



RIPE NCC

RIPE NETWORK COORDINATION CENTRE

RPKI: Enhancing Security with Robust Deployment

Presentation

Gerardo Viviers | 7-8 March 2024 | DKNOG 14

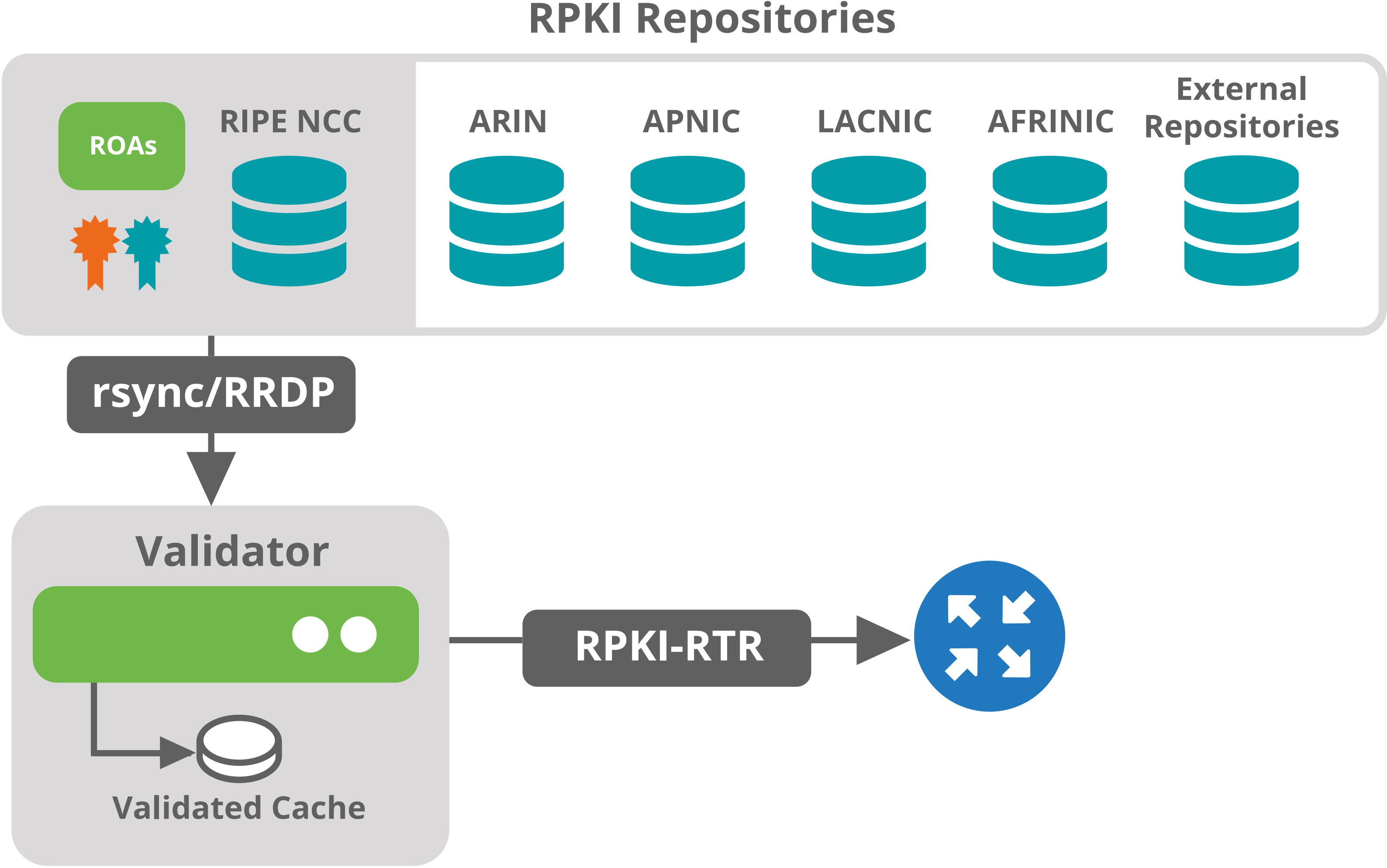
Introduction



- **RPKI:** a framework for Internet routing security
- Helps to validate and verify routing information
- Prevents route hijacking and malicious activities



