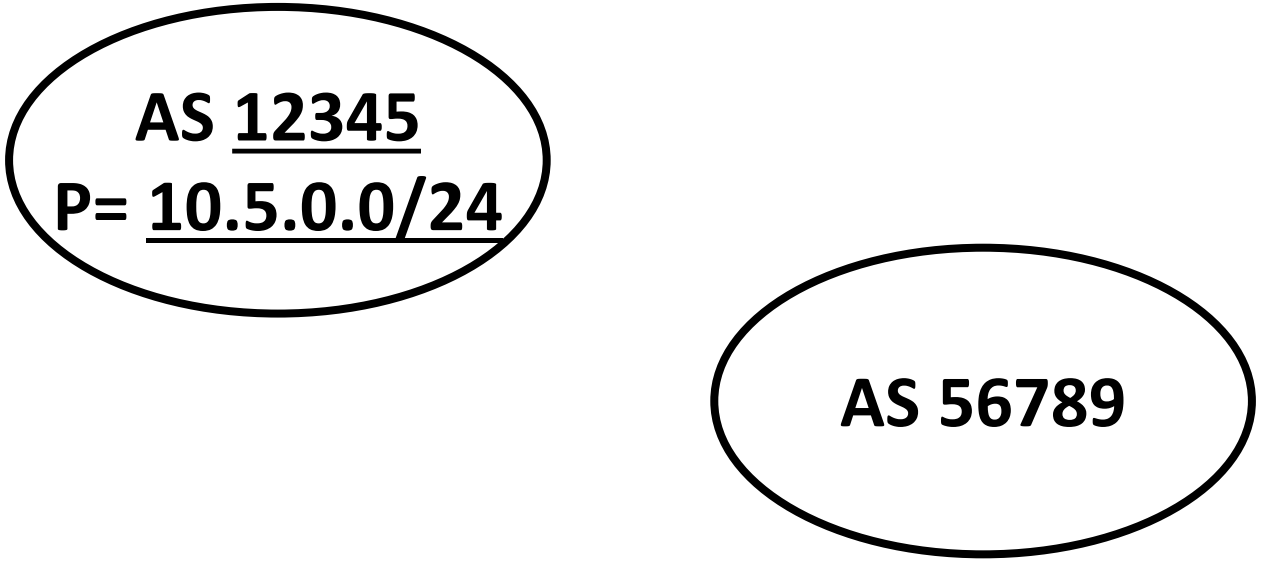
iROV: Breaking the Silence of RPKI with Interactive Validation

Younsoo Kim, Seungjin Baek, Weitong Li, Taejoong Chung, and Min Suk Kang

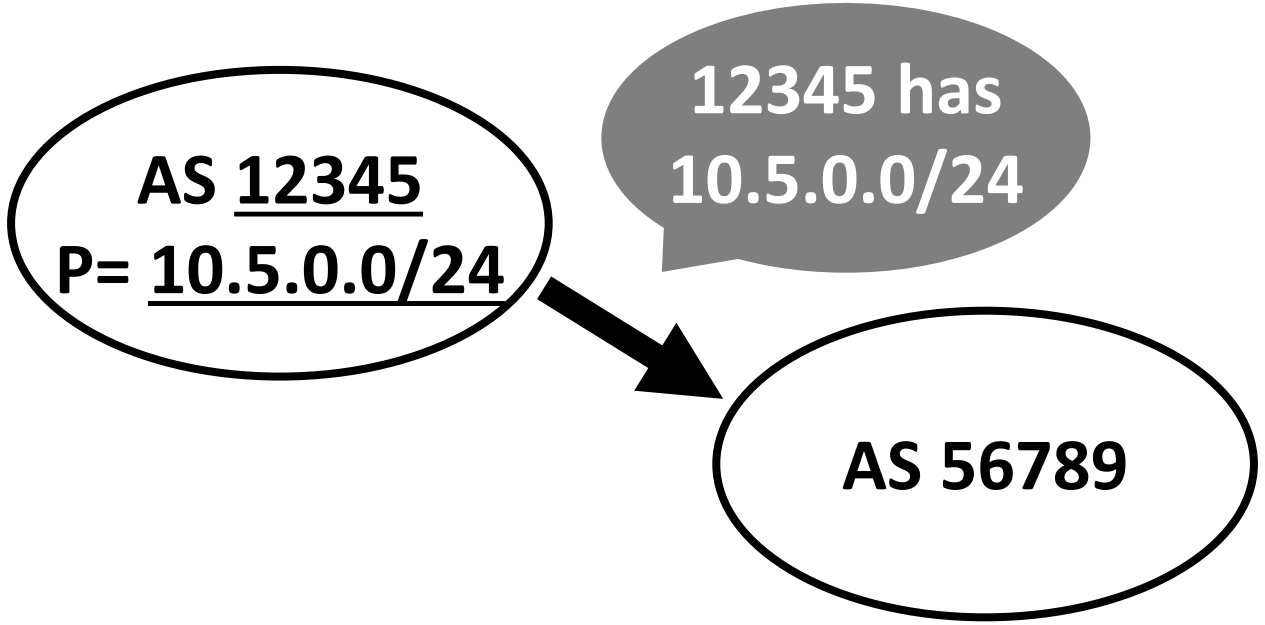
KAIST

VIRGINIA TECH

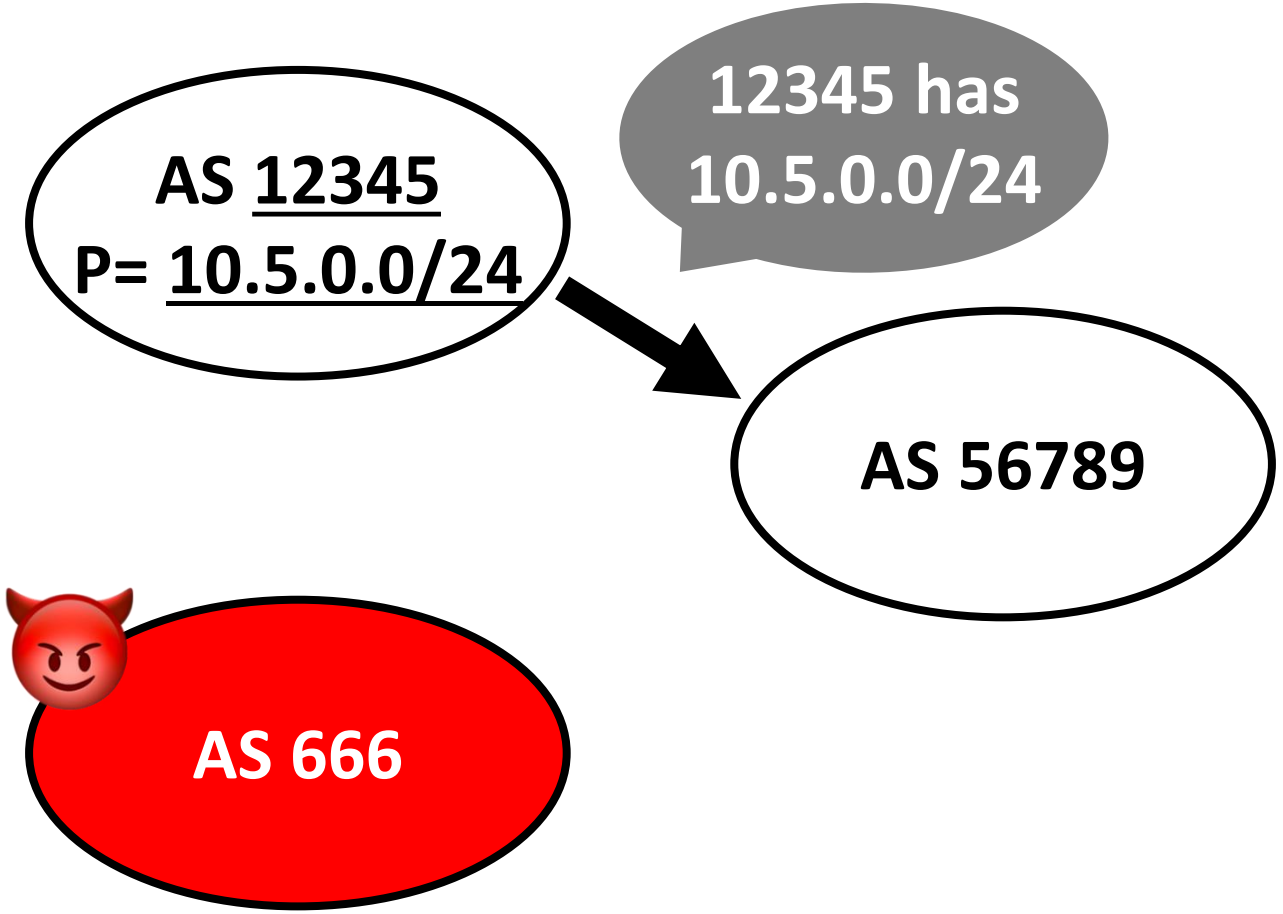
BGP is Vulnerable to Hijacking Attacks



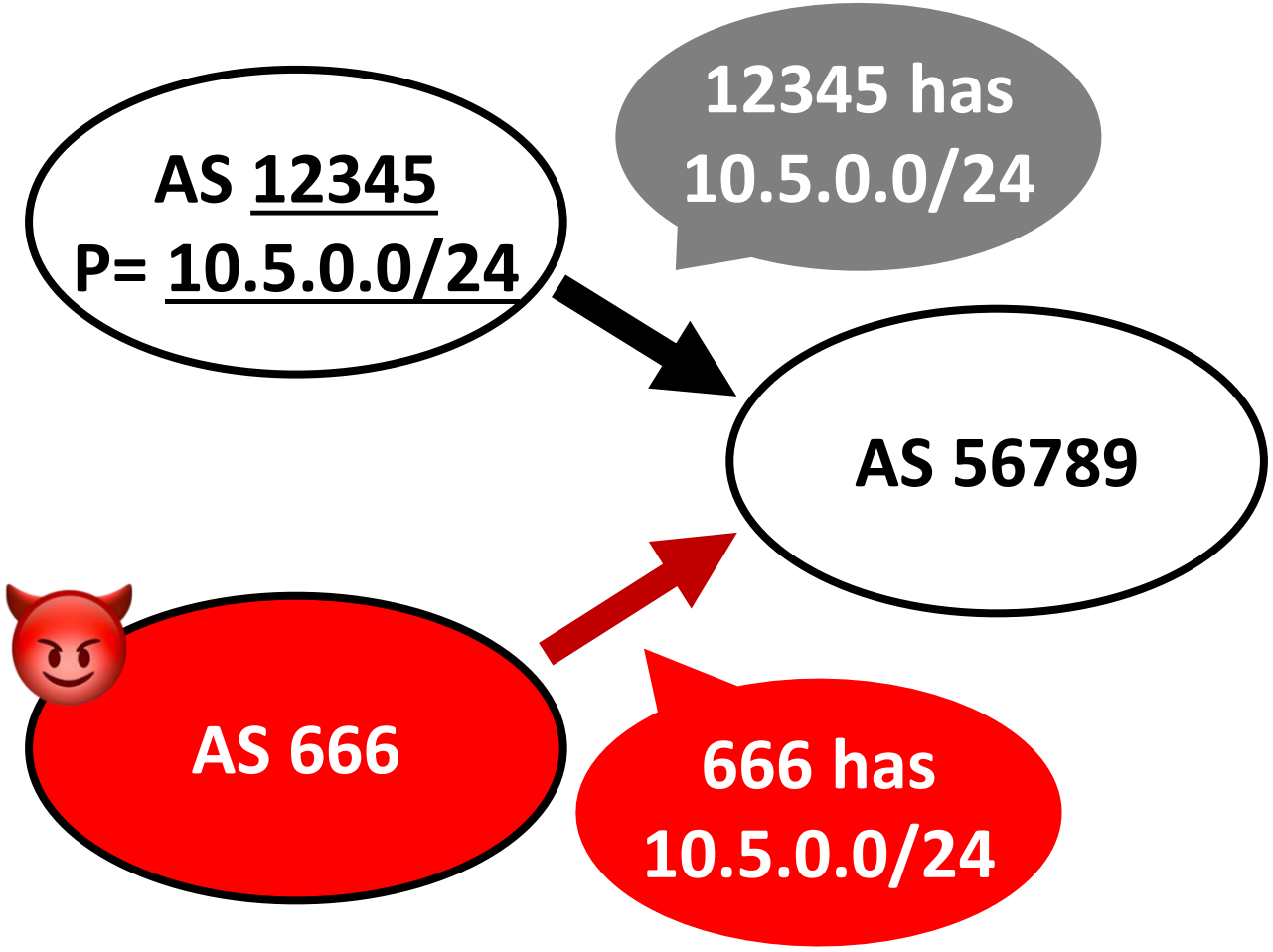
BGP is Vulnerable to Hijacking Attacks



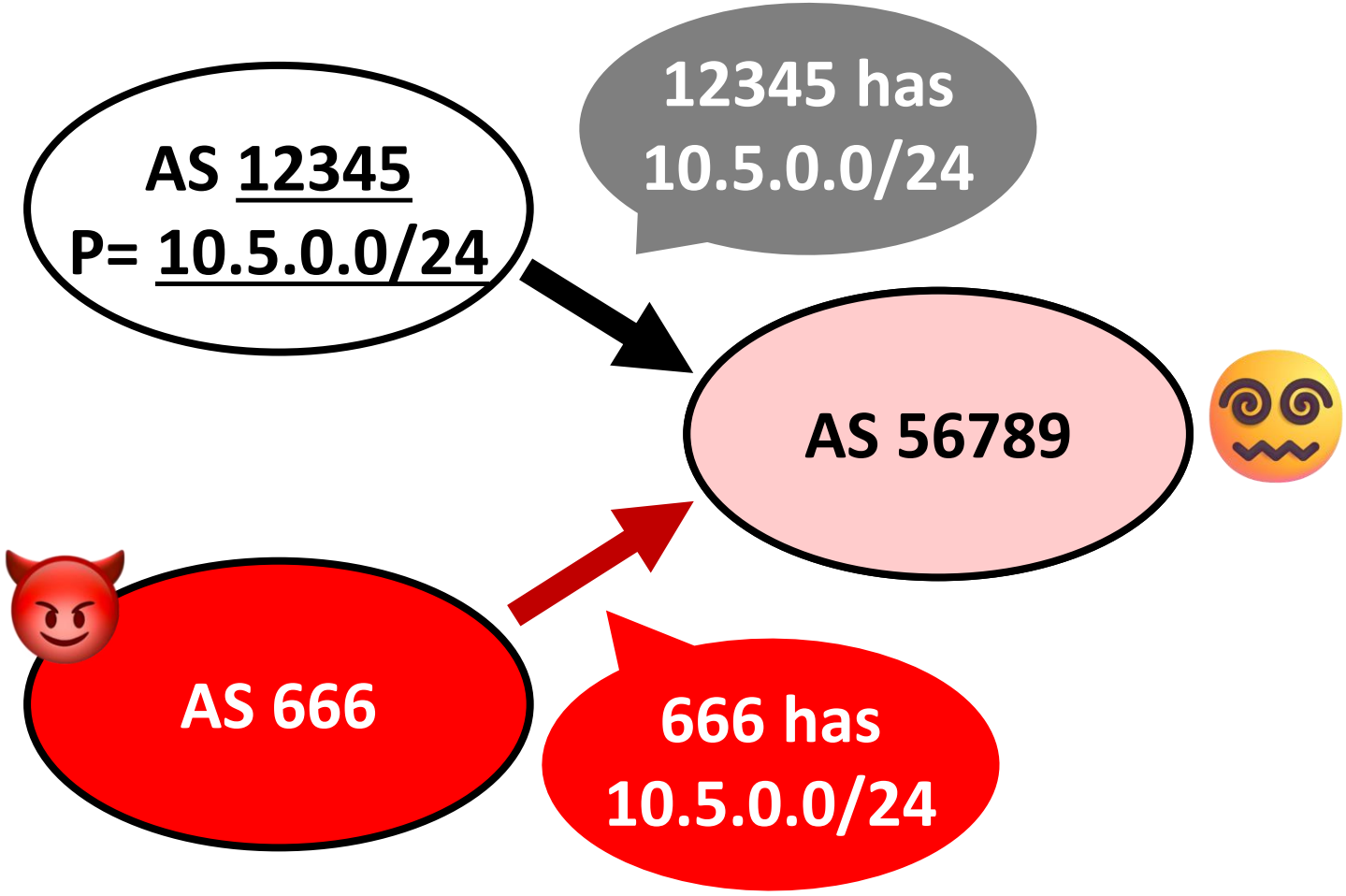
BGP is Vulnerable to Hijacking Attacks



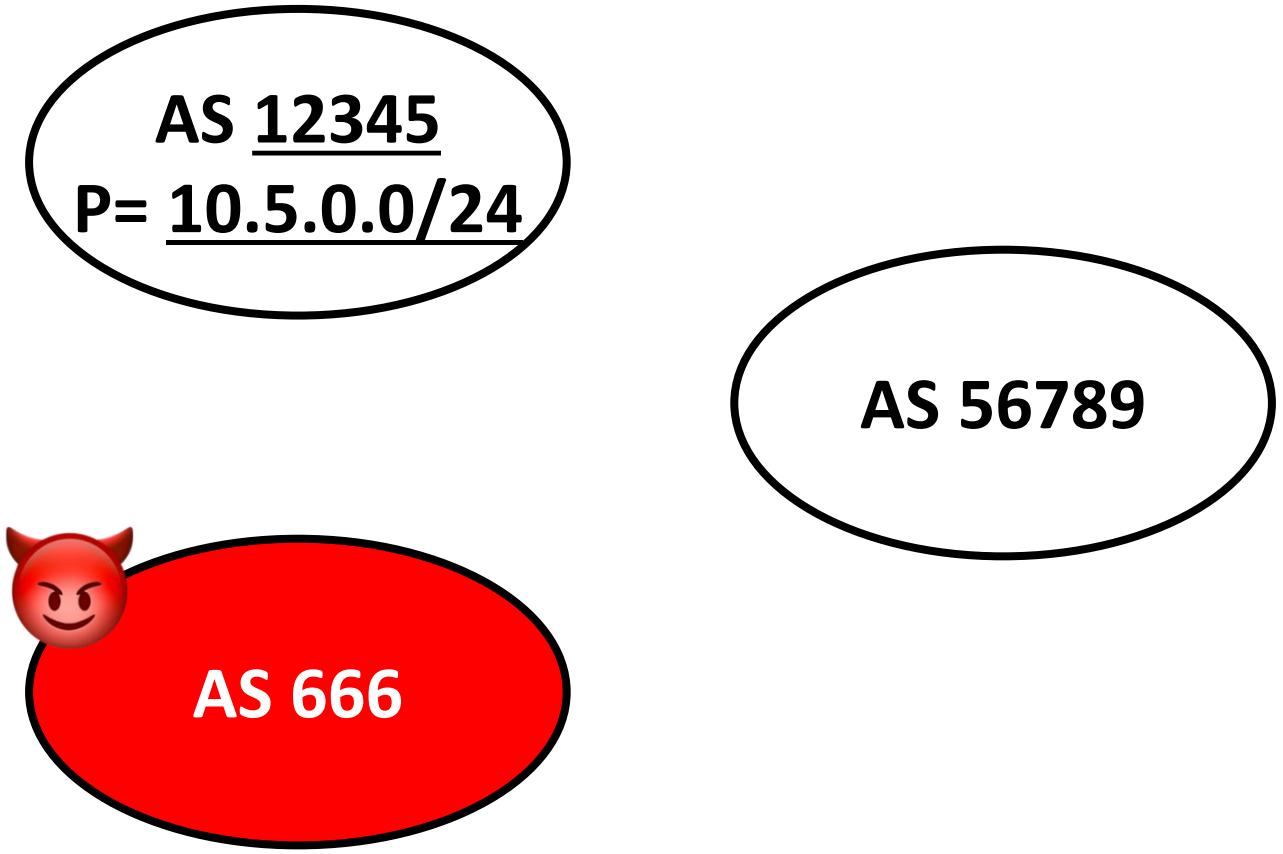
BGP is Vulnerable to Hijacking Attacks



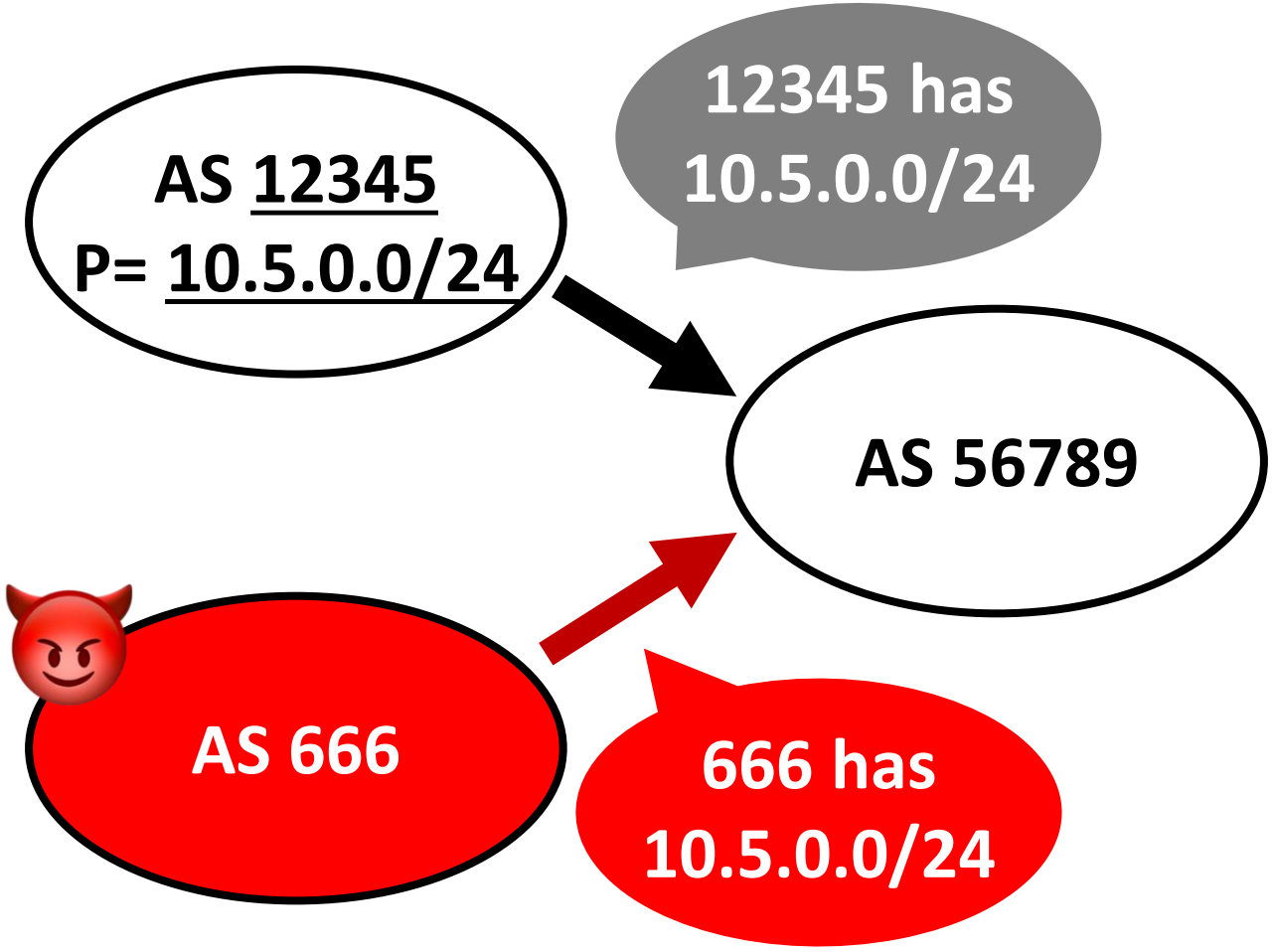
BGP is Vulnerable to Hijacking Attacks



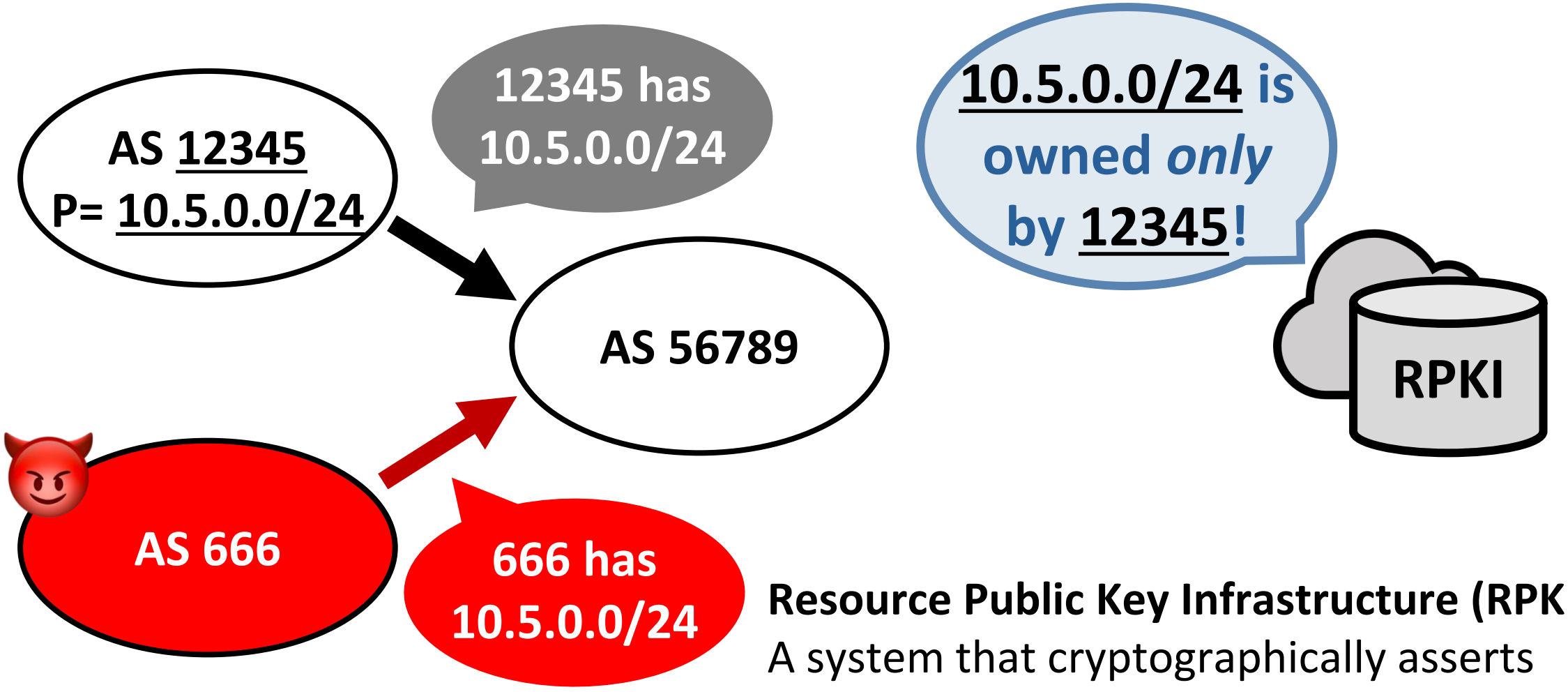
RPKI/ROV Prevents Prefix Hijacking Attacks



RPKI/ROV Prevents Prefix Hijacking Attacks

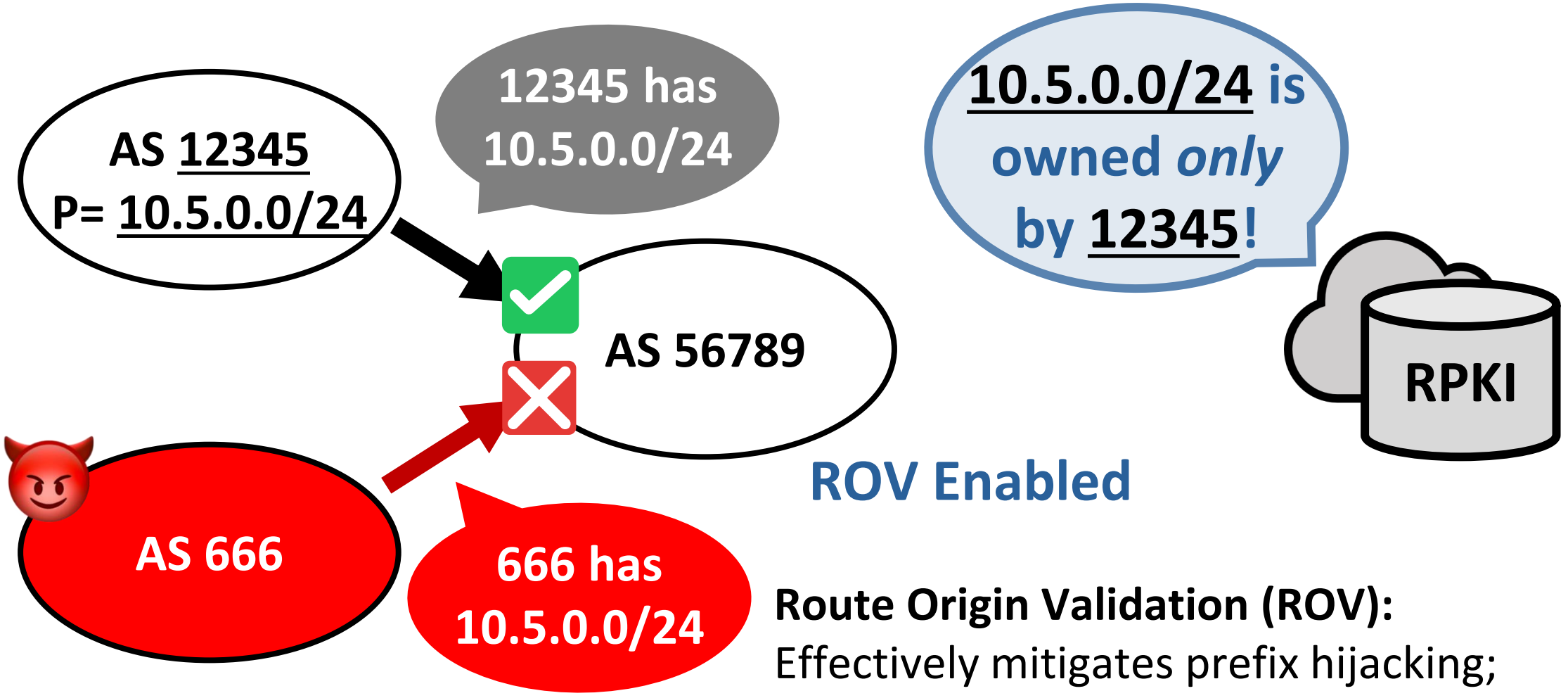


RPKI/ROV Prevents Prefix Hijacking Attacks



Resource Public Key Infrastructure (RPKI):
A system that cryptographically asserts Internet Number Resource (INR) ownership

RPKI/ROV Prevents Prefix Hijacking Attacks



Route Origin Validation (ROV):
Effectively mitigates prefix hijacking;
its global adoption is steadily increasing
every year

RPKI/ROV Prevents Prefix Hijacks…

RPKI/ROV Prevents Prefix Hijacks…

However, it faces **several operational challenges**:

RPKI/ROV Prevents Prefix Hijacks…

However, it faces **several operational challenges**:

(No error visibility)

[C1] Errors (e.g., typos) are difficult to detect and fix





RPKI/ROV Prevents Prefix Hijacks…

However, it faces **several operational challenges**:

(No error visibility)

[C1] Errors (e.g., typos) are difficult to detect and fix



RPKI/ROV Prevents Prefix Hijacks…

However, it faces **several operational challenges**:

(No error visibility)

[C1] Errors (e.g., typos) are difficult to detect and fix



(No attack visibility)

[C2] Prefix hijacks are not flagged to the owner AS





RPKI/ROV Prevents Prefix Hijacks…

However, it faces **several operational challenges**:

(No error visibility)

[C1] Errors (e.g., typos) are difficult to detect and fix



(No attack visibility)

[C2] Prefix hijacks are not flagged to the owner AS



RPKI/ROV Prevents Prefix Hijacks…

However, it faces **several operational challenges**:

(No error visibility)

[C1] Errors (e.g., typos) are difficult to detect and fix



(No attack visibility)

[C2] Prefix hijacks are not flagged to the owner AS



RPKI/ROV Prevents Prefix Hijacks…

However, it faces **several operational challenges**:

(No error visibility)

[C1] Errors (e.g., typos) are difficult to detect and fix



(No attack visibility)

[C2] Prefix hijacks are not flagged to the owner AS



(Defense incompatibility)

[C3] DoS defense (traffic redirection) is disrupted by ROV





e.g., Cloudflare

RPKI/ROV Prevents Prefix Hijacks…

However, it faces **several operational challenges**:

(No error visibility)

[C1] Errors (e.g., typos) are difficult to detect and fix



(No attack visibility)

[C2] Prefix hijacks are not flagged to the owner AS

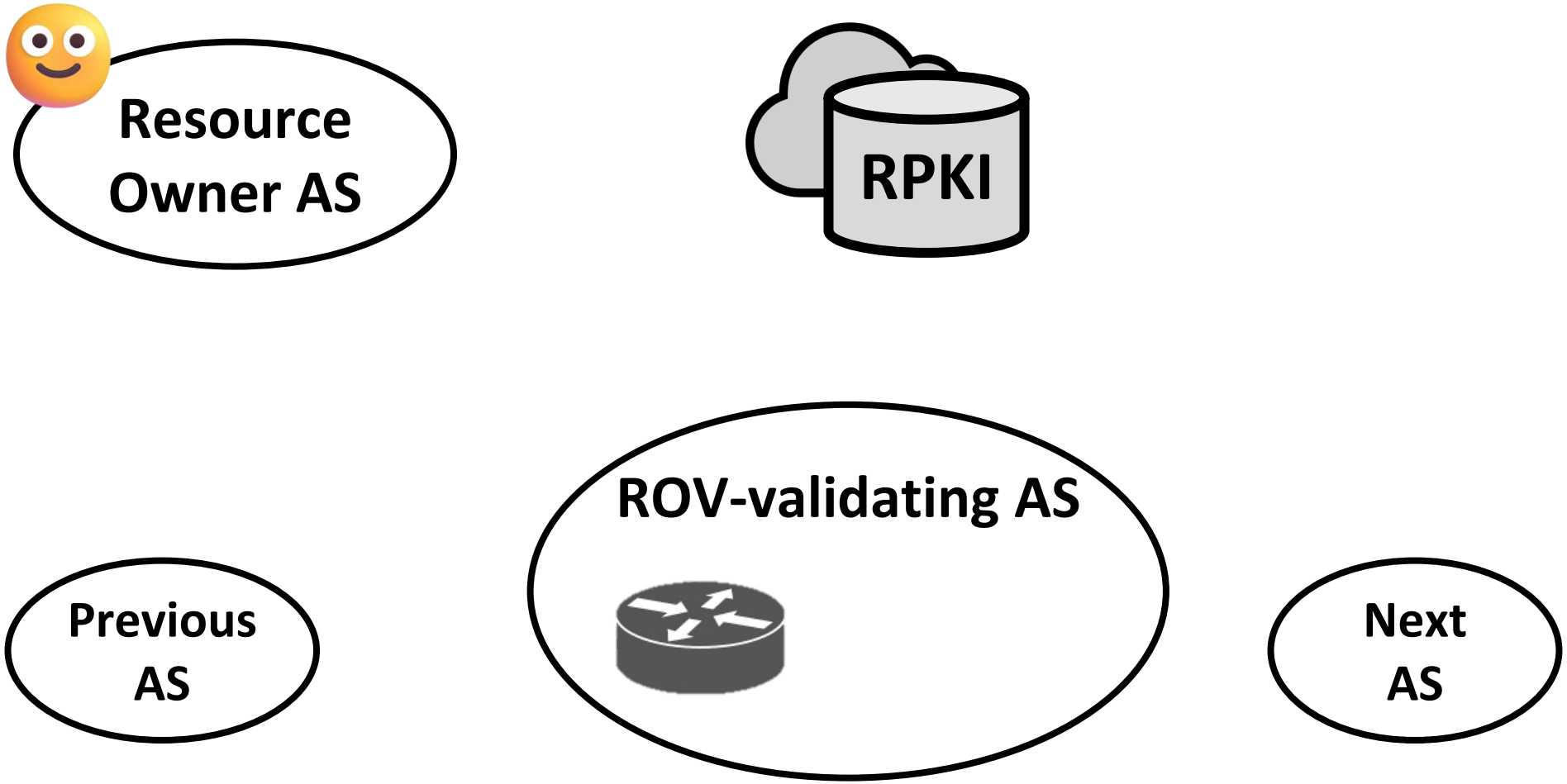


(Defense incompatibility)

