Freie Universität Berlin

# BGPsec: Get ready for the next step in secure inter-domain routing

**Matthias Wählisch**

**m.waehlisch@fu-berlin.de**

**www.cs.fu-berlin.de/~waehl**

# Does RPKI Origin Validation solve all BGP security problems?

Freie Universität Berlin

# Does RPKI Origin Validation solve all BGP security problems?

NO!

# Motivation: Threat models for BGP

**Prefix Origin Hijacking**

**AS Path Manipulation**

**Route Leaks**

Freie Universität Berlin

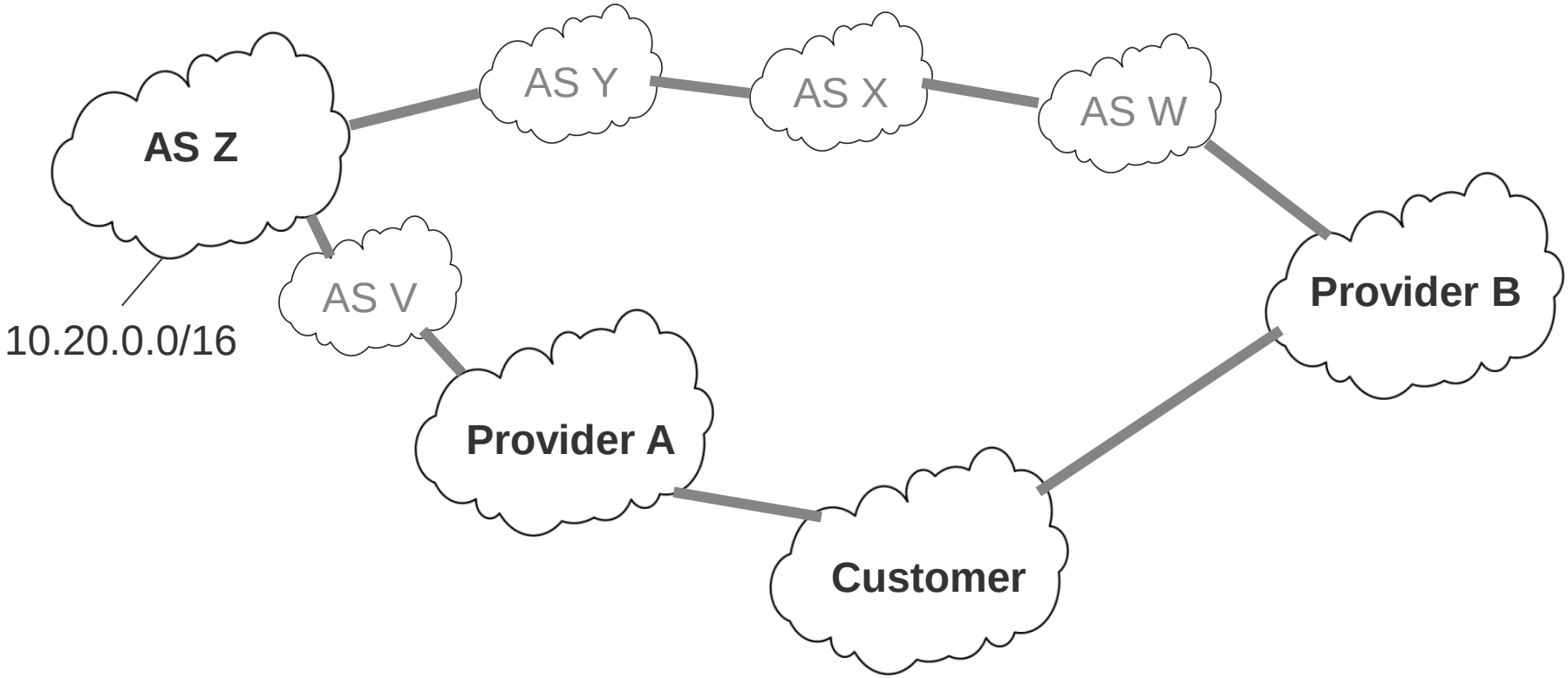
