Protecting BGP with TCP-AO

Kateřina Kubecová • Nov 21th, 2025

CZ DOMAIN REGISTRY

Why to protect BGP connections

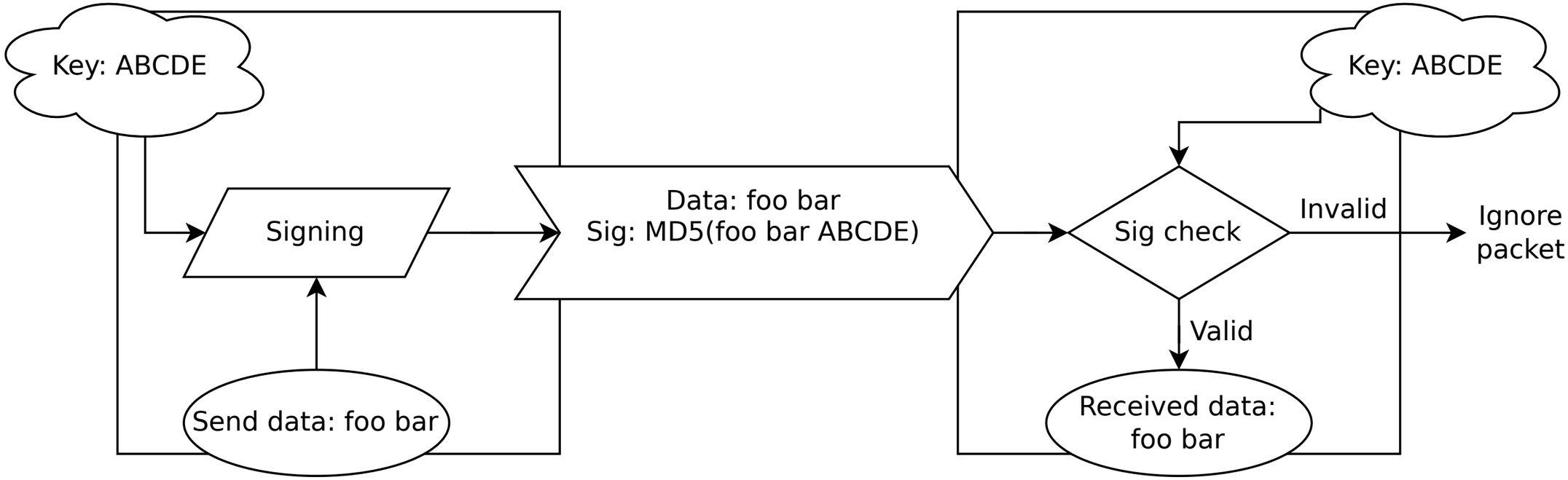
- connection content is not private, but we need to protect it from:
  - disrupting connections by RST packets
  - session replay attacks
  - packet injection

How to protect BGP connections

- TLS is an overkill
- old good MD5 signatures (RFC 2385, obsolete)
- newer TCP Authentication Option (RFC 5925)