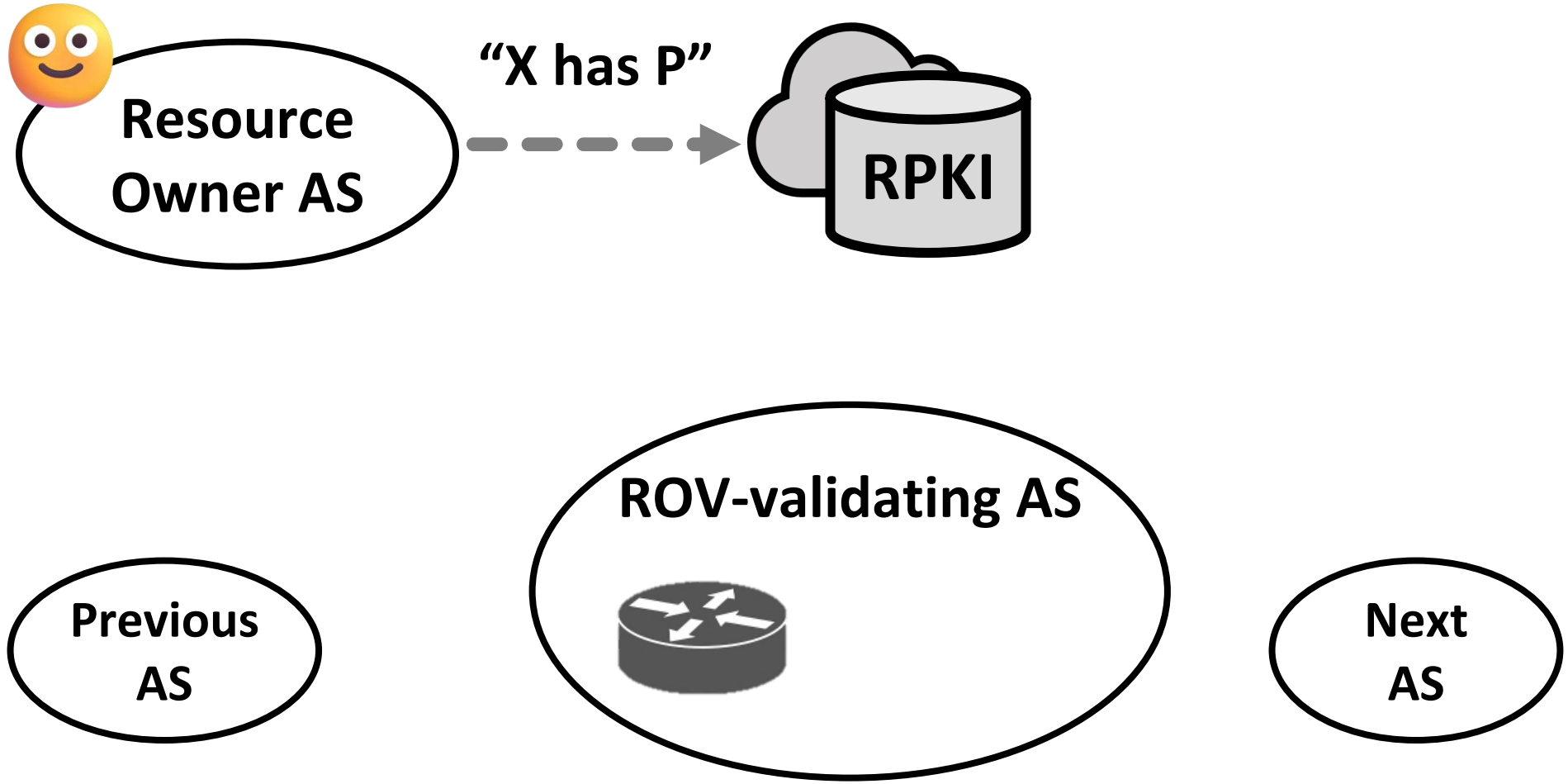
[C3] DoS defense (traffic redirection) is disrupted by ROV



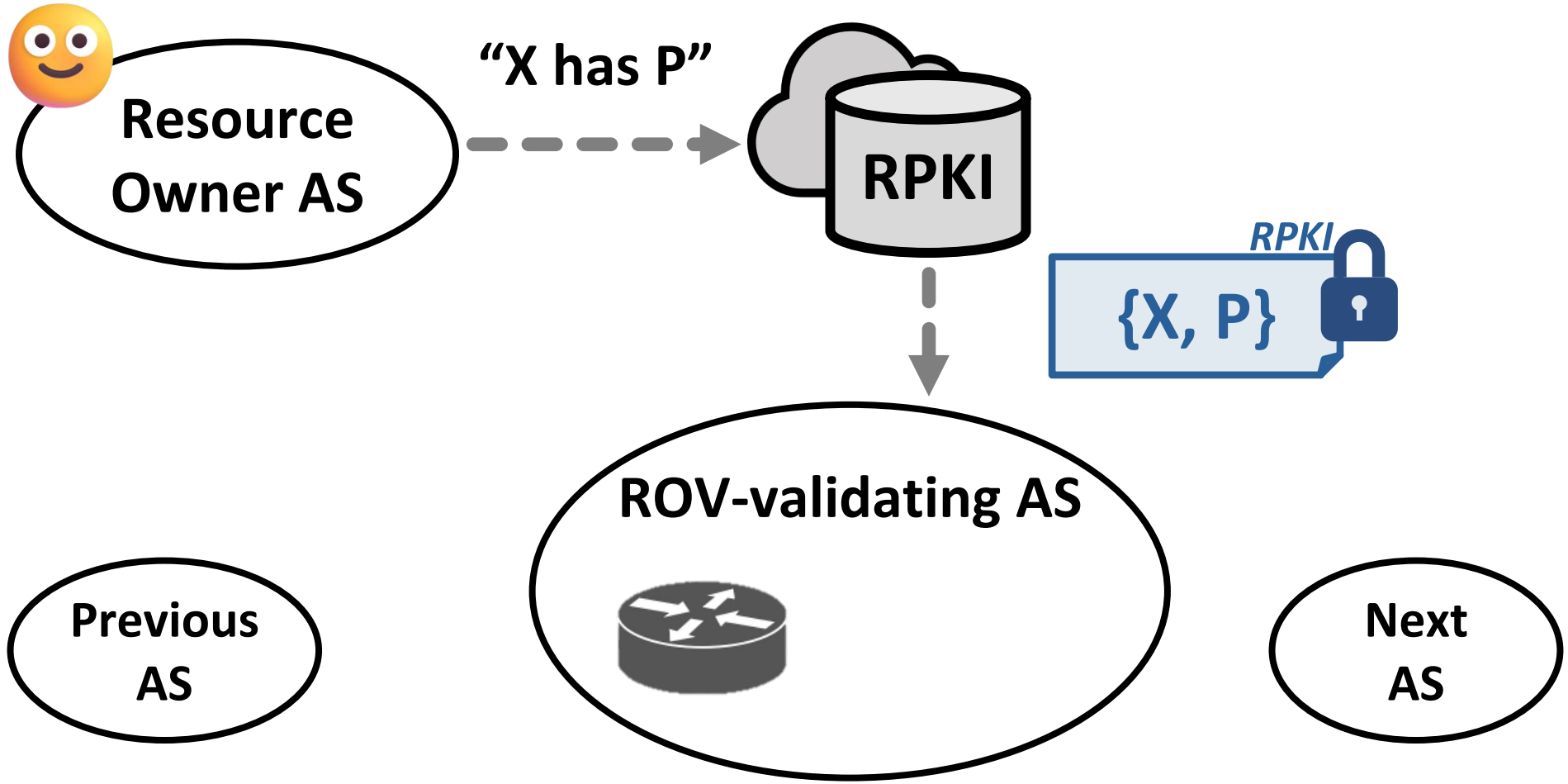
ROV ***Silently Drops*** Invalid Announcements



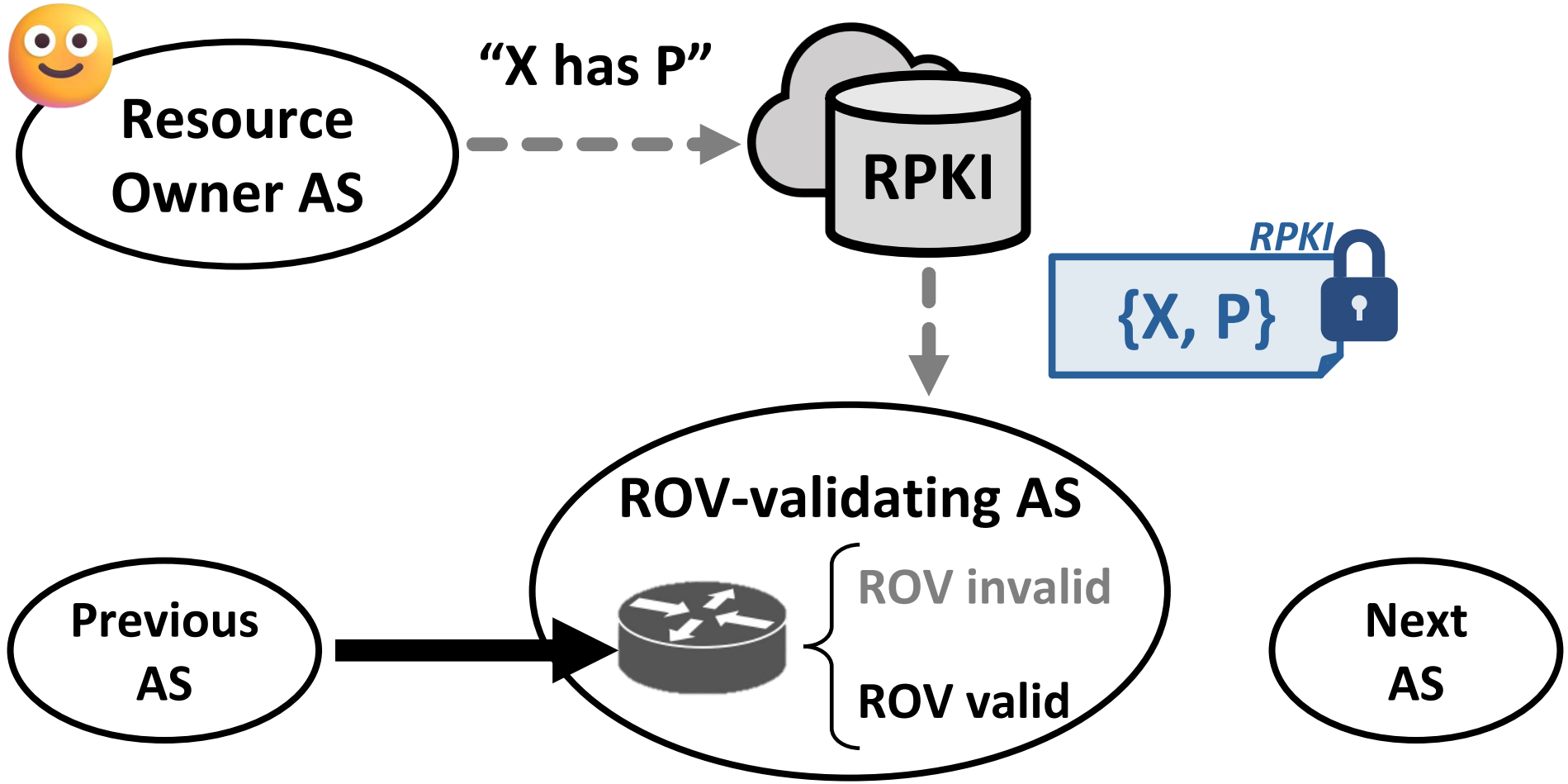
ROV ***Silently Drops*** Invalid Announcements



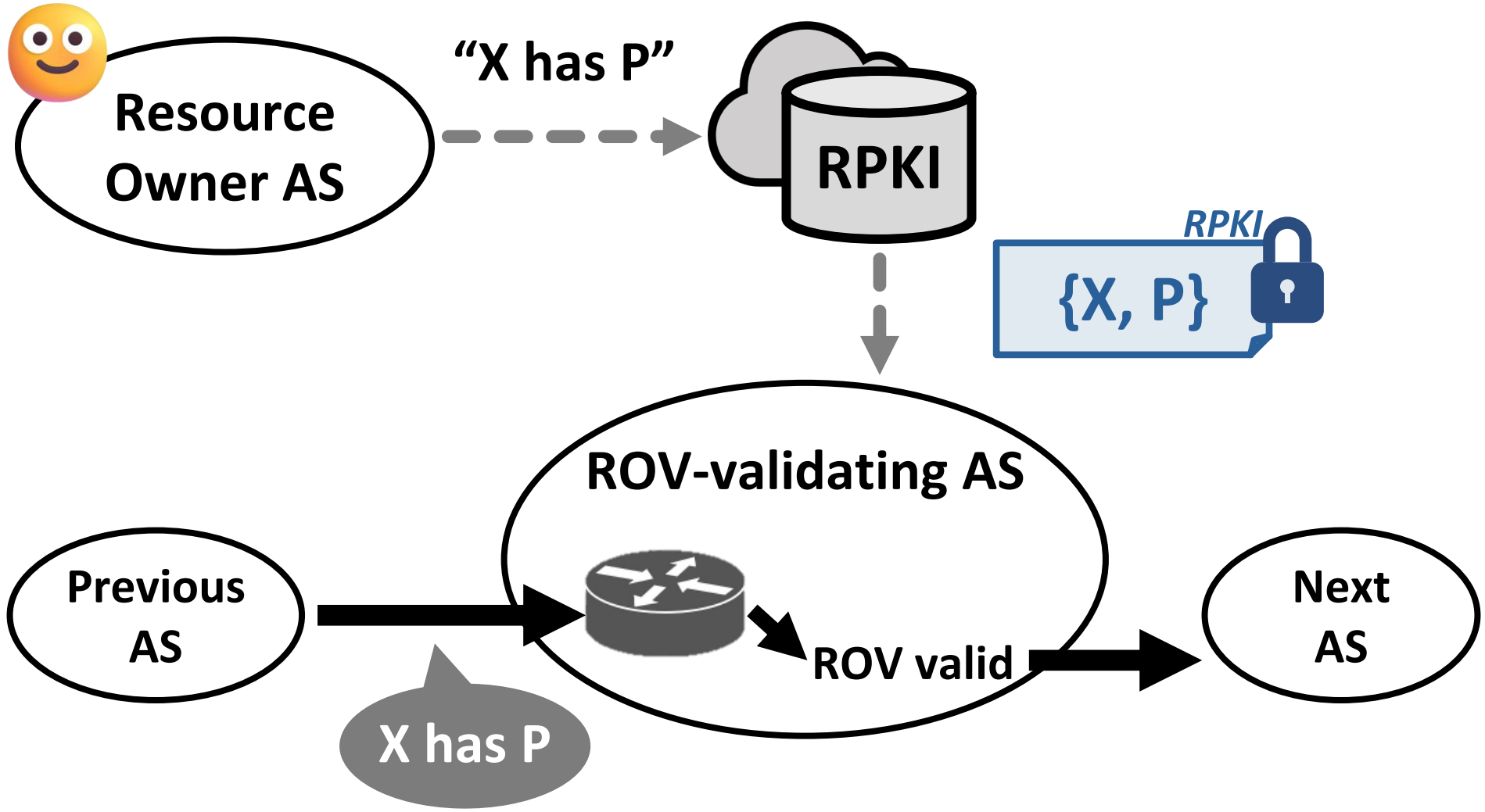
ROV ***Silently Drops*** Invalid Announcements



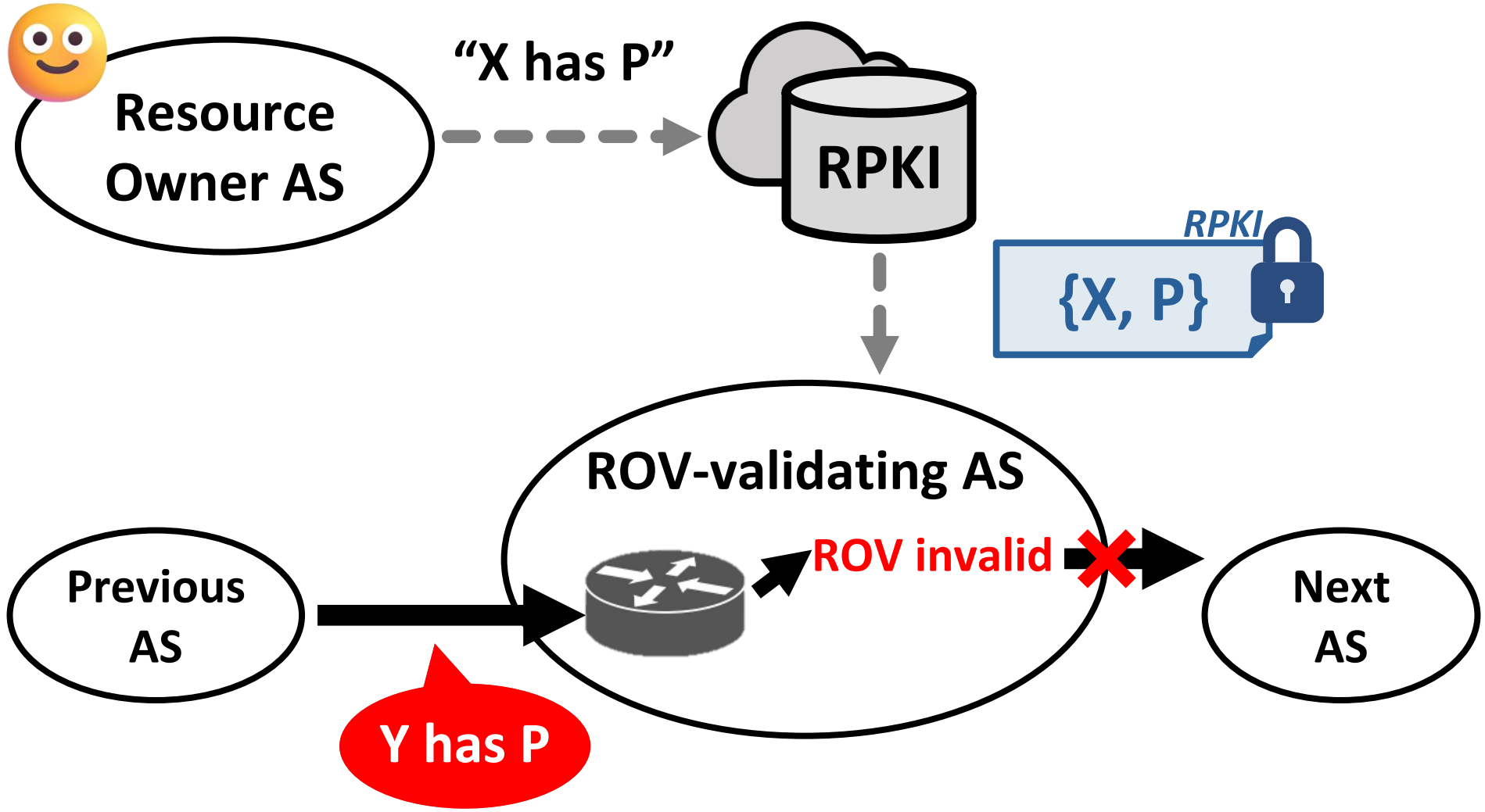
ROV ***Silently Drops*** Invalid Announcements



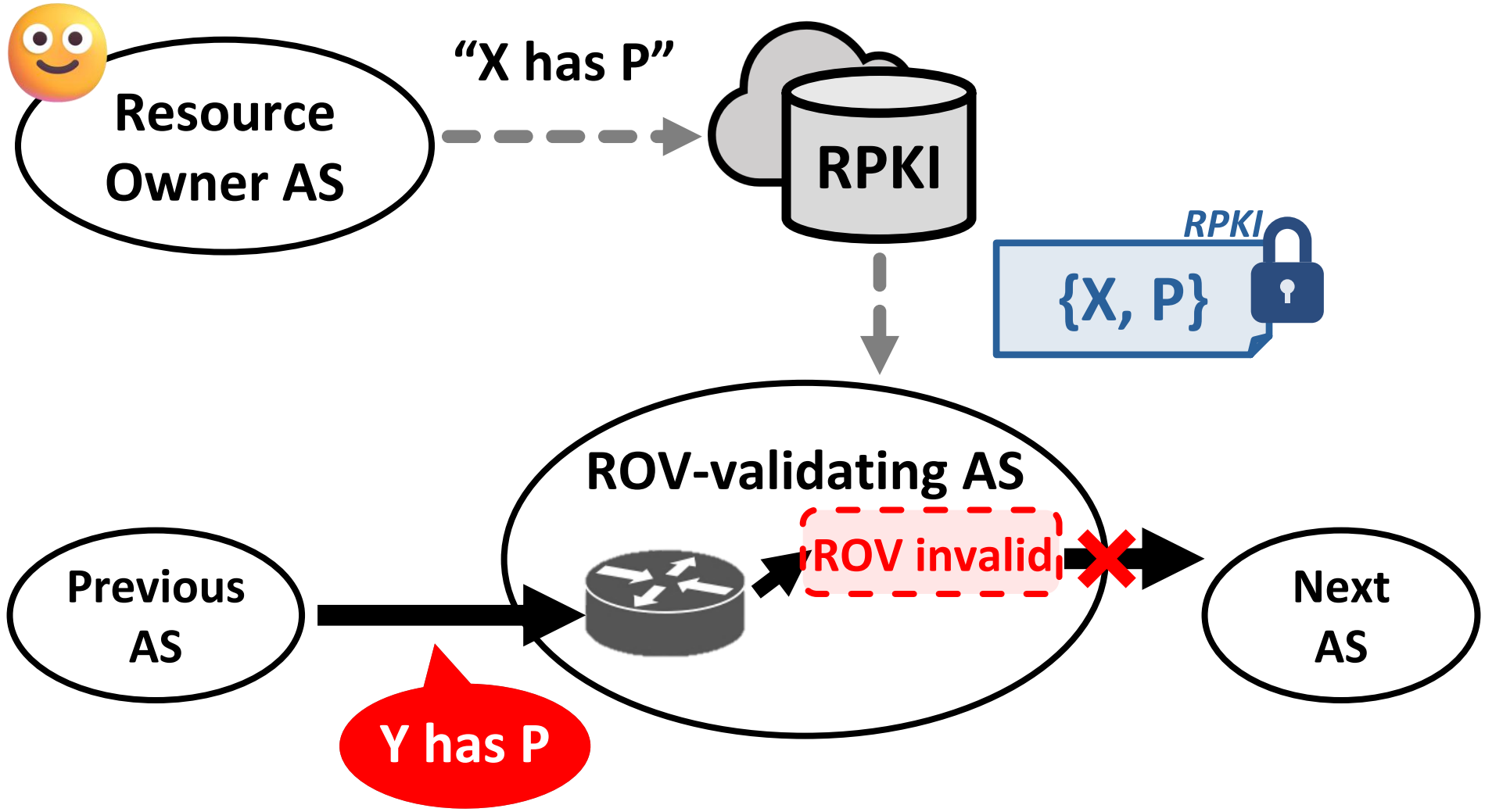
ROV ***Silently Drops*** Invalid Announcements



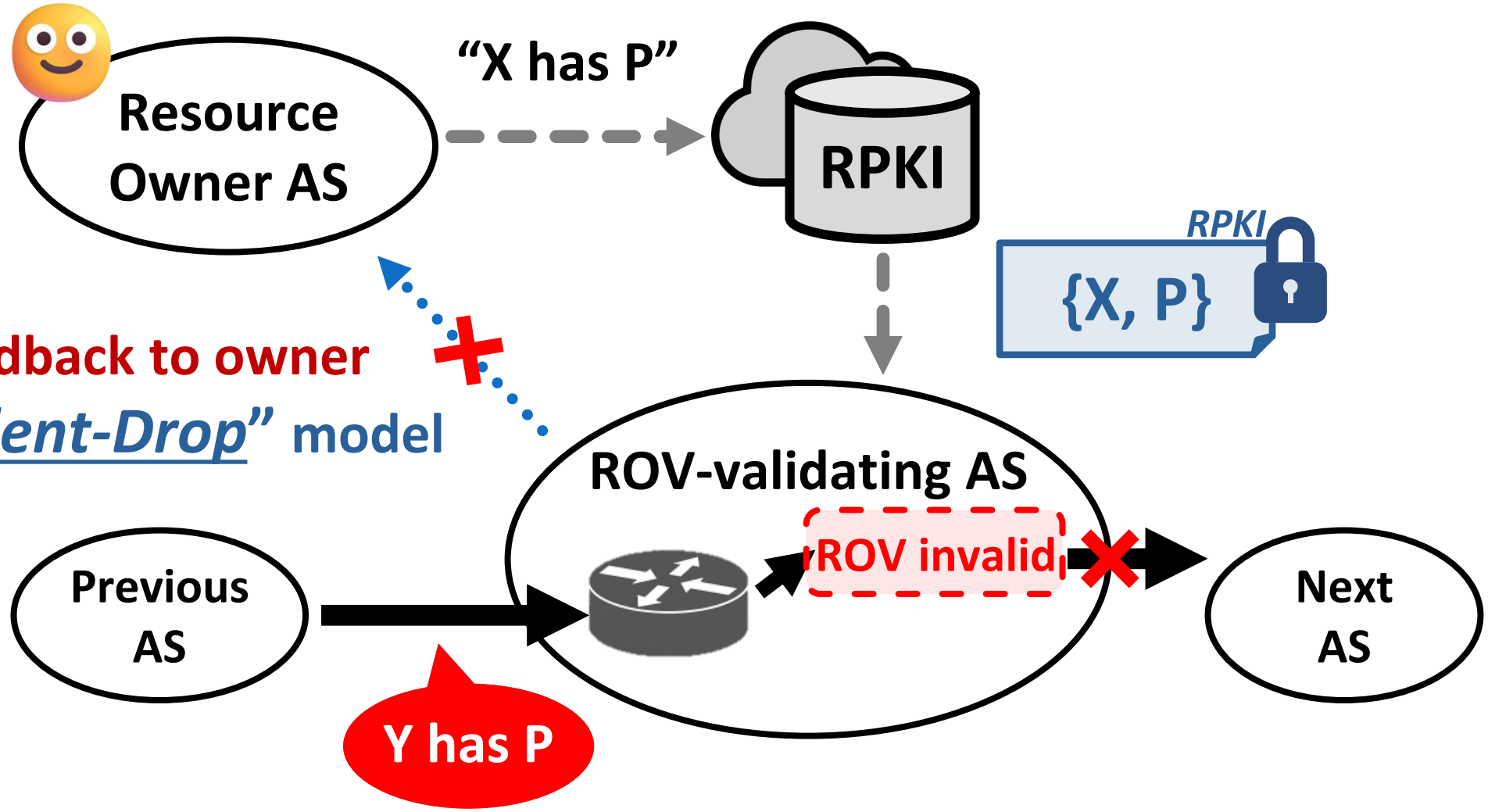
ROV ***Silently Drops*** Invalid Announcements



ROV ***Silently Drops*** Invalid Announcements

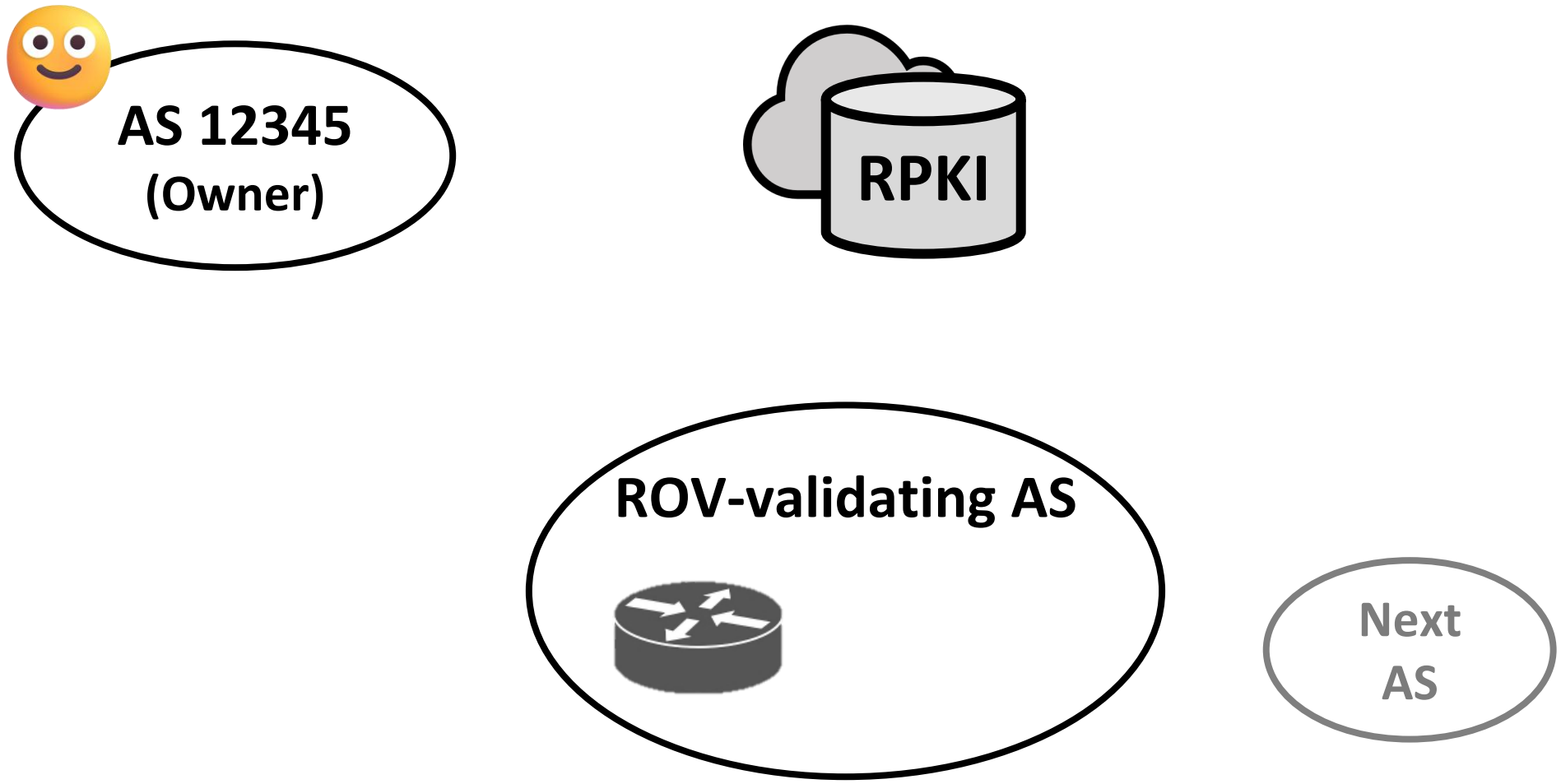


ROV ***Silently Drops*** Invalid Announcements



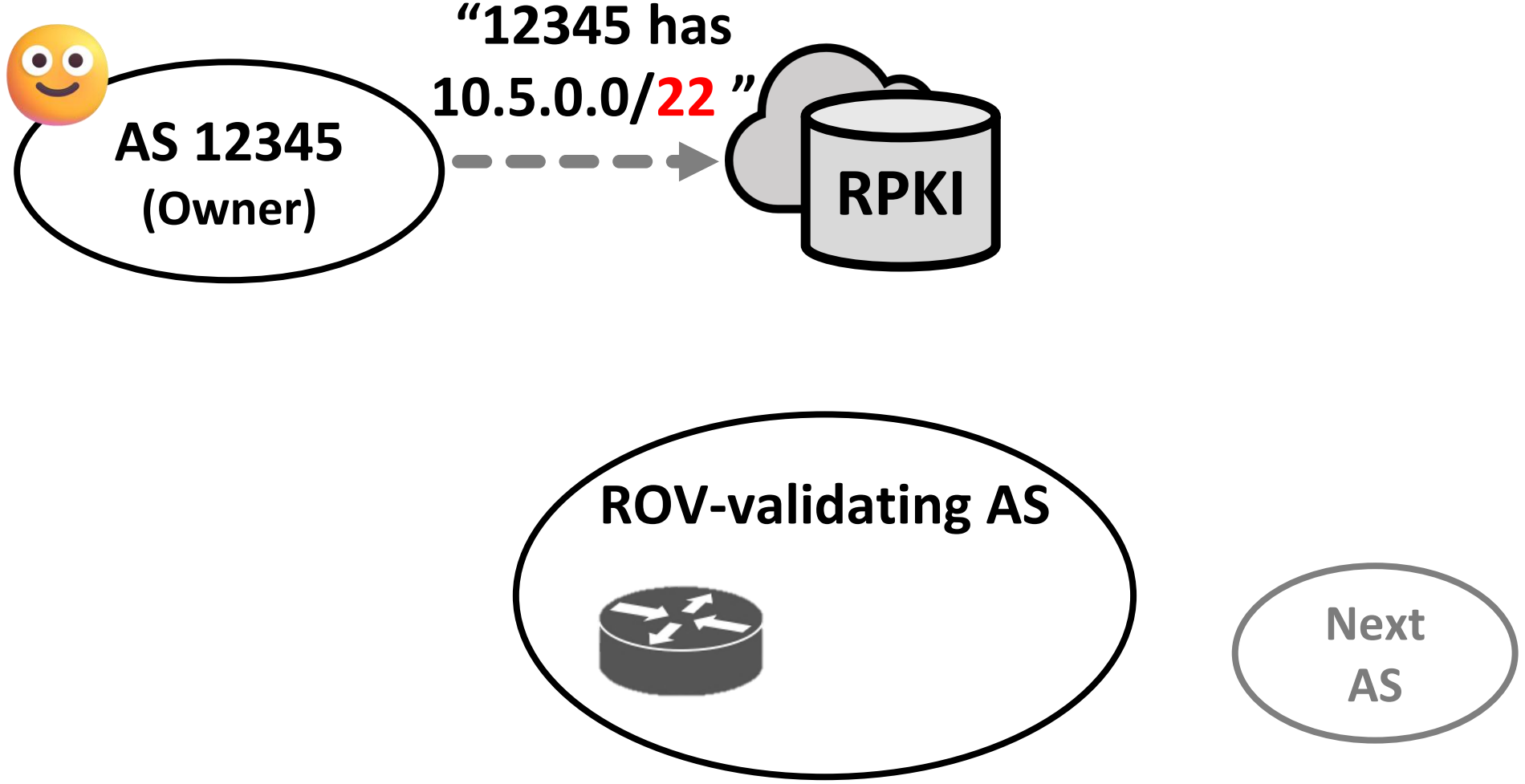
Challenges Due to ROV's Silent-Drop Model

[C1] Persistent misconfigurations: MaxLength typo etc.