RPKI System



Routing Security using RPKI



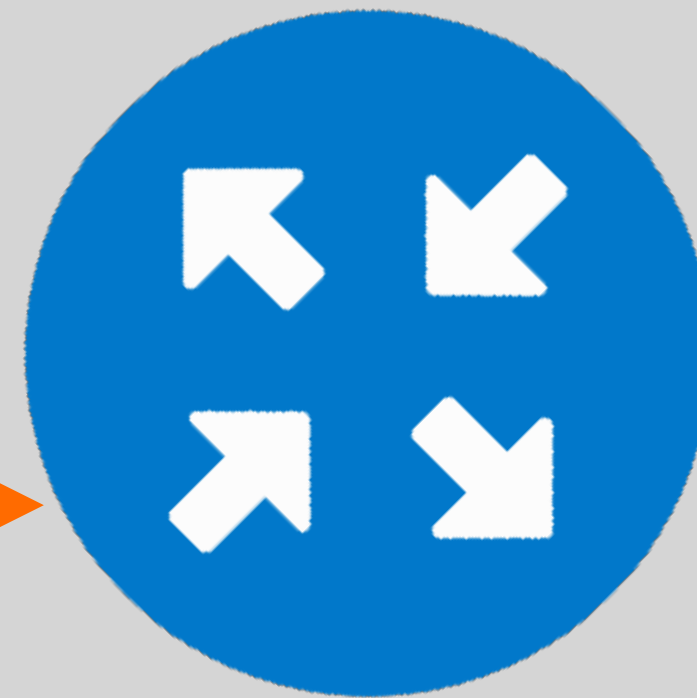
Trust Anchors



RPKI repository



ASN **K** is authorised
to announce
prefix **Y**



Routing Security using RPKI



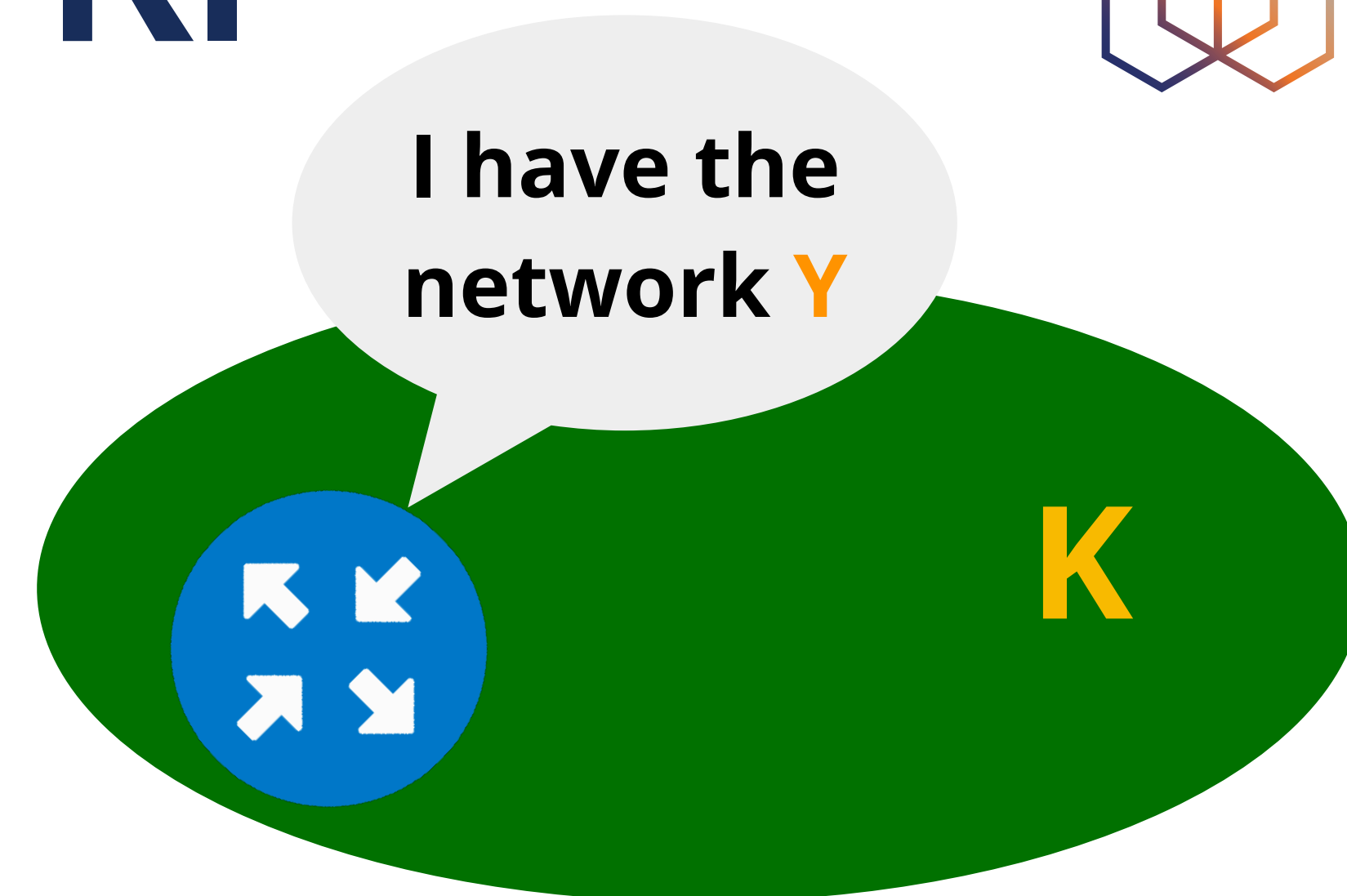
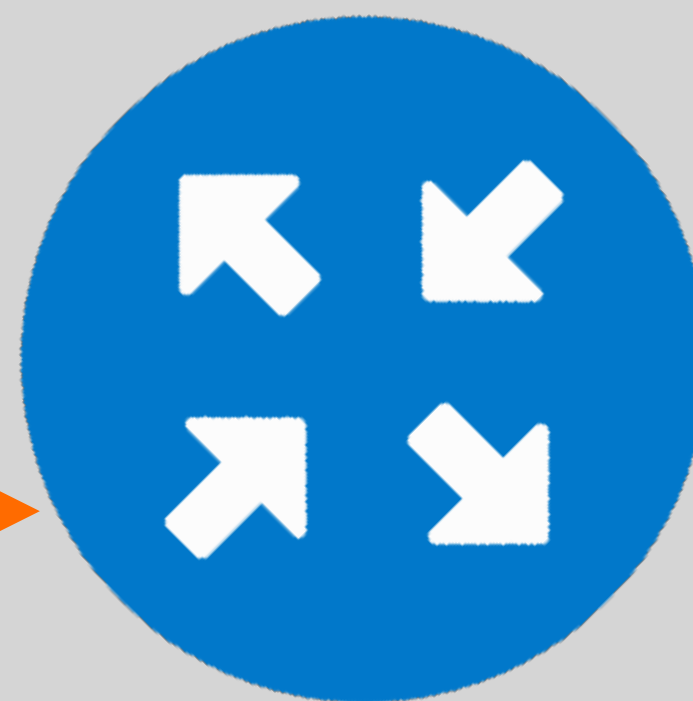
Trust Anchors