How TCP-MD5 works

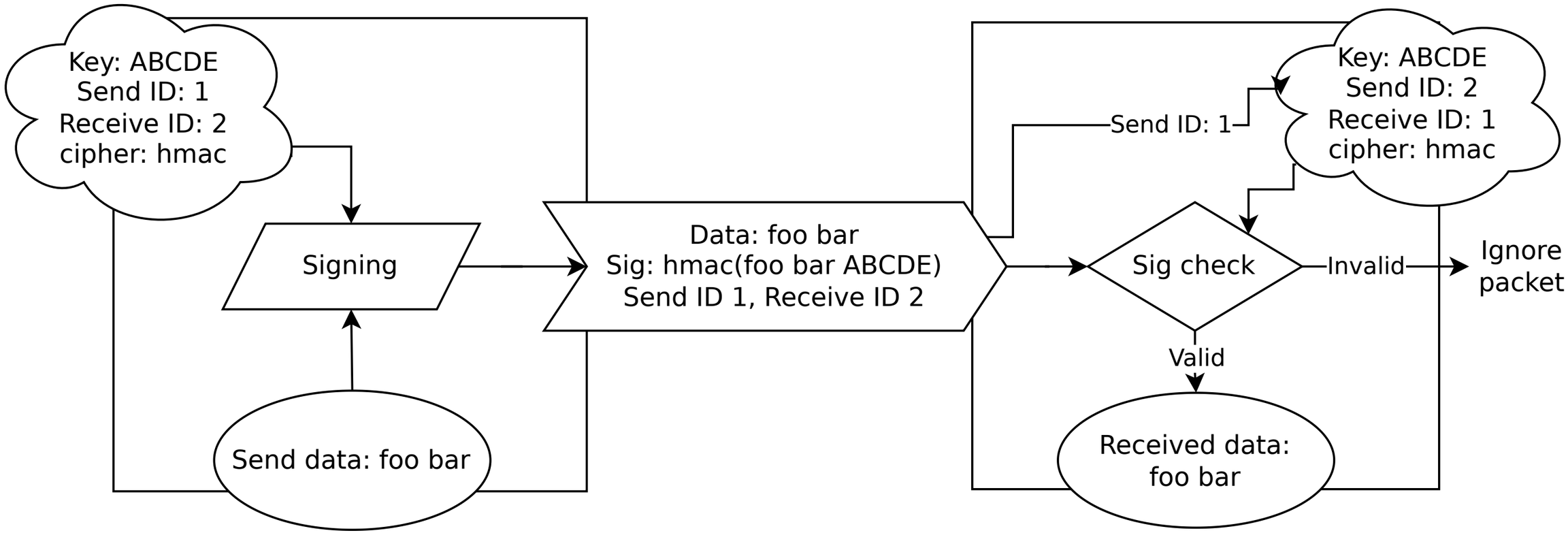
- both sides share a password
- MD5 algorithm is used to create a digest (hash)



