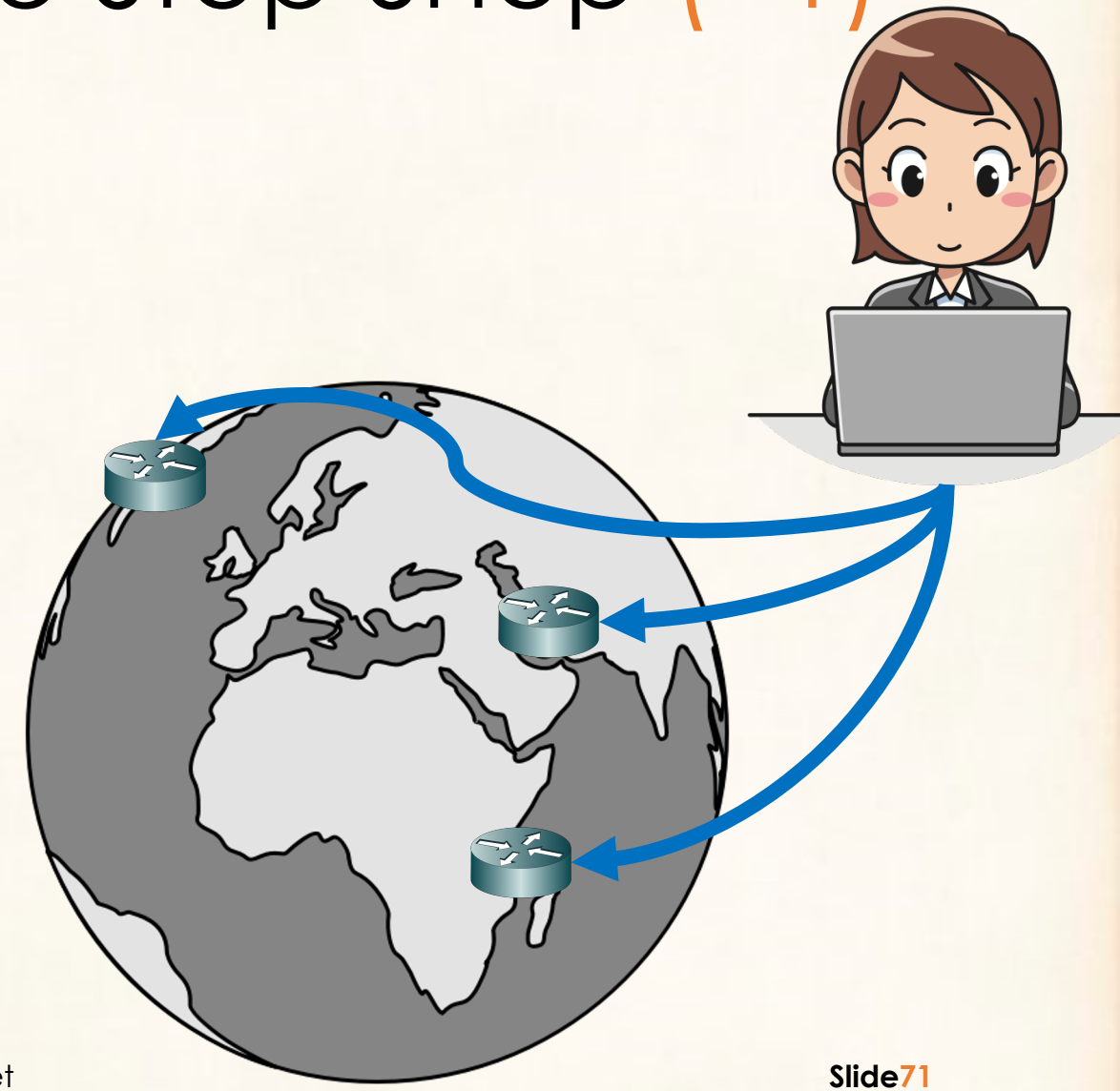


RPKI: Delegated Implementation

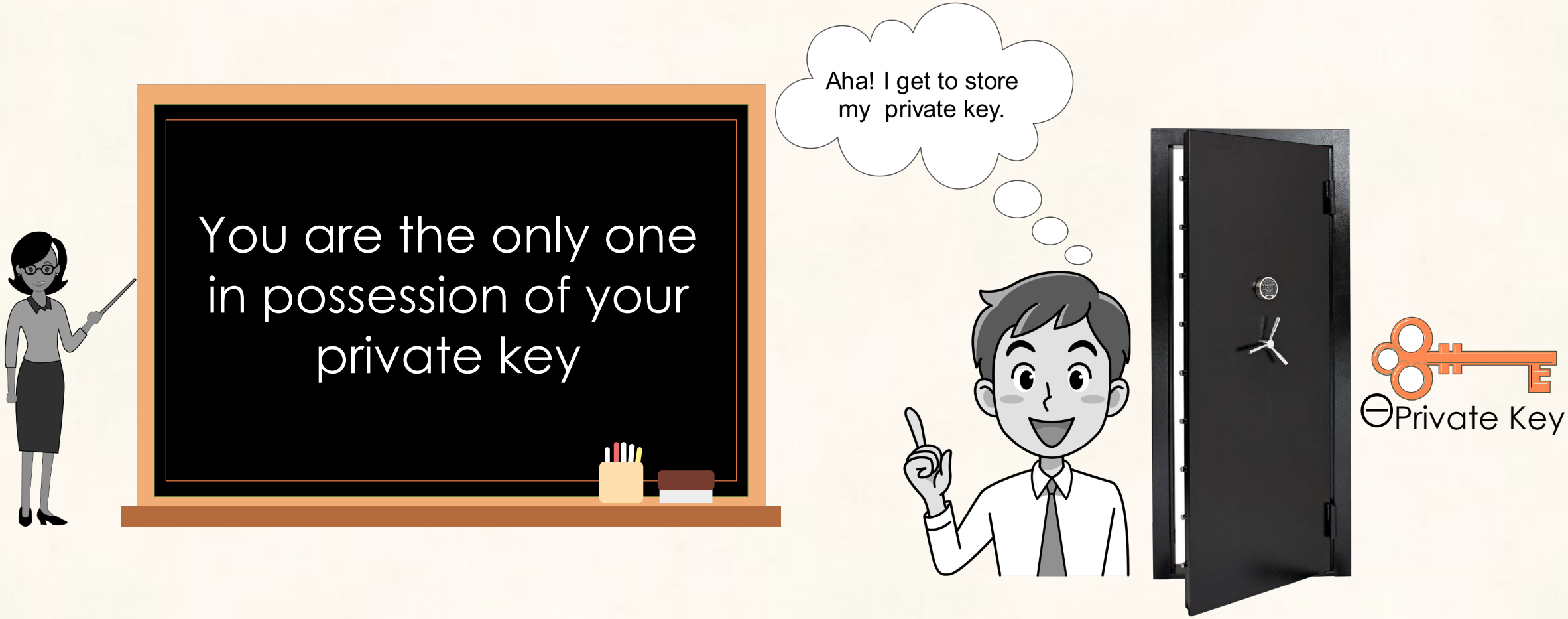