# Motivation: Threat models for BGP

**Prefix Origin Hijacking**

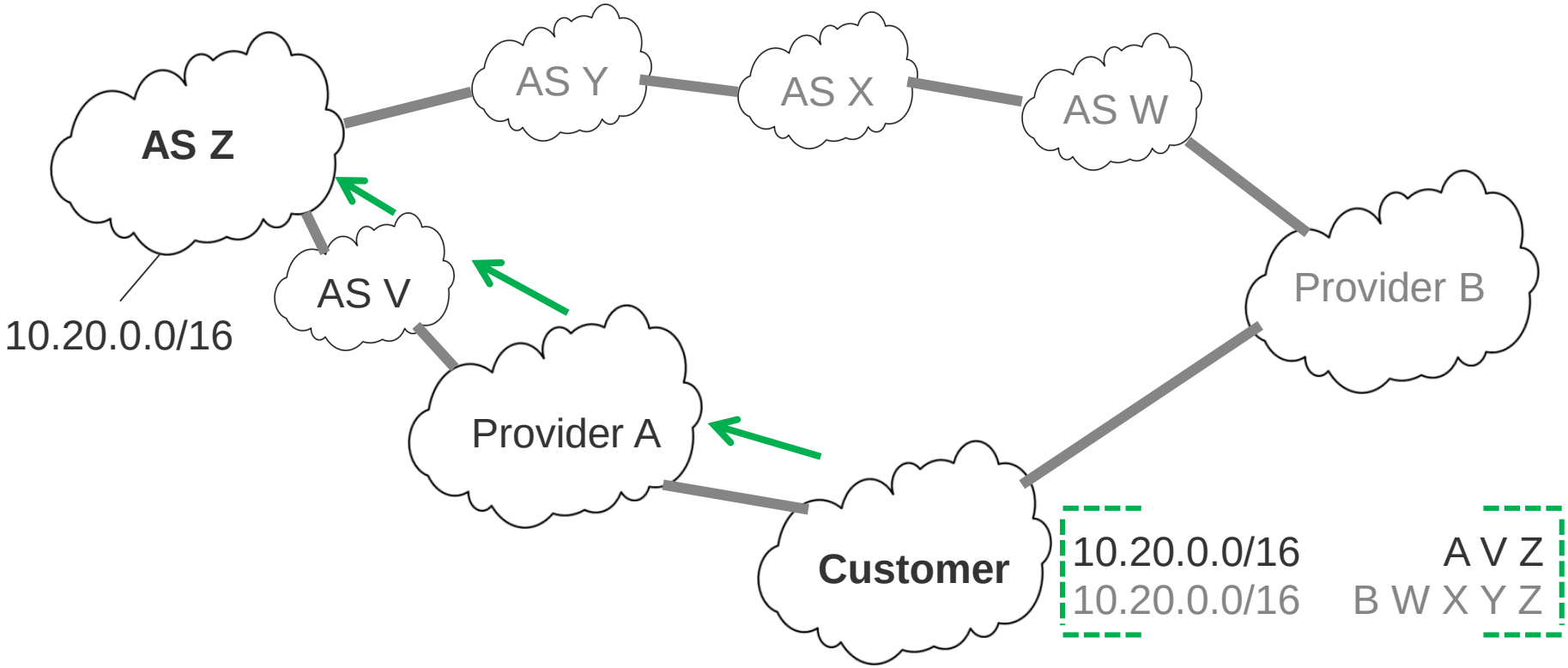
**AS Path Manipulation**

**Route Leaks**

# Simple example



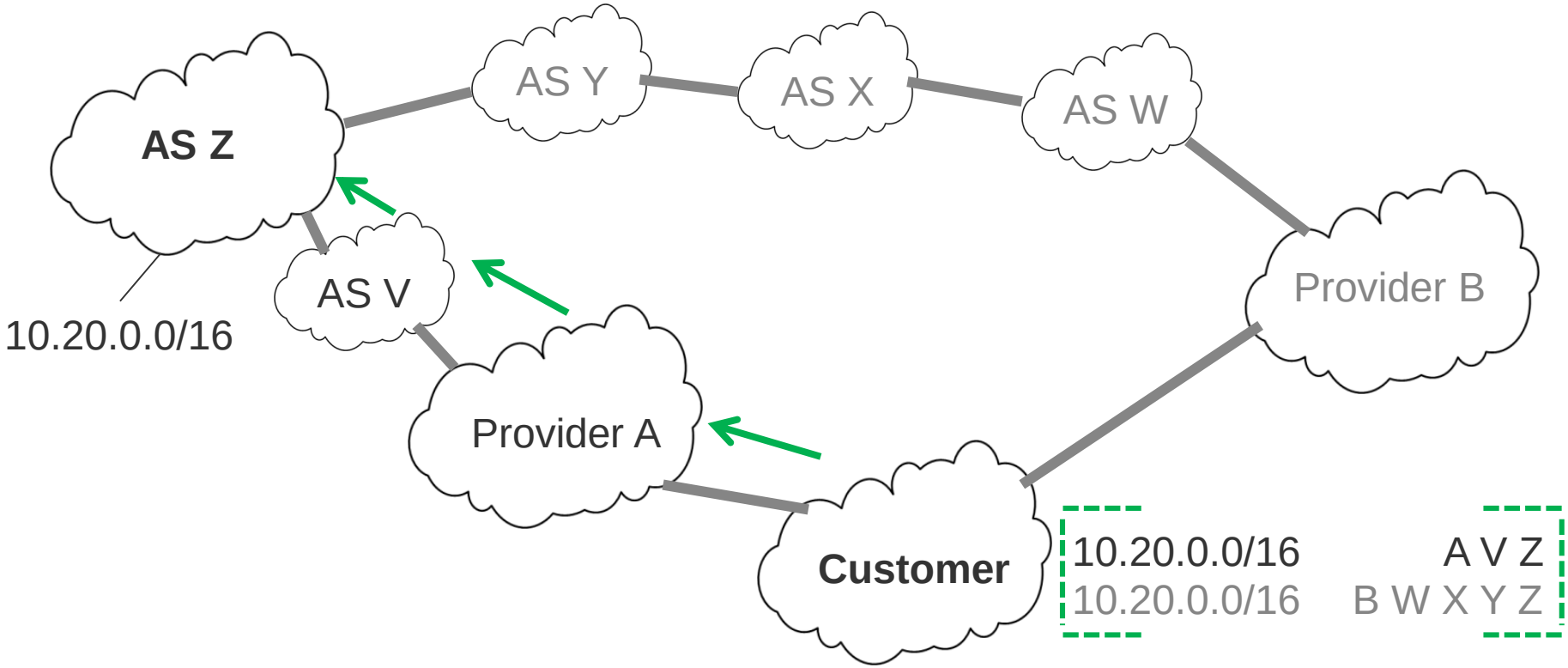