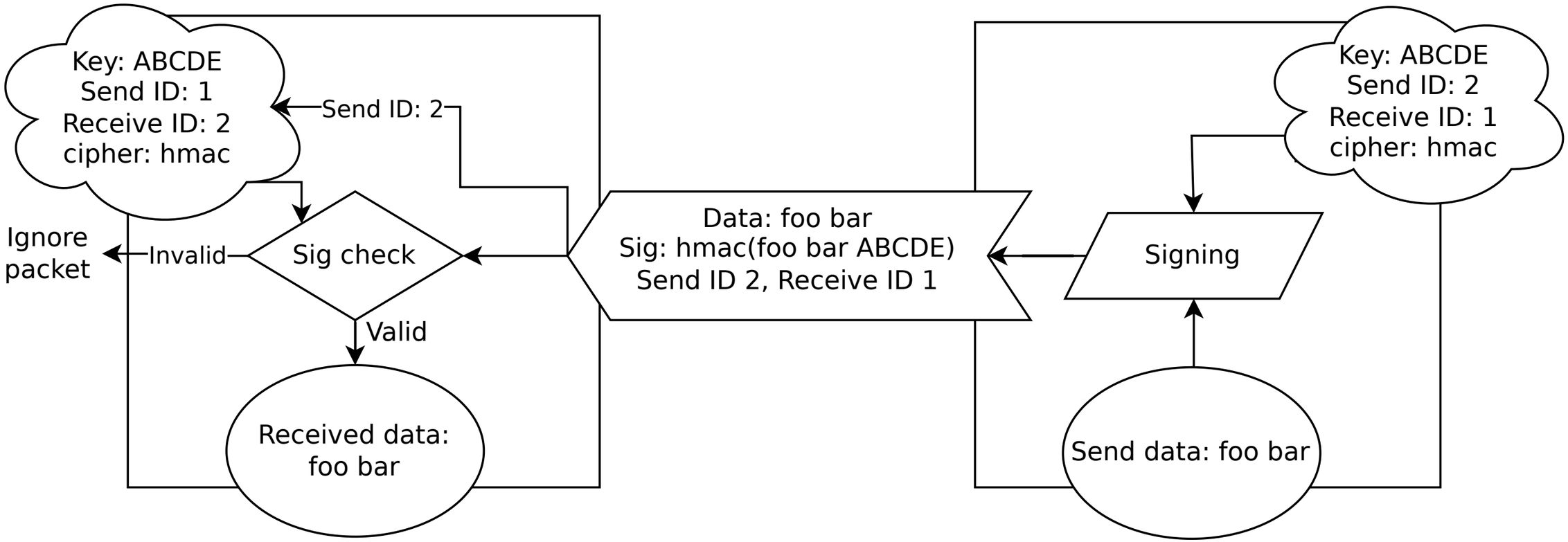
TCP-AO

- change key without interrupting connection
- different keys for different connections
- more possible digest counting algorithms

