# Secure the future

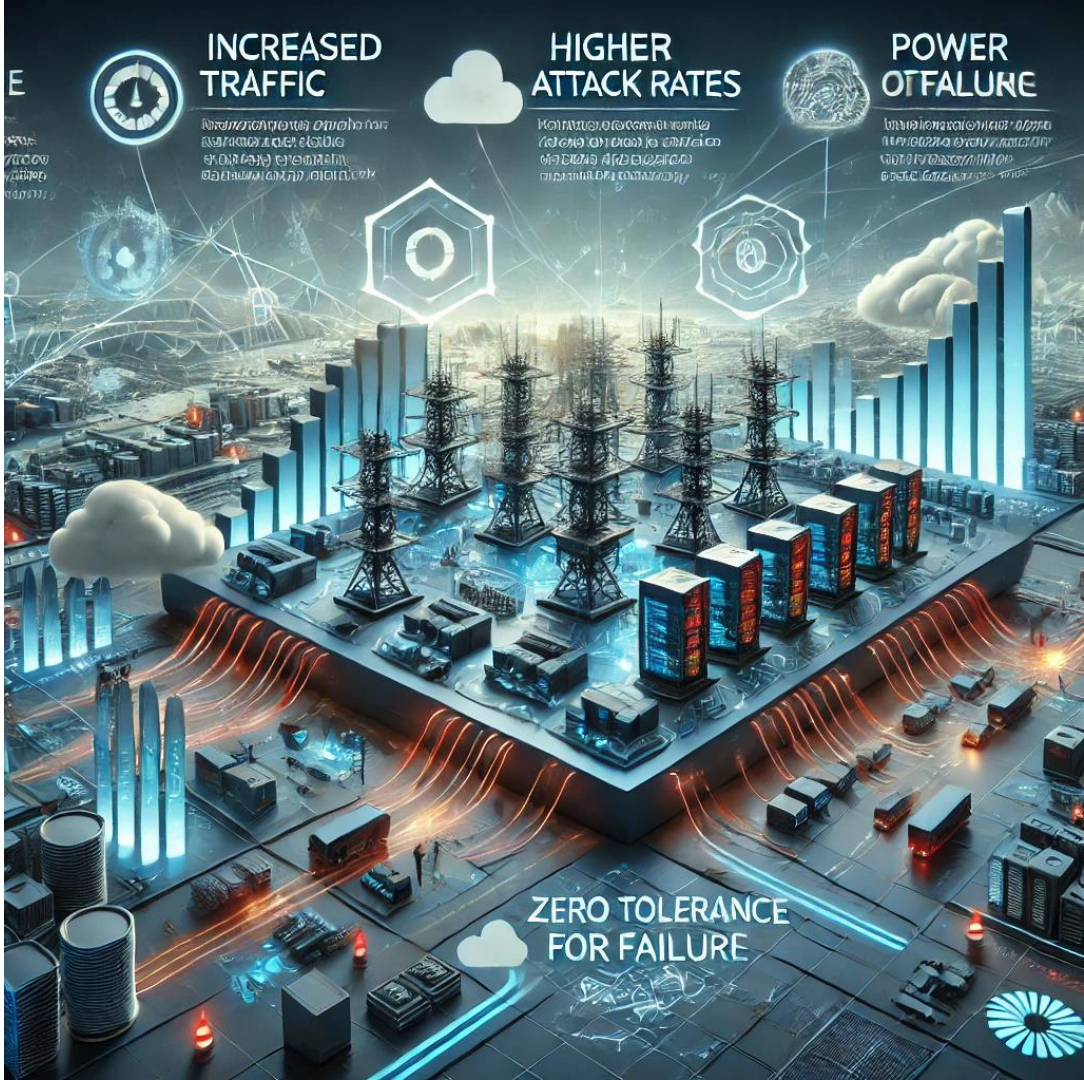
Dominique Schaeffer
Director IP Consulting Engineering EMEA

European Peering Forum
Vienna, 16-18 September 2024

# Peering landscape
## Introduction

- More and more traffic
- More and more attacks
- Zero tolerance for failure
- Less power consumption per Gb

**Choosing the right peering router is key**




Disclaimer : Illustration pictures of this presentation have been generated with DALL-E 3