Delegated RPKI: One Stop Shop (+1)



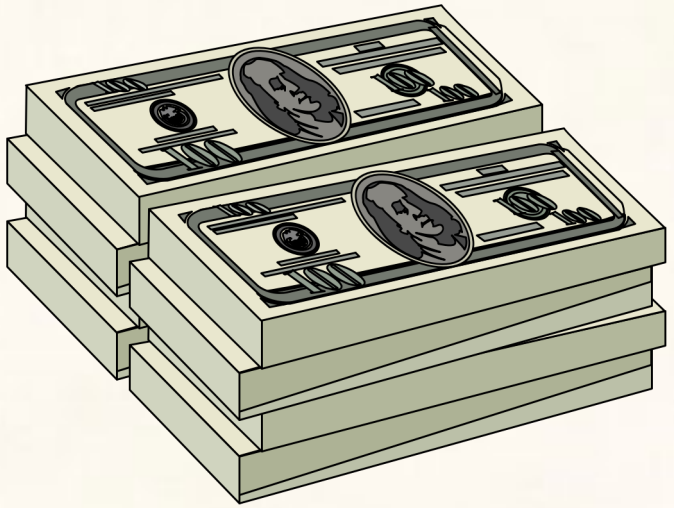


Delegated RPKI: Private Key Storage (+1)