RPKI repository



ASN **K** is authorised
to announce
prefix **Y**



Routing Security using RPKI



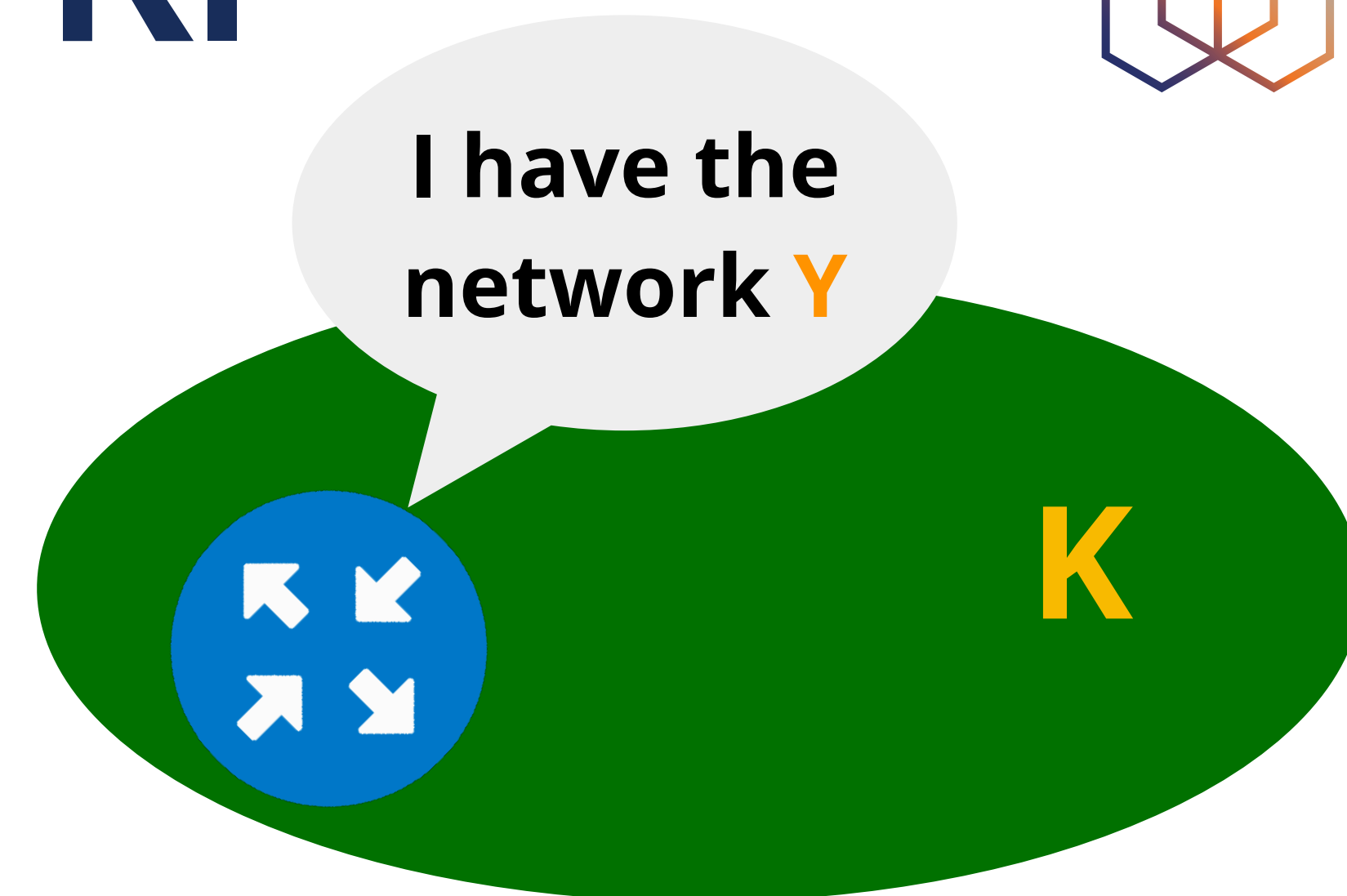
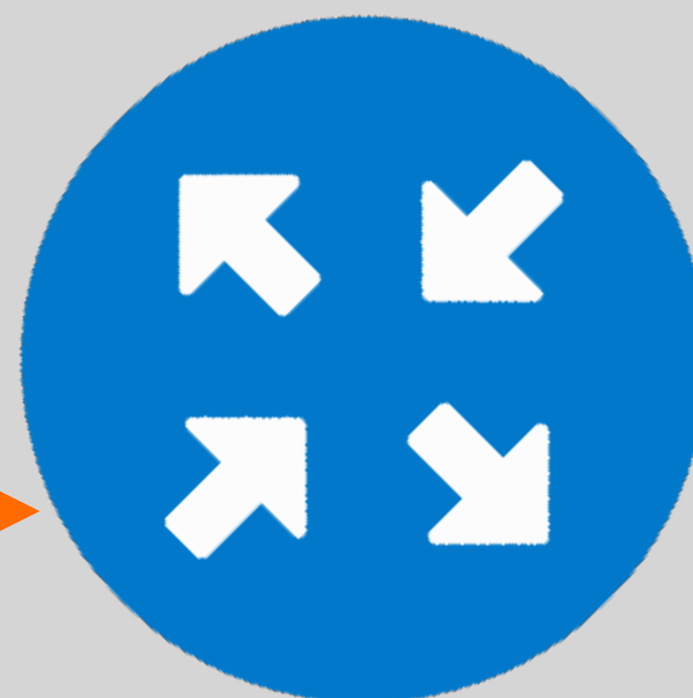
Trust Anchors