How TCP-AO works



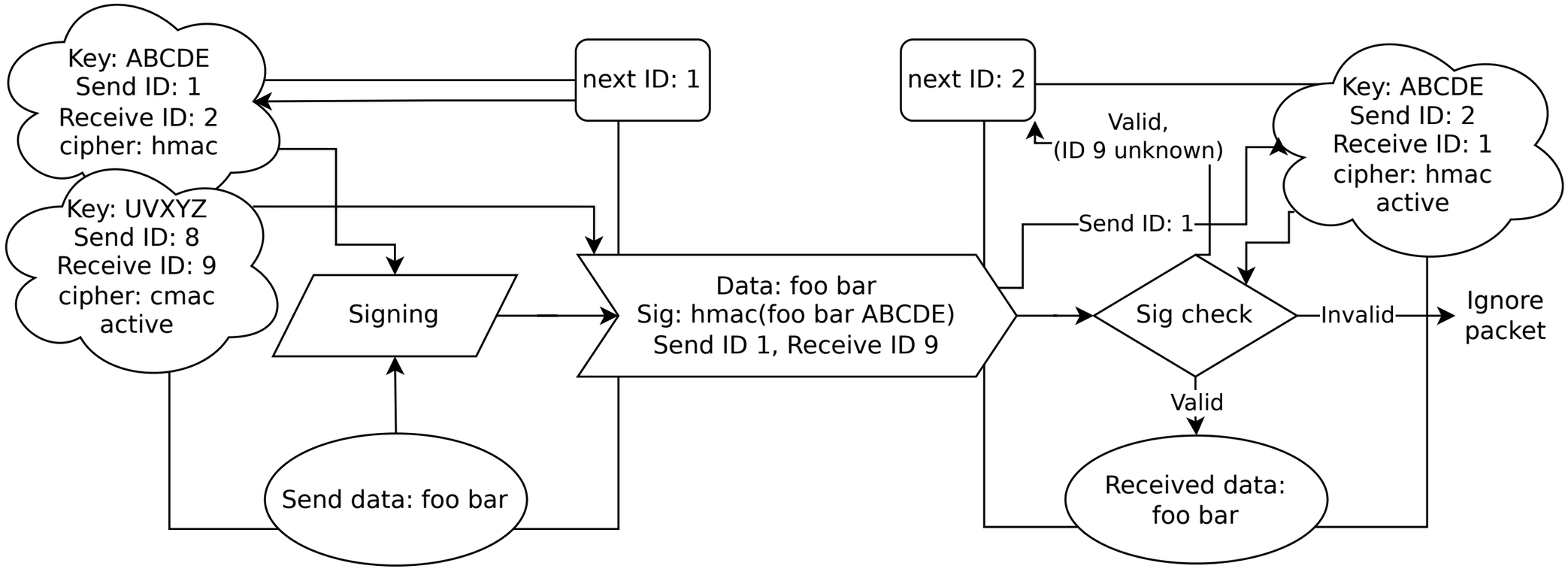
How TCP-AO works



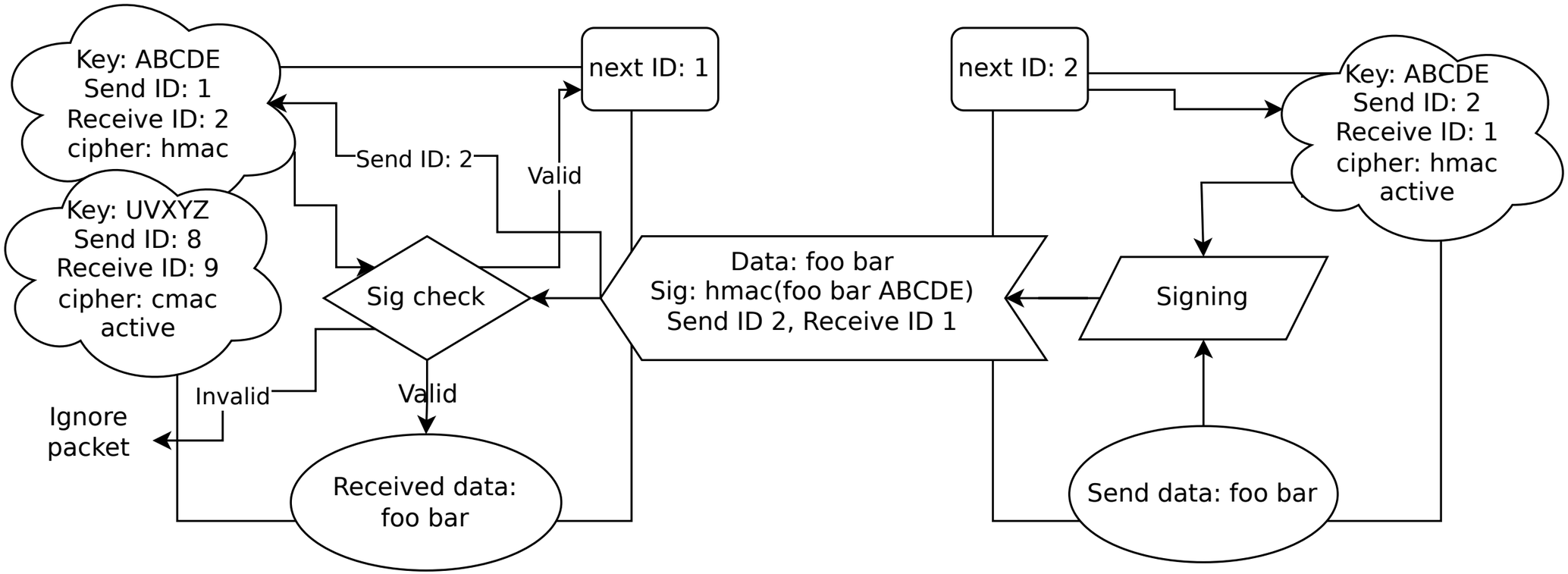
Master Key Tuple (MKT)

- TCP connection identifier - (IP adresses, ports)
- TCP option flag – include also other TCP options in digest
- IDs - a SendID and a RecvID (number 0-255)
- Master key - passphrase to create passwords (incoming, outgoing, incoming SYN, outgoing SYN)
- Key Derivation Function - to create passwords from Master key
- Message Authentication Code (MAC) algorithm