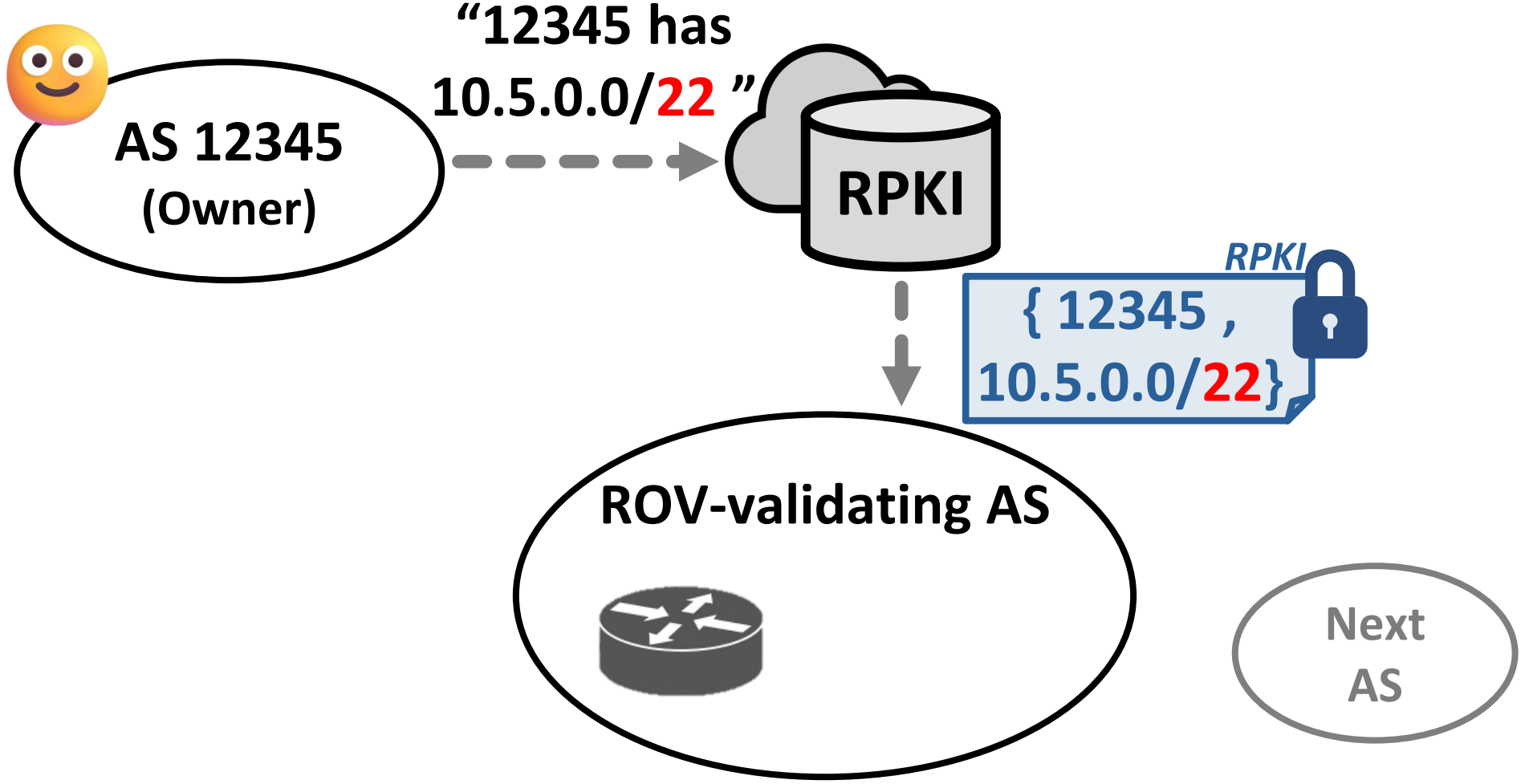
Challenges Due to ROV's Silent-Drop Model

[C1] Persistent misconfigurations: MaxLength typo etc.



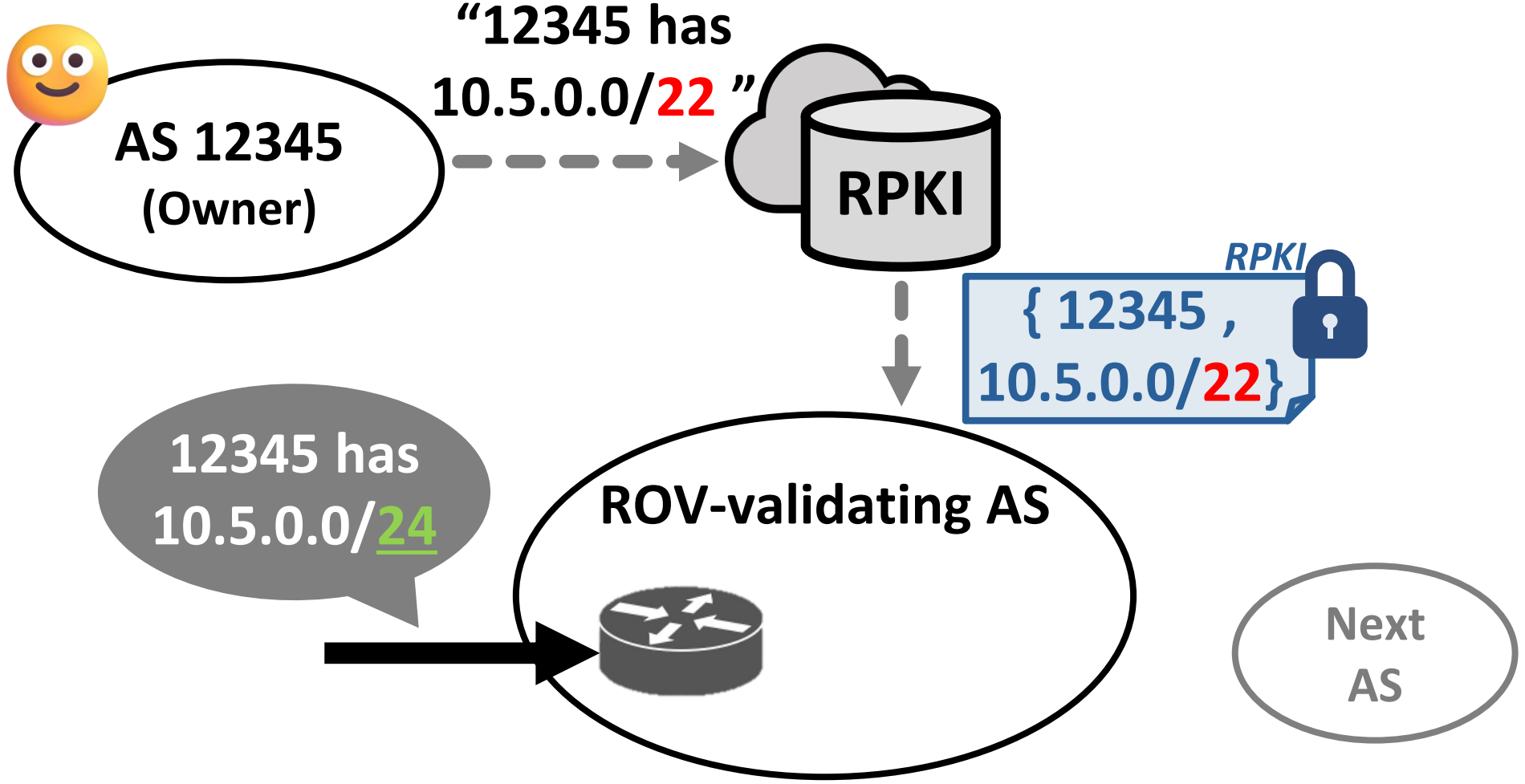
Challenges Due to ROV's Silent-Drop Model

[C1] Persistent misconfigurations: MaxLength typo etc.



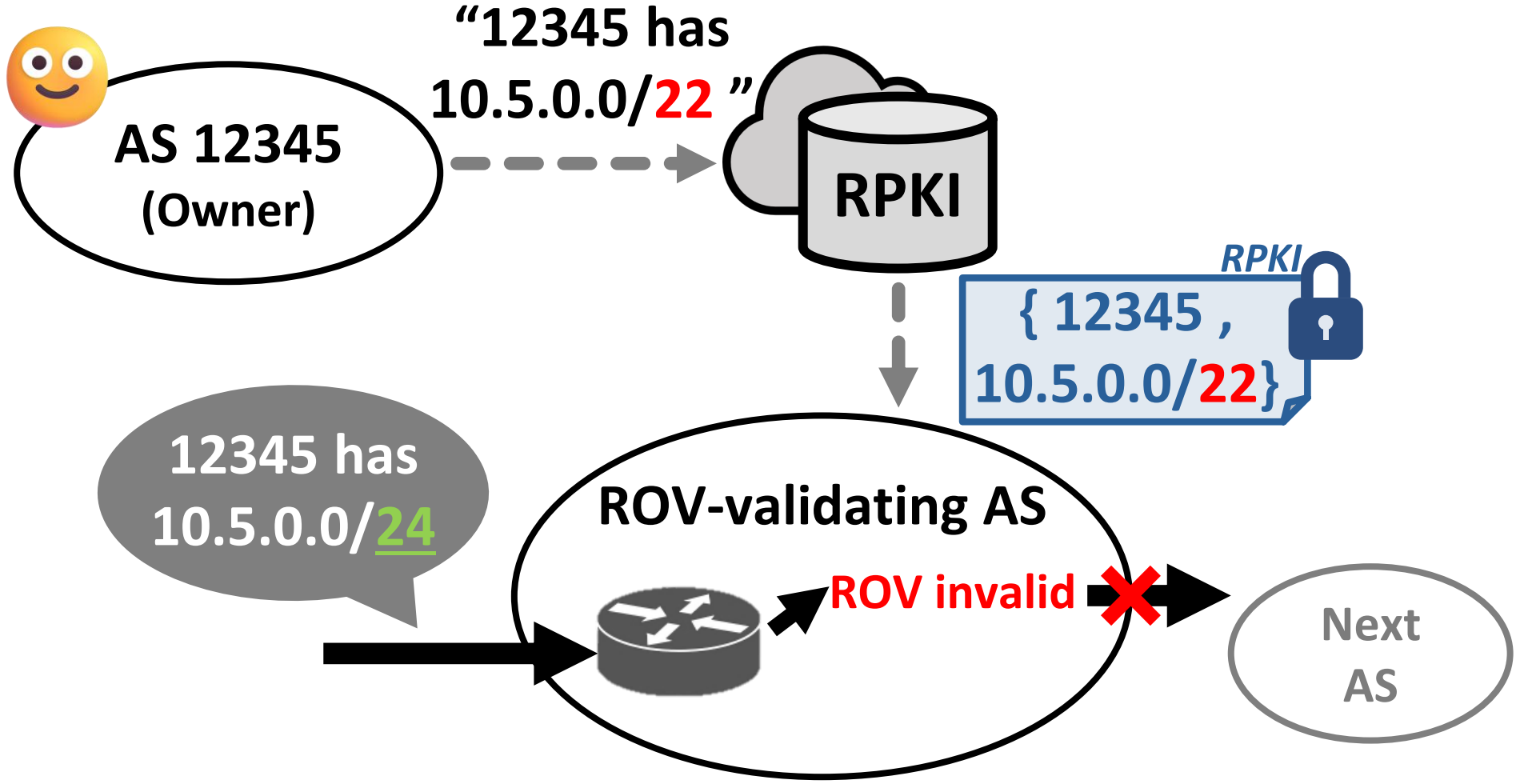
Challenges Due to ROV's Silent-Drop Model

[C1] Persistent misconfigurations: MaxLength typo etc.



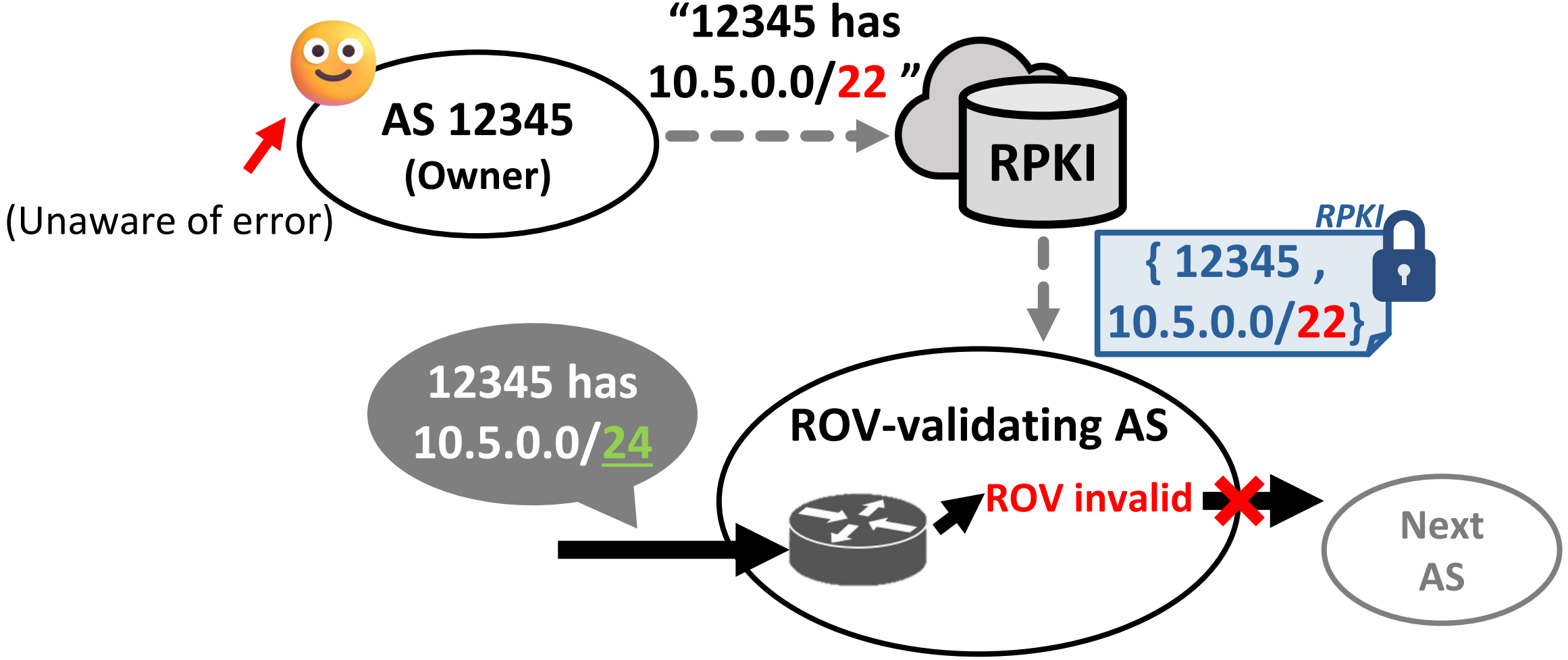
Challenges Due to ROV's Silent-Drop Model

[C1] Persistent misconfigurations: MaxLength typo etc.



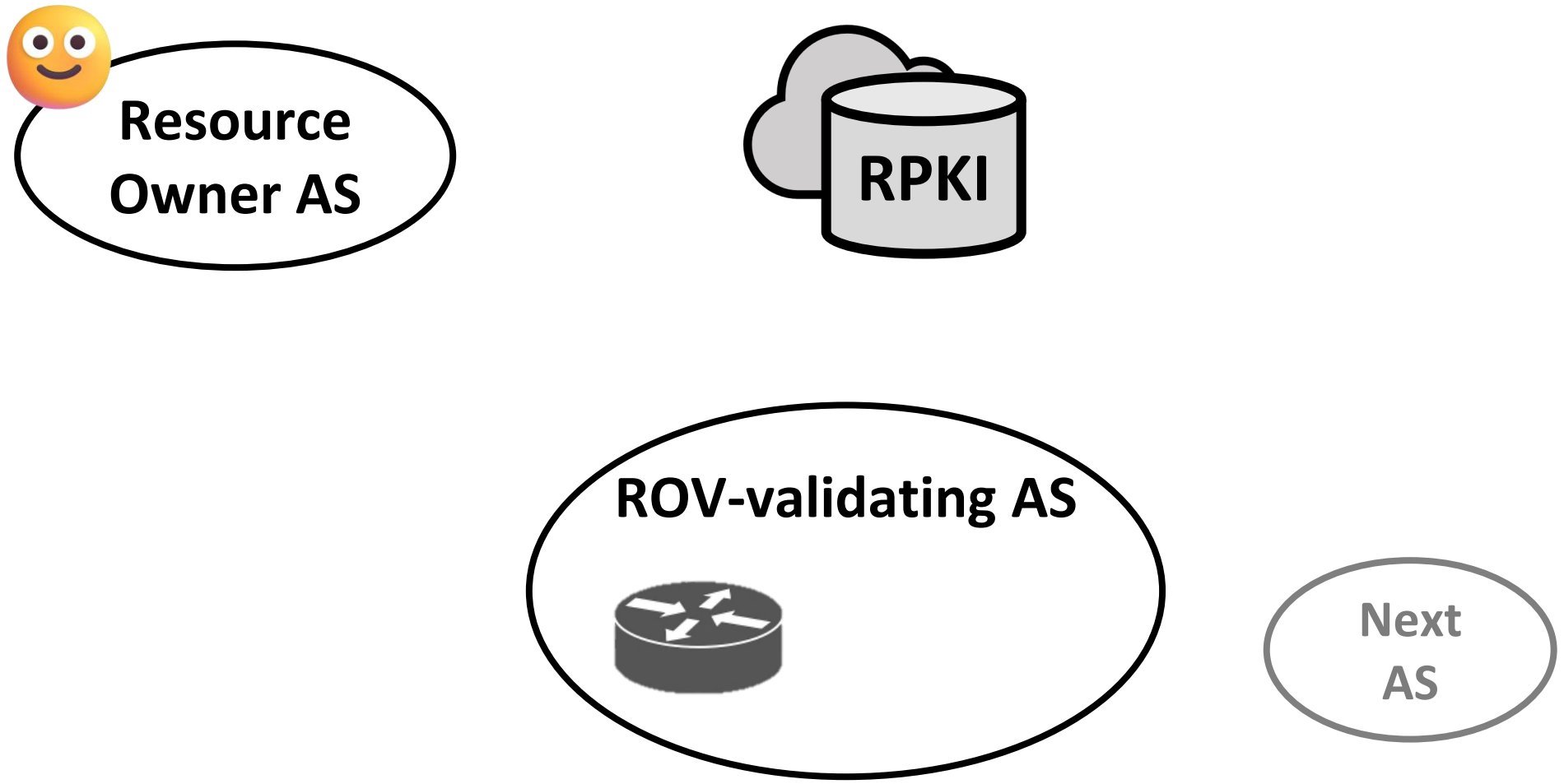
Challenges Due to ROV's Silent-Drop Model

[C1] Persistent misconfigurations: MaxLength typo etc.



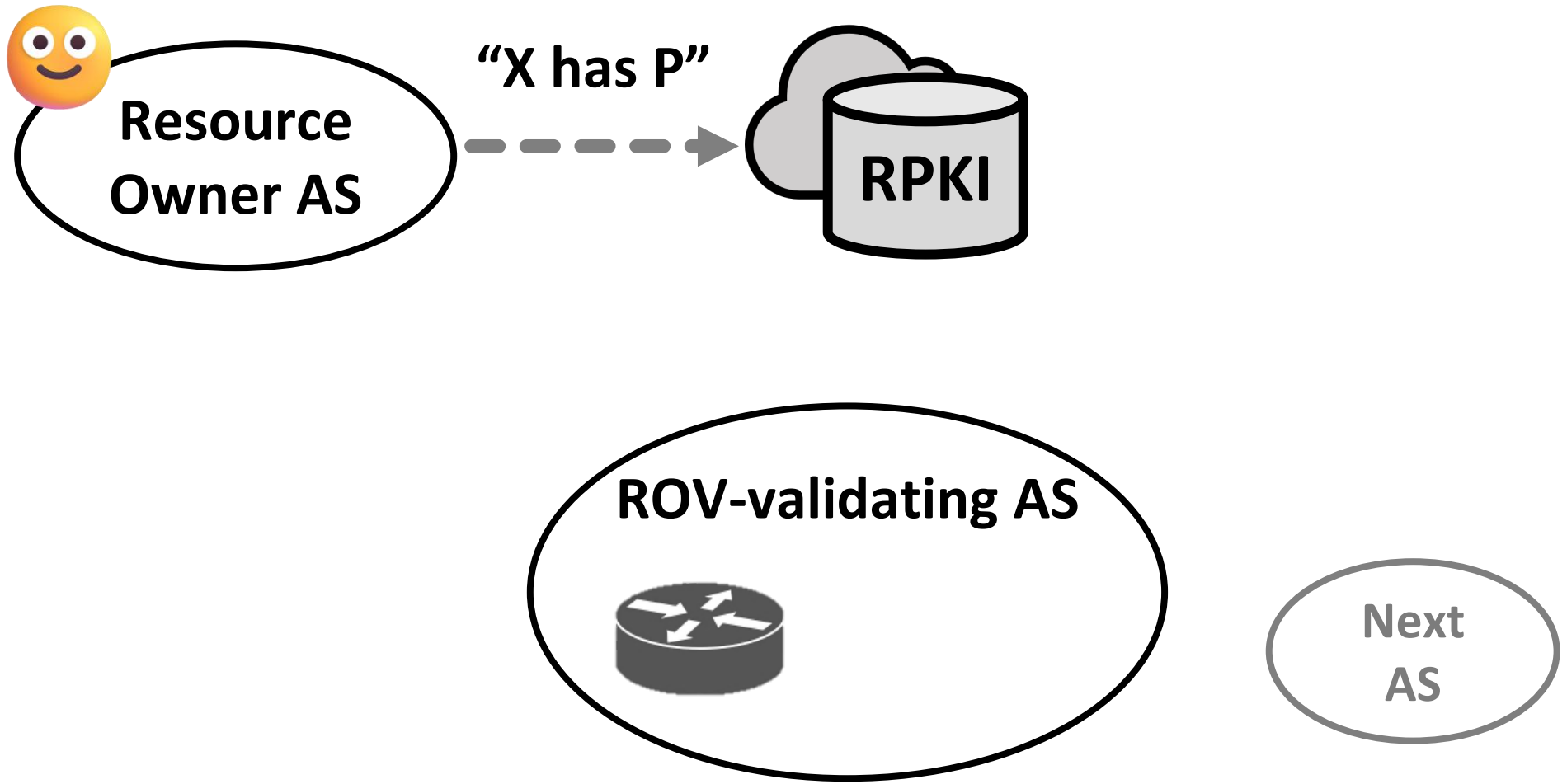
Challenges Due to ROV's Silent-Drop Model

[C2] Limited Attack Visibility



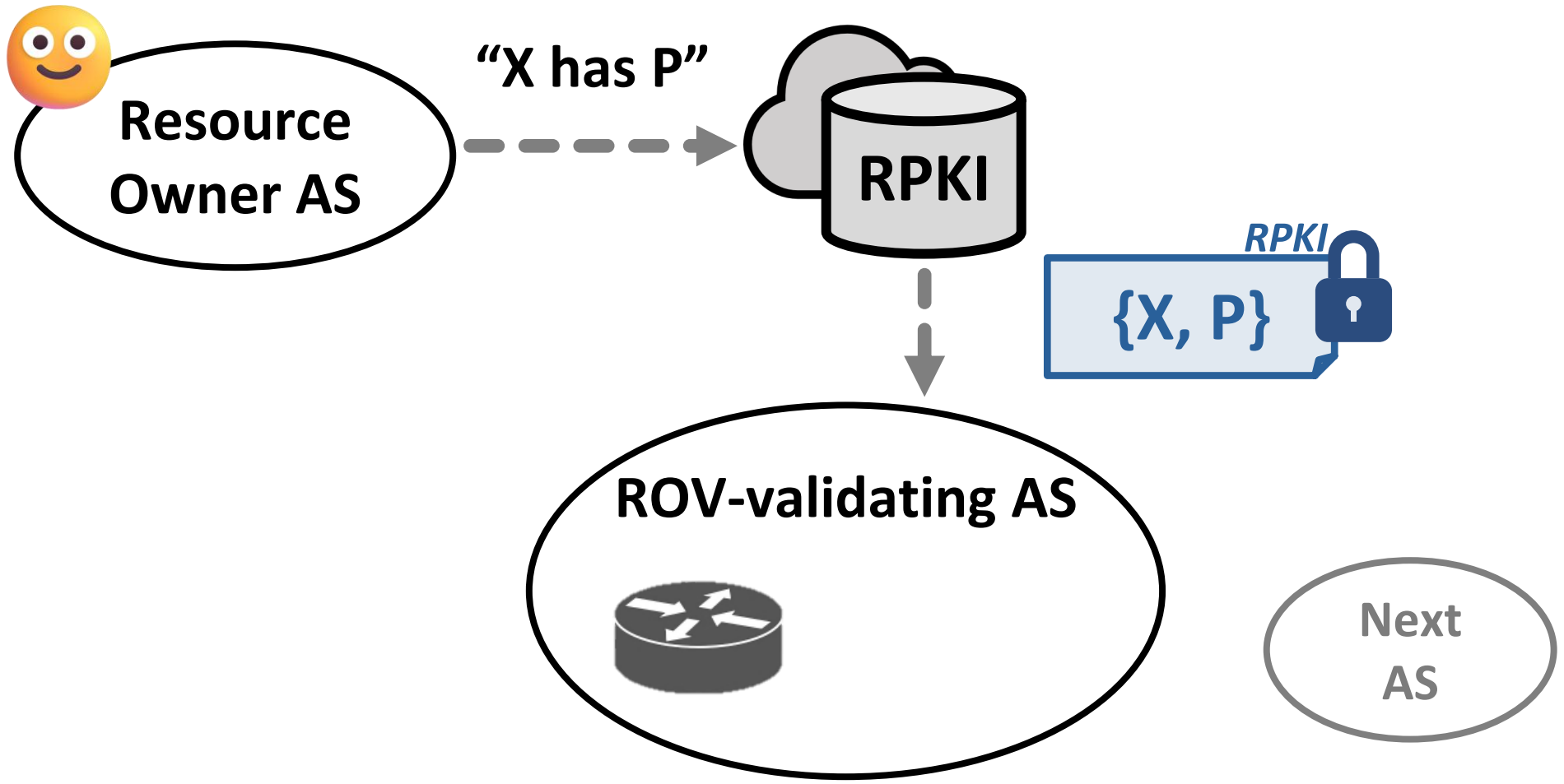
Challenges Due to ROV's Silent-Drop Model

[C2] Limited Attack Visibility



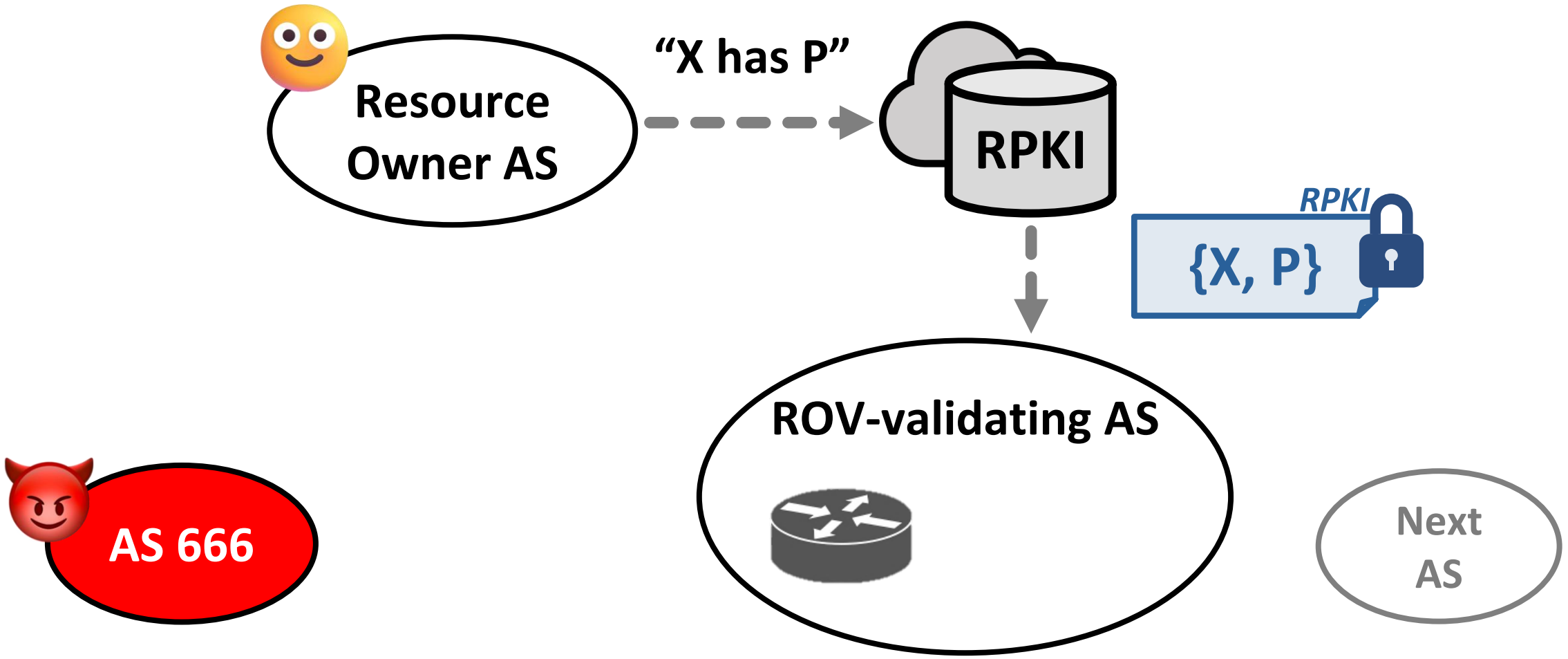
Challenges Due to ROV's Silent-Drop Model

[C2] Limited Attack Visibility



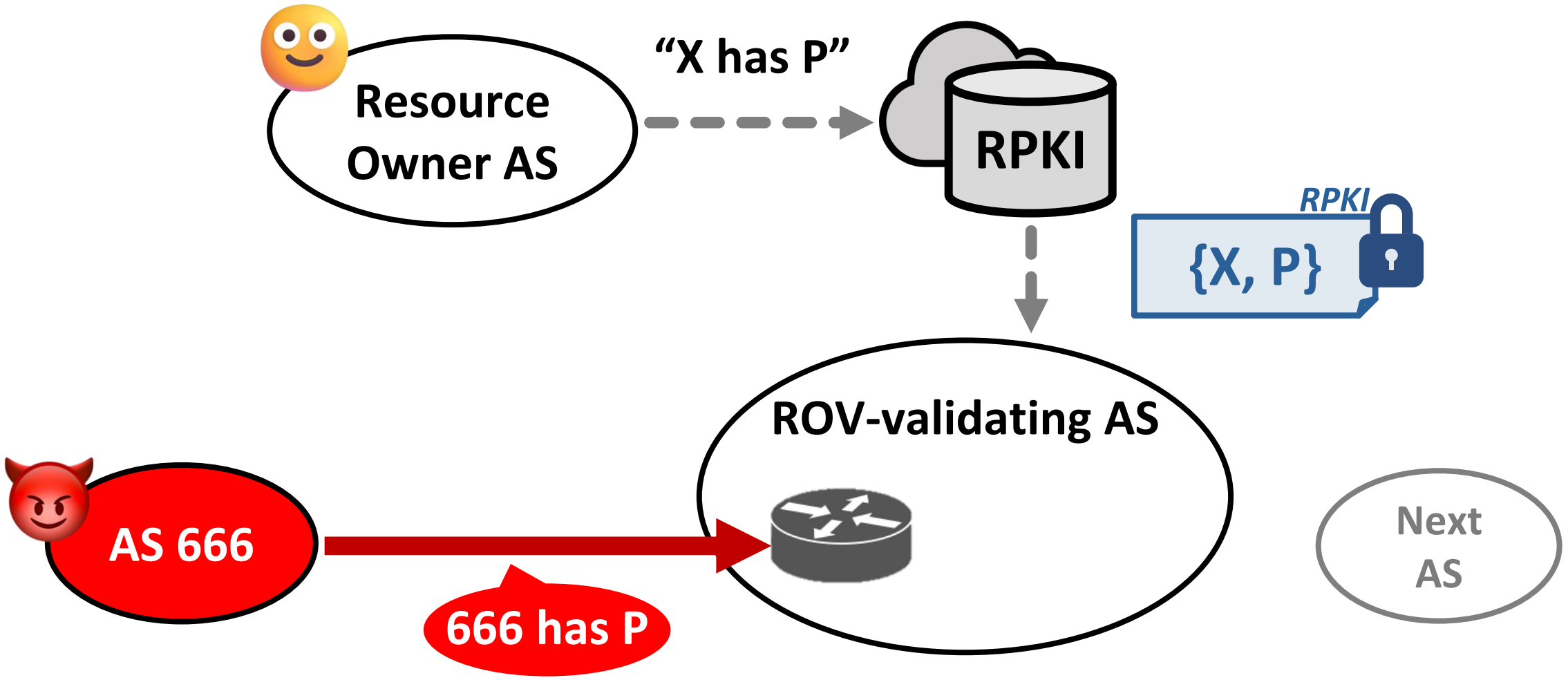
Challenges Due to ROV's Silent-Drop Model