RPKI repository



ASN **K** is authorised
to announce
prefix **Y**



Routing Security using RPKI



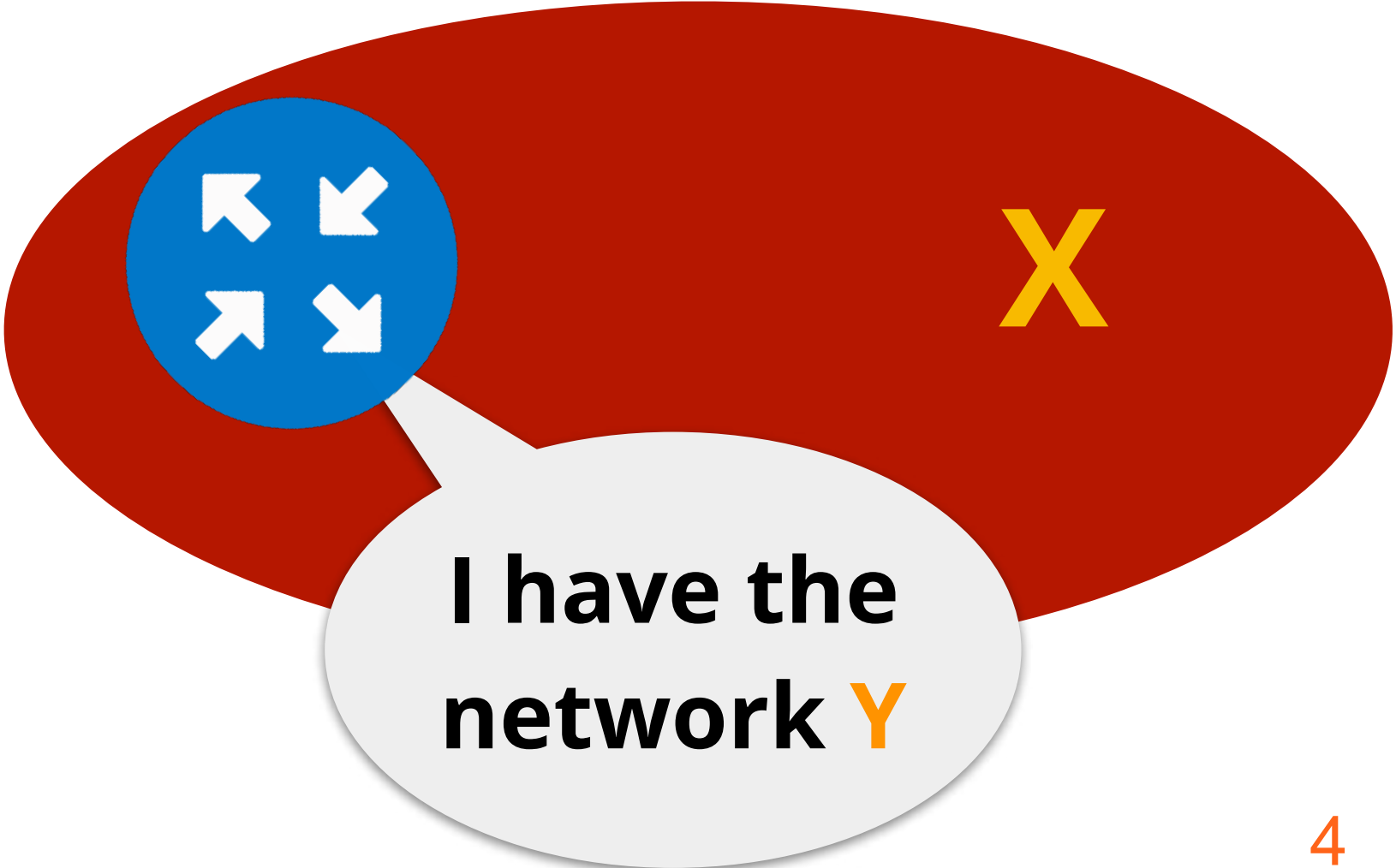
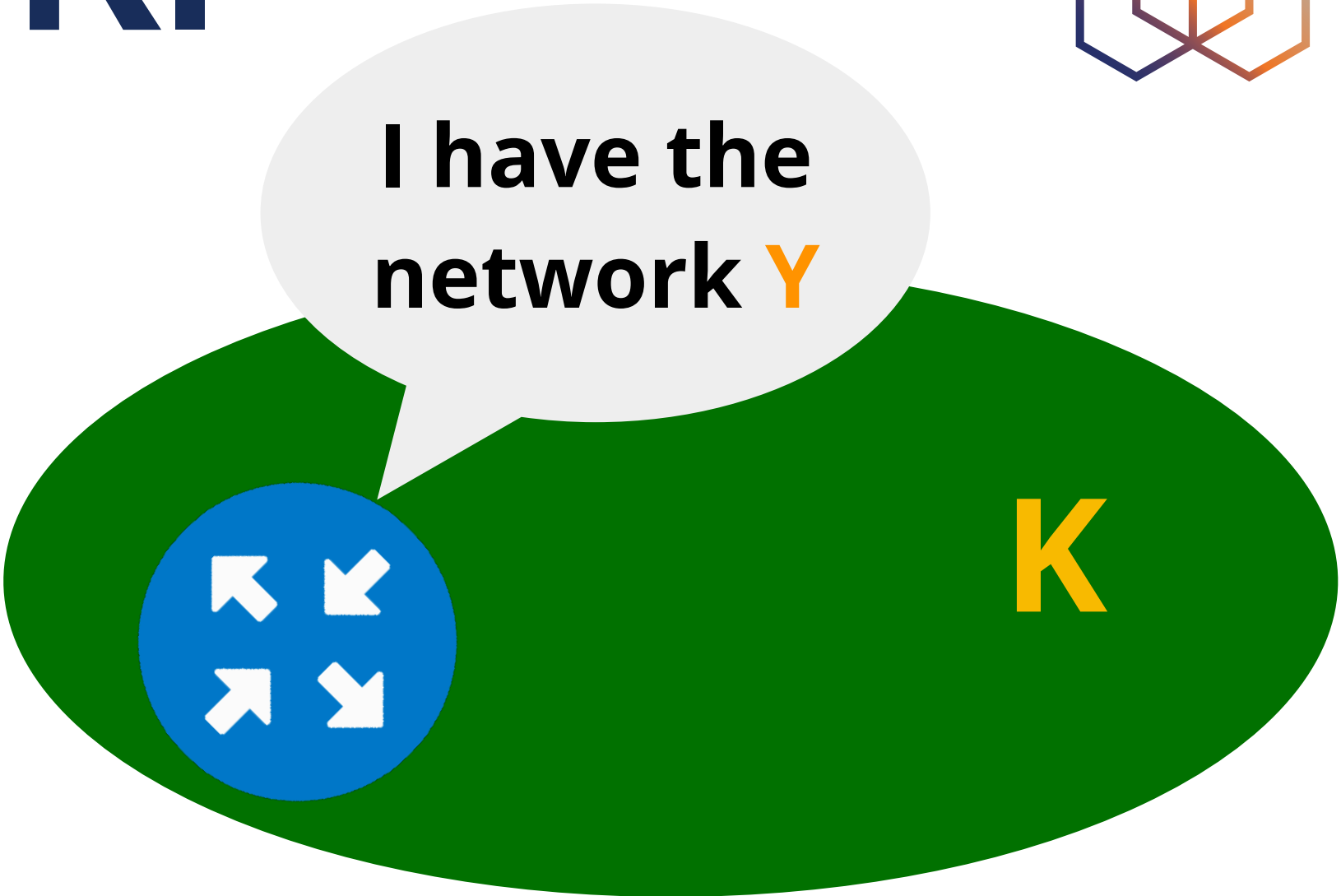
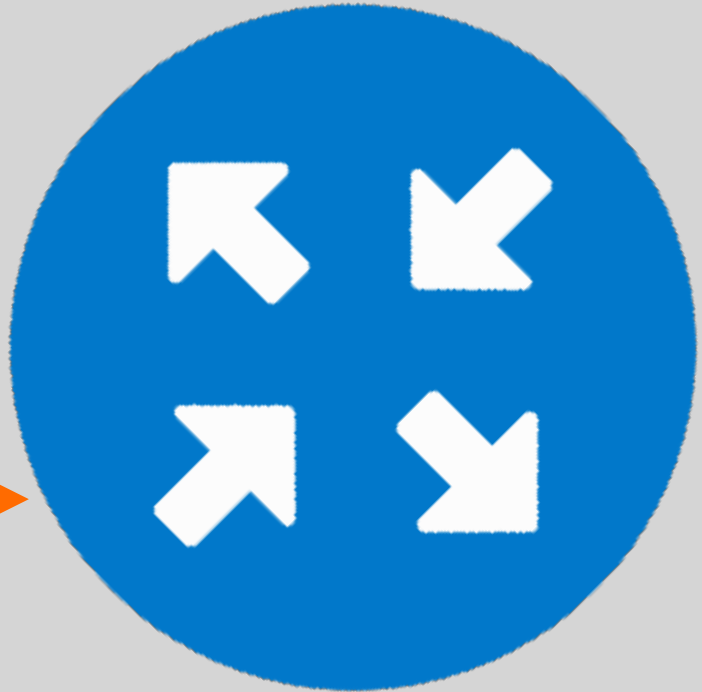
Trust Anchors



