

Resource Public Key Infrastructure ieviešana

Seminārs Interneta pakalpojumu sniedzējiem

AS51955

NIC-LV-ANYCAST-AS

4936th place in IPv4 connectivity rating

↓ Last month: -32 positions

1064th place in IPv6 connectivity rating

↓ Last month: -12 positions

[Overview](#) >

[Graph](#) >

[Whois](#) >

IPv4 Connectivity

Providers 7

Customers 0

Peerings 1

Unspecified 0

Prefixes 6

IPv6 Connectivity

Providers 7

Customers 0

Peerings 0

Unspecified 0

Prefixes 6

Security Issues

Route Leaks 0

Hijacks 0

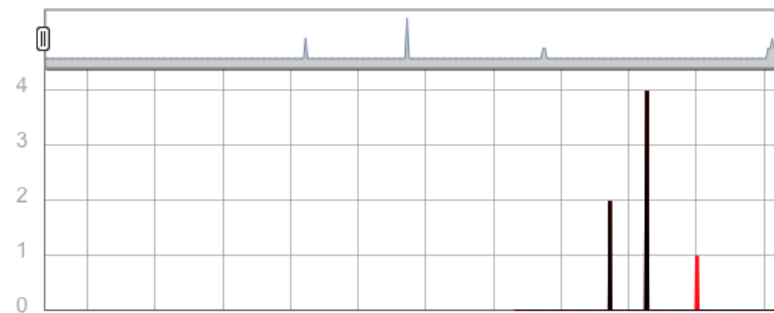
Bogons 0

Static Loops 0

Vulnerable Ports 0

DDoS amplifiers 0

Hijacks



Apr 17 Jul 17 Oct 17 Jan 18 Apr 18 Jul 18 Oct 18 Jan 19 Apr 19 Jul 19 Oct 19

2017-02-02 – 2019-10-30

"Hijacking" of the address space refers to a situation where the AS announces prefixes that do not have the correct route object/ROA record and that conflict with the prefixes of another AS.

EXPORT

ANGOLA-CABLES

ALL (1) CREATED (0) AFFECTED (1)