# Simple example: Shorter path wins



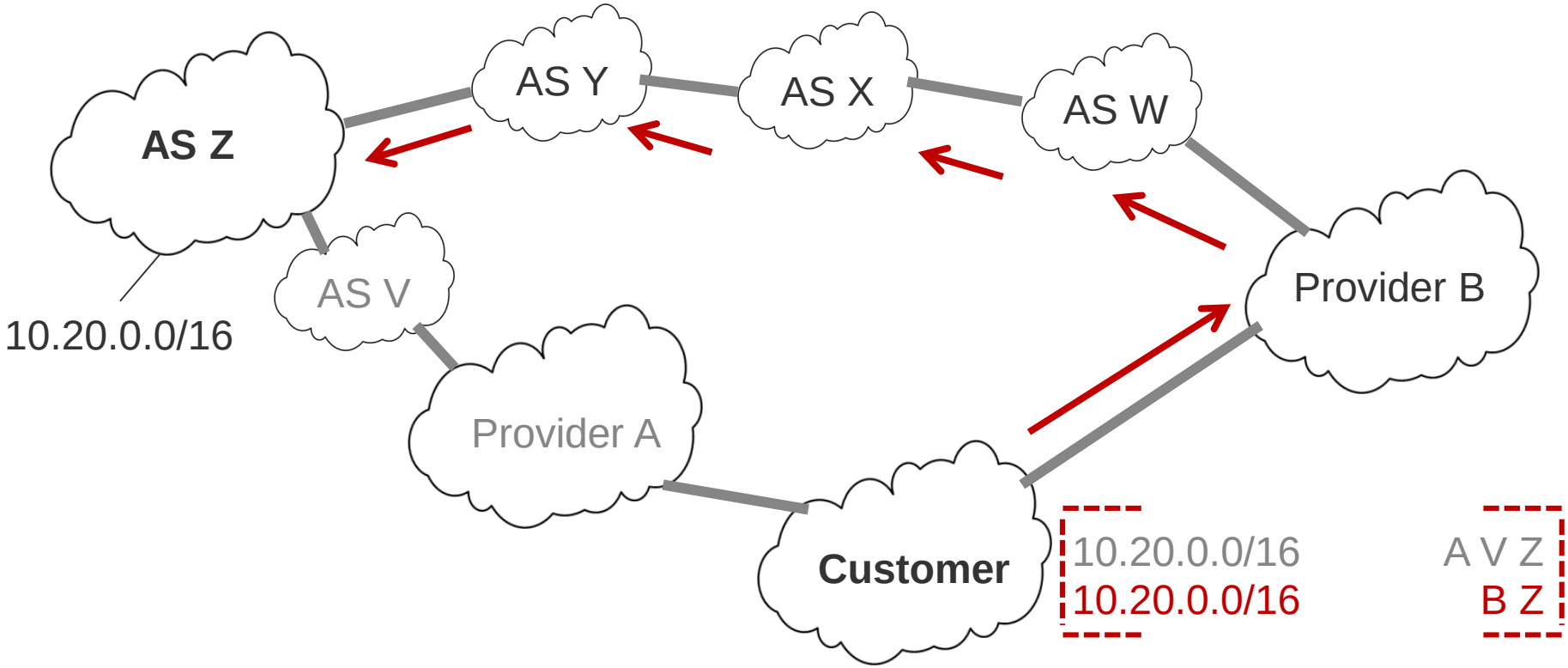
# Shorter path wins, AS B configures:

```
if net = 10.20.0.0/16 then {
            bgp_path.empty;
            bgp_path.prepend(B);
            bgp_path.prepend(Z);
            accept;
}
```