# BGP implementation

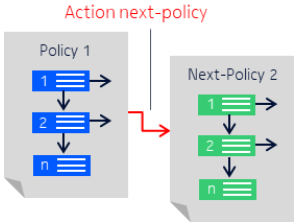
## Robust and feature-rich

### Best in class implementation includes :

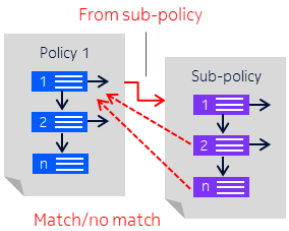
- Scale
- Path visibility and reconvergence
- Robustness
- Error handling (RFC7606)
- Rib-out processing
- High availability
- Rapid BGP convergence leveraging multi-processing architecture

# Route policy framework

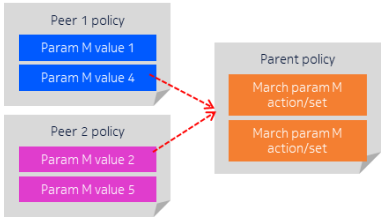
## Flexible and scalable route policy language




Nested policies

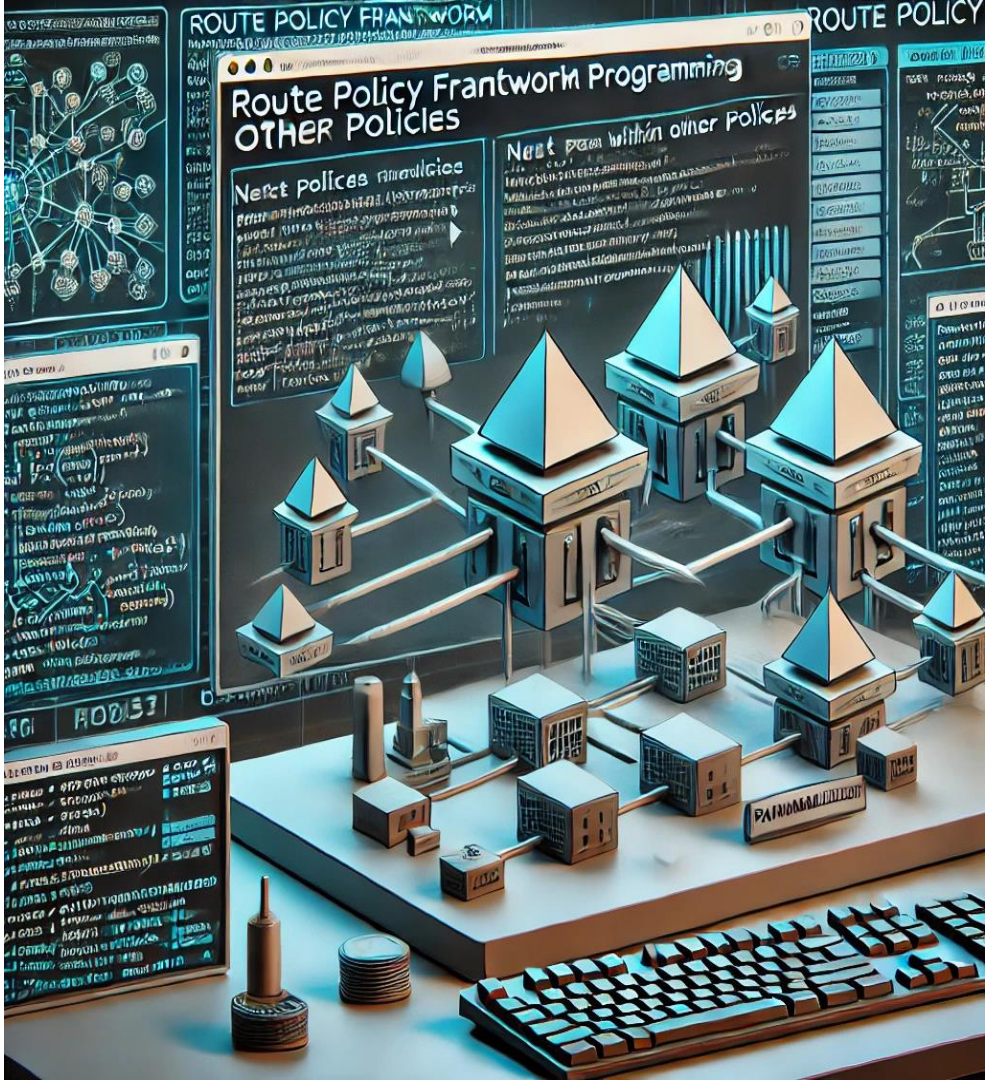