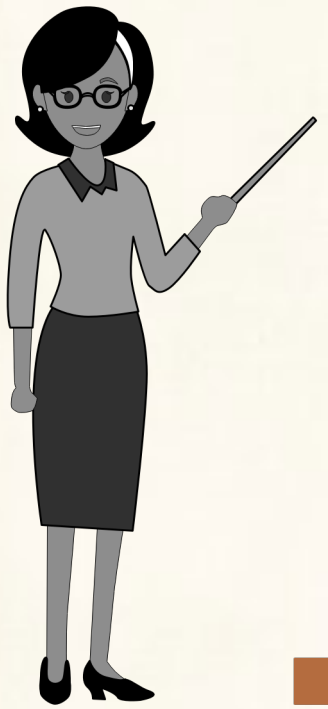


Delegated RPKI: Cost (-1)





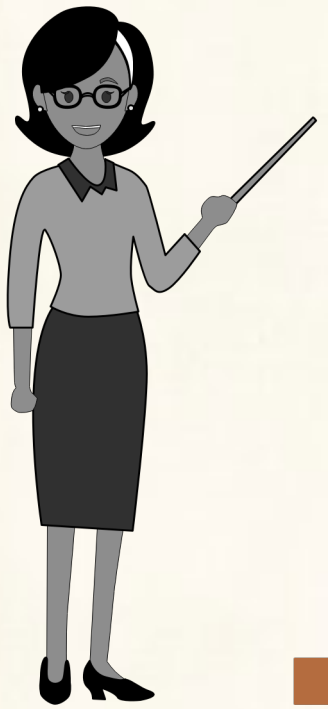
RPKI: Choosing an Implementation Model



Hosted Implementation:

- A multi-homed network operator operating in a single RIR region can opt for the hosted RPKI service

RPKI: Choosing an Implementation Model



Delegated Implementation:

- A multi-homed network operator operating in multiple RIR regions
- You are multiple Organisations under a single RIR

AGENDA



How to Create a ROA

"Show me and I understand"

1. The Limits of BGP
2. Why the IRR alone is not Sufficient
3. How RPKI makes BGP more Secure
4. **How to Create a ROA**



5. **Questions & Answers**

QUESTIONS

ANSWERS



Deployment Support Helpdesk

bit.ly/6deployEN

$0.00

Please scan me!



Request assistance in deploying Internet protocols & services

AFRINIC Academy

bit.ly/afrinicacademy

$0.00

Please scan me!



Learn at your own pace

training@afrinic.net

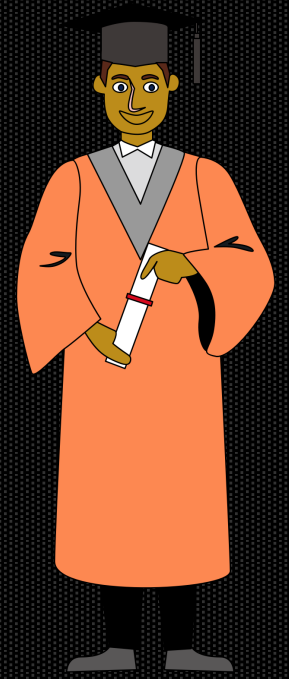
$0.00

Please scan me!

U-Connect



+



Partnering with higher academic institutions

Certi6

bit.ly/certi6EN

Please scan me!



Get recognized IPv6 certification

Thank you !