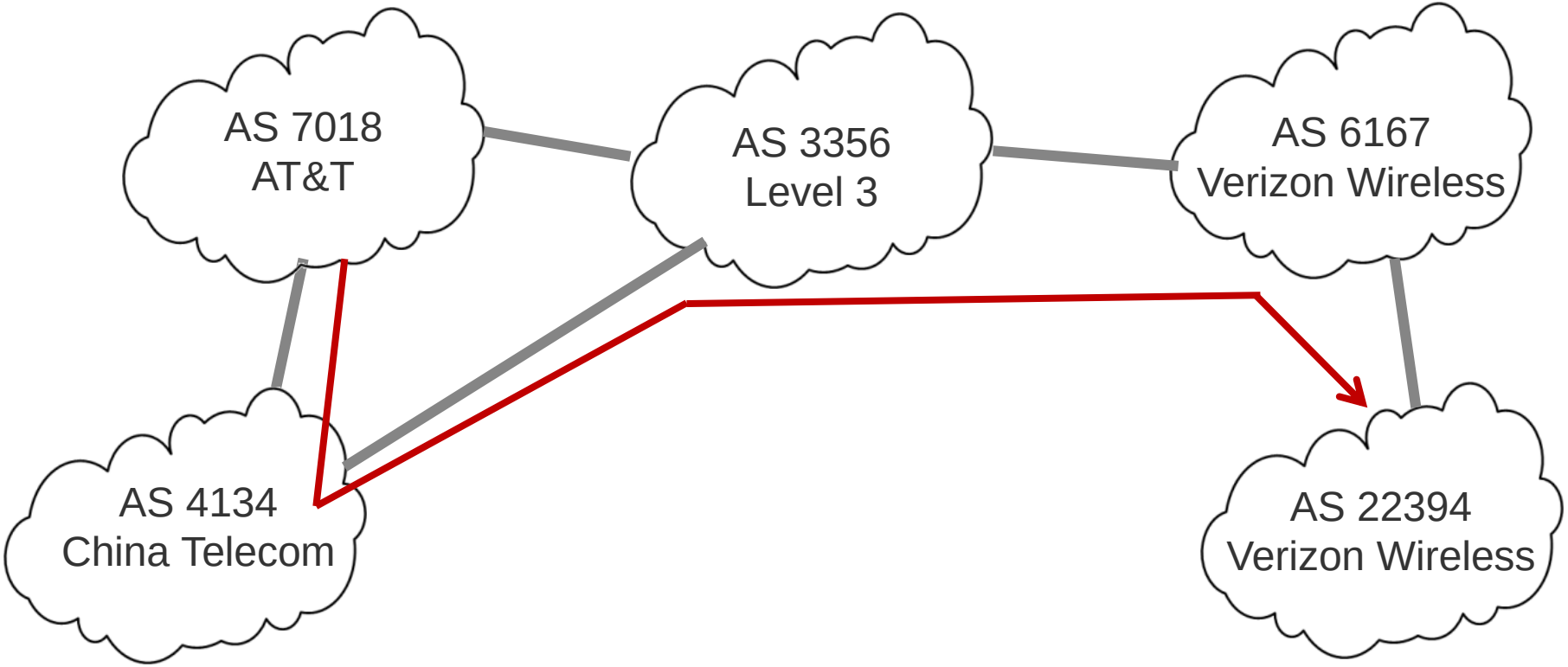
# Simple example: Shorter path wins



# Simple example: Shorter path wins



# Real-world example, 2010



# Recap: Why do we need the AS Path?

Loop detection

Breaking Ties (Phase 2) [RFC 4271]

"(a) **Remove** from consideration **all routes** that are **not** tied for **having the smallest number of AS numbers** present **in their AS_PATH** attributes. [...]"