Scaling with sub-routines



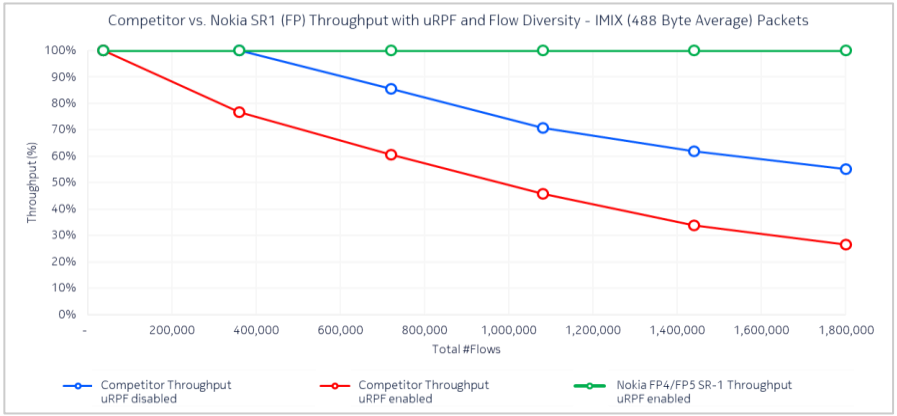

Simplification with parameterization

Possibility to allow for test evaluation of policy before applying



# Determinist performance

## Performant silicon and memory architecture




- High number of flows result in performance degradation due to cache miss
- Enabling uRPF (loose mode) results in a further ~25% decline in throughput for IMIX traffic
- Fully buffered architecture for determinist performance

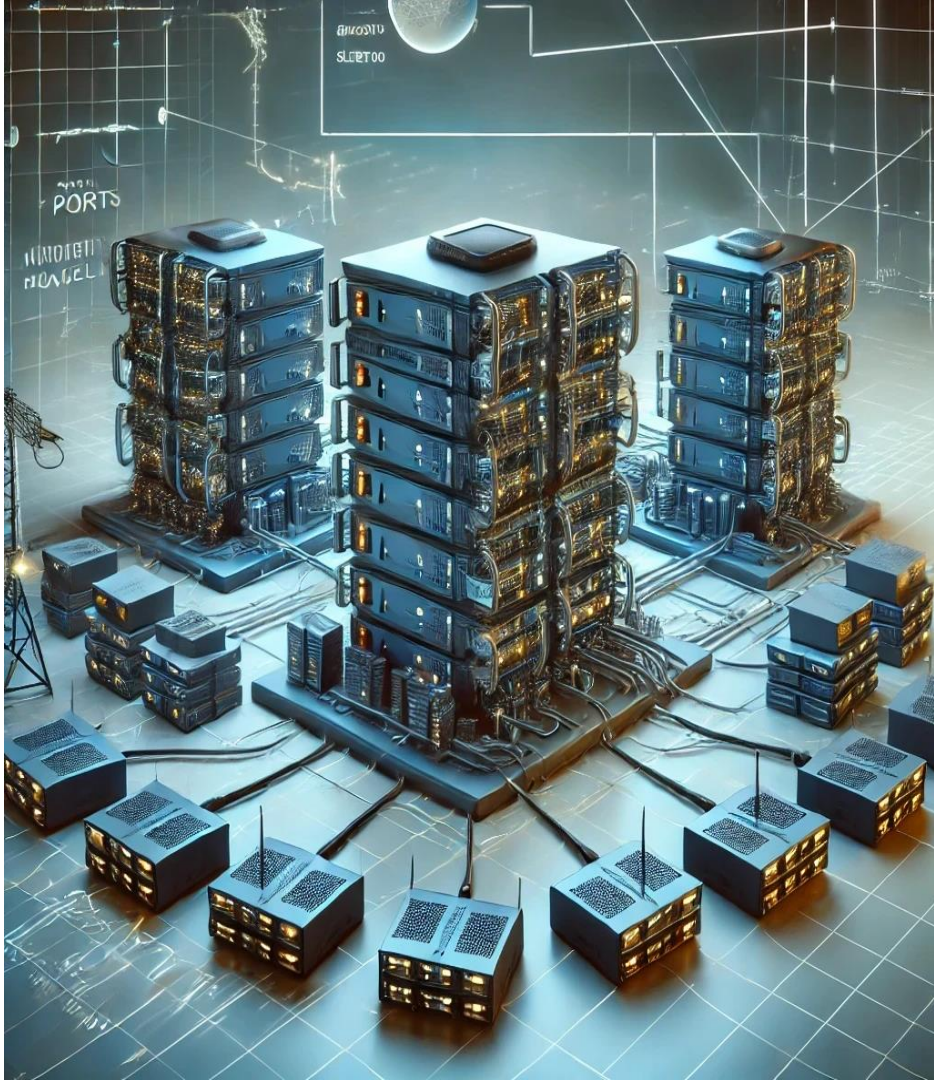
# High slot capacity with low speeds ports fanout