[C2] Limited Attack Visibility



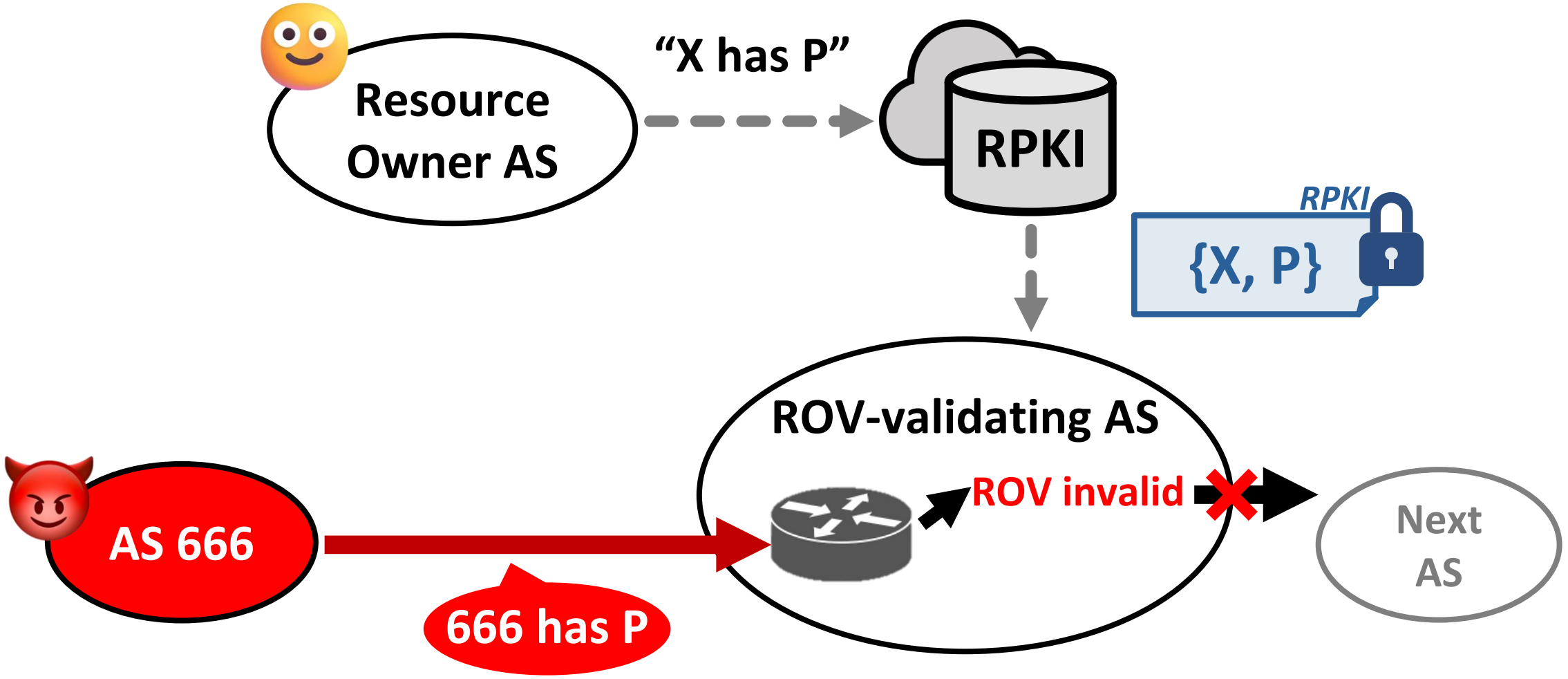
Challenges Due to ROV's Silent-Drop Model

[C2] Limited Attack Visibility



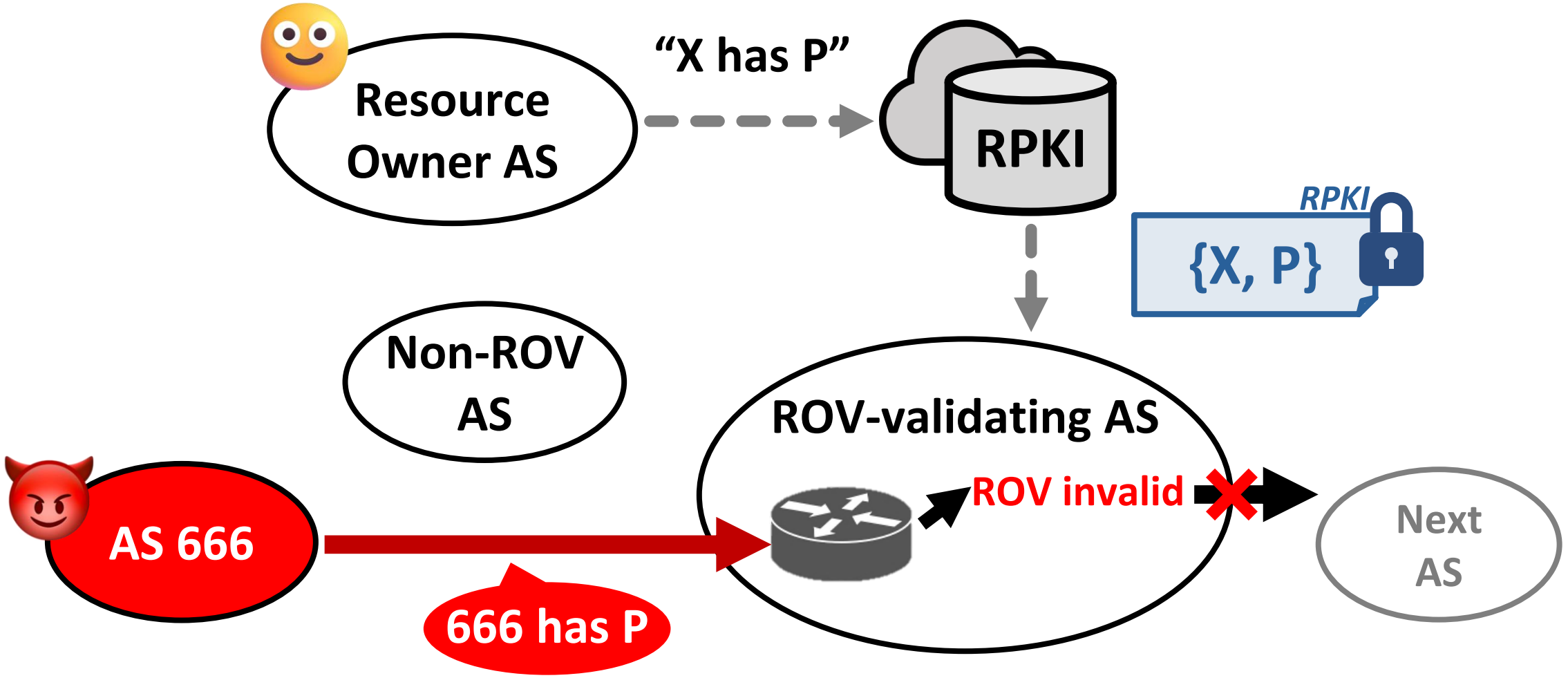
Challenges Due to ROV's Silent-Drop Model

[C2] Limited Attack Visibility



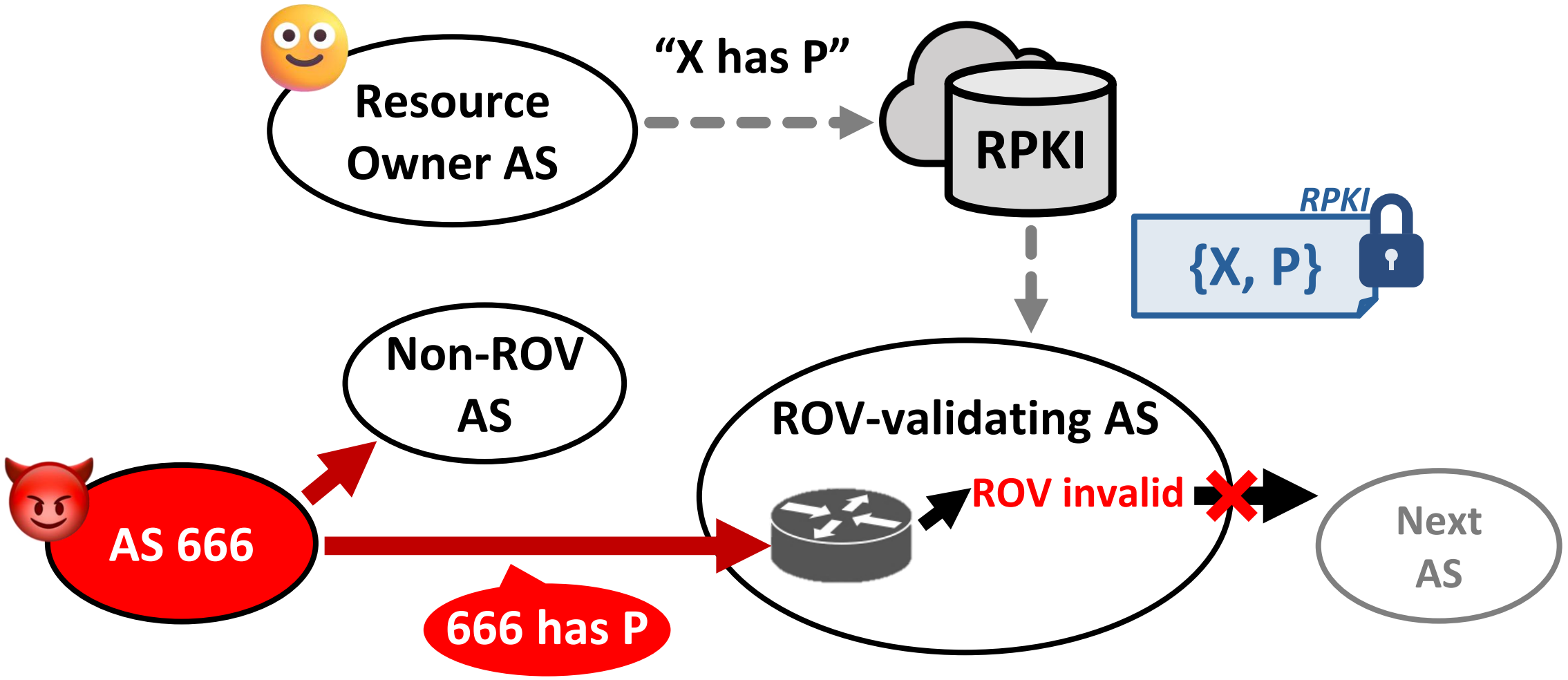
Challenges Due to ROV's Silent-Drop Model

[C2] Limited Attack Visibility



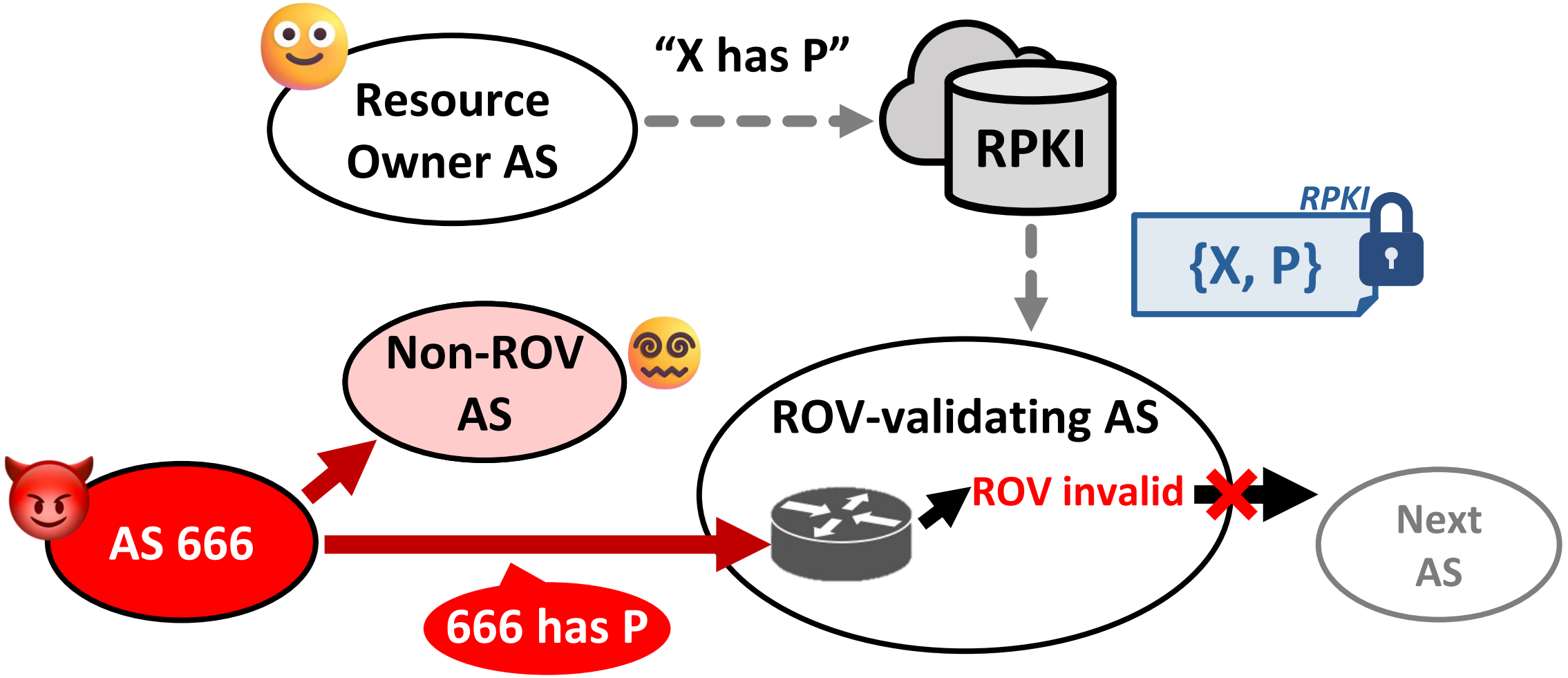
Challenges Due to ROV's Silent-Drop Model

[C2] Limited Attack Visibility



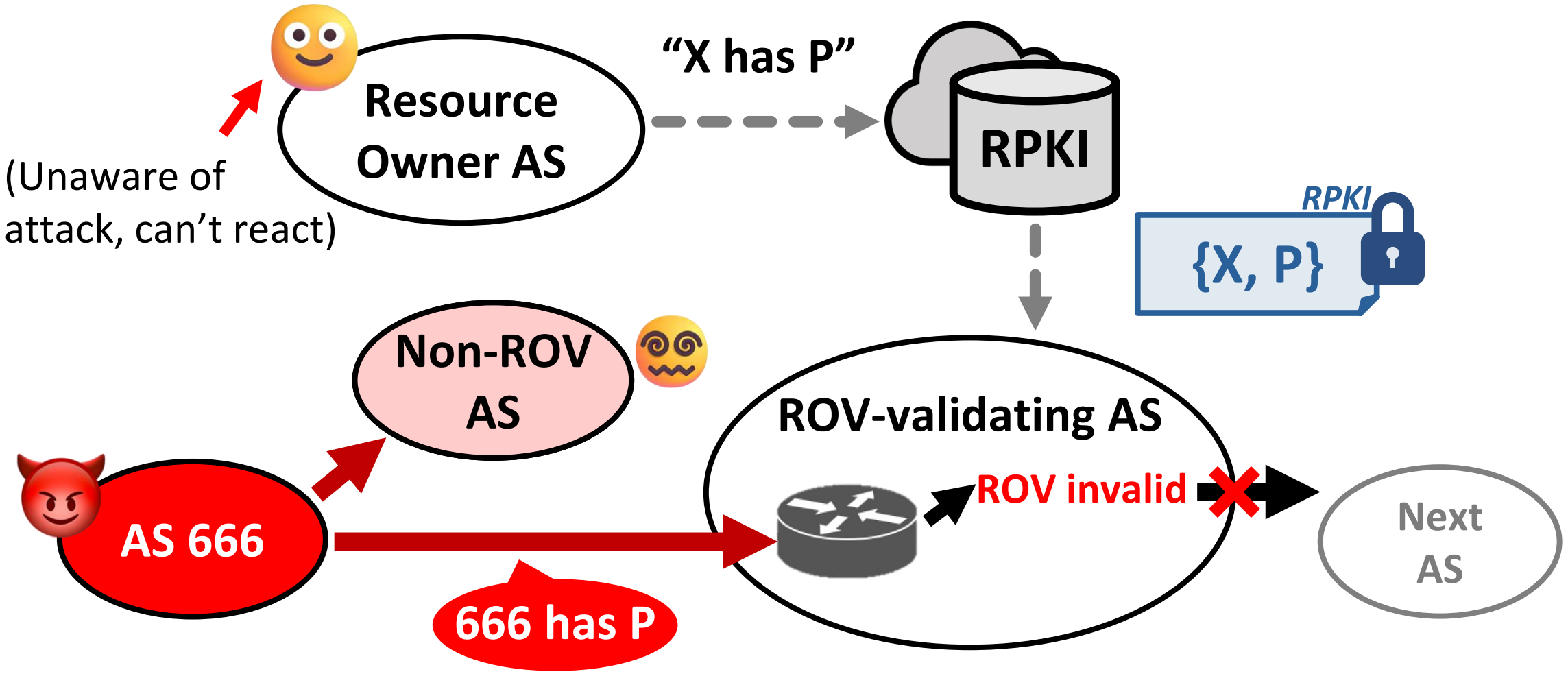
Challenges Due to ROV's Silent-Drop Model

[C2] Limited Attack Visibility



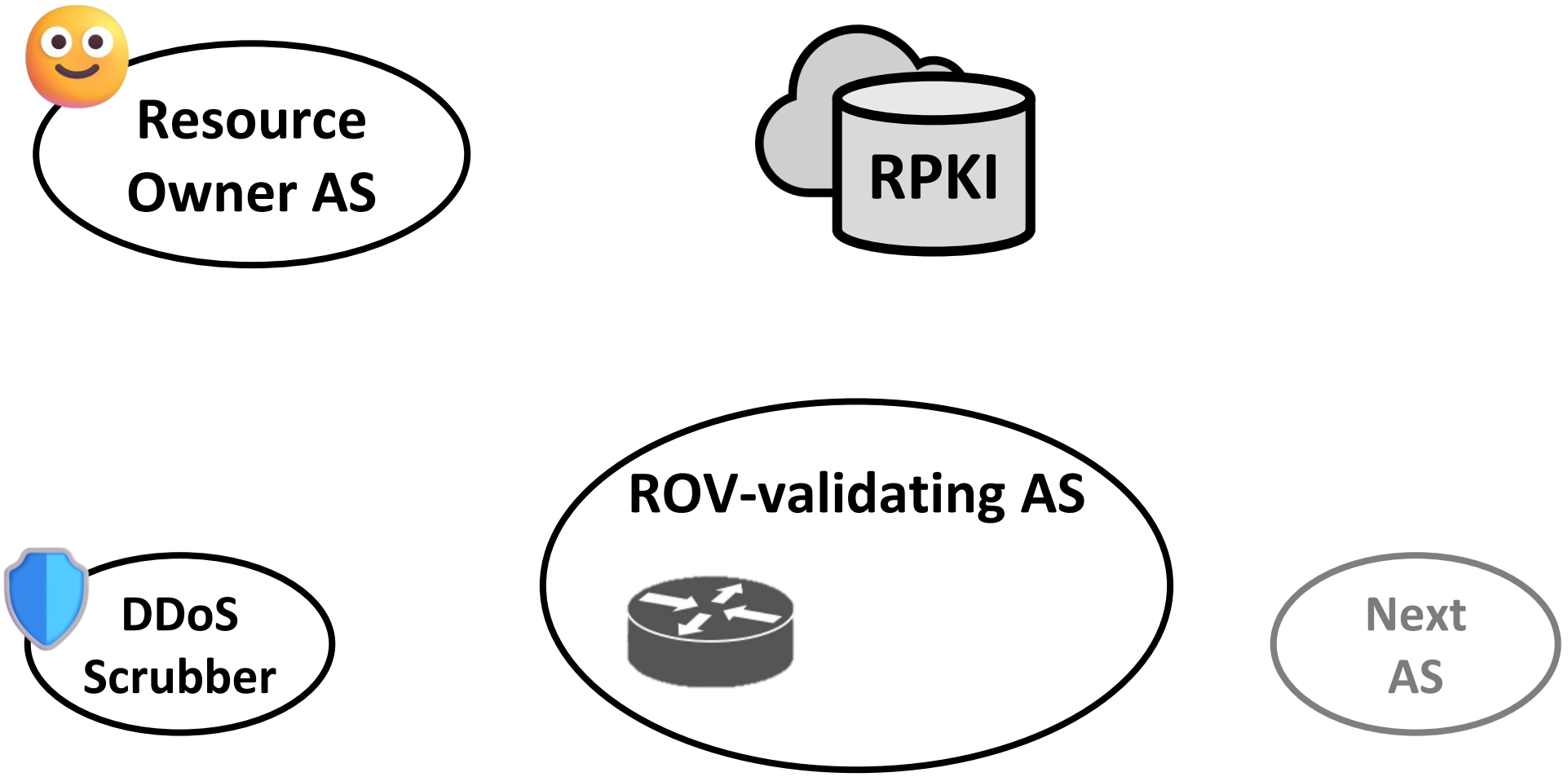
Challenges Due to ROV's Silent-Drop Model

[C2] Limited Attack Visibility



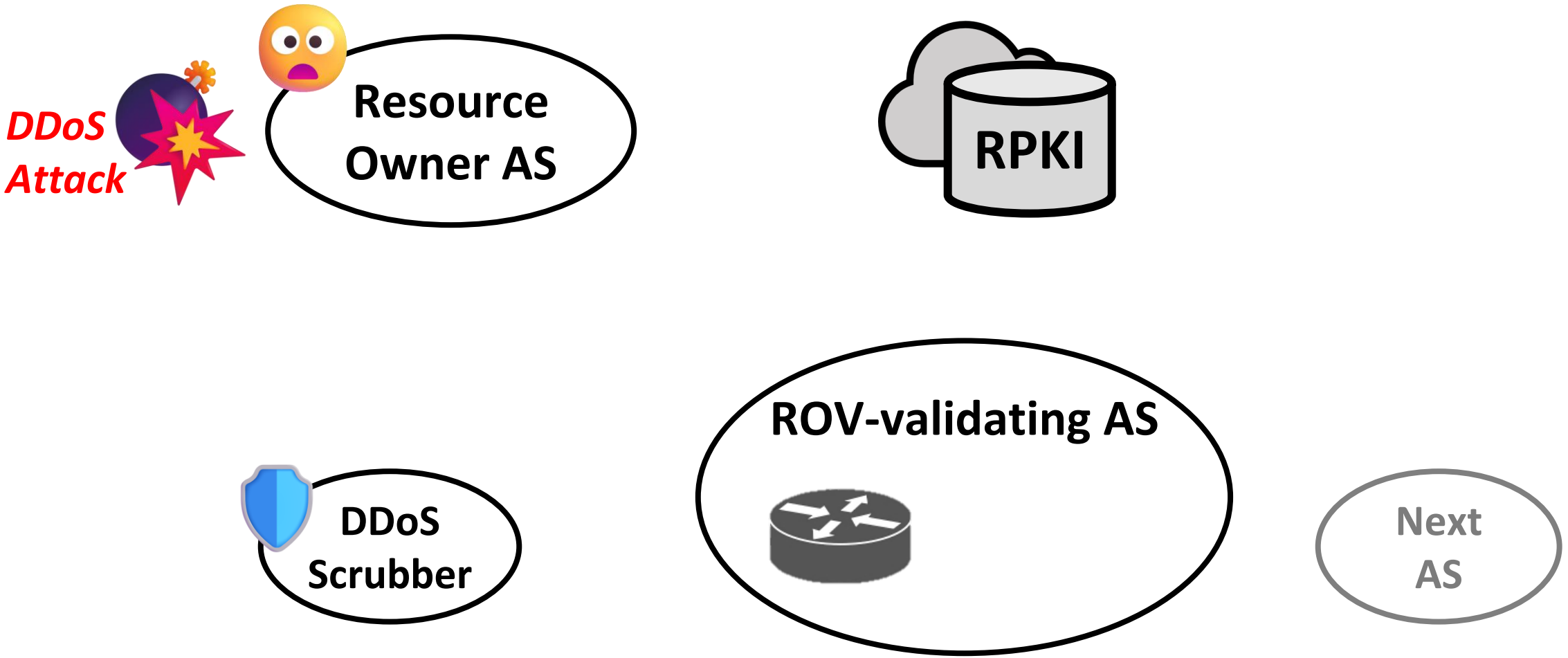
Challenges Due to ROV's Silent-Drop Model

[C3] Inability to authorize urgent route changes



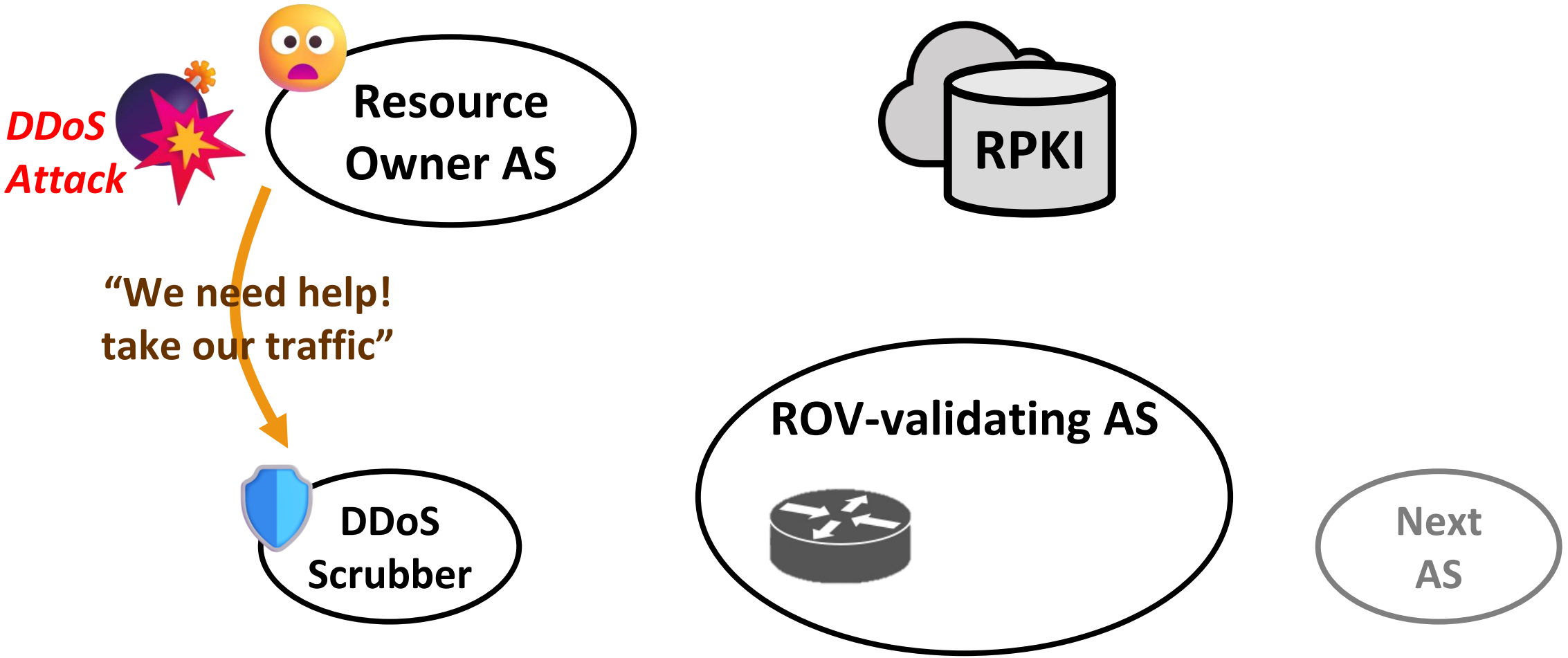
Challenges Due to ROV's Silent-Drop Model

[C3] Inability to authorize urgent route changes



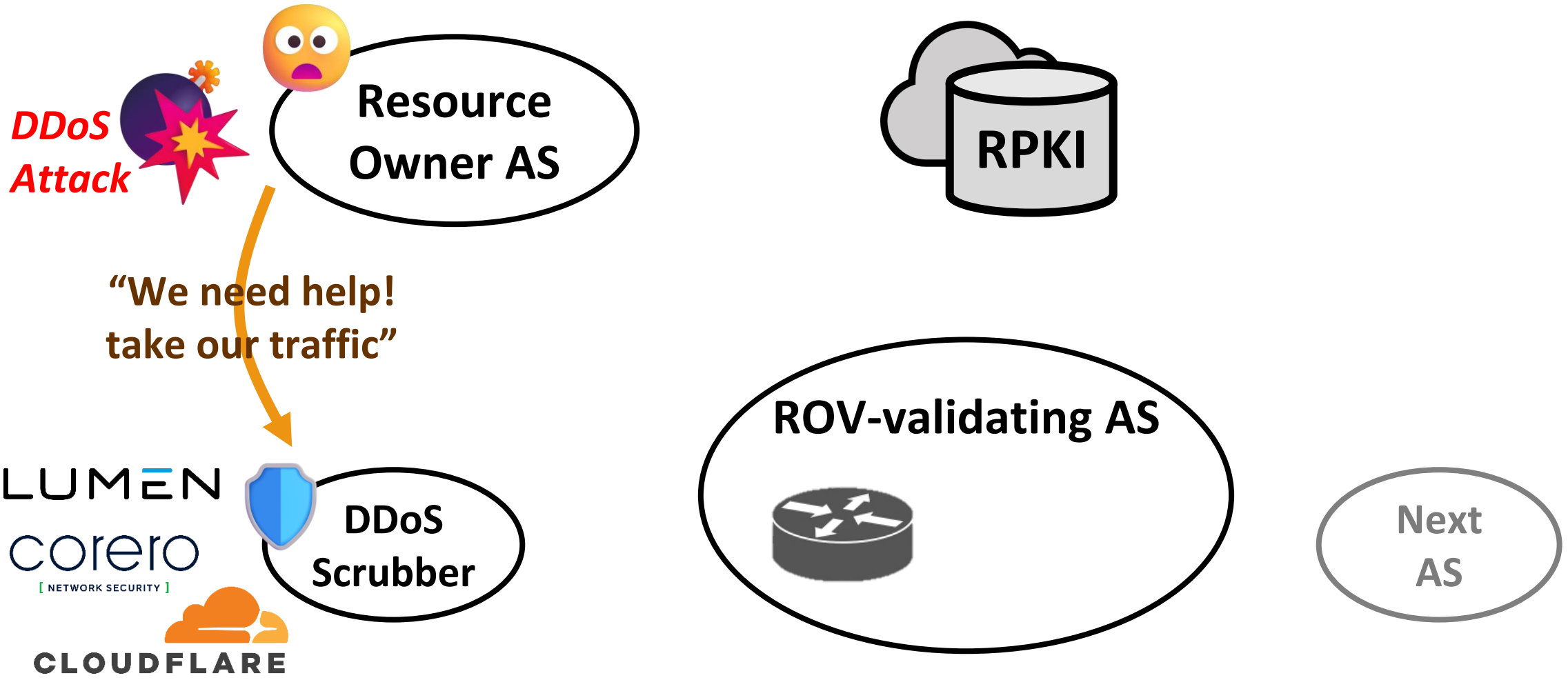
Challenges Due to ROV's Silent-Drop Model

[C3] Inability to authorize urgent route changes



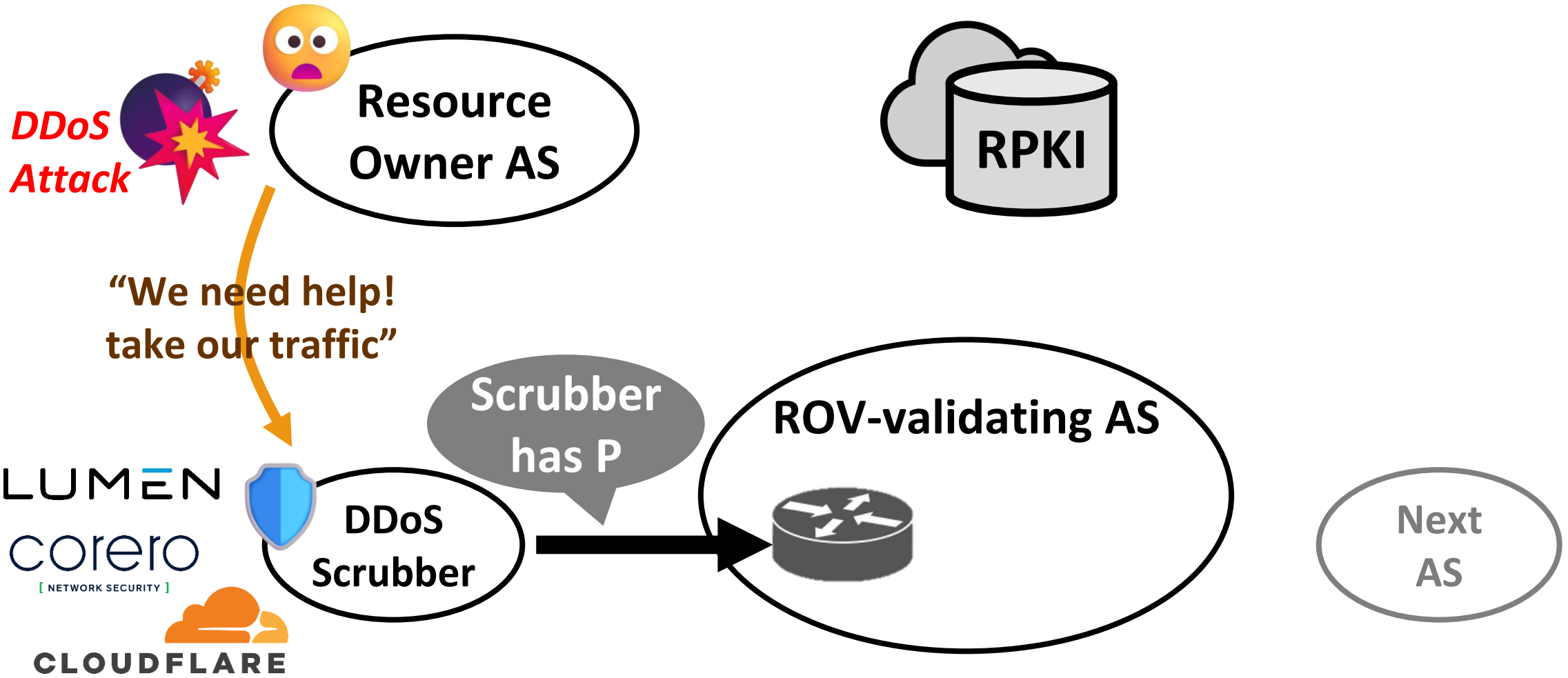
Challenges Due to ROV's Silent-Drop Model