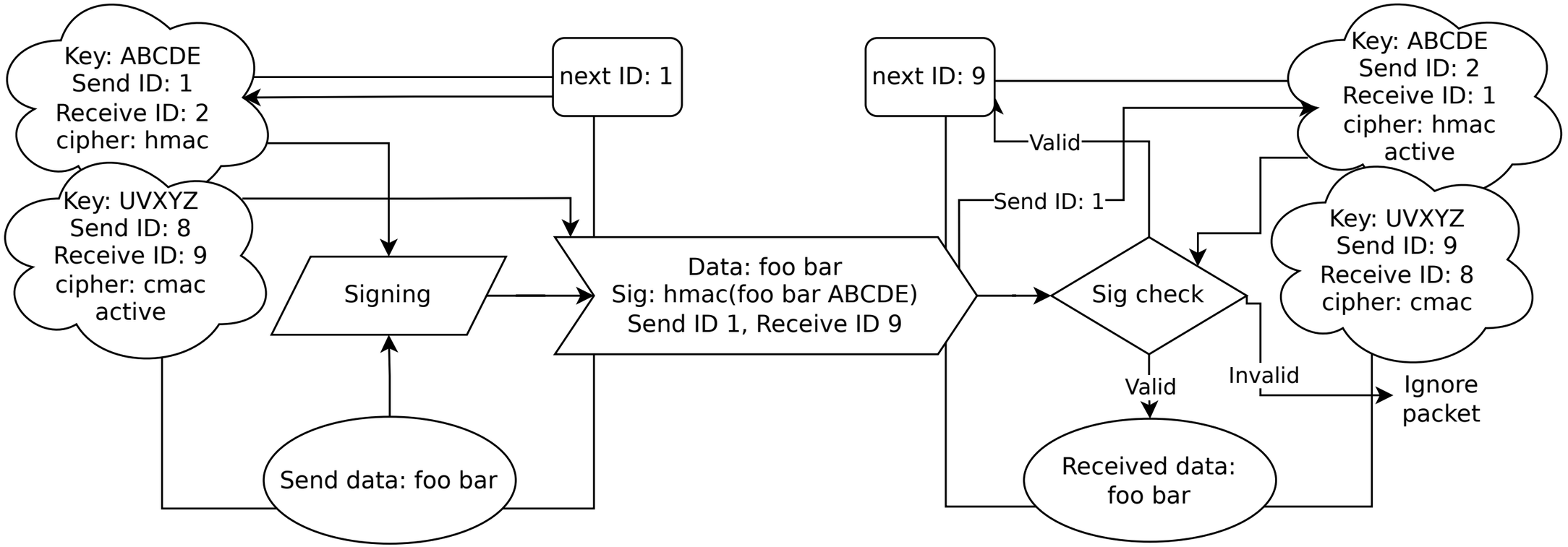
TCP-AO rekeying - new key



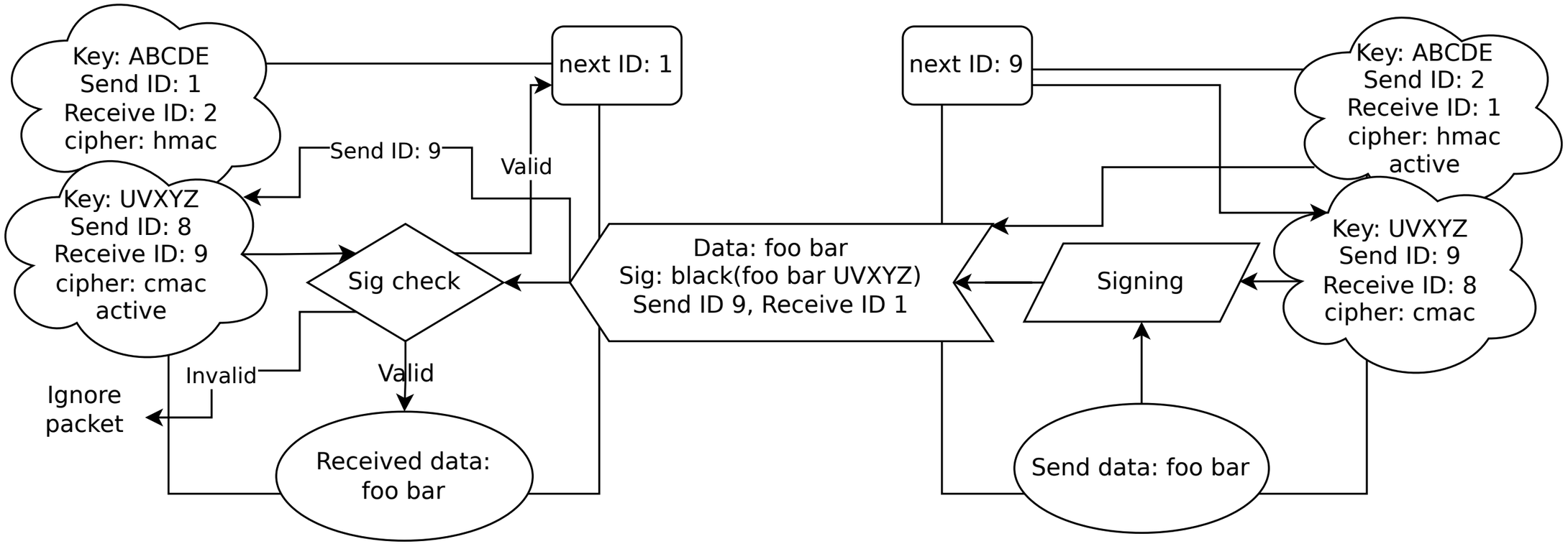