# Objective of BGPsec:
# Prevent path manipulation

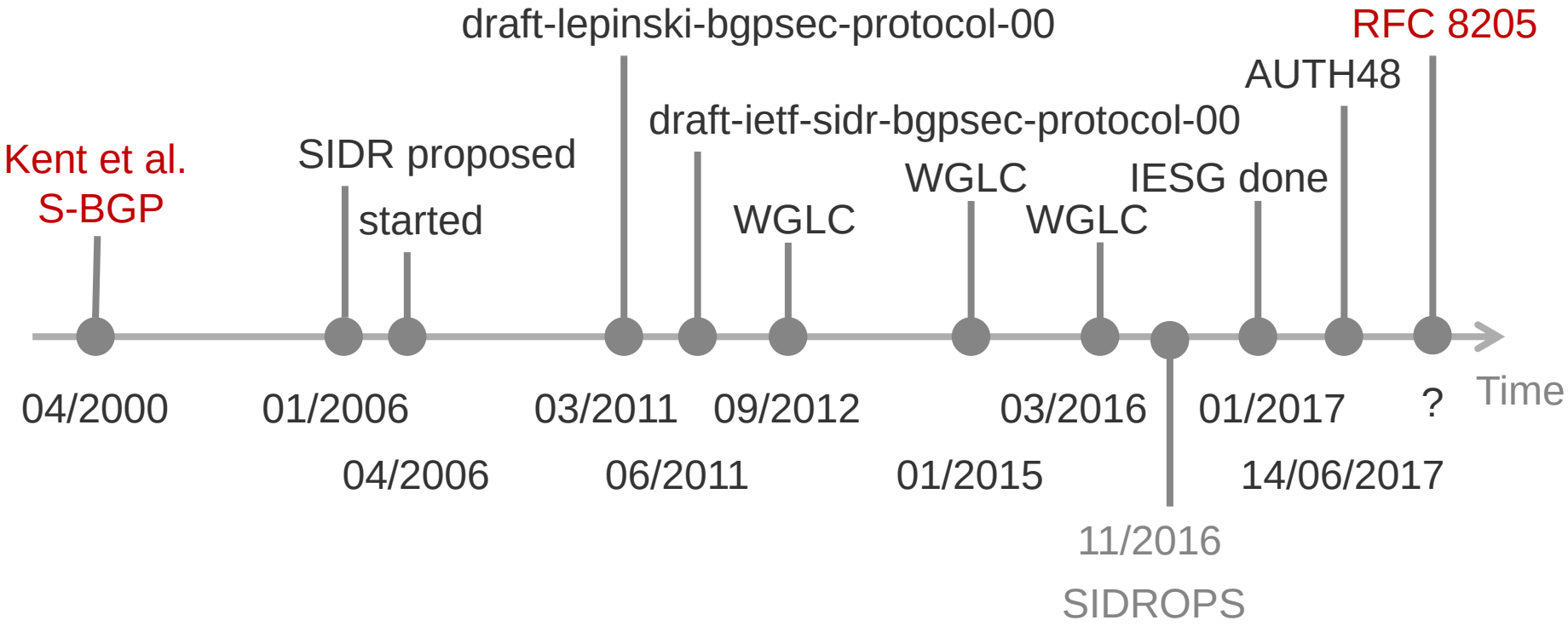
Freie Universität Berlin

# Objective of BGPsec:
# Prevent path manipulation

Freie Universität Berlin

"Provide confidence that **every AS on the path of ASes** listed in the update message has **explicitly authorized** the **advertisement of the route.**" [draft-ietf-sidr-bgpsec-protocol]

# A brief history of BGPsec



Freie Universität Berlin

# BGPsec primer

Basic idea, per prefix and BGP update,
every BGPsec router creates `BGPsec_Path`, including signatures

- list of previous ASNs (~ AS path)
- signatures from previous ASNs
- next ASN [forward signing]

Every BGPsec router verifies received `BGPsec_Path`

# BGPsec primer

Basic idea, per prefix and BGP update,
every BGPsec router creates `BGPsec_Path`, including signatures

- list of previous ASNs (~ AS path)
- signatures from previous ASNs
- next ASN [forward signing]

Every BGPsec router verifies received `BGPsec_Path`

I received prefix P via AS … and send it to AS Y **signed**


I received prefix P from AS X and via AS … **verified**

# We need router certificates

Signing BGPsec router needs a public private key pair

operator vs. router generated keys

Validating BGPsec router needs the (verified) public keys of all other BGPsec routers (on the path)

verified locally or at cache servers

# Some operational considerations

BGPsec validation performed at edge

Yes, your router needs more memory

Yes, your router needs better CPU or crypto support

# Some operational considerations

**Talk with your vendor**

**Ask for implementations**

**Can be ready in the next ~5 years**

BGPsec validation performed at edge

Yes, your router needs more memory

Yes, your router needs better CPU or crypto support

# Implications for IXP Route Server

Route server is transparent

A client router needs to validate paths which are forward signed

?