## Cost optimized architecture

Consider 800Gb/s ports for backbone links with breakout possibility allowing power optimization and investment protection

Consider using satellite for client links

- Cost effective solution
- Only host is configured
- Satellite is seen as port extender
- Can be local or remote



# Full security implementation

## Robust and feature-rich

### Best in class implementation includes :

- Secure Boot
- CPU protection with hardware queues
- Protocol encryption
- RPKI implementation
- RTBH, GTSM
- Flowspec
- Unparalleled ACL scale

# The DDoS problem is shifting

## New detection approach needed

| 2000 – 2020 | 2020 – 2024 | 2024+ |
|---|---|---|
| **Spoofed** | **Botnet** | **AI** |

**More volume / more automation**

- Botnet and proxy-based attacks increasing
  - 1M active IoT bot devices, >10M residential proxies
  - >100 Tb/s aggregate capacity
- Cost of attacking is very low
- Increasing level of automation
  - Attack variability (bursts, carpet bombs, …)
  - Realistic HTTP/DNS/VoIP requests

# Best in class DDoS detection engine

## AI-powered detection without complex threshold configuration & maintenance

Cloud infra

**Collect all DDoS**

Samples from honeypots, customers, GDTA intelligence sharing, public forums, CVE repos

**Crawl every IP**

Crawl entire IPv4 & active IPv6 Internet discovering IoT types, proxy services, compromised servers, vulnerable applications with CVE

**Supervised learning and model training**

On-prem

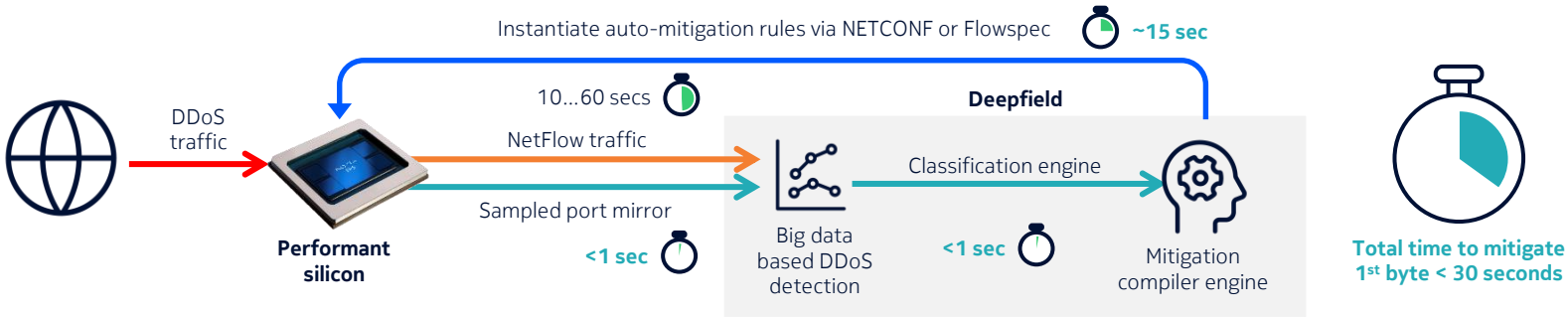
**AI-powered ultra-fast DDoS detection**