TCP-AO rekeying - new key



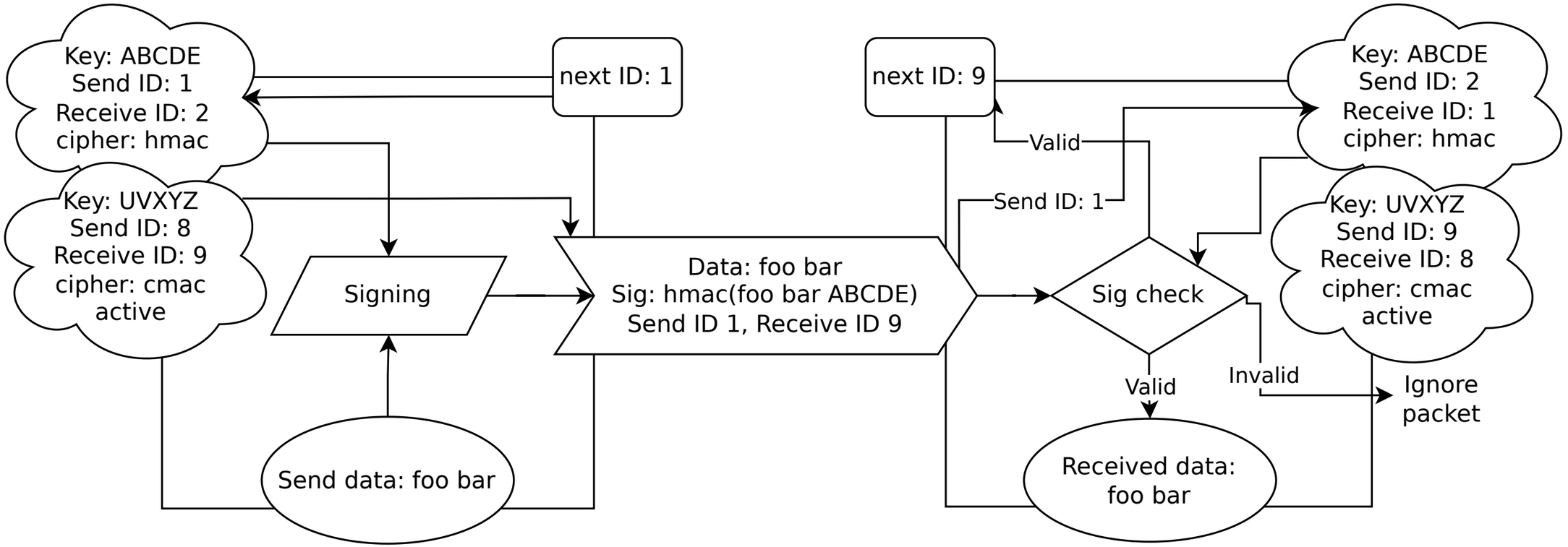
TCP-AO rekeying - the other side requests old key