# Implications for IXP Route Server

Route server is transparent

A client router needs to validate paths which are forward signed

Route server AS is inserted and signs AS path but doesn't increase path length (attribute `pCount=0`)

# State of BGPsec support

Cache servers

RPKI.net (https://github.com/dragonresearch/rpki.net)

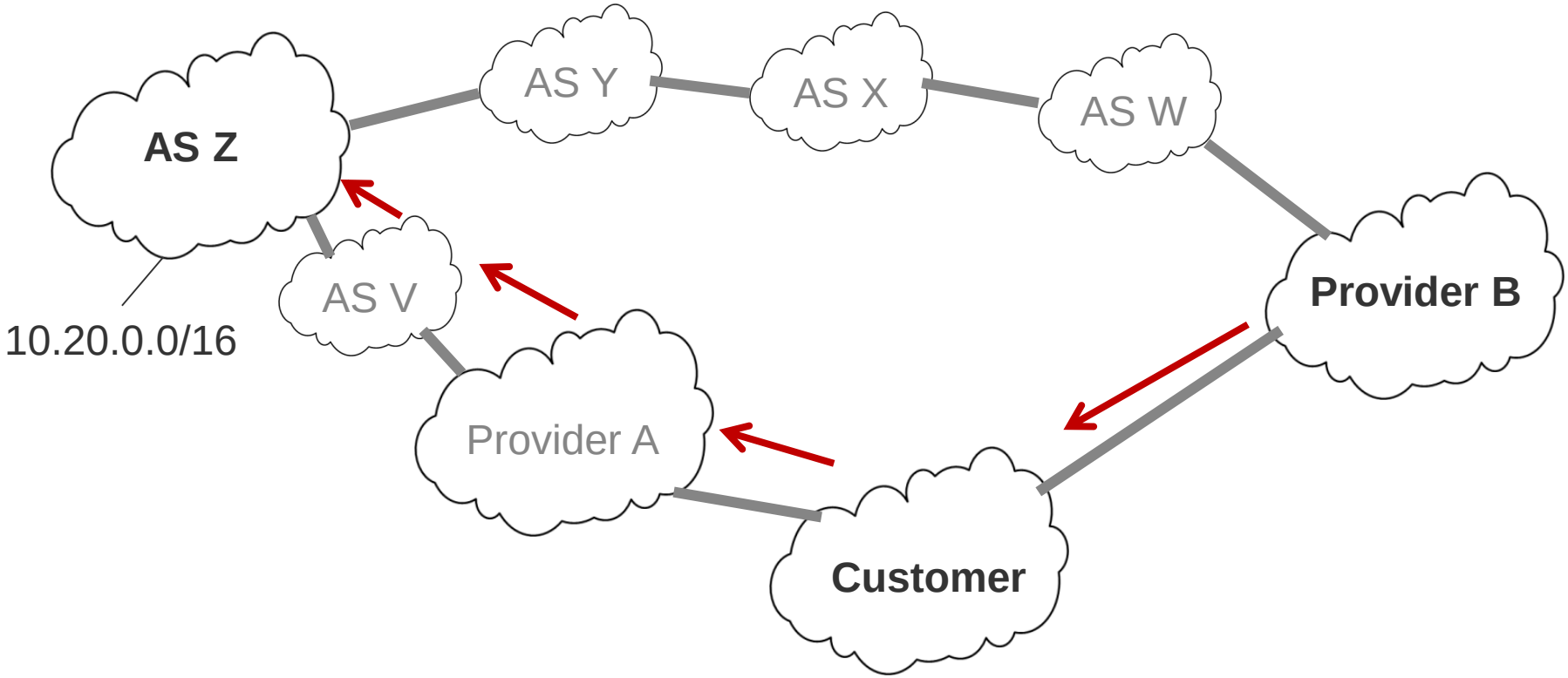
RTR clients

RTRlib (http://rtrlib.realmv6.org)

BGP daemons

Bird extension (http://www.securerouting.net/tools/bird/)
QuaggaSRx (https://www-x.antd.nist.gov/bgpsrx/)

# Caveat: BGPsec does not protect against route leaks



# Does BGPsec solve all BGP security problems?

Does BGPsec solve
all BGP security problems?

NO!

Does BGPsec solve
all BGP security problems?

NO!

But it's one next step towards a more secure Internet backbone.