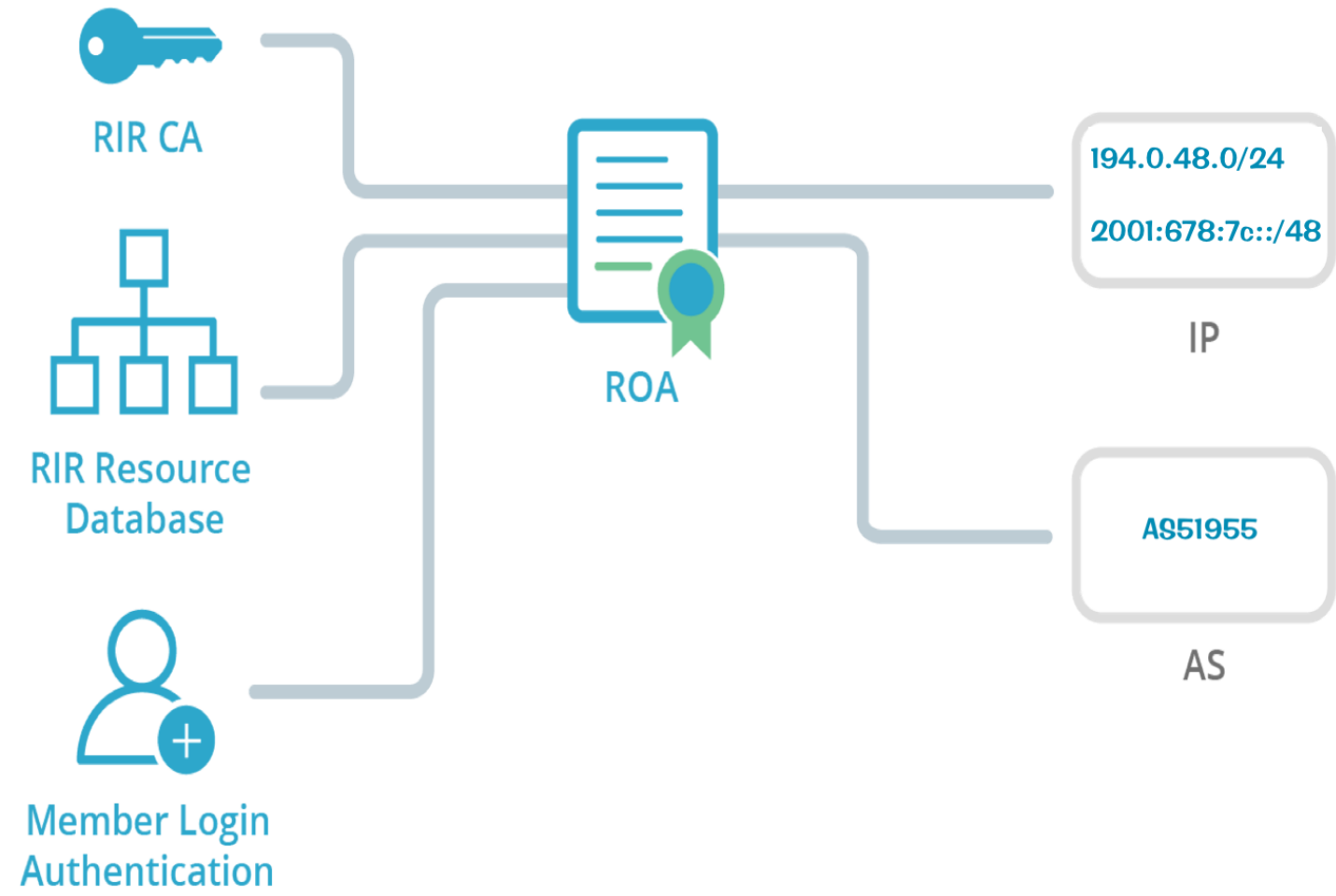
Prefix 1	Origin 1	Prefix 2	Origin 2	Type	First seen	Last seen
194.0.48.0/24	AS51955	194.0.48.0/24	AS37468	Affected	2019-04-26 01:34:00	2019-04-26 01:41:00
194.0.48.0/24	AS51955	194.0.48.0/24	AS37468	Affected	2019-04-26 00:59:00	2019-04-26 01:30:00
194.0.48.0/24	AS51955	194.0.48.0/24	AS24875	Affected	2019-03-07 14:02:00	2019-03-07 14:04:00

NOVOSERVE-AS

BGP maršrutēšanas drošība

- Filtri BGP peeriem IN &OUT
- BCP38 – Unicast Reverse Path Forwarding
- Aktuāli ieraksti “route”ojektiem RIR (RIPE NCC) datubāzē
- Route Origin Authorisation izmantojot RPKI

<https://www.manrs.org/manrs>



CERT.LV

Resource Public
Key Infrastructure



Router

A rounded purple rectangle containing the logos of five Regional Internet Registries (RIRs): lacnic, APNIC, AFRINIC, ARIN, and RIPE NCC. The logos are arranged in two rows. lacnic, APNIC, and AFRINIC are in the top row. ARIN and RIPE NCC are in the bottom row.