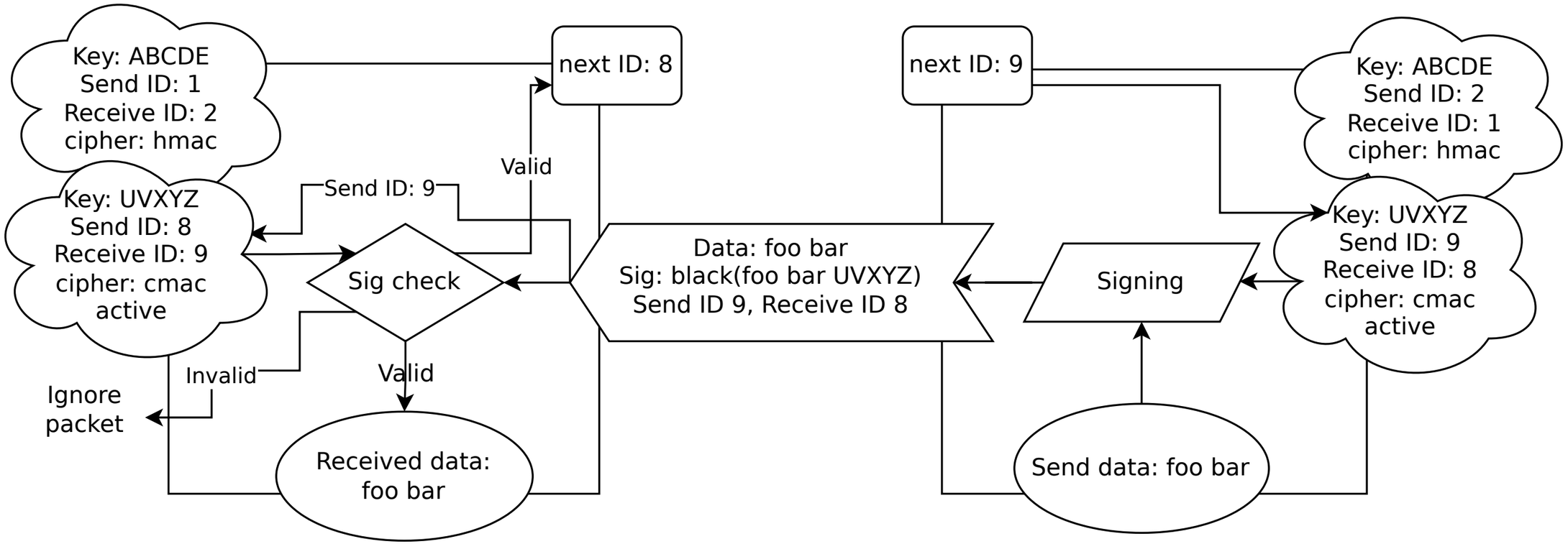
TCP-AO rekeying - the other side requests old key



TCP-AO rekeying - success



TCP-AO rekeying - success



Setting up TCP-AO - BIRD

```
authentication ao;
keys {
  key {
    send id 101;
    recv id 202;
    algorithm hmac sha1;
    secret "7u8i9o";
    preferred;
  }
}
```

Setting up TCP-AO - JunOS

```
user@R1# show security authentication-key-chains key-chain
new_auth_key {
    key 0 {
        secret "7u8i9o"; ## SECRET-DATA
        start-time "2024-01-10.03:00:00 -0700";
        algorithm ao;
        ao-attribute {
            send-id 101; recv-id 202;
            tcp-ao-option enabled;
            cryptographic-algorithm hmac-sha-1-96;
    }}}
```

Setting up TCP-AO - CISCO

```
Router1#show run | sec key
key chain kc1 tcp
 key 0
  send-id 101
  recv-id 202
  cryptographic-algorithm hmac-sha-1
  key-string 7u8i9o
```

Rekeying TCP-AO in BIRD

```
authentication ao;
keys {
  key {
    send id 1;
    recv id 2;
    secret "4r5t6y";}
  key {
    send id 33;
    recv id 44;
    algorithm hmac sha256";
    secret "7u8i9o";
    preferred;}
}
```

Basic troubleshooting

- password or id typo? → correct it, reconfigure - BIRD will remove the wrong key and add the corrected one
- do not modify the currently used key

Contacts

Kateřina Kubecová | BIRD Developer at CZ.NIC
katerina.kubecova@nic.cz

BIRD Users Mailing list: bird-users@network.cz
BIRD Support: https://bird.nic.cz/

Questions, Explanations, Discussion

Kateřina Kubecová • Nov 21th, 2025

CZ DOMAIN REGISTRY