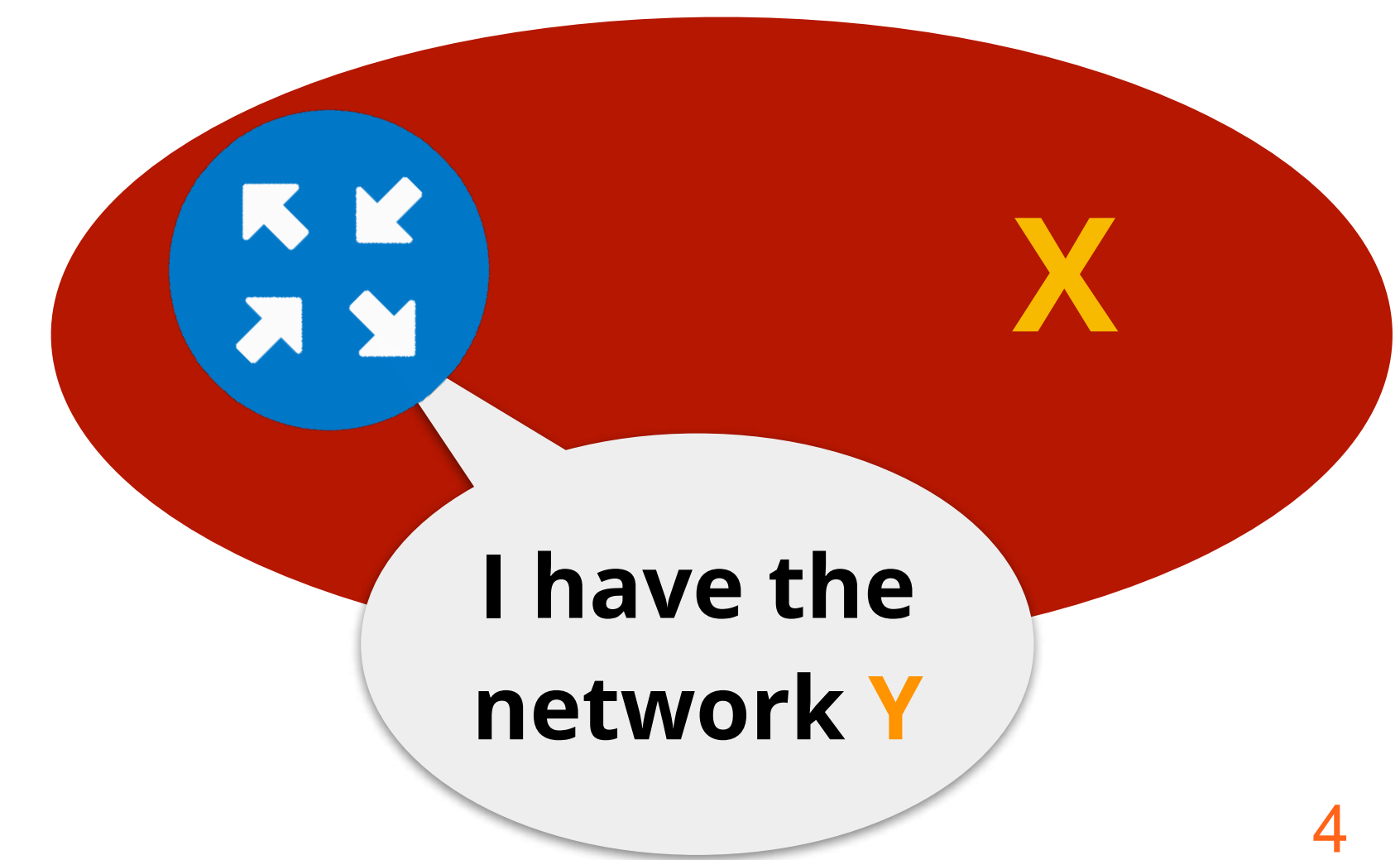
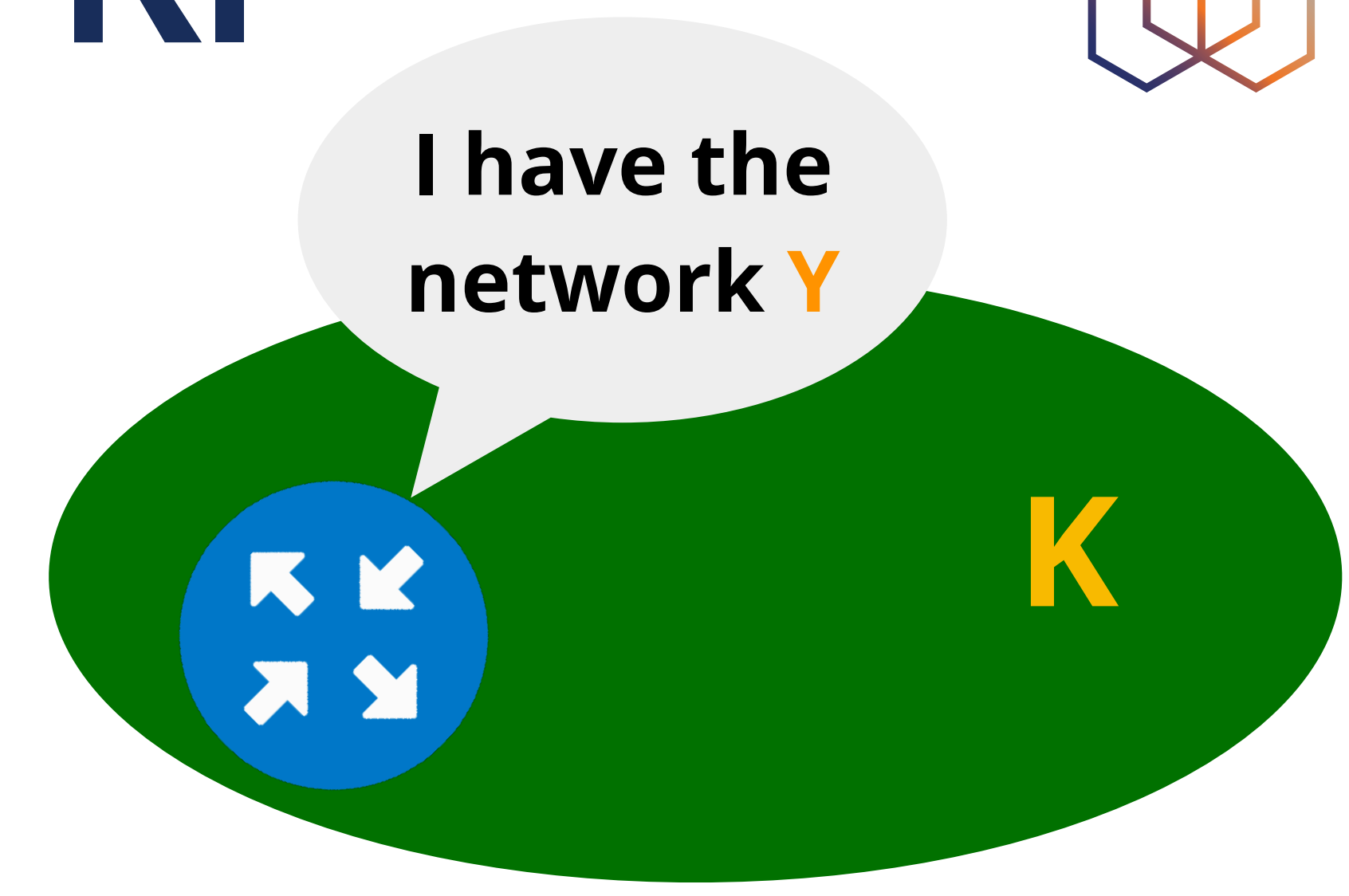