RIRs



RPKI-RTR Protocol

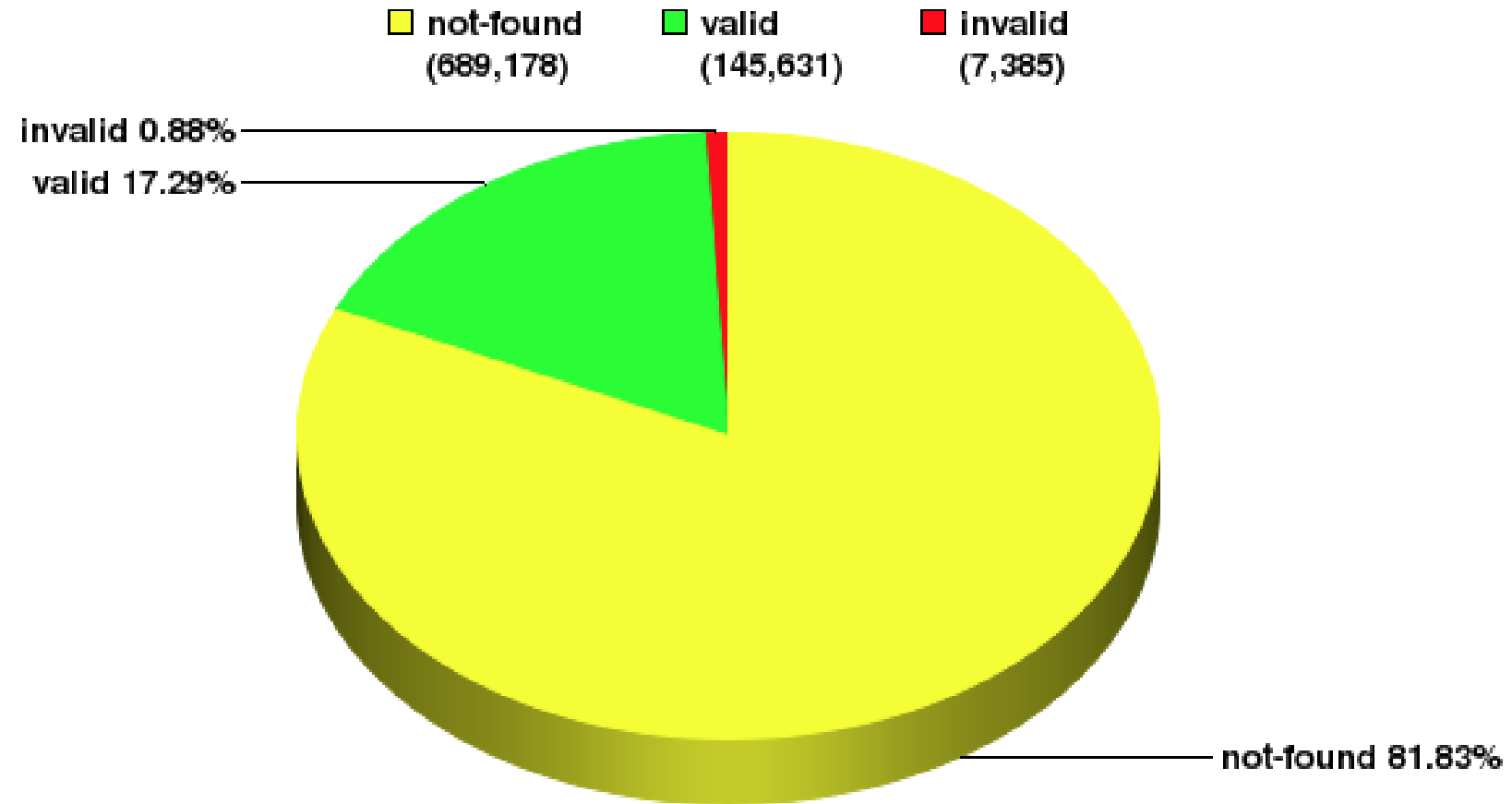


Validator

Validation Results of Unique IPv4 Prefix/Origin Pairs using Global RPKI

Global: Validation Snapshot of Unique P/O pairs

842,194 Unique IPv4 Prefix/Origin Pairs



You are here: [Home](#) > [Manage IPs and ASNs](#) > LIR Portal

You are editing Institute of Mathematics and C...

My Account >

Resources >

My Resources

Sponsored Resources

Request Resources

Request Transfer

IPv4 Transfer Listing Service

[RPKI Dashboard](#)

RIPE Database >

RPKI Dashboard

15 CERTIFIED RESOURCES

ALERTS ARE SENT TO 3 ADDRESSES

37 BGP Announcements

37 Valid 0 Invalid 0 Unknown

37 ROAs

37 OK 0 Causing problems

BGP Announcements

Route Origin Authorisations (ROAs)

History

Search...