Eliminating need for configuration

Minimizing false positives

# Using silicon ACL power to protect against DDoS

## Combined forces for cost-effective DDoS protection




### AI-powered intelligence

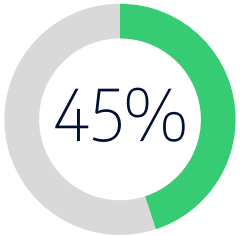
- Zero-touch big-data based DDoS detection
- Real-time compilation of optimal filter list

### Performant silicon

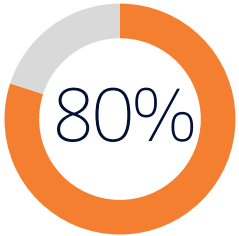
- Large-scale ACLs to block large/complex DDoS attacks
- Line-rate filtering with no performance impact
- Fast filter-population for fastest possible mitigation

# Network analytics for peering and CDN optimization

## Reduce transit costs while improving customer experience




Internet Peering traffic sourced indirectly from paid transit*



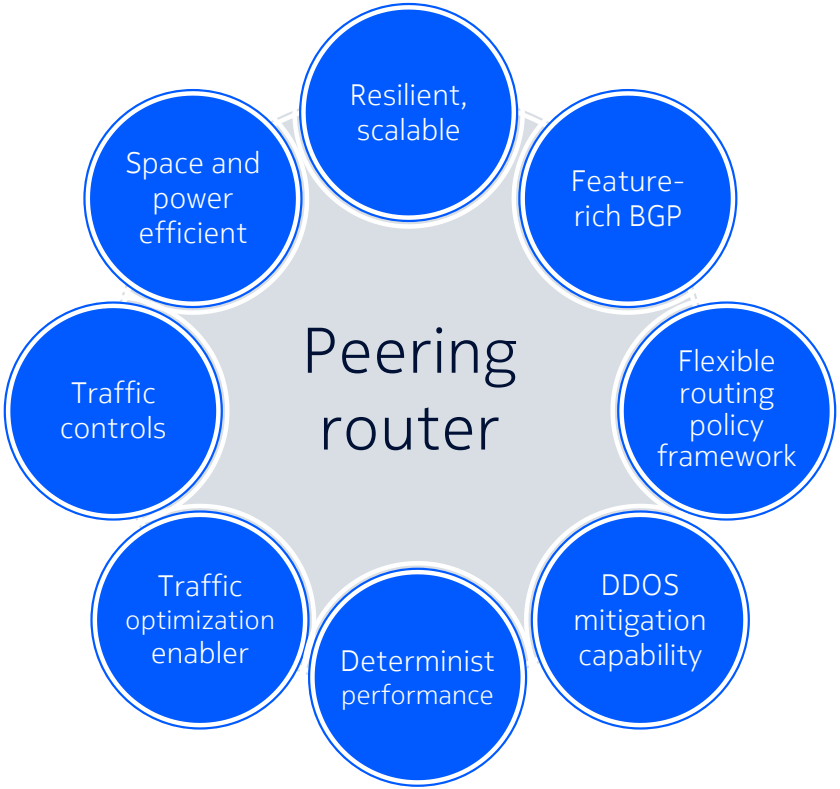

ISP traffic sourced from CDNs and internal caches*


*Data from several European ISPs

# Best in class peering router

## Summary and takeaways

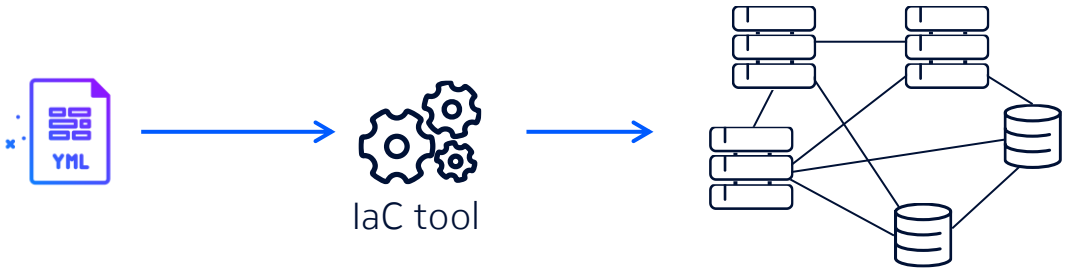
- Resilient, scalable, and feature-rich BGP process
- Flexible routing policy framework for frequent route policy updates
- Secure routing and DDoS mitigation on network entry
- Guaranteed performance for high number of flows and filters
- Traffic optimization enablers for moving prefixes across peering links
- Application traffic controls for peak load management
- Space and power efficient