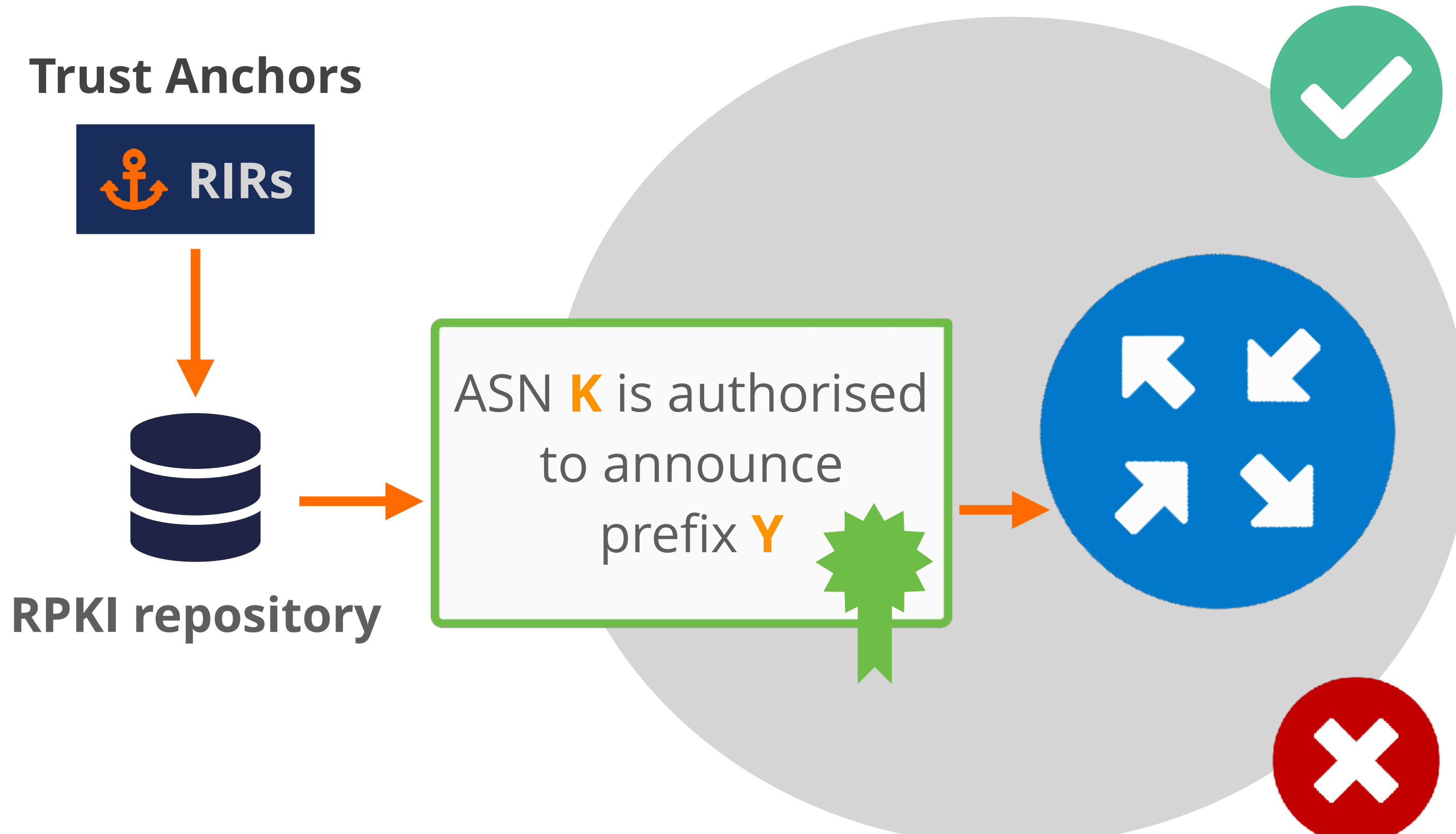
RPKI repository