[C3] Inability to authorize urgent route changes



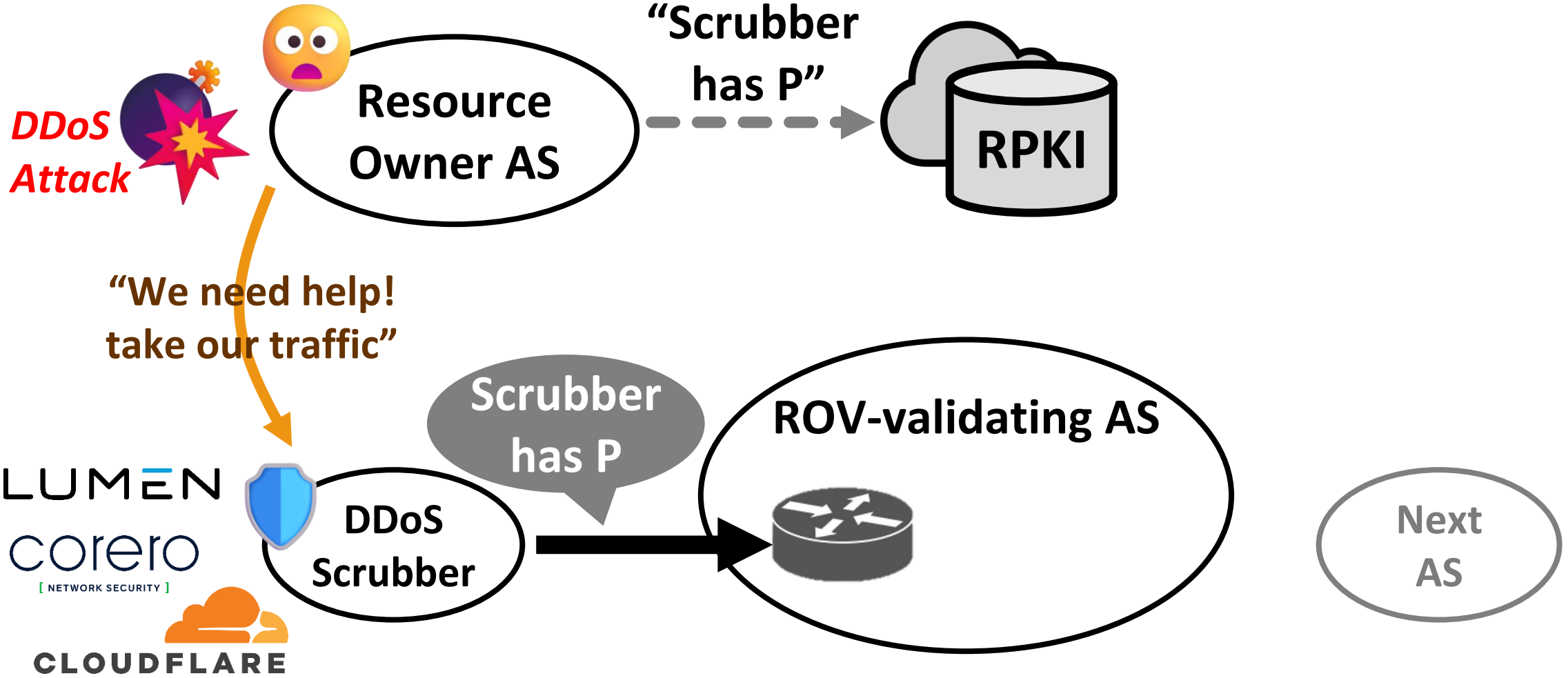
Challenges Due to ROV's Silent-Drop Model

[C3] Inability to authorize urgent route changes



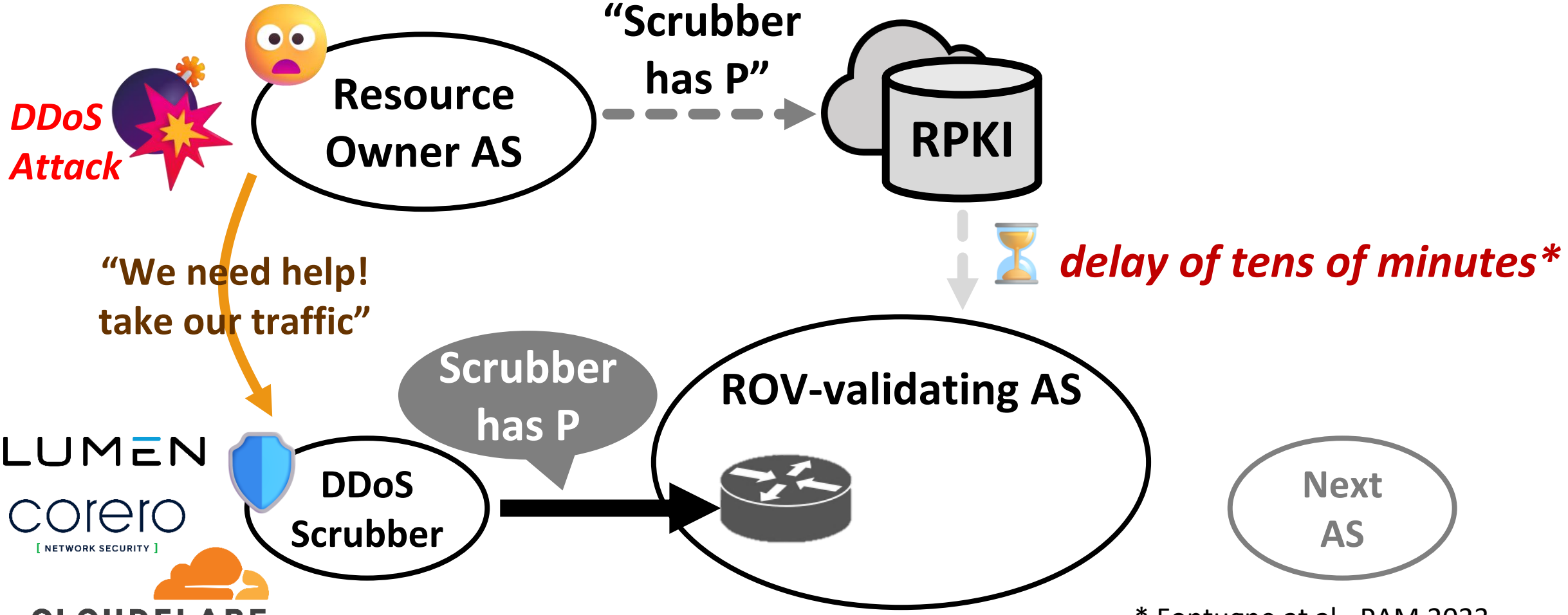
Challenges Due to ROV's Silent-Drop Model

[C3] Inability to authorize urgent route changes



Challenges Due to ROV's Silent-Drop Model

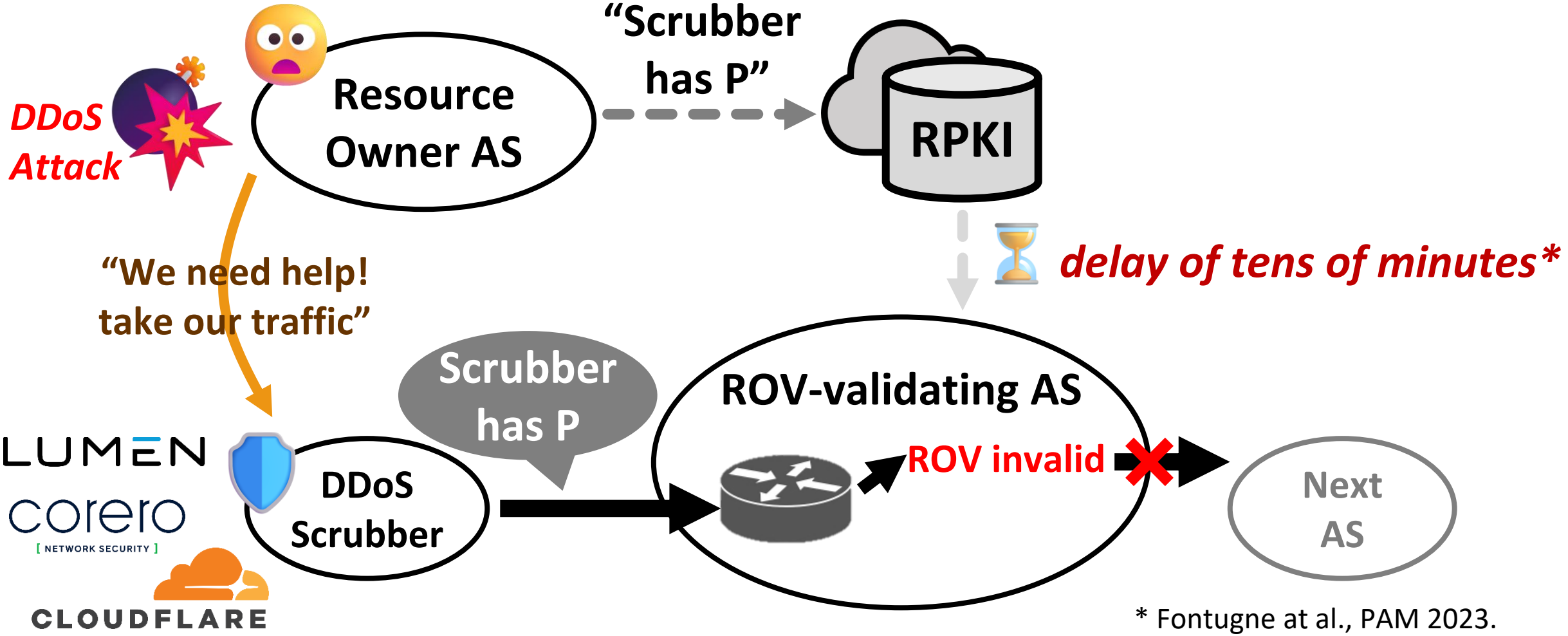
[C3] Inability to authorize urgent route changes



* Fontugne at al., PAM 2023.

Challenges Due to ROV's Silent-Drop Model

[C3] Inability to authorize urgent route changes



* Fontugne at al., PAM 2023.

Challenges Due to ROV's Silent-Drop Model

[C3] Inability to authorize urgent route changes

RPKI and Cloud DDoS Protection

Cloud DDoS protection is a popular mitigation strategy for ensuring service continuity against volumetric DDoS attacks that risk bandwidth or resource saturation. This is most commonly accomplished by using BGP advertisements to redirect traffic through the cloud DDoS provider either on-demand or at all times.

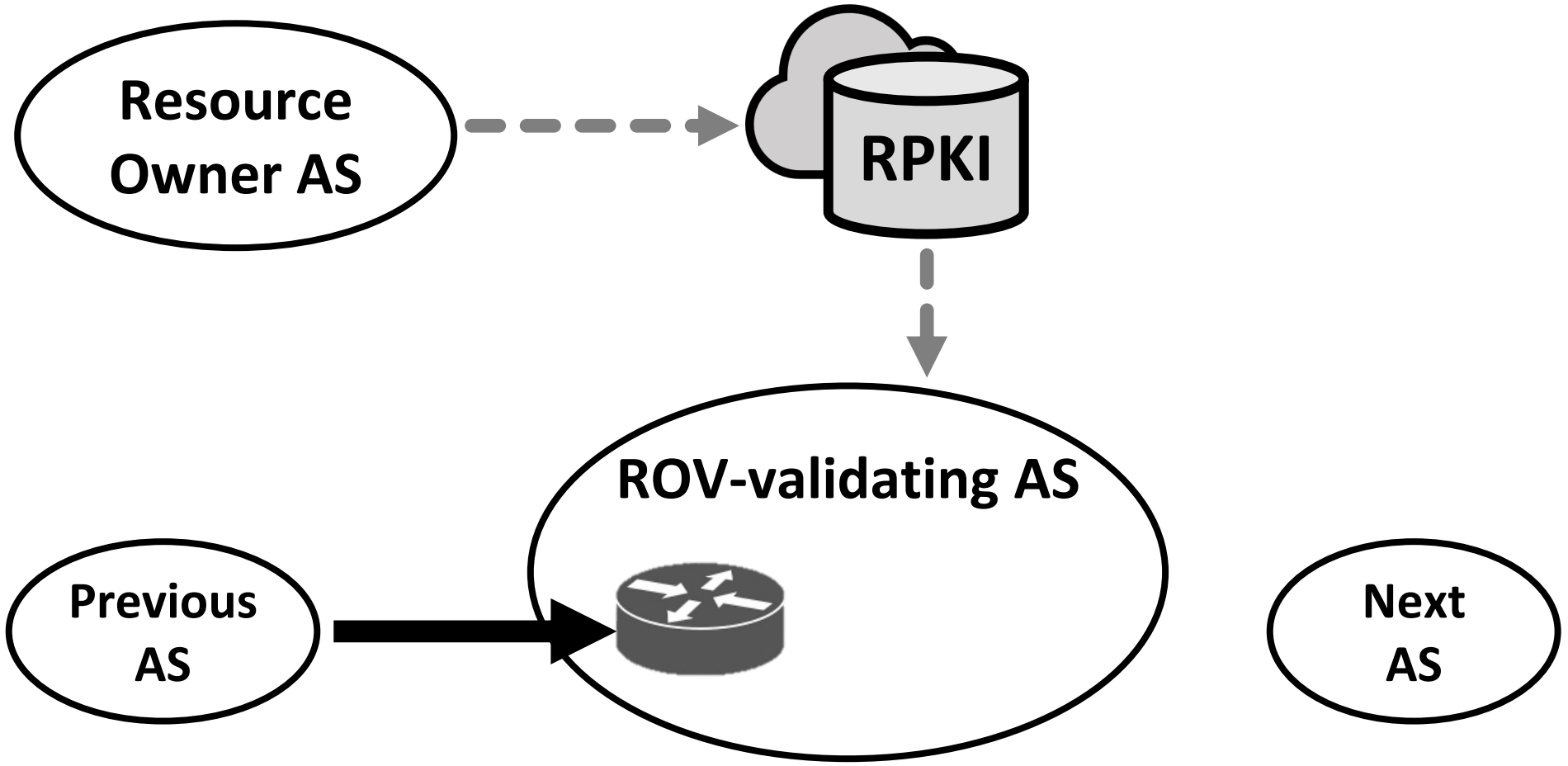
As RPKI Validation becomes more common, it's important to understand the implications of using a BGP-based cloud DDoS solution.

Most of these cloud DDoS services will include guidance or requirements for RPKI ROAs. This is important, as incorrect or misconfigured ROAs can at least reduce the efficacy of the cloud DDoS protection, or at worst cause actual harm to normal traffic.

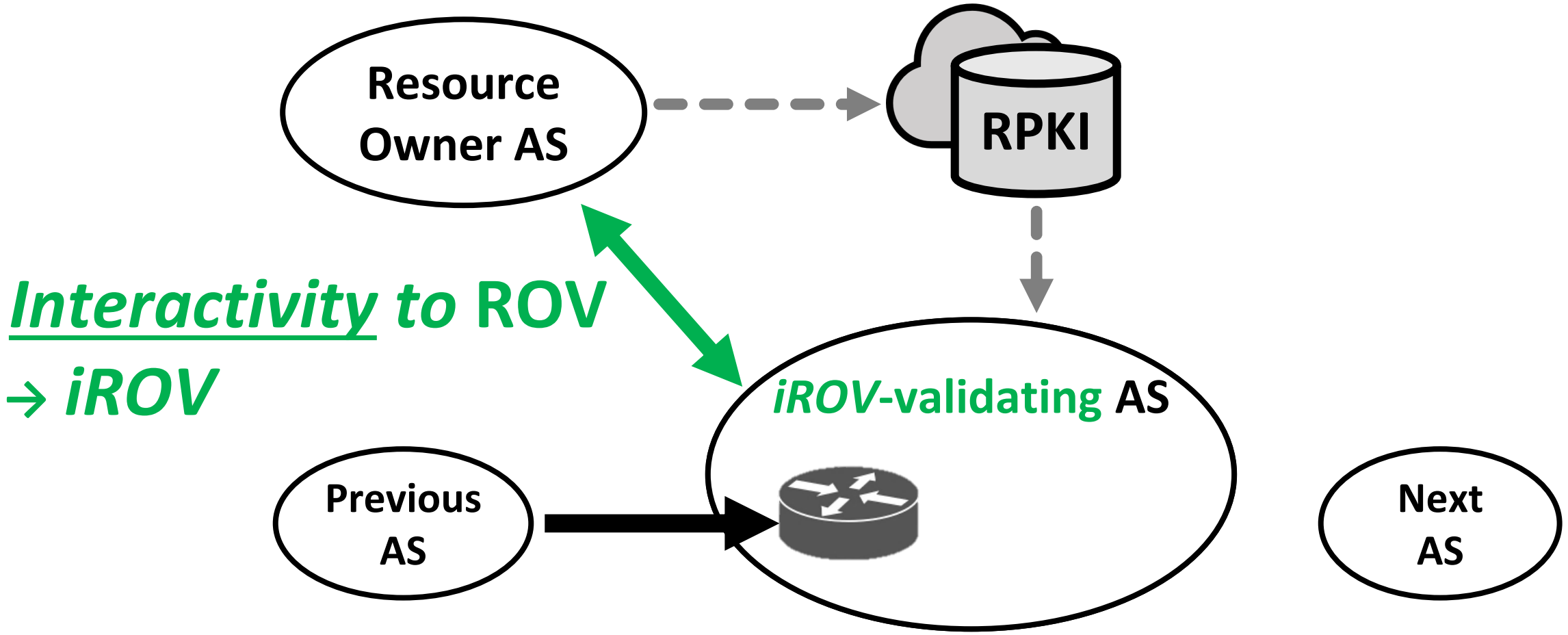
https://www.corero.com/rpki-and-cloud-ddos-protection/

* Fontugne at al., PAM 2023.

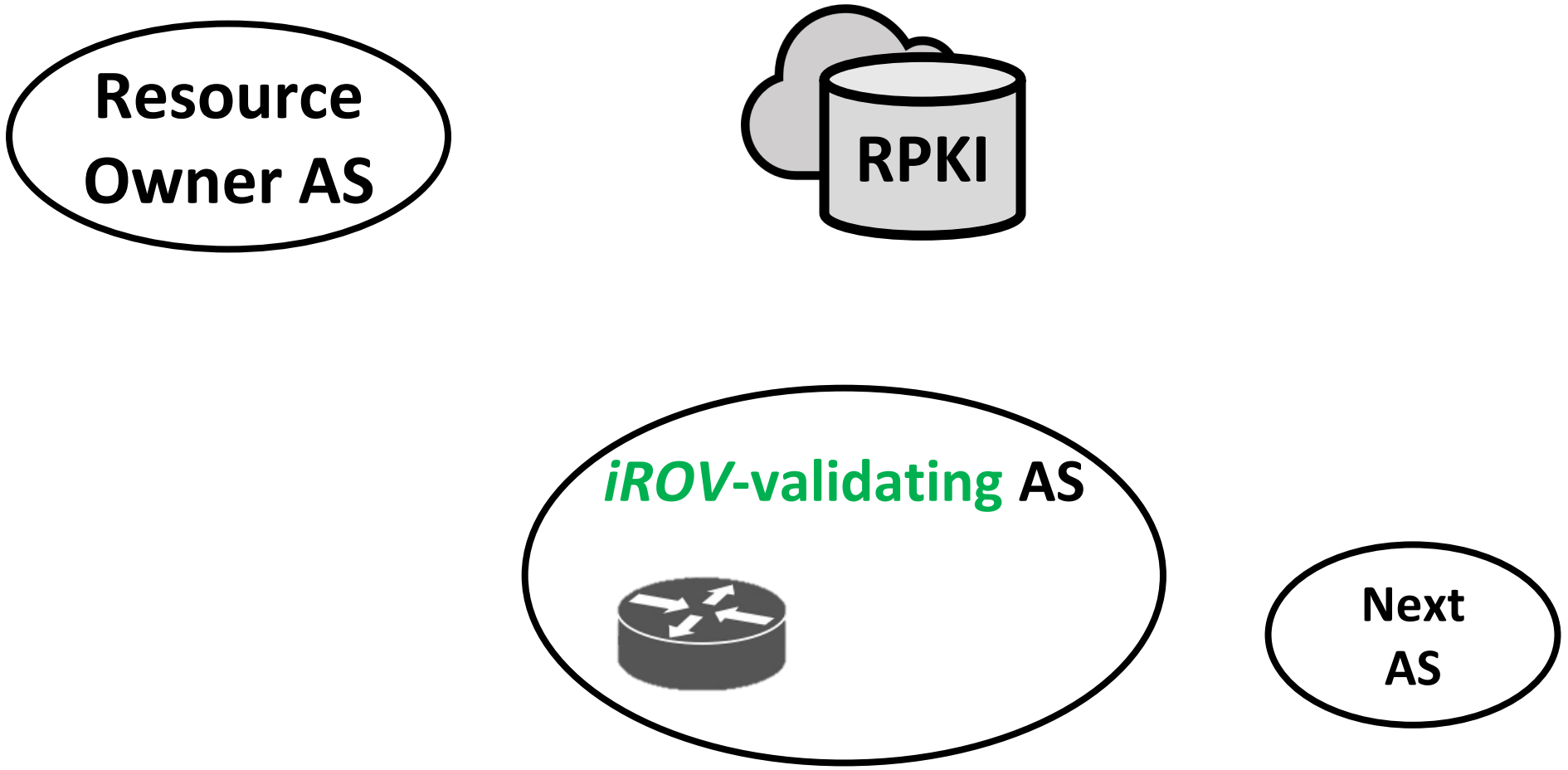
To address these challenges, we introduce:



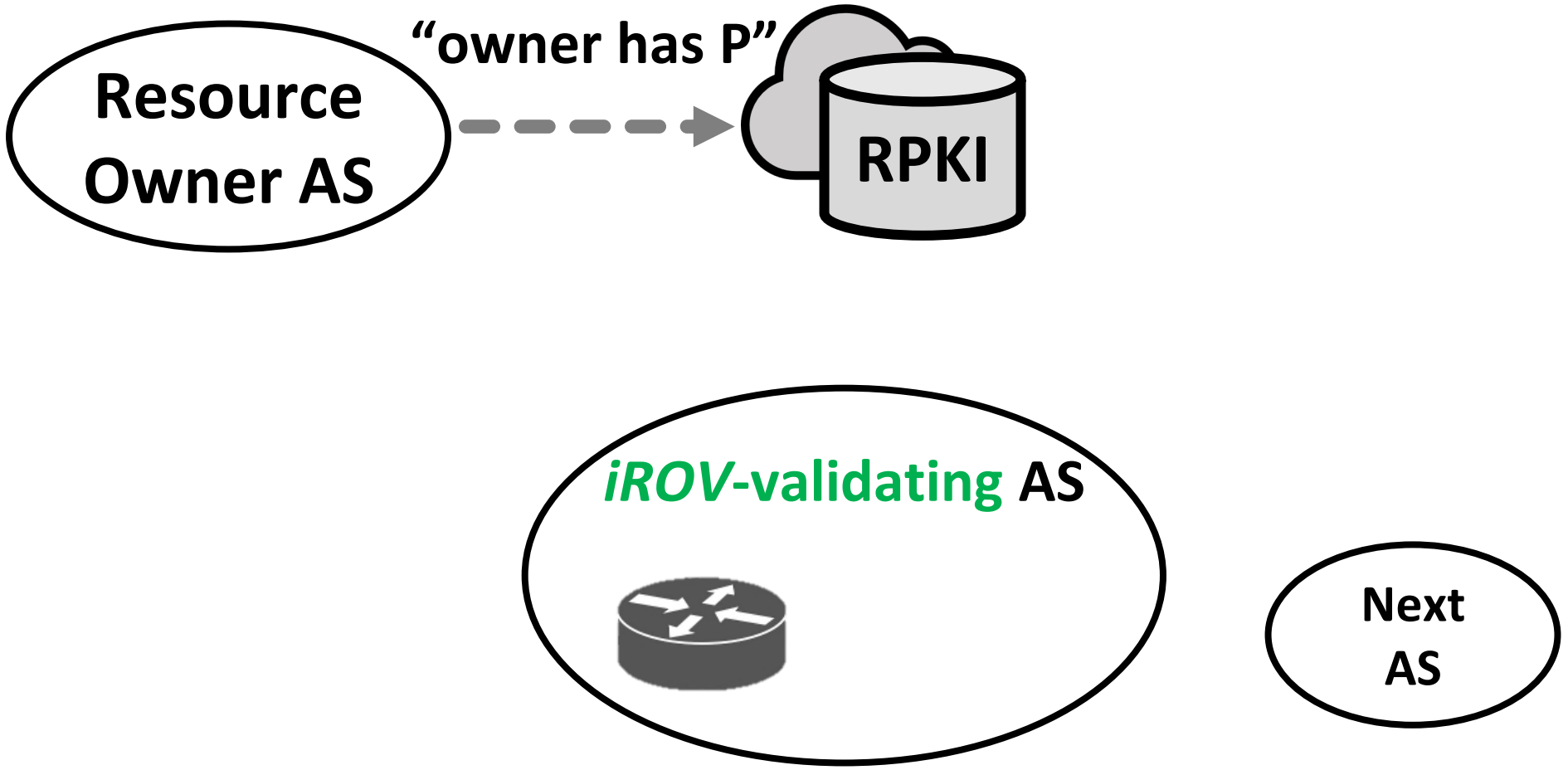
To address these challenges, we introduce:



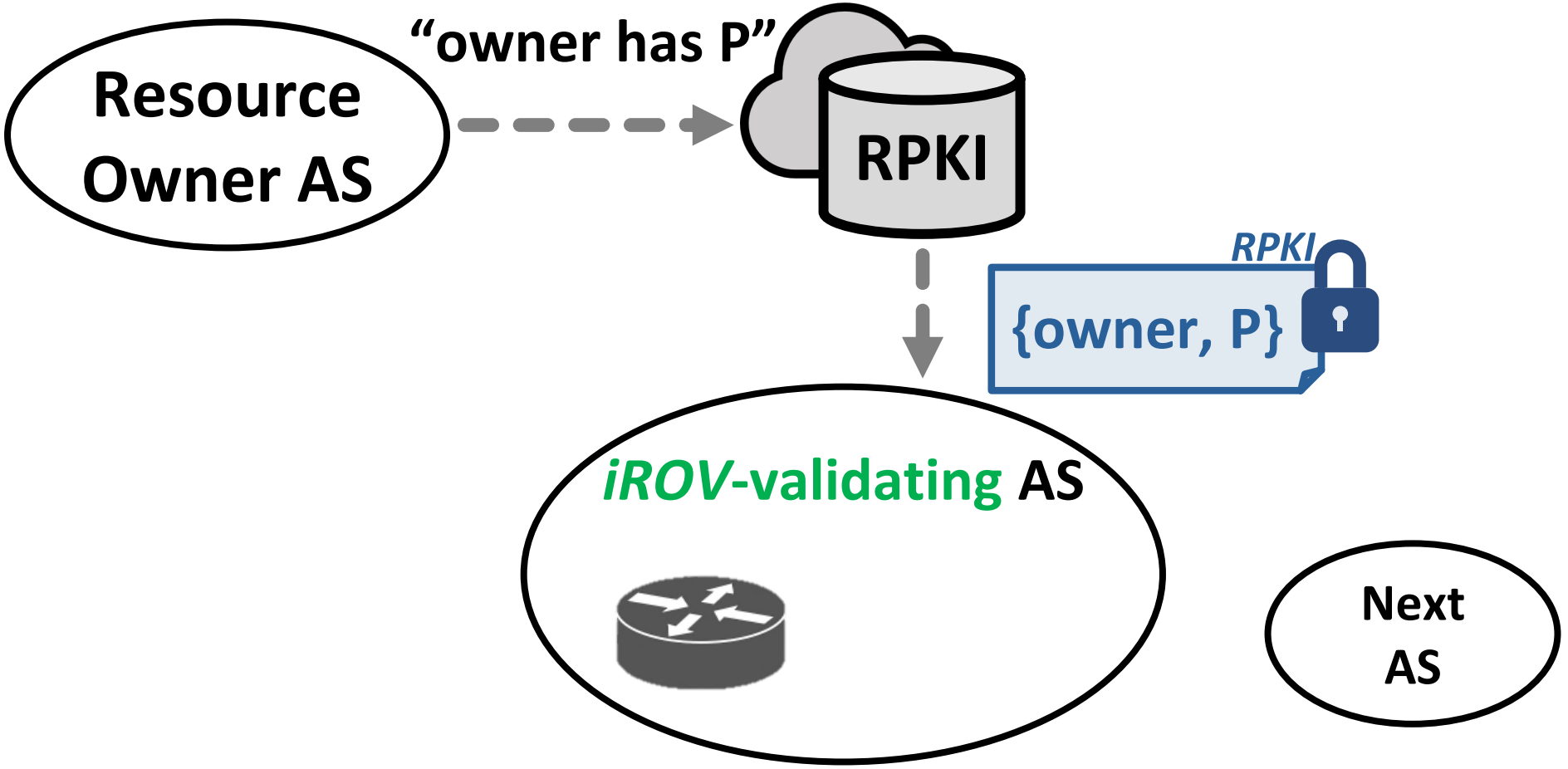
How *Interactivity* addresses **C1** and **C2**



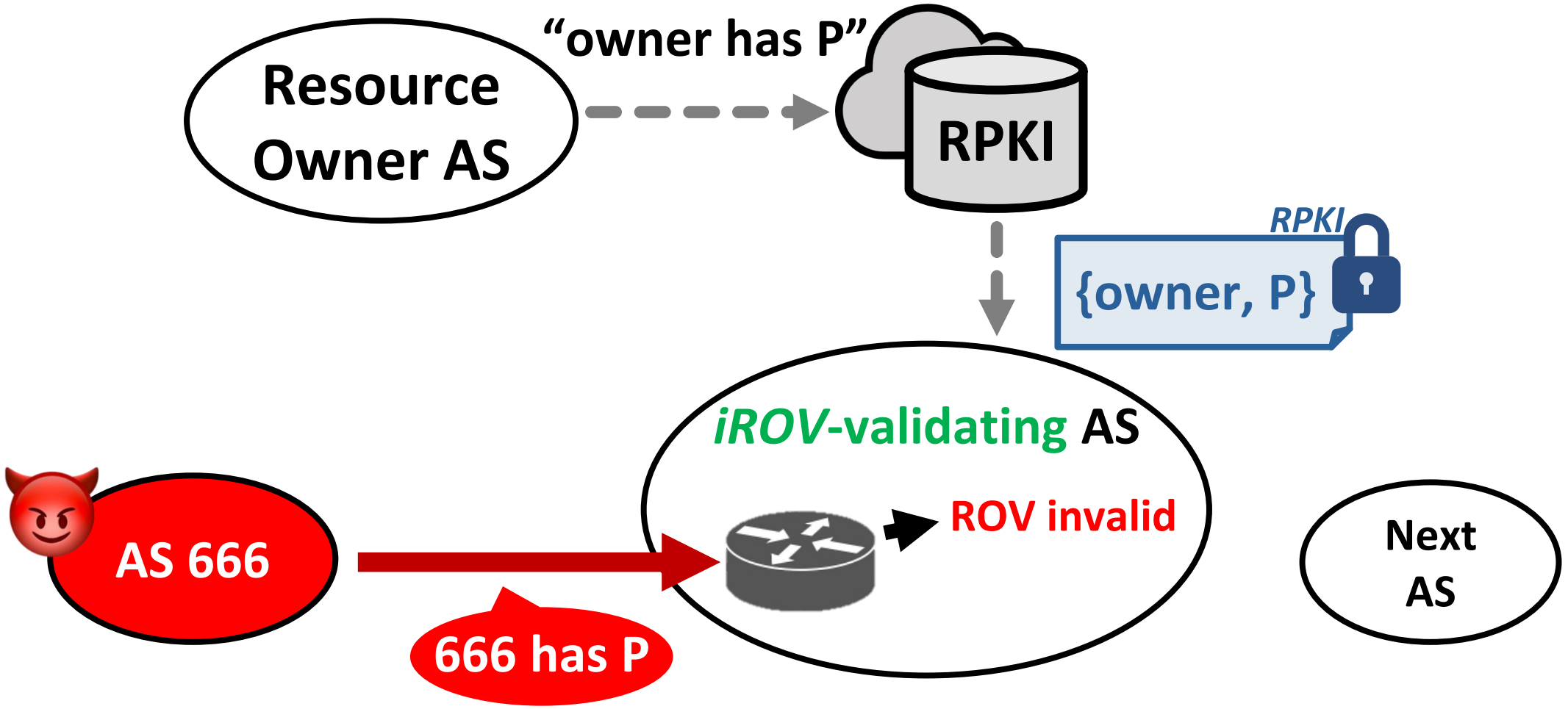
How *Interactivity* addresses **C1** and **C2**



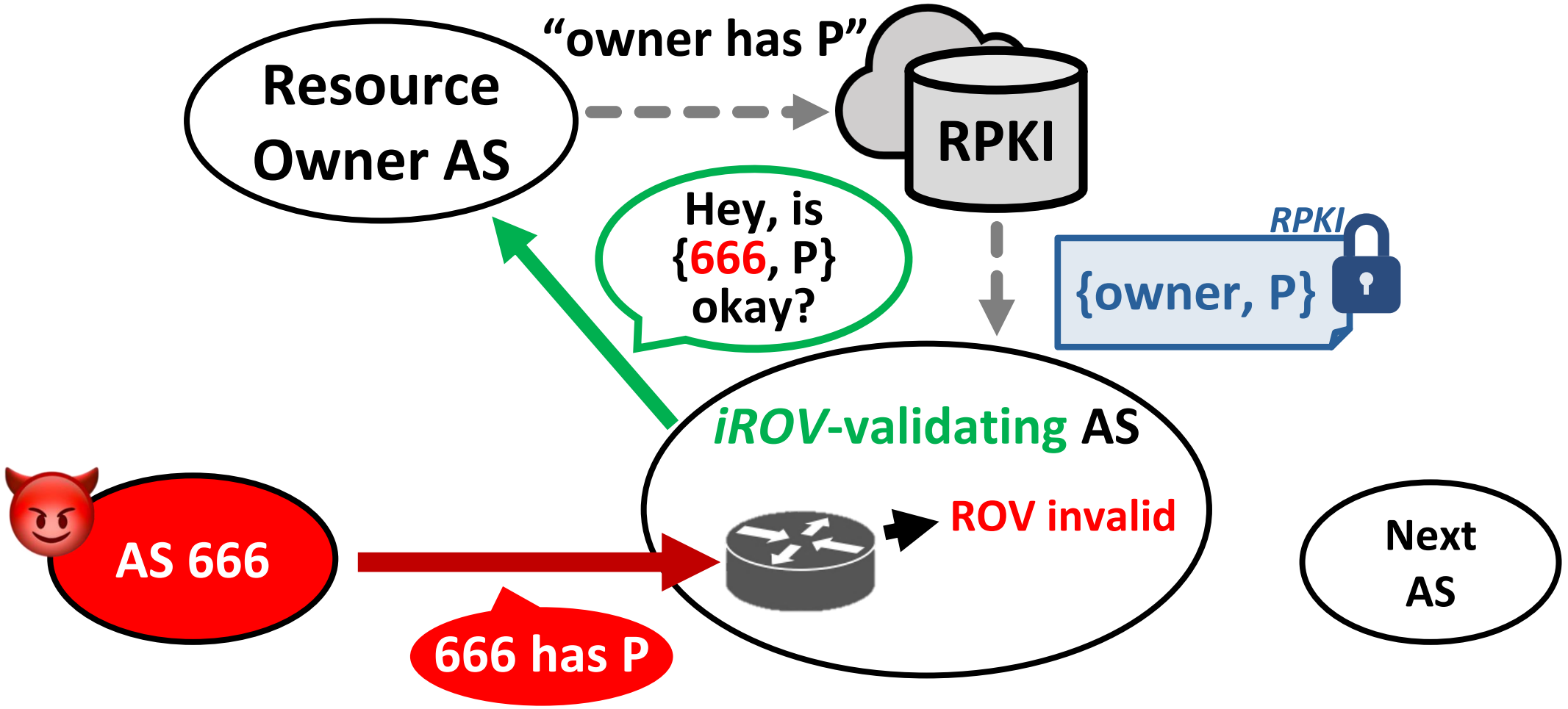
How *Interactivity* addresses **C1** and **C2**