# Testing peering configuration with Containerlab

## Bringing declarativeness to networking labs

IT




Discord server

Network Labs

```
name: mylab

topology:
  nodes:
    [ ] : [ ]
    [ ] : [ ]

  links:
    - [ ] : [ ]
```

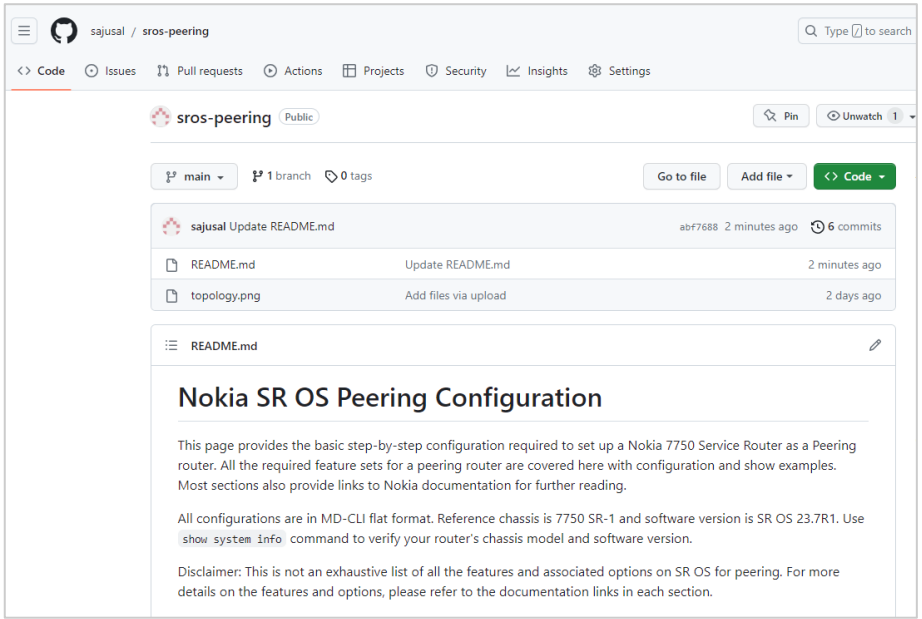

https://containerlab.dev




NOKIA

# Peering reference configuration

https://github.com/sajusal/sros-peering




## Route Policies

Routing policies control the size and content of the routing tables, the routes that are advertised, and the best route to take to reach a destination.

For more details on route policy configuration and options, visit SR OS Route Policies Documentation.

In these examples, we are creating AS path lists, community and prefix lists.

```
/configure policy-options as-path "PEERING" { expression "64503" }
/configure policy-options as-path-group "BOGON" { entry 10 expression ".* 0 .*" }
/configure policy-options as-path-group "BOGON" { entry 20 expression ".* [64496-64511] .*" }
/configure policy-options as-path-group "BOGON" { entry 30 expression ".* 65535 .*" }

/configure policy-options community "LARGE-PEER" { member "65100:100" }
/configure policy-options community "SMALL-PEERS" { member "65200:200" }
/configure policy-options community "SMALL-PEERS" { member "65400:.*$" }
/configure policy-options community "SMALL-PEERS" { member "65500:.*" }
```

## RPKI

SR OS supports RPKI for BGP prefix origin validation.

In this example, we are configuring a RPKI session with an external server and then enabling prefix origin validation under the BGP group. We are also configuring BGP to not use any routes whose origin is invalid.

For more details on RPKI implementation, visit SR OS RPKI Documentation.

```
/configure router "Base" origin-validation rpki-session 172.31.1.2 { admin-state enable }
/configure router "Base" origin-validation rpki-session 172.31.1.2 { local-address 10.10.1.4 }
/configure router "Base" origin-validation rpki-session 172.31.1.2 { port 8282 }
/configure router "Base" bgp group "eBGP-Peering" { origin-validation ipv4 true }
/configure router "Base" bgp group "eBGP-Peering" { origin-validation ipv6 true }
/configure router "Base" bgp best-path-selection { origin-invalid-unusable true }
```


NOKIA

# Copyright and confidentiality