ASN **K** is authorised to announce prefix **Y**



Routing Security using RPKI



The RPKI Incident



- On January 3, 2024, a RIPE NCC member experienced a national outage that lasted for several hours
- The outage was caused by unexpected changes made to their RPKI ROAs



The RPKI Incident



- These changes were done by a threat actor that gained access to the RPKI Dashboard in the RIPE NCC LIR Portal
- The threat actor gained access using a **leaked password!**



Impact of the Incident



- Globally routed routes originated by AS12479 dropped from around **9,200** to **7,400**
- Backbone carriers that reject **RPKI-invalid** routes stopped carrying a large portion of the member's IP space
- The outage caused **disruptions** in Internet connectivity and services provided by the member



How the Member Resolved it



- The RIPE NCC member **quickly identified** the issue
 - ...and took steps to restore its RPKI certificates
- They worked together with the RIPE NCC for a **resolution**
- **Improved security measures** were taken to prevent this from happening again in the future



Key Lessons Learned



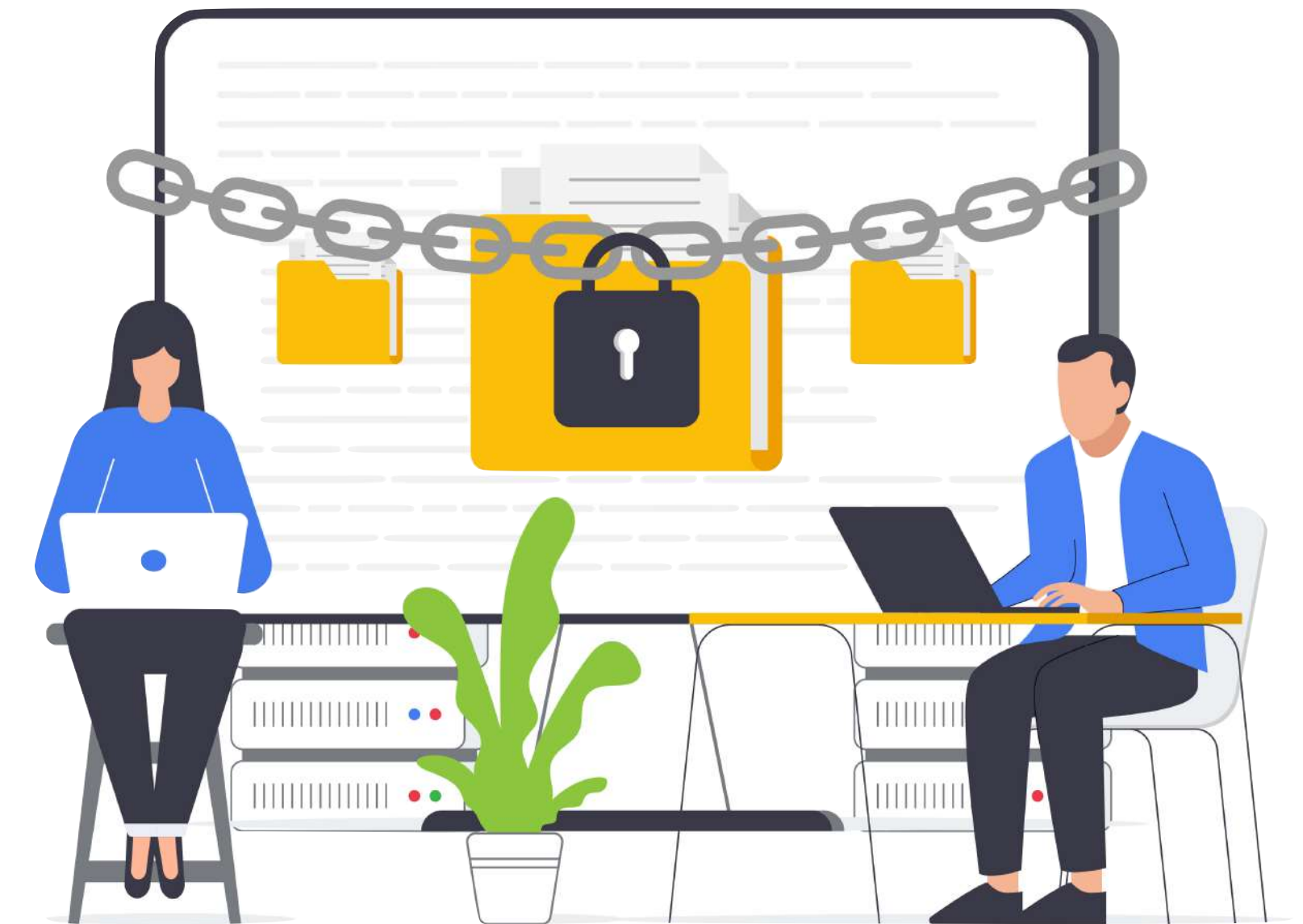
- The importance of **strong passwords** and **multi-factor authentication (MFA)**
- The importance of **network security monitoring**
- The importance of having a **robust incident response plan**



Becoming Resilient



- Use strong passwords
- Implement MFA
- Monitor networks for suspicious activity
- Develop and test an incident response plan
- Regularly monitor RPKI deployments
- Educate staff on the importance of RPKI
 - and the potential impact of outages!



Conclusions



- RPKI is a critical part of Internet routing security
- Learn from the recent RPKI Incident
- Implement the best practices to become more resilient
- Increased investment in RPKI strengthens security and stability





Questions



gviviers@ripe.net