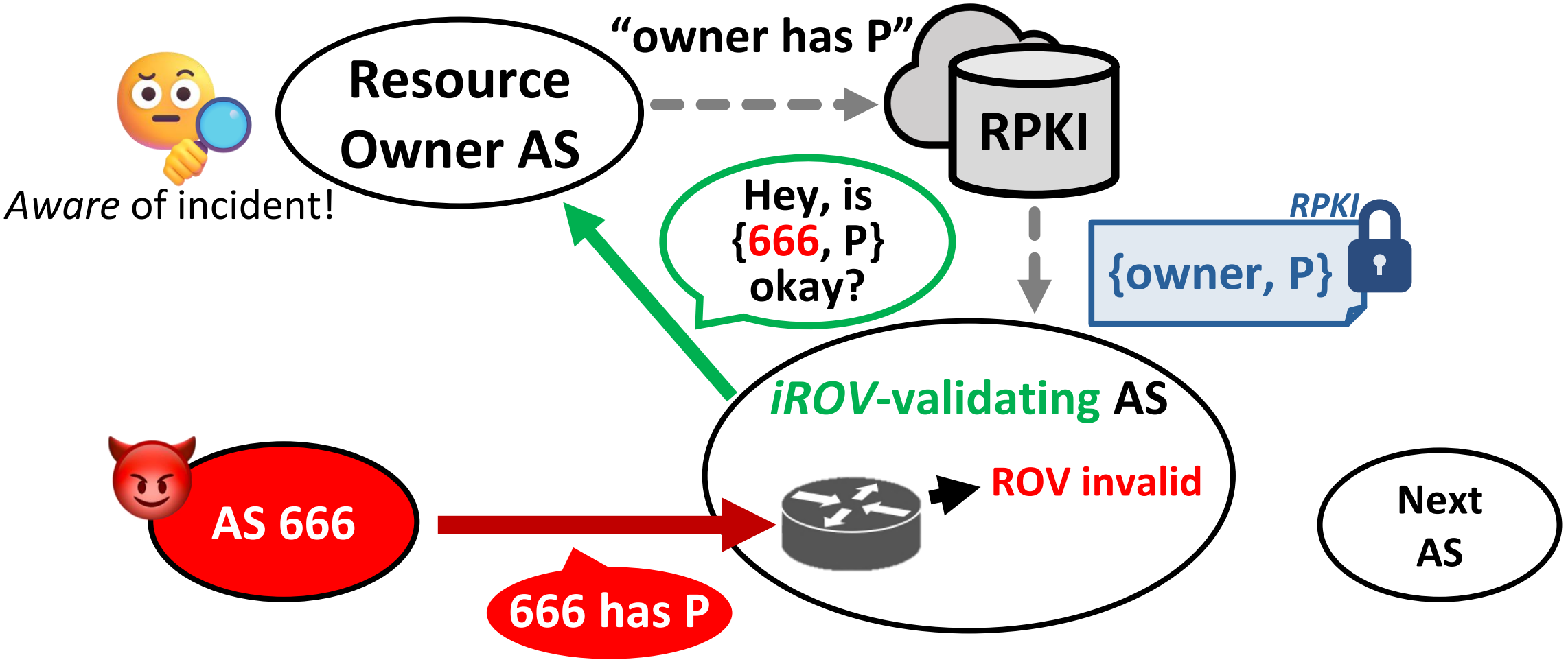
How *Interactivity* addresses **C1** and **C2**



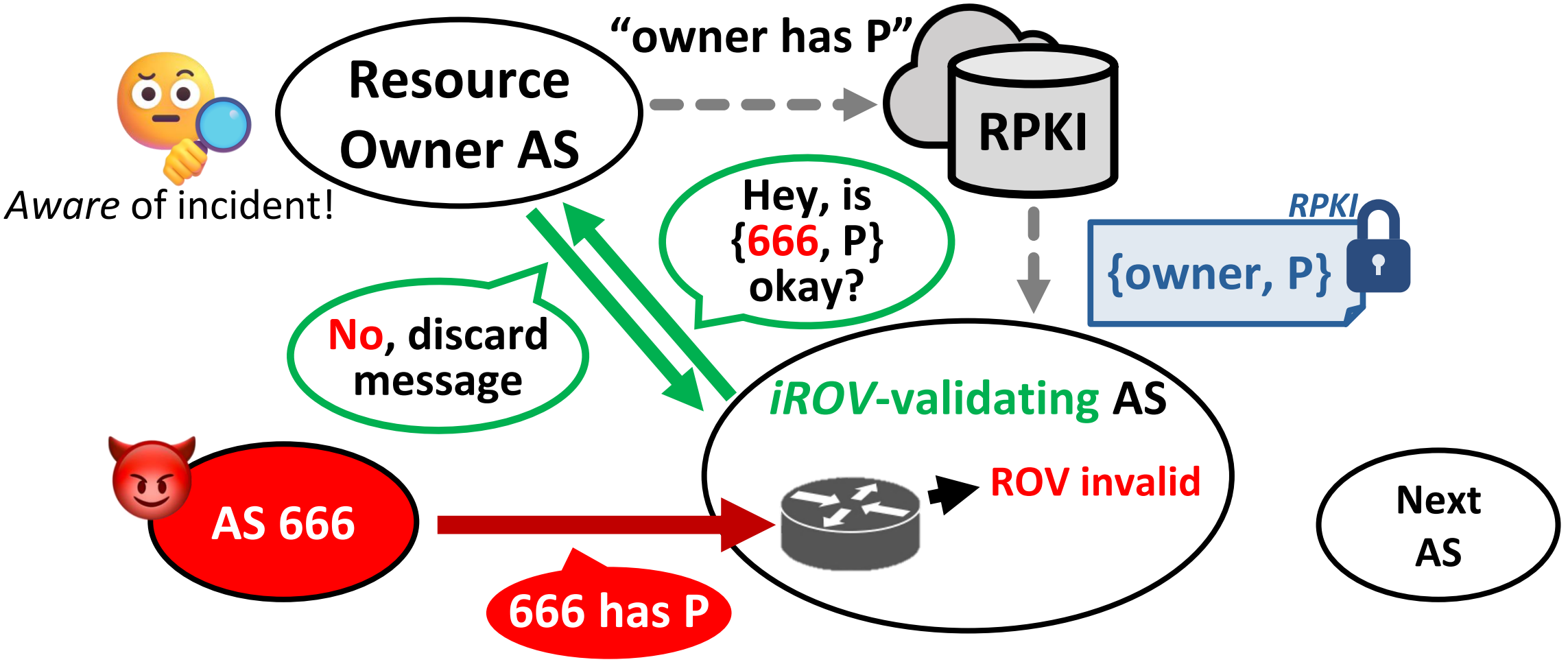
How *Interactivity* addresses **C1** and **C2**



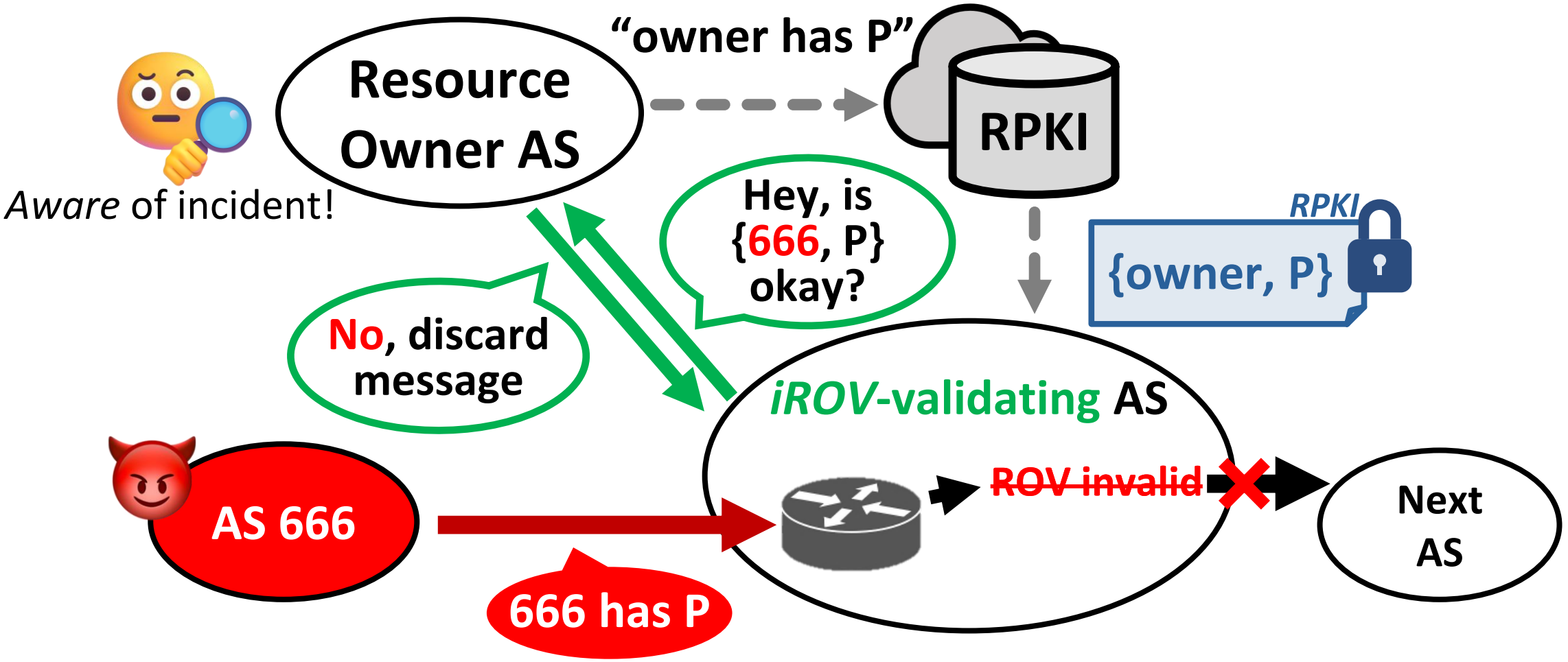
How *Interactivity* addresses **C1** and **C2**



How *Interactivity* addresses **C1** and **C2**



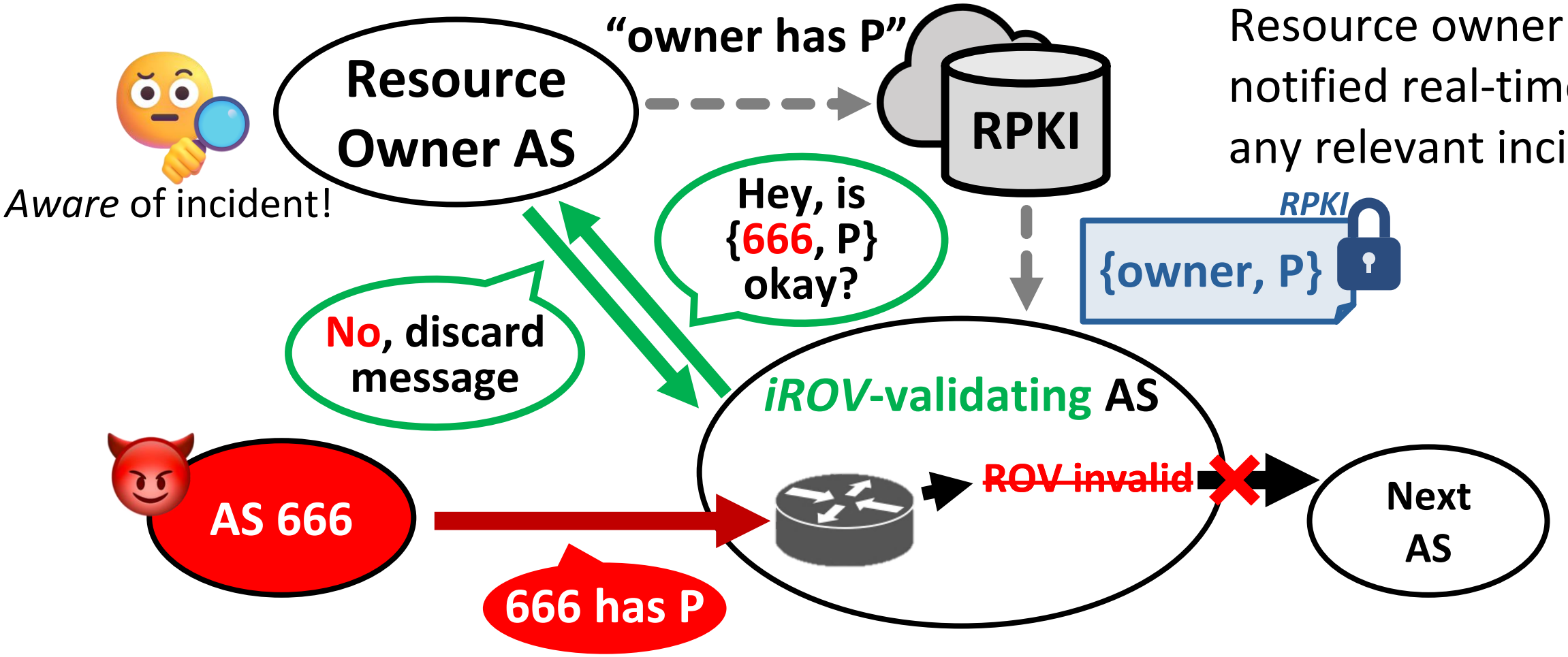
How *Interactivity* addresses **C1** and **C2**



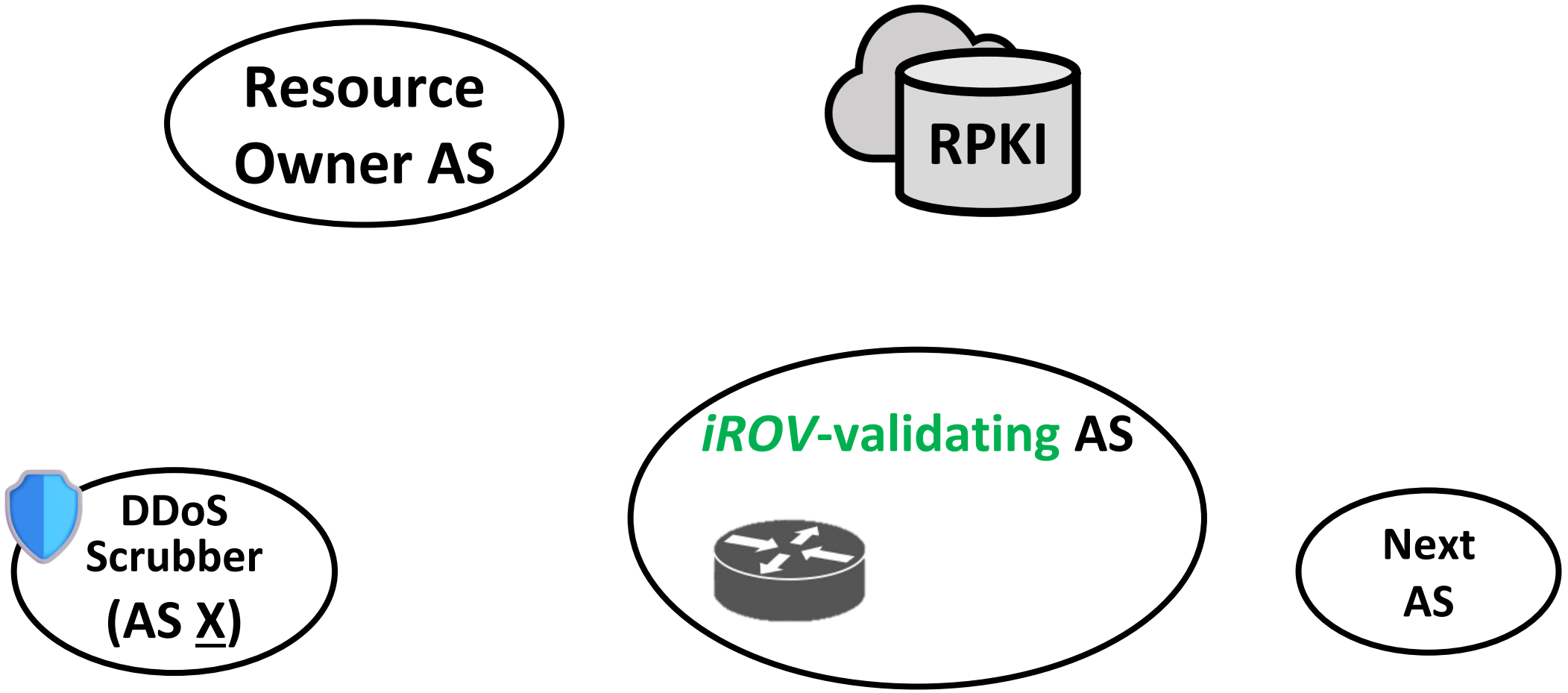
How *Interactivity* addresses **C1** and **C2**

iROV gives visibility:

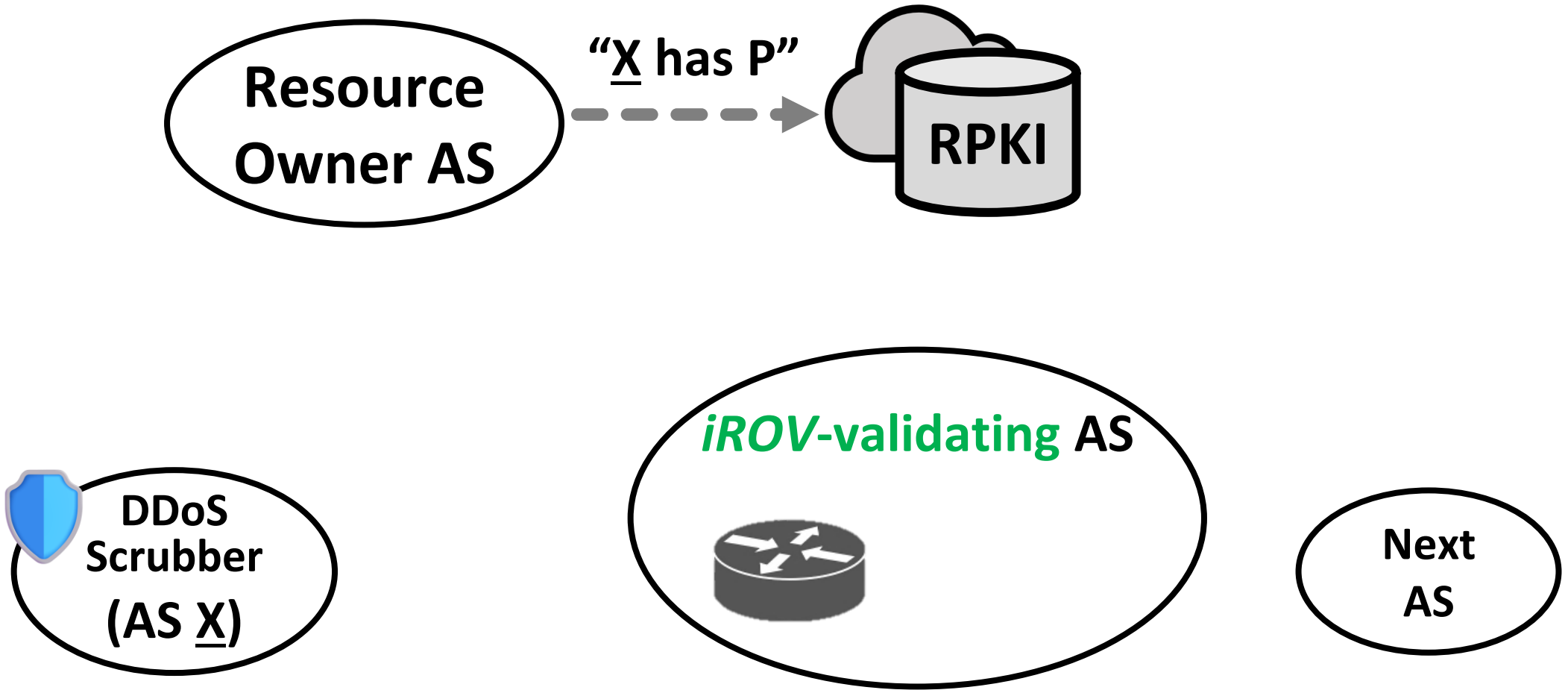
Resource owner is notified real-time of any relevant incidents