<input type="checkbox"/>	AS number	Prefix	Most specific length allowed	Affected announcements	
<input type="checkbox"/>	AS29345	2a02:501::/32	32	1	<input type="button" value="edit"/> <input type="button" value="delete"/>
<input type="checkbox"/>	AS29345	91.240.246.0/23	23	1	<input type="button" value="edit"/> <input type="button" value="delete"/>
<input type="checkbox"/>	AS29345	85.254.193.0/24	24	1	<input type="button" value="edit"/> <input type="button" value="delete"/>
<input type="checkbox"/>	AS24620	85.254.224.0/22	22	1	<input type="button" value="edit"/> <input type="button" value="delete"/>
<input type="checkbox"/>	AS24620	85.254.216.0/21	21	1	<input type="button" value="edit"/> <input type="button" value="delete"/>
<input type="checkbox"/>	AS24620	85.254.214.0/23	23	1	<input type="button" value="edit"/> <input type="button" value="delete"/>

Izveidot Route Origin Authorization, rekomendācijas

- Veidot ROA tieši tādus, kā tiek lietoti (*anonsēti* BGP)
- Ja nepieciešams, var būt vairāki ROA vienam tīklam
- Izvairīties lietot maxLength atribūtu, ja vien tas nav nepieciešams
- Uzstādīt brīdinājumu saņemšanu, lai saņemtu brīdinājumu, kad kāds sāk anonstēt jūsu tīklu

RPKI validatori

- **NLnet Labs Routinator**

- <https://www.nlnetlabs.nl/projects/rpki/routinator/>
 - <https://github.com/NLnetLabs/routinator>

- **Dragon Research validator**

- <https://rpki.net>
 - <https://github.com/dragonresearch/rpki.net/>

- **RIPE NCC validator**

- <https://github.com/RIPE-NCC/rpki-validator-3/wiki>

- **LACNIC/NIC Mexico validator (FORT)**

- <https://github.com/NICMx/FORT-validator>

- **Cloudflare validator (OctoRPKI)**

- <https://github.com/cloudflare/cfrpki>

ROA validācija maršrutētājos

- Maršrutētājam jāatbalsta RPKI
- Maršrutētājos nenotiek kriptogrāfiska apstrāde, RPKI tabulas apstrāde nav resursu prasīga
- Maršrutētājs ielasa ROA tabulu un katram tīklam nosaka kādu no šiem stāvokļiem:
 - **Valid** – tīklam $x.x.x.x/y$ ROA izveidots un tīkls $x.x.x.x/y$ tiek anaunsēts ar tiešii tādu $/y$ un AS kāda ROA
 - **Invalid** – ROA izveidots un tīkls $x.x.x.x/y$ tiek anaunsēts no jebkādas citas AS vai citu tīkla izmēru
 - **Not-Found** – tīklam $x.x.x.x/24$ nav atrodams ROA

sho bgp rpki summary

Tue Oct 29 15:08:06.150 eet

RPKI cache-servers configured: 2

RPKI global knobs

Origin-AS validation is ENABLED globally

Origin-AS validity WILL affect bestpath selection globally

Origin-AS 'invalid' routes CAN be bestpaths

Origin-AS validity signaling towards iBGP is DISABLED globally

RPKI database

Total IPv4 net/path: 90069/195102

Total IPv6 net/path: 151¹ /328⁴



sho bgp rpk table

Tue Oct 29 15:08:48.707 eet

Network	Maxlen	Origin-AS	Server
1.0.0.0/24	24		.16 ⁸ .11 ³ .11
1.0.0.0/24	24		.16 ⁸ .11 ³ .9
1.1.1.0/24	24		.16 ⁸ .11 ³ .11
1.1.1.0/24	24		.16 ⁸ .11 ³ .9
1.9.0.0/16	24		.16 ⁸ .11 ³ .11
1.9.0.0/16	24		.16 ⁸ .11 ³ .9
1.9.12.0/24	24		.16 ⁸ .11 ³ .11
1.9.12.0/24	24		.16 ⁸ .11 ³ .9
1.9.21.0/24	24		.16 ⁸ .11 ³ .11
1.9.21.0/24	24		.16 ⁸ .11 ³ .9
1.9.23.0/24	24		.16 ⁸ .11 ³ .11
1.9.23.0/24	24		.16 ⁸ .11 ³ .9
1.9.31.0/24	24		.16 ⁸ .11 ³ .11
1.9.31.0/24	24		.16 ⁸ .11 ³ .9
1.9.65.0/24	24		.16 ⁸ .11 ³ .11
1.9.65.0/24	24		.16 ⁸ .11 ³ .9



sho bgp origin-as validity

Tue Oct 29 15:09:48.803 eet

BGP router identifier 85.254.255.240, local AS number 5538

BGP generic scan interval 60 secs

Non-stop routing is enabled

BGP table state: Active

Table ID: 0xe0000000 RD version: 924261908

BGP main routing table version 924261908

BGP NSR Initial initsync version 671856 (Reached)

BGP NSR/ISSU Sync-Group versions 0/0

BGP scan interval 60 secs

Status codes: s suppressed, d damped, h history, * valid, > best

i - internal, r RIB-failure, S stale, N Nexthop-discard

Origin codes: i - IGP, e - EGP, ? - incomplete

Origin-AS validation codes: V valid, I invalid, N not-found, D disabled

Network	Next Hop	Metric	LocPrf	Weight	Path	
V*> 1.0.0.0/24	149.14.74.73	1010	245	0 174	13335 i	
V*	195.244.145.64	102	0 8194	1299	13335 i	
N* 1.0.4.0/22	.14.74.73	177150	150			i
	5 4 5					
N*	19 .24 .14 .64	115	0 8			?
	5 6 7					
N*	19 .24 .22 .49	10	151			i
	5 6 7					
N*>	19 .24 .22 .49	0	151			i
	5 6 7					
N*	19 .24 .22 .49	10	151			?
N* 1.0.4.0/24	.14.74.73	177150	150			i
	5 4 5					
N*	19 .24 .14 .64	115	0 8			?
	5 6 7					
N*	19 .24 .22 .49	10	151			i
	5 6 7					
N*>	19 .24 .22 .49	0	151			i
	5 6 7					
N*	19 .24 .22 .49	10	151			?
N* 1.0.5.0/24	.14.74.73	177150	150			i
	5 4 5					
N*	19 .24 .14 .64	115	0 8			?
	5 6 7					
N*	19 .24 .22 .49	10	151			i
	5 6 7					
N*	19 .24 .22 .49	0	151			i
	5 6 7					

Route Origin validation apstrāde maršrutētājos

- Visdrīzāk maršurtētājos *Valid* routes būs labākas par *Not-Found* pirms *LocalPref* u.c. BGP atribūtu pārbaudes.
- Operators var veikt maršruta izvēli balstoties uz RPKI rezultātu:
 - *Invalid* – uzstādīt viszemāko *local preference* /izmest *prefix*
 - *NotFound* – uzstādīt zemāku *local preference*
 - *Valid* – uzstādīt augstāku *local preference*

```
route-policy UPSTREAM-IN
  if destination in BOGONS-RFC1918 then
    drop
  else
    if validation-state is valid then
      set local-preference 245
    else
      if validation-state is invalid then
        set local-preference 14
      else
        if validation-state is not-found then
          set local-preference 150
        else
          set local-preference 104
        endif
      endif
    endif
  endif
end-policy
```

RPKI Unreachable IPv4 Networks ▲

- by ASN
- by Country
- by RIR
- by ROA
- all Prefixes

RPKI Unreachable IPv6 Networks ▲

- by ASN
- by Country
- by RIR
- by ROA
- all Prefixes

Unreachable networks per country (IPv4)

Data as of 2019-10-21 11:30:00 UTC

Show entries

Search:

# ▲	Country ⚡	affected ASNs ⚡	affected prefixes ⚡	unreachable /24s ⚡
0	CN	7	22	457
1	IN	31	182	443
2	FR	3	10	388
3	CL	4	18	367
4	HK	16	59	326
5	US	38	83	161
6	TW	3	5	129
7	TR	14	74	77
8	AR	23	60	68
9	IR	17	40	62

Showing 1 to 10 of 55 entries

Previous 2 3 4 5 6 Next

This is an **early prototype** of the RPKI Sentry software. We publish the it as it is, along with the current data and results without any guarantees of data quality, accuracy or completeness. Our intention is to speed up development, debugging and allow community to participate and provide early feedback. You may use the software, data, results or any other artifacts solely at your own risk.