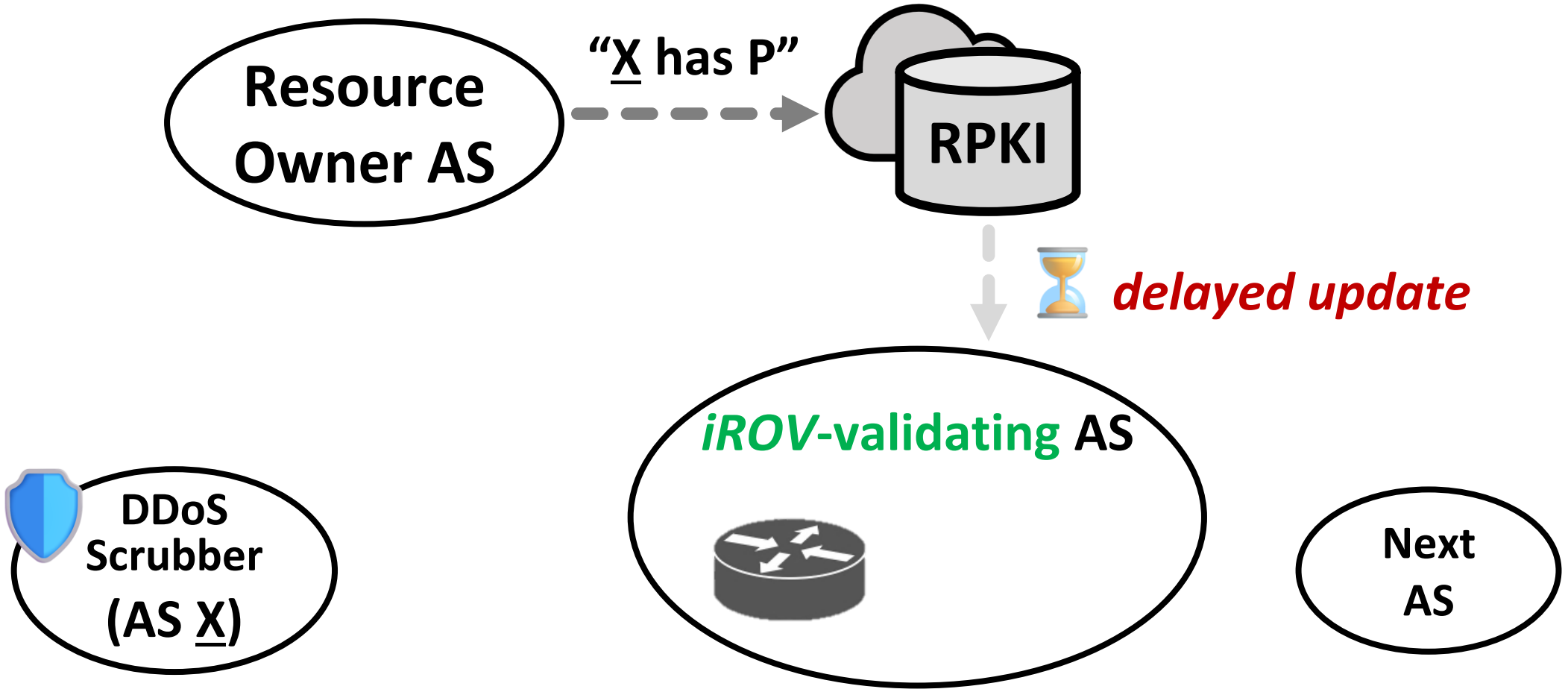
How *Interactivity* addresses **C3**



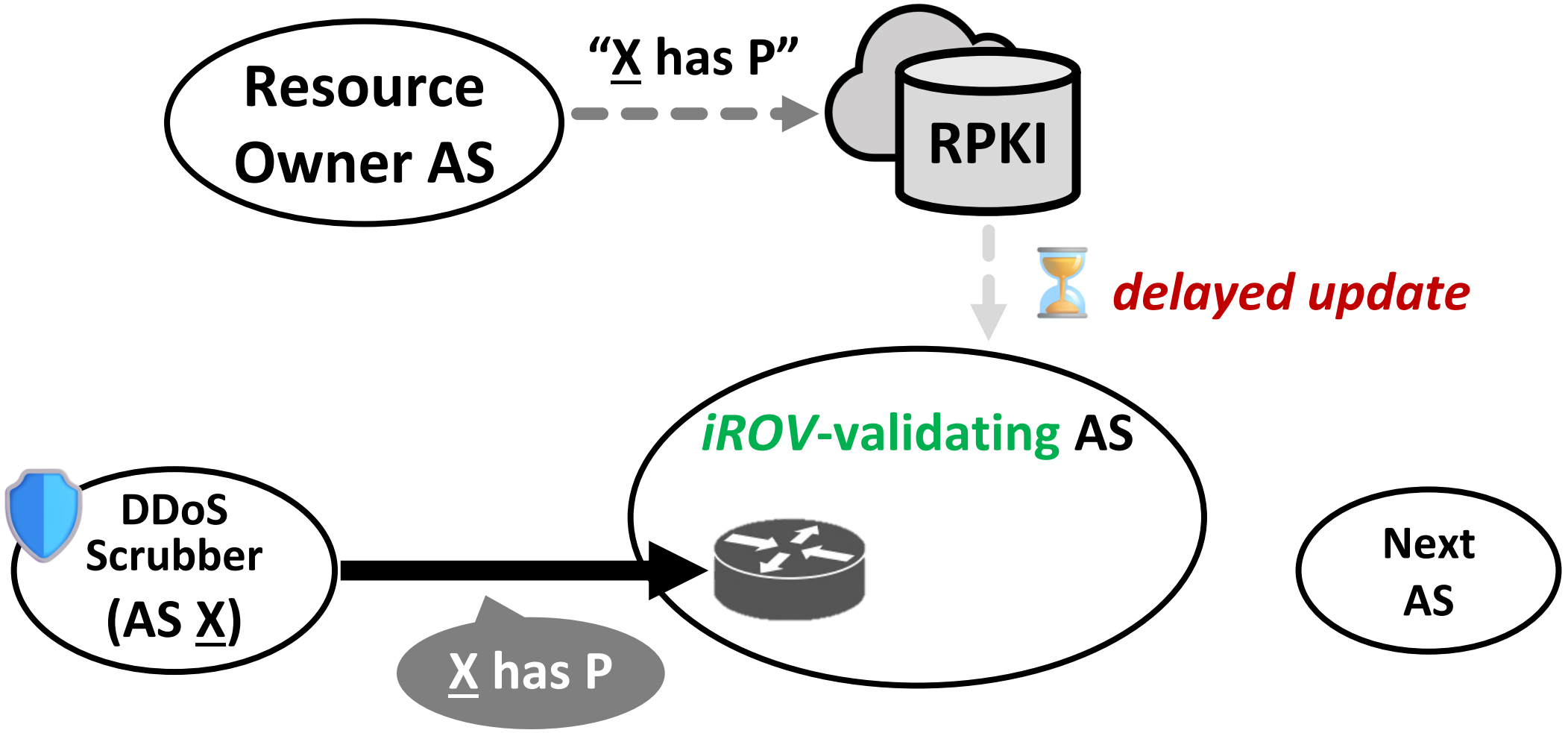
How *Interactivity* addresses **C3**



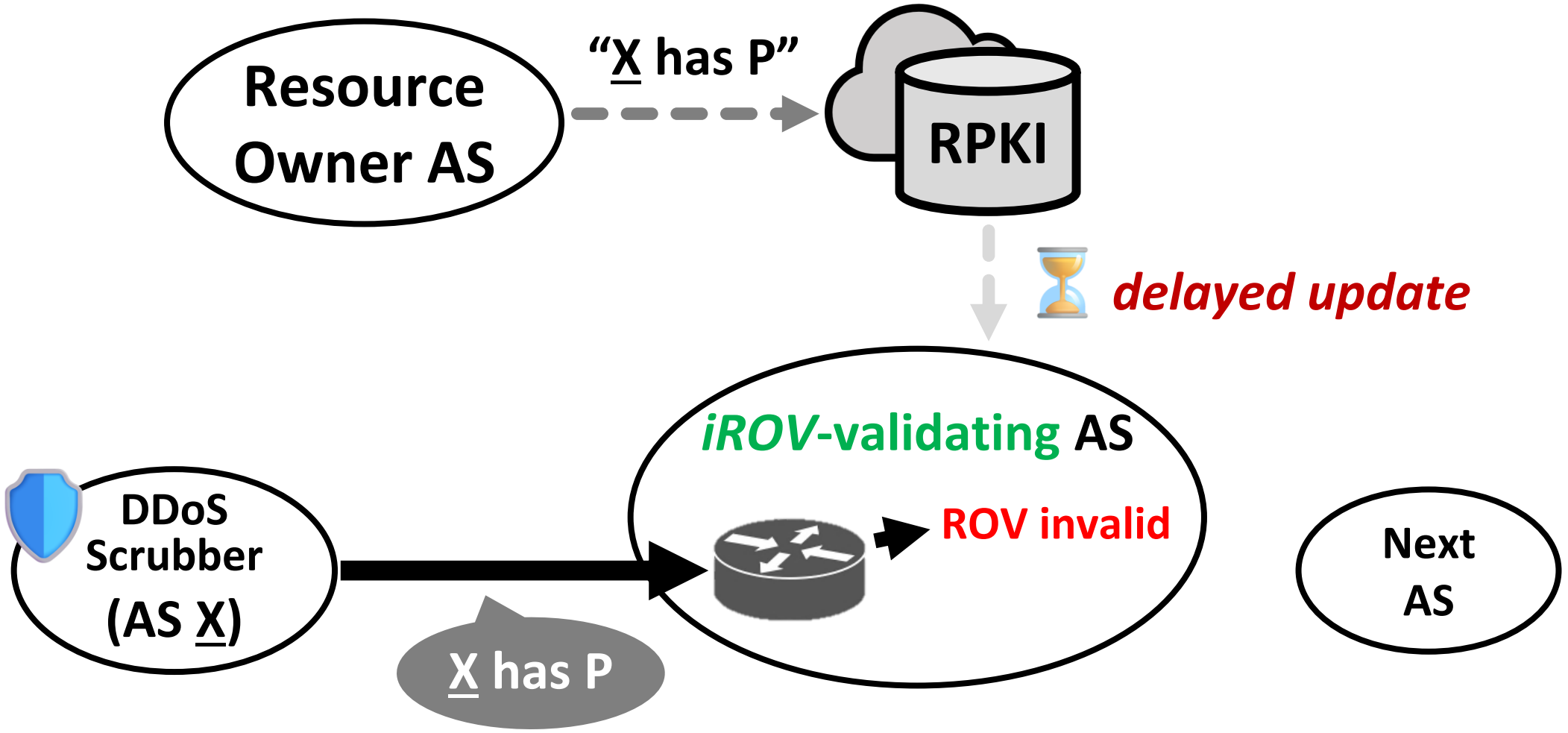
How *Interactivity* addresses **C3**



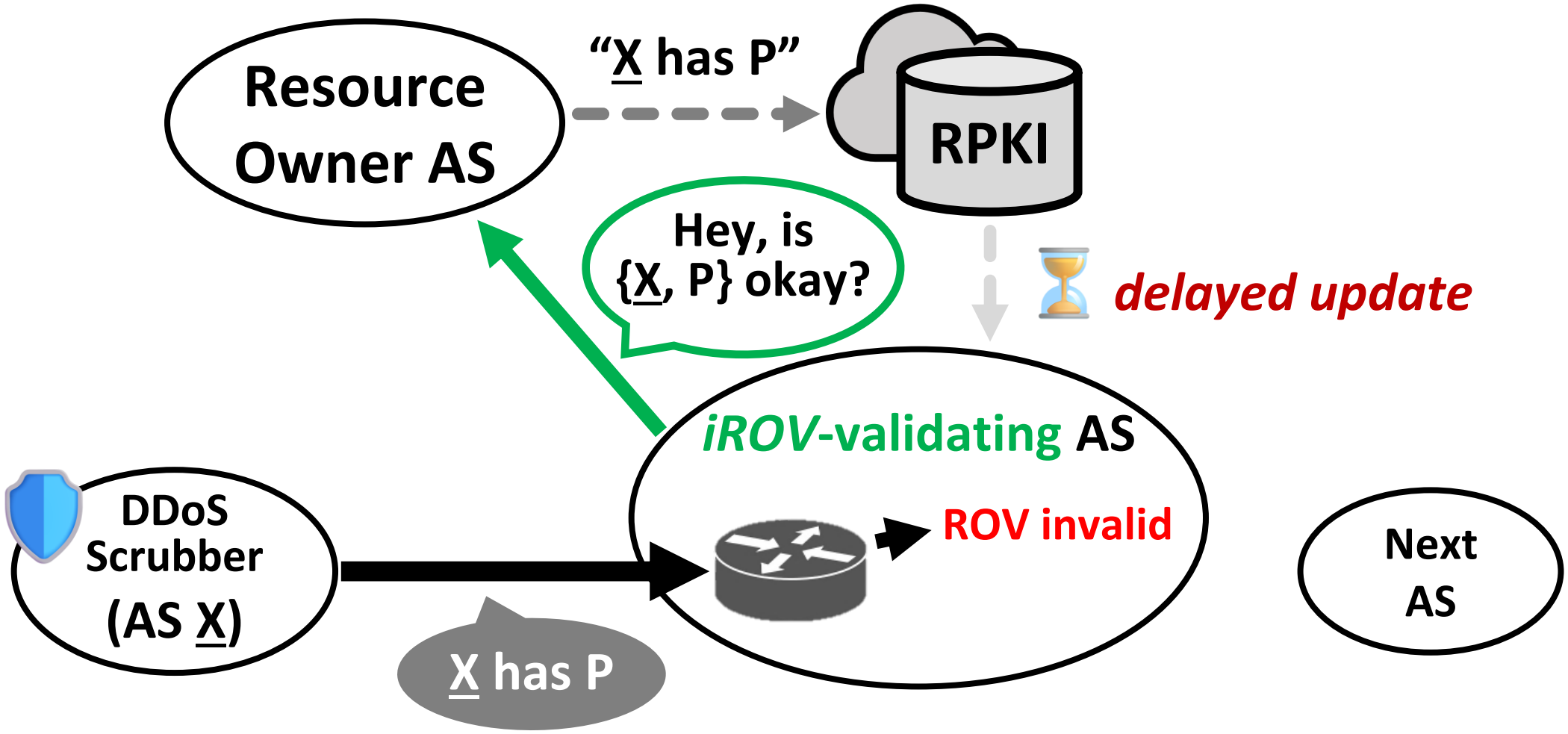
How *Interactivity* addresses **C3**



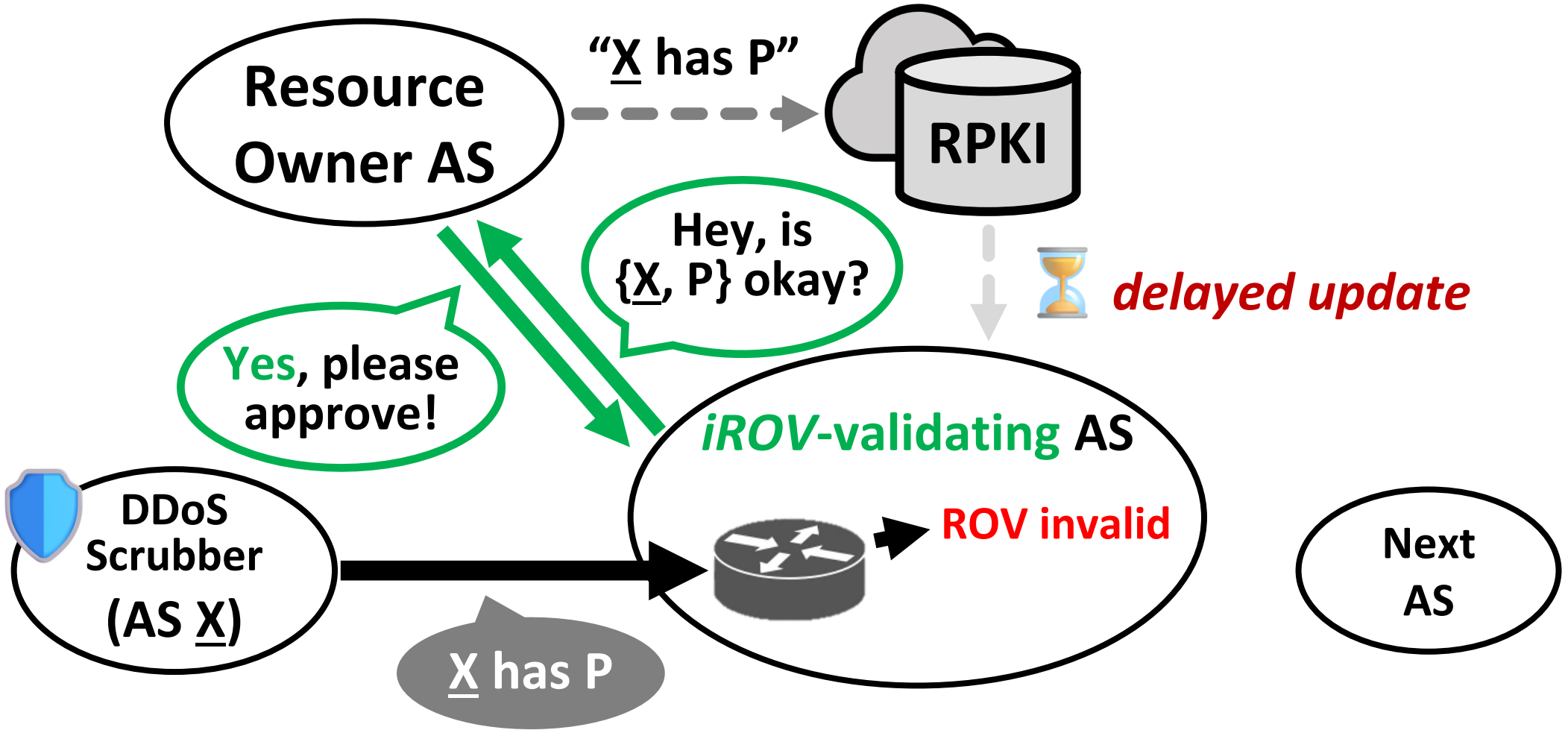
How *Interactivity* addresses **C3**



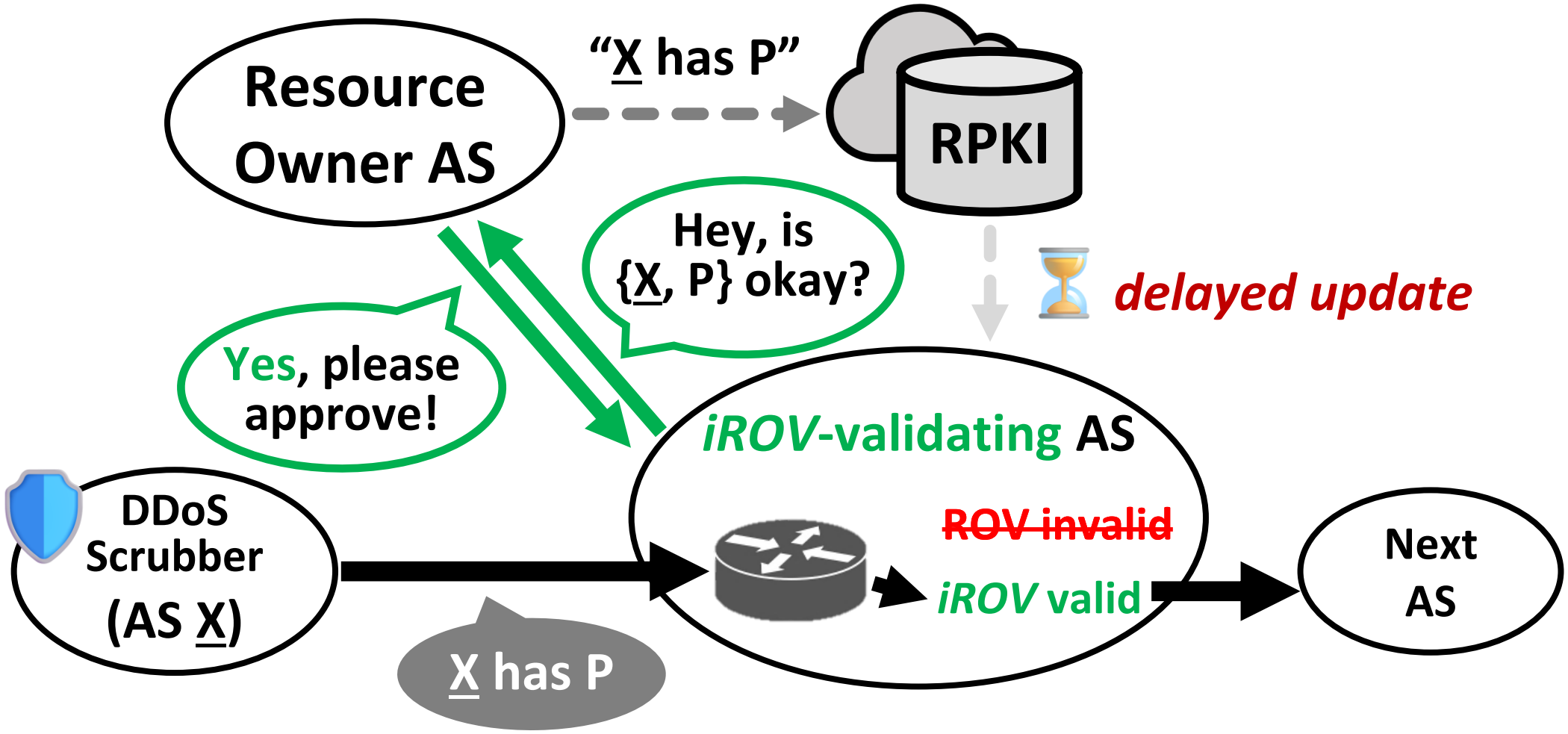
How *Interactivity* addresses **C3**



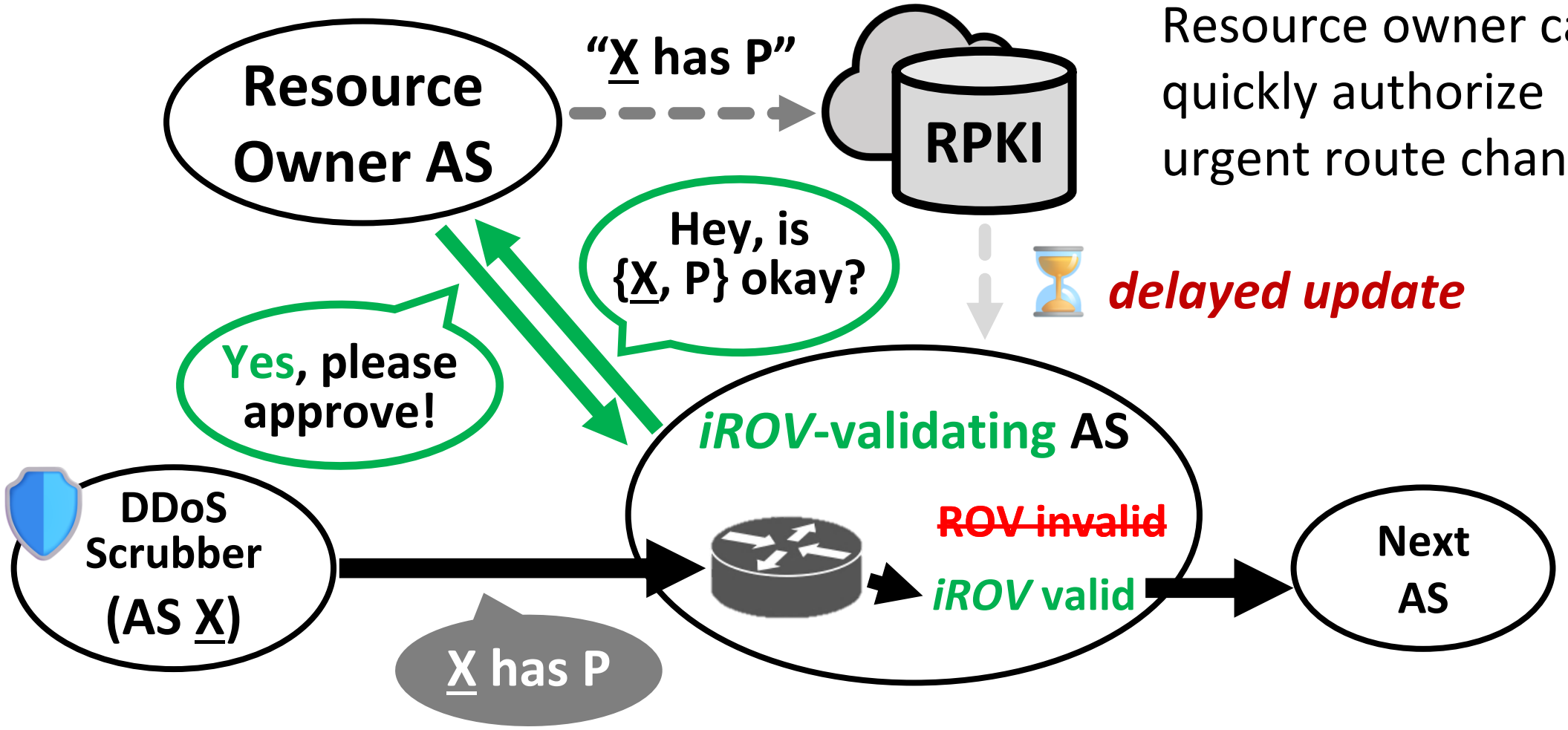
How *Interactivity* addresses **C3**



How *Interactivity* addresses **C3**



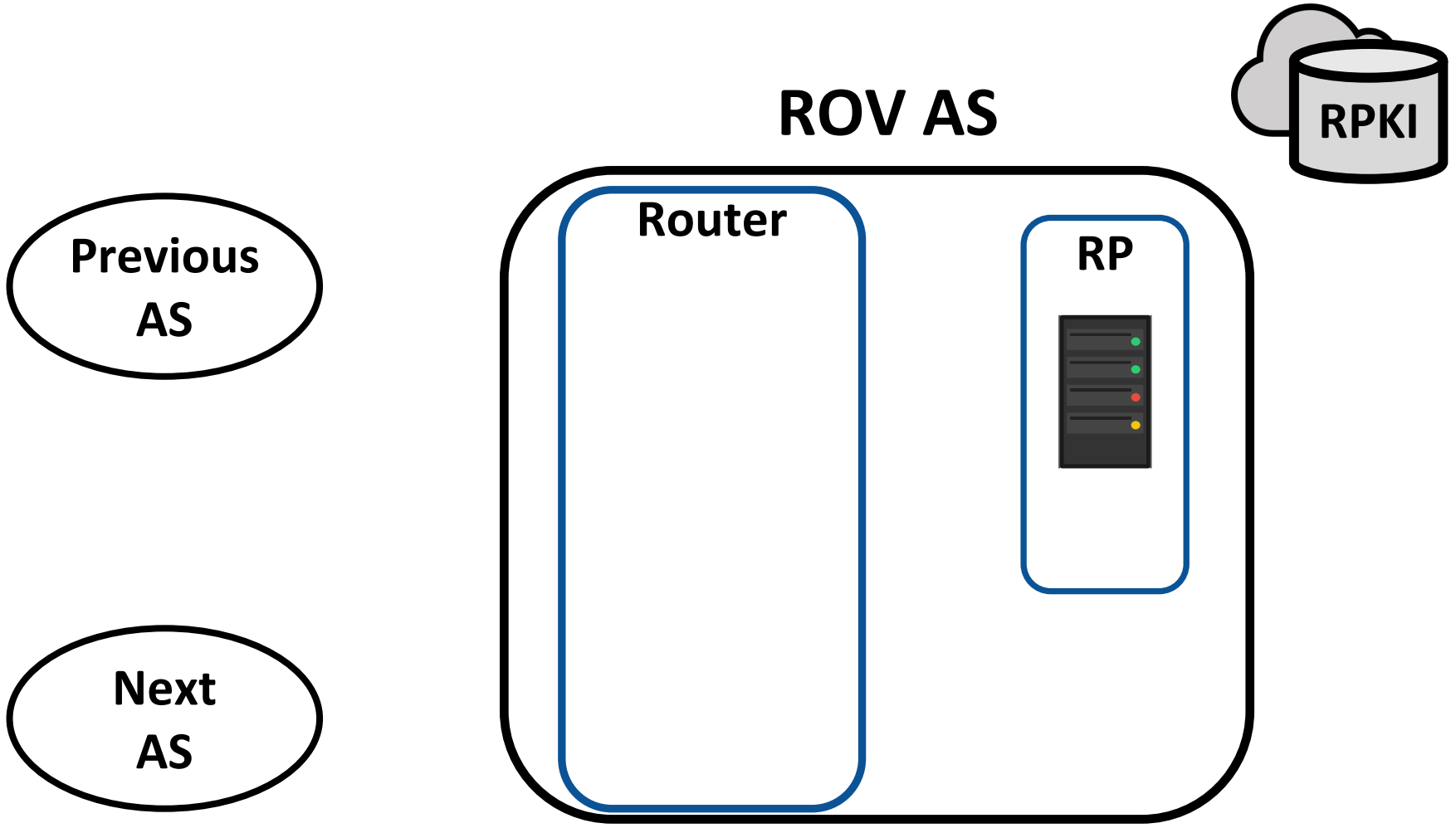
How *Interactivity* addresses **C3**



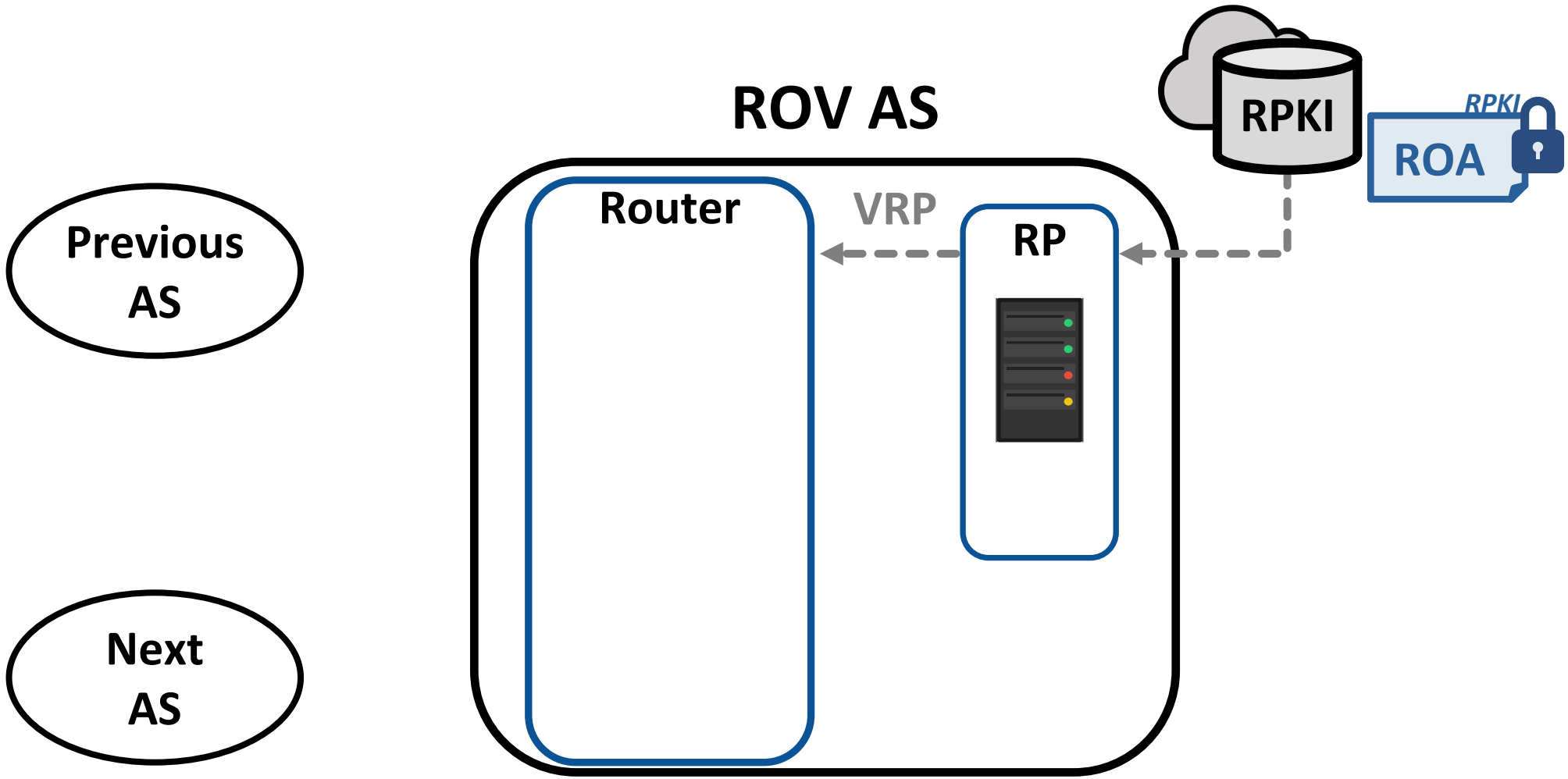
iROV gives agility:

Resource owner can quickly authorize urgent route changes

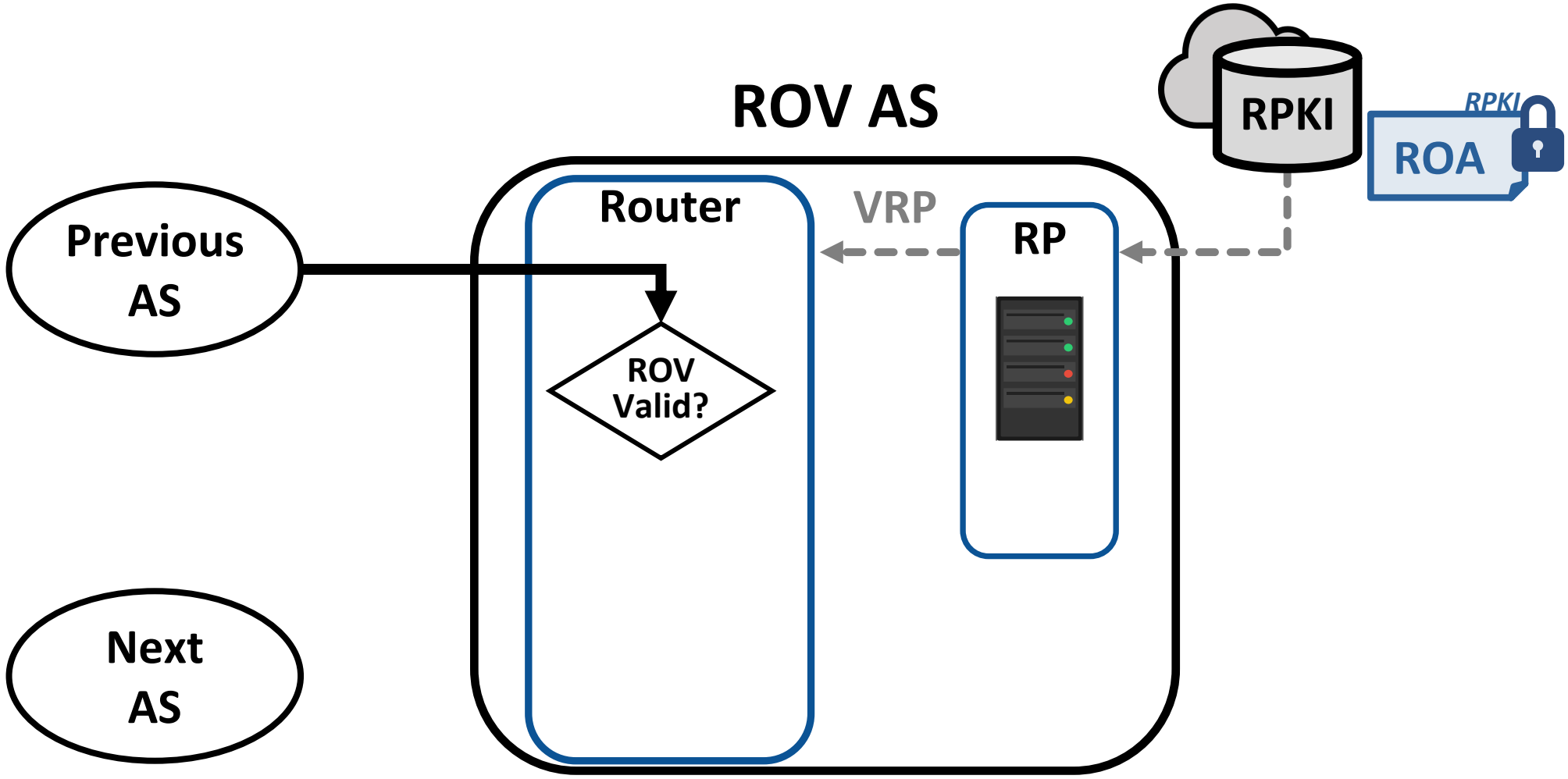
iROV Overview



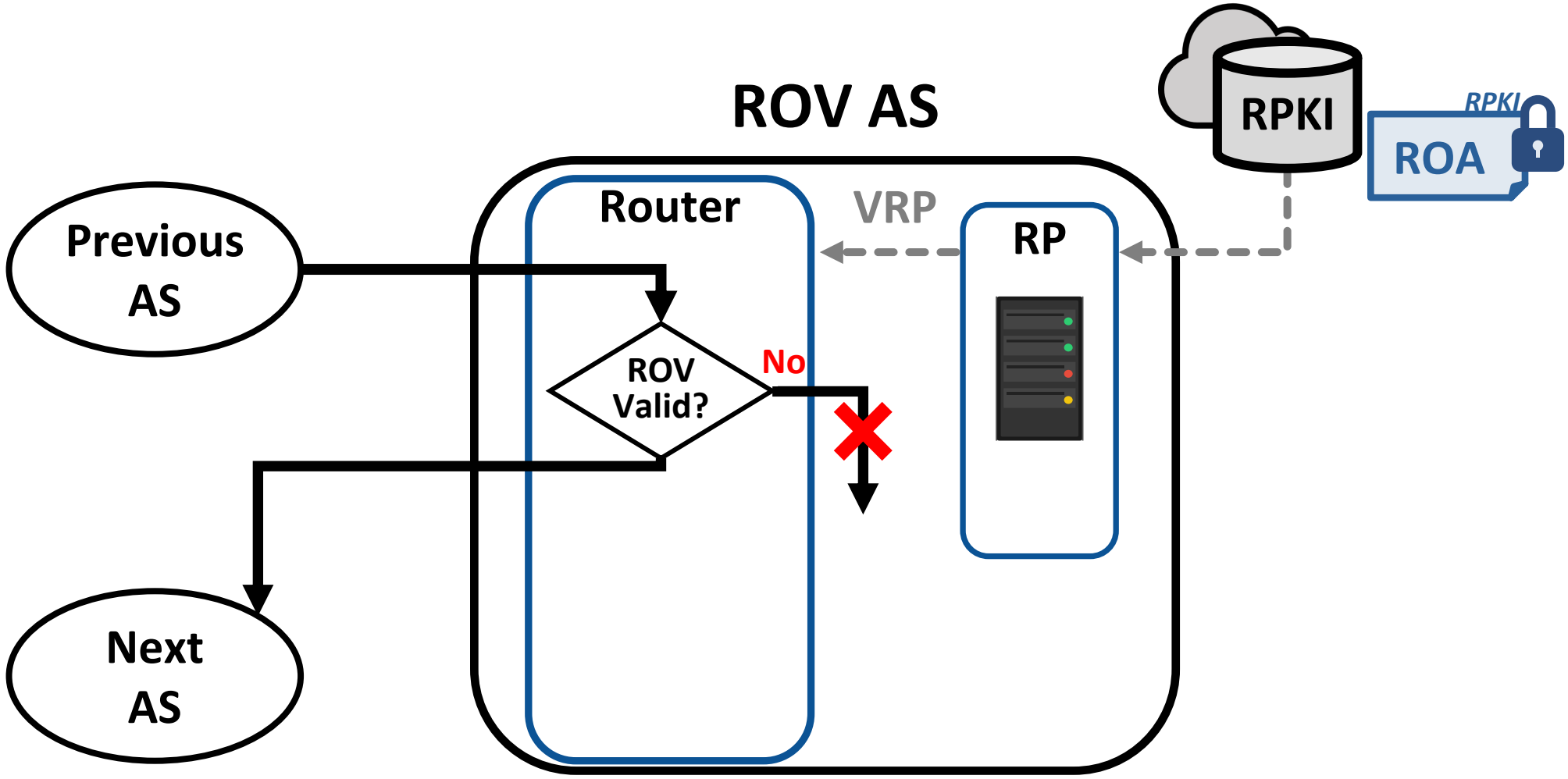
iROV Overview



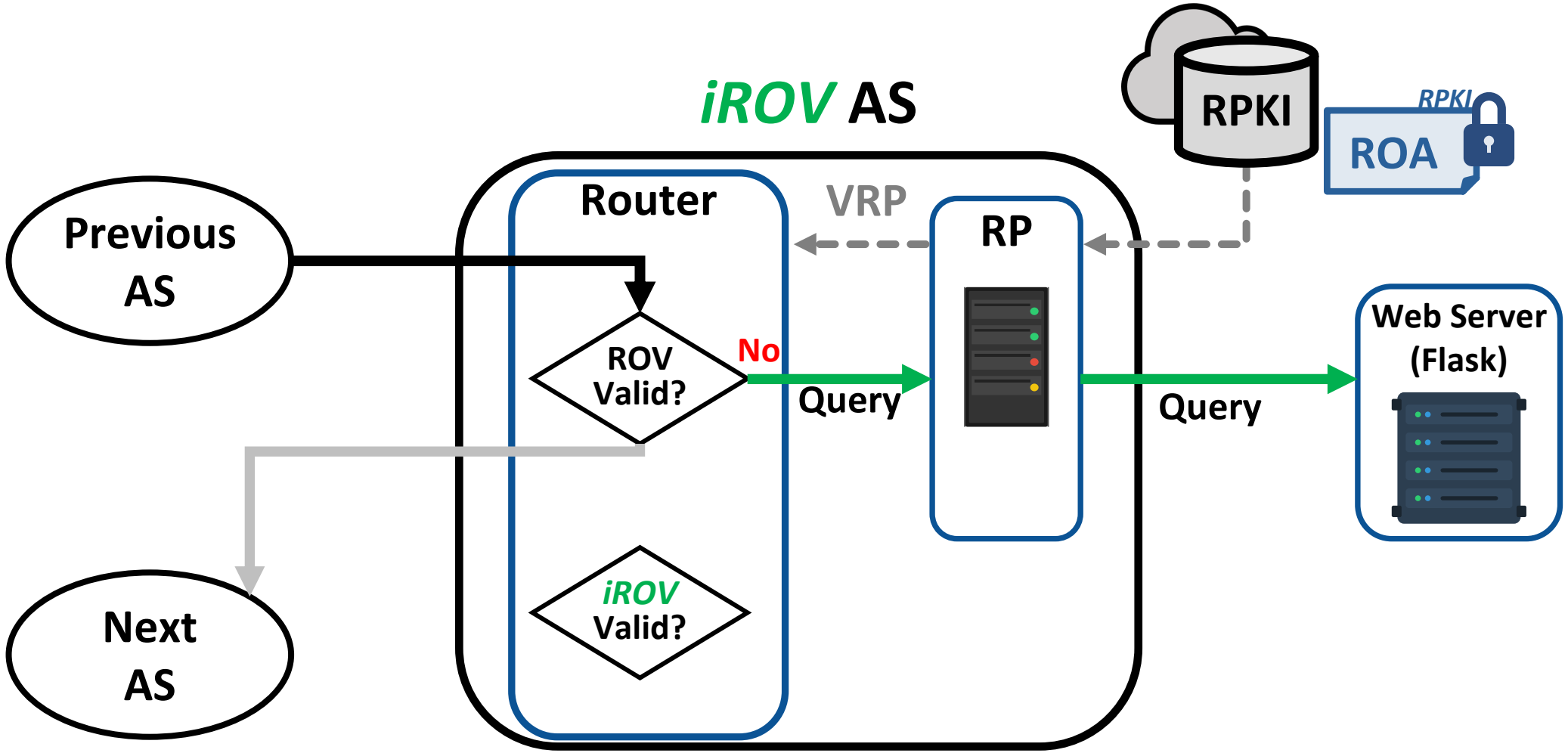
iROV Overview



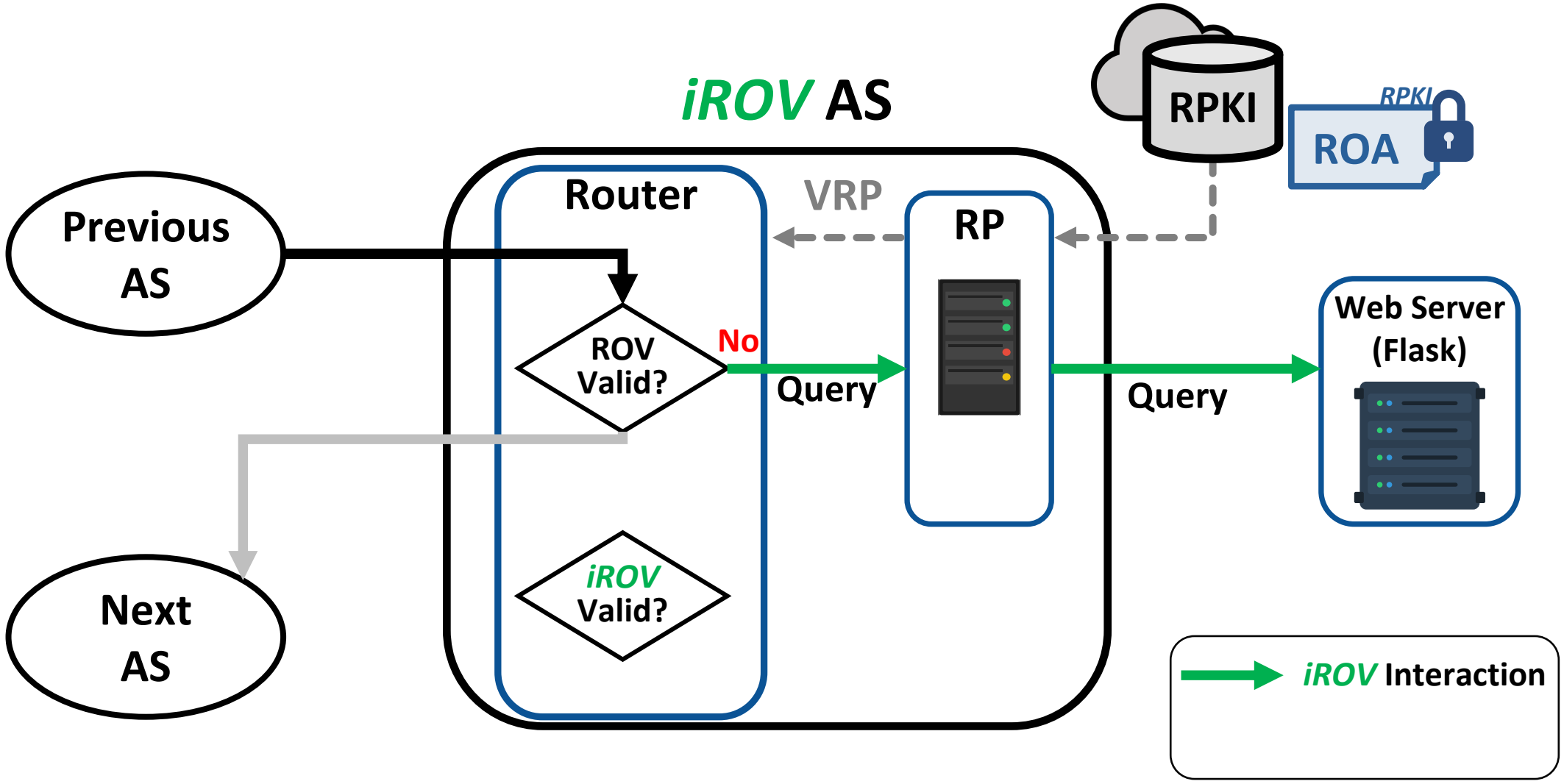
iROV Overview



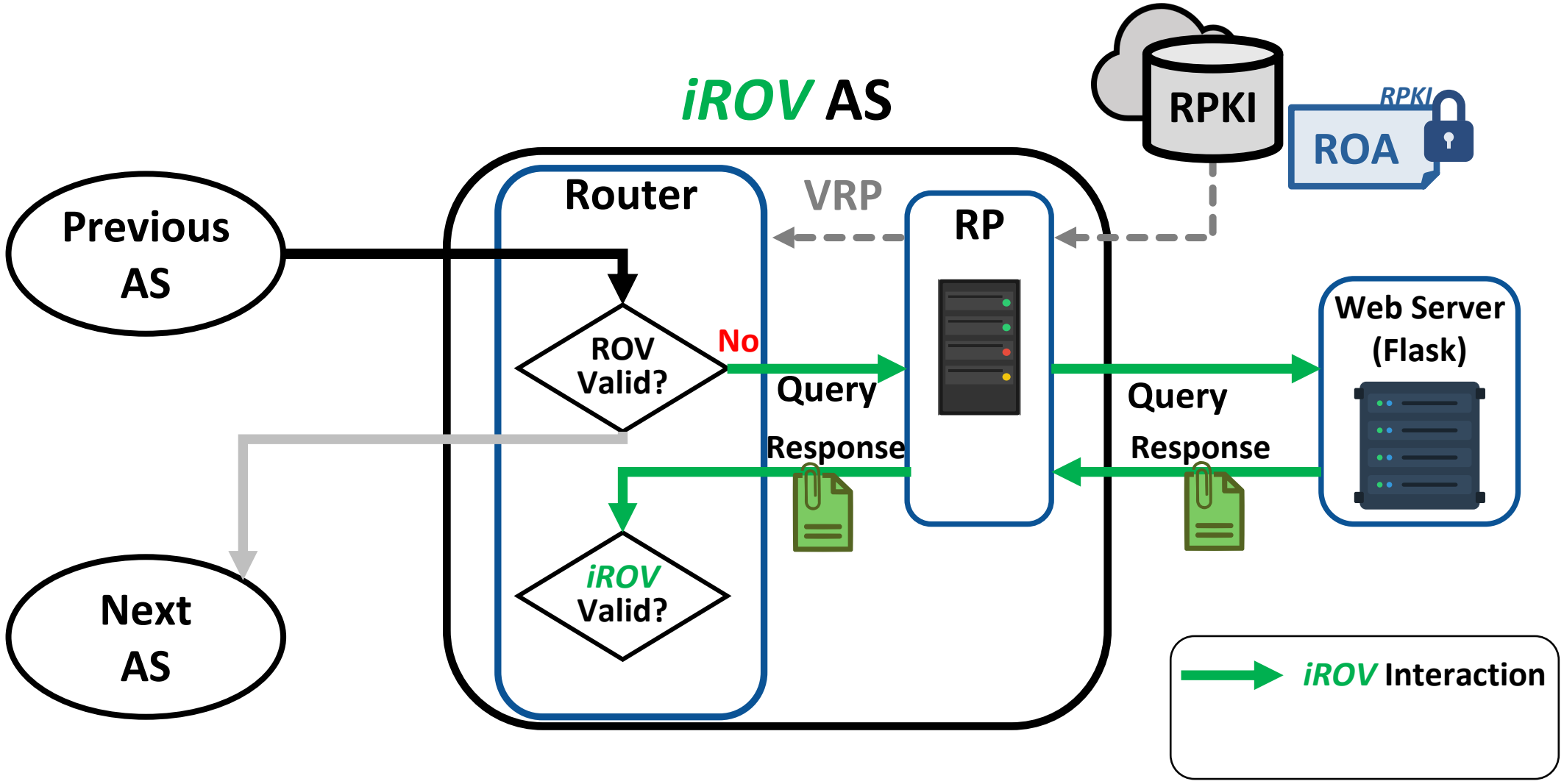
iROV Overview



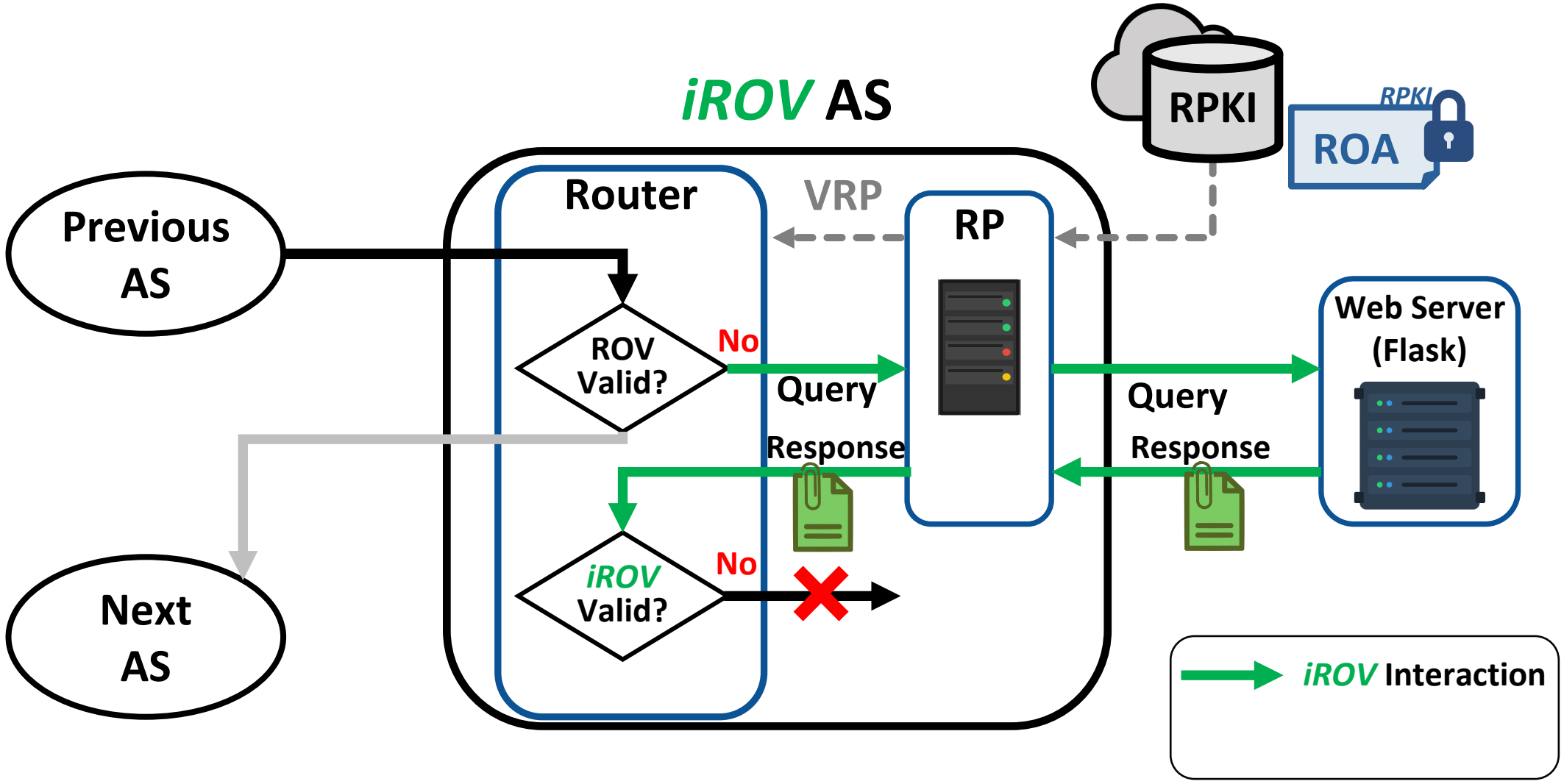
iROV Overview



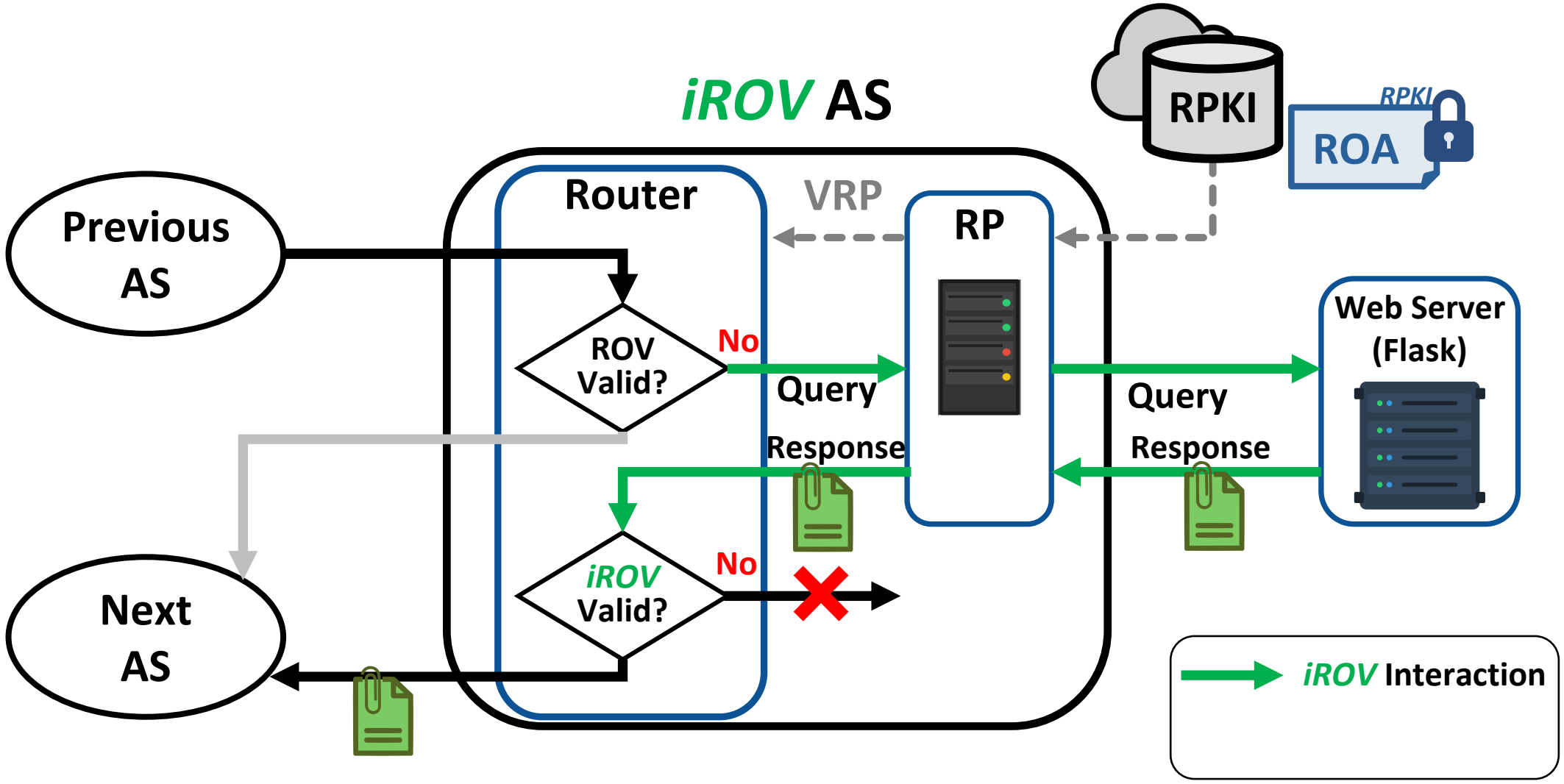
iROV Overview



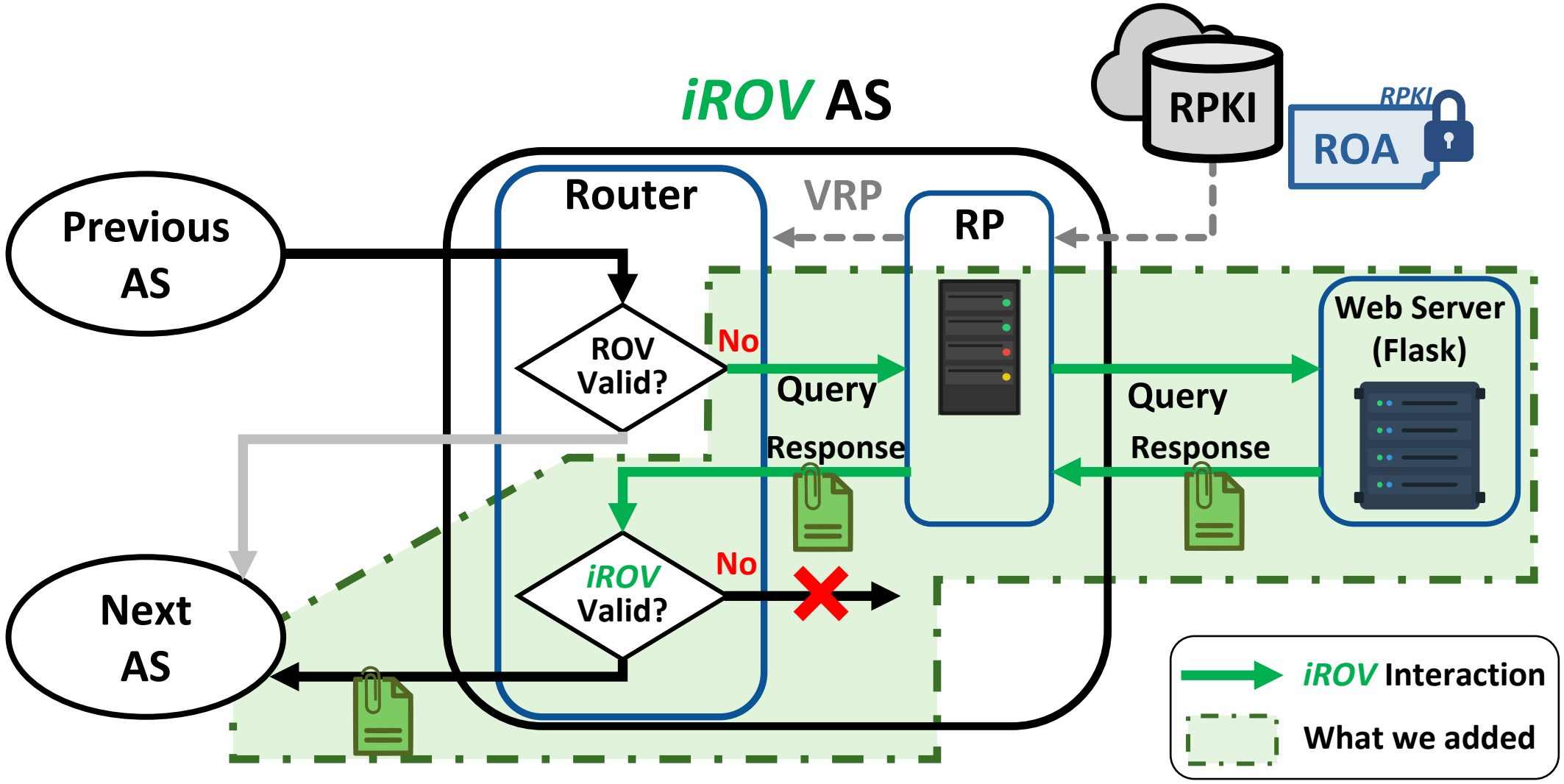
iROV Overview



iROV Overview



iROV Overview



So, all you need to do is “**add interactivity**”:

So, all you need to do is “**add interactivity**”:

- Gives resource owners **visibility** into errors and attacks

So, all you need to do is “**add interactivity**”:

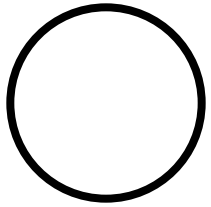
- Gives resource owners **visibility** into errors and attacks
- Enables **agile** operational maneuvers

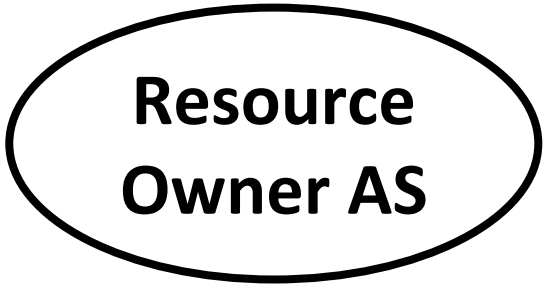
So, all you need to do is “**add interactivity**”:

- Gives resource owners **visibility** into errors and attacks
- Enables **agile** operational maneuvers

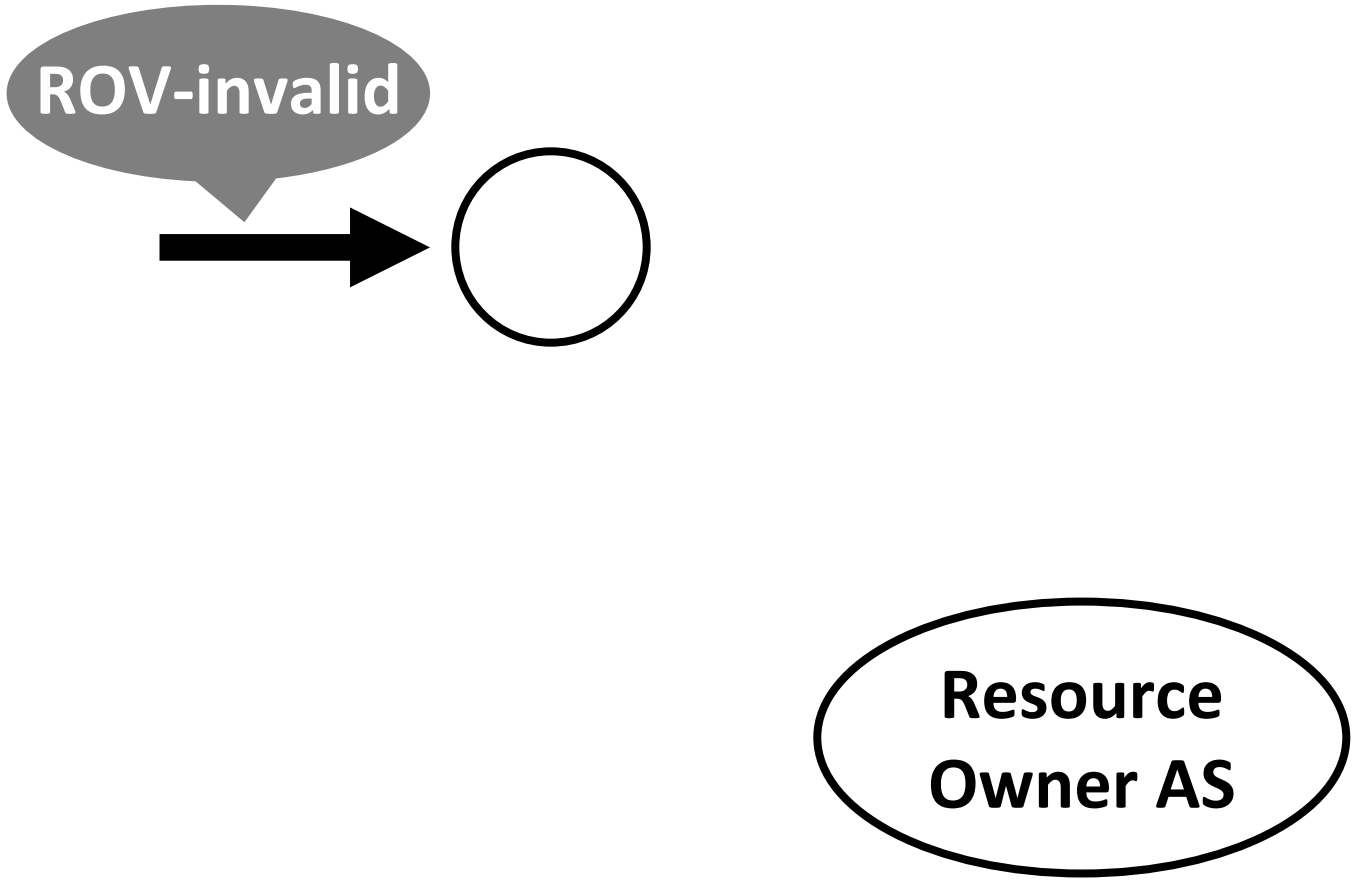
Is it really that simple? Any pitfalls? 🤔

Interactivity Can Overwhelm Owners

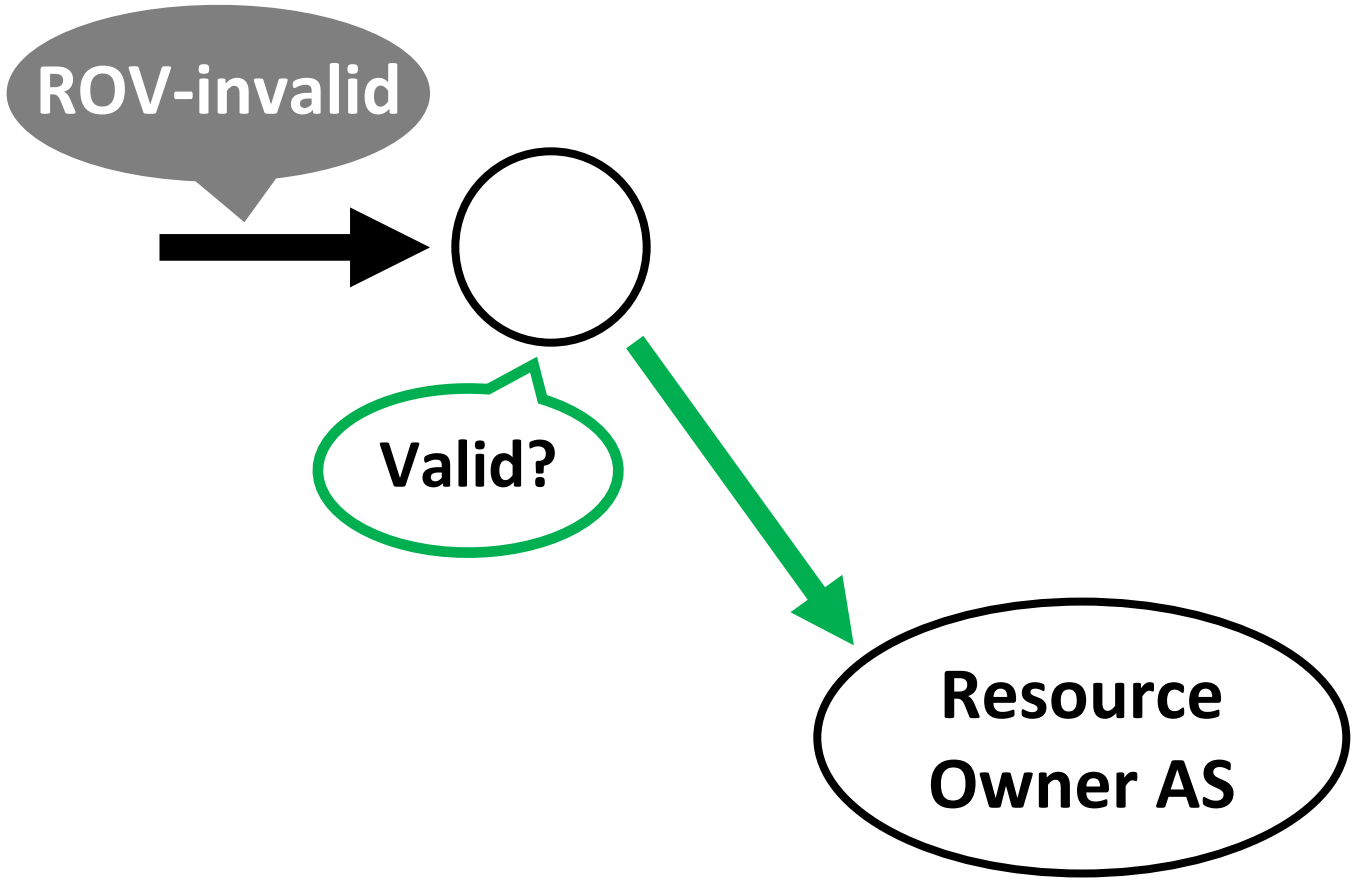




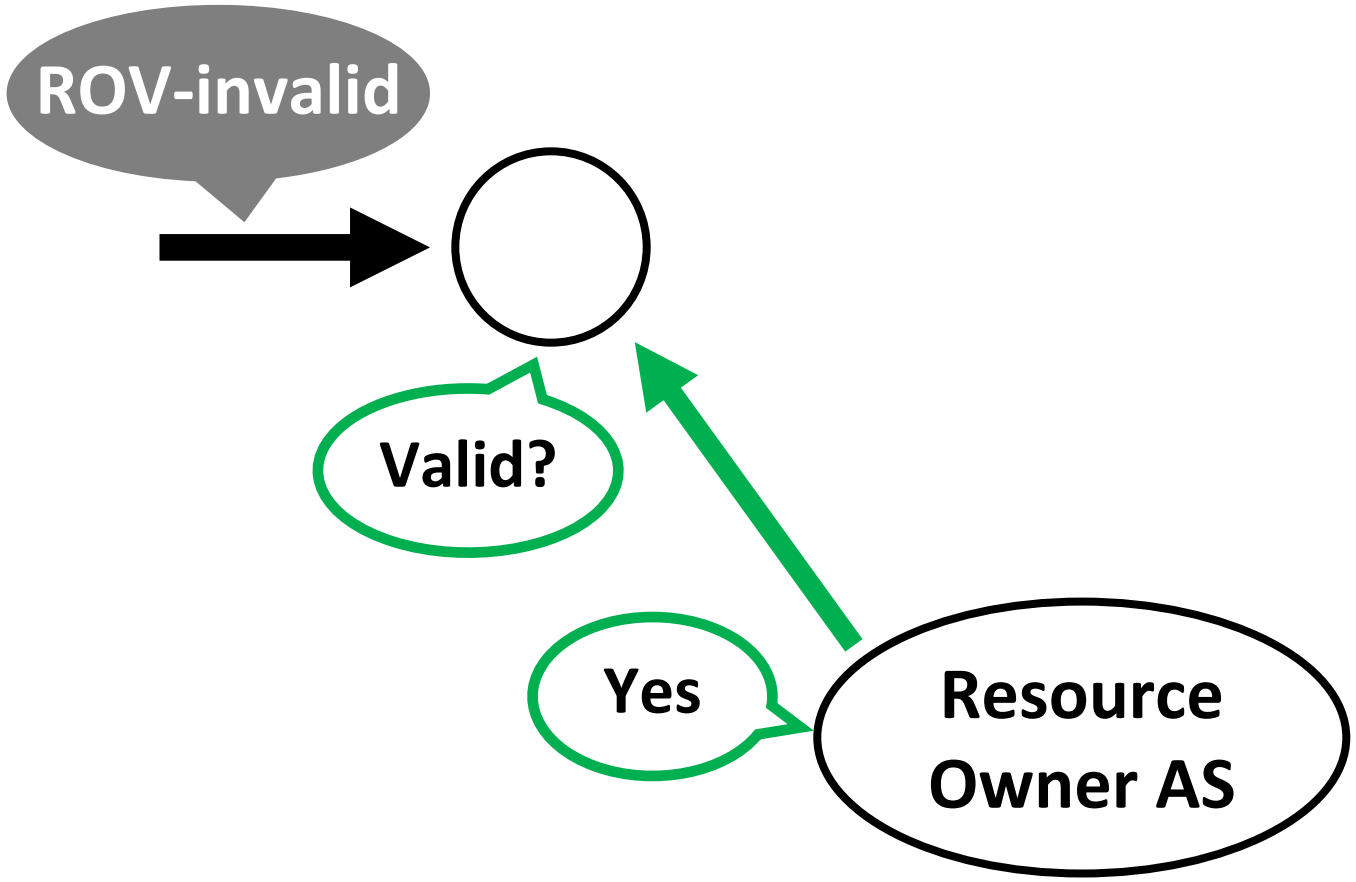
Interactivity Can Overwhelm Owners



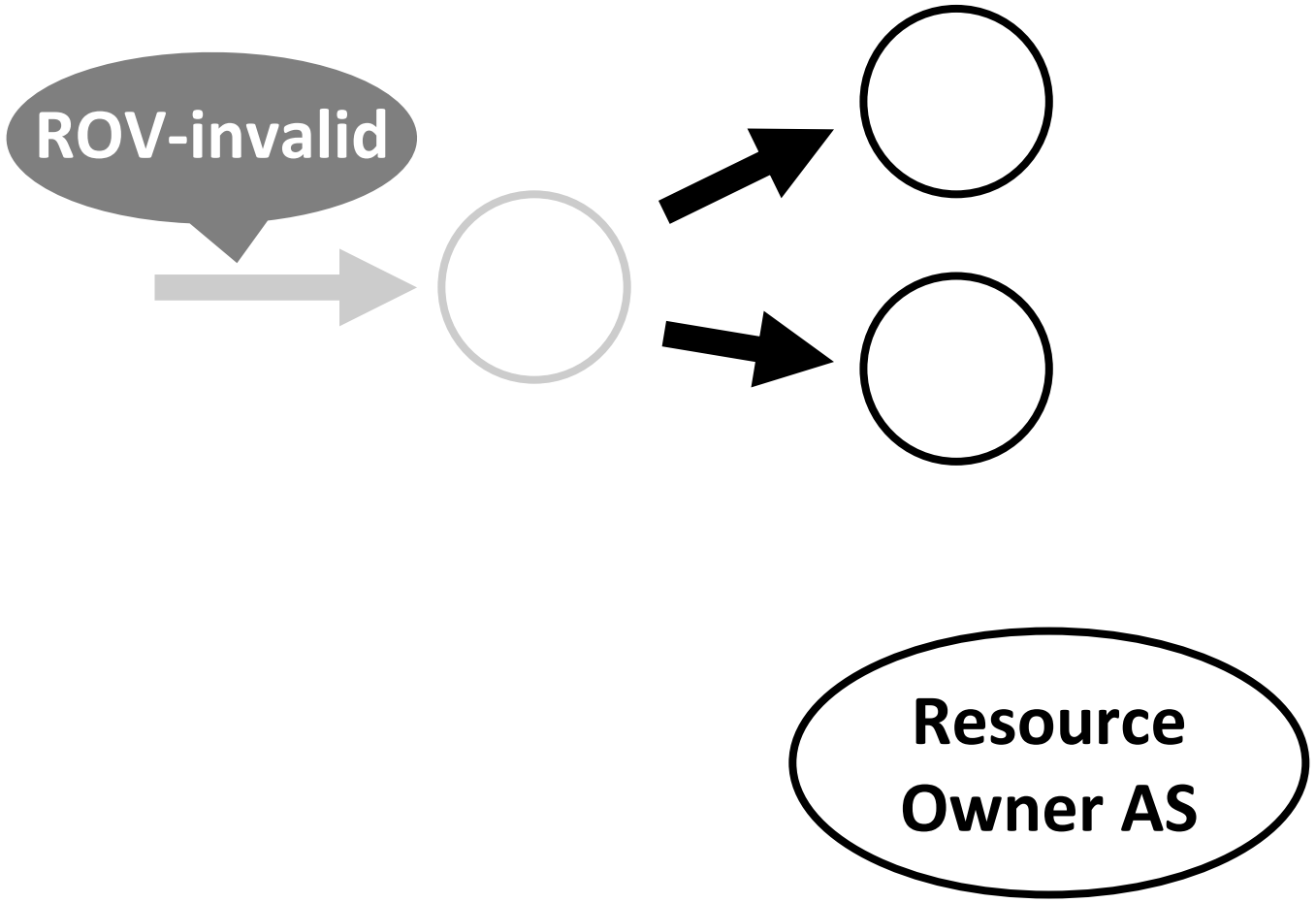
Interactivity Can Overwhelm Owners



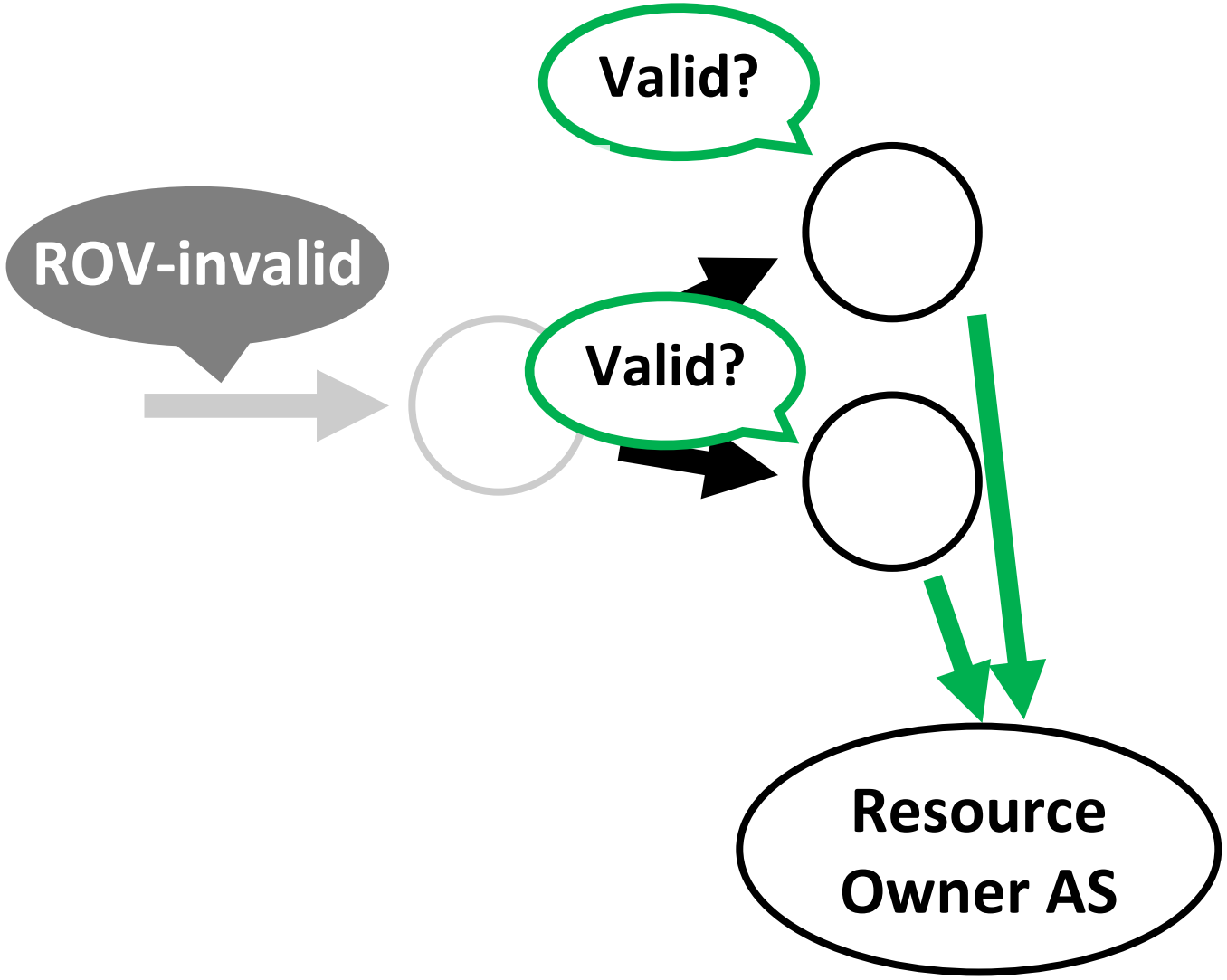
Interactivity Can Overwhelm Owners