Search recorded conflicts in Conflict history between RPKI ROAs and announced routes in DFZ [Default Free Zone] BGP table in time period from **2018-08-28 16:00:00** to **2019-10-30 00:00:00**.

Enter ASN to search all conflicts caused by that AS. Enter prefix to search all conflicts concerning that prefix. For exact match enter both criteria.

ASN	1234 (default *)
CIDR	1.1.1.1/32 (default *)
Country	LV
Exclude	Ignore a country...



CURRENTLY FOUND

« **1** [2](#) [3](#) [4](#) [5](#) ... [12](#) [13](#) »

CIDR	ASN	Error root cause	Start	End	Country
2a02:503:1::/48	51955	prefix length	2019-07-22 16:00:00	2019-07-23 08:00:00	LV
195.26.20.0/23	31519	origin	2019-09-05 16:00:00	2019-09-13 00:00:00	LV
195.26.20.0/23	31519	origin	2019-07-30 16:00:00	2019-07-31 00:00:00	LV
195.26.20.0/23	31519	origin	2019-07-29 16:00:00	2019-07-30 08:00:00	LV
85.254.58.0/24	2588	prefix length	2019-07-16 08:00:00	2019-07-18 16:00:00	LV
91.198.156.0/24	51955	origin	2019-07-02 08:00:00	2019-07-03 16:00:00	LV
85.254.183.0/24	48798	prefix length	2019-06-05 16:00:00	2019-06-06 08:00:00	LV
85.254.101.0/24	13194	prefix length	2019-06-03 16:00:00	2019-06-04 16:00:00	LV
85.254.100.0/24	13194	prefix length	2019-06-03 16:00:00	2019-06-04 16:00:00	LV
62.63.160.0/19	5518	prefix length	2019-05-31 08:00:00	2019-05-31 16:00:00	LV

To Do

- 1. RIPE NCC LIR portāla saskarnē publicēt/aktualizēt ROA, uzstādīt brīdinājumu izsūtīšanu.***
- 2. Uzstādīt RPKI validācijas cache serverus***
- 3. Veikt konfigurāciju maršrutētājos – sāukumā priotarizēt, vēlāk izmest “invalid”.***



ROA

Jau implementēts:

- AT&T rejects invalids on peering sessions
- KPN / AS 286 rejects invalids on customer sessions
- Nordunet rejects invalids on all EBGP sessions
- Seacomm & Workonline
- INEX, AMS-IX, DE-CIX, France-IX, Netnod, MSK-IX
- XS4ALL, Redhosting, BIT, Atom86, Fusix, True, Amsio...
- TELIA CARRIER
- Cloudfare

Noderīgas saites

- **Rīki un resursi (maršrutētāju konfigurācijas paraugi, validatori):**
 - <https://www.ripe.net/manage-ips-and-asns/resource-management/certification/tools-and-resources>
- **Soli pa solim:**
 - http://www.bgp4all.com.au/pfs/_media/workshops/02-rpki.pdf
 - <https://rpki.readthedocs.io/en/latest/rpki/bgp-routing.html>
- **Monitorings:**
 - <https://rpki-sentry.csirt.cz/search?asn=&cidr=&cc=lv>
 - https://nusenu.github.io/RPKI-Observatory/unreachable_countries-v4.html
- **Apraksts, ko ņemt vērā veidojot ROA:**
 - <https://datatracker.ietf.org/doc/draft-ietf-sidrops-rpkimaxlen/>



Paldies!

cert@cert.lv

<https://www.cert.lv>



certlv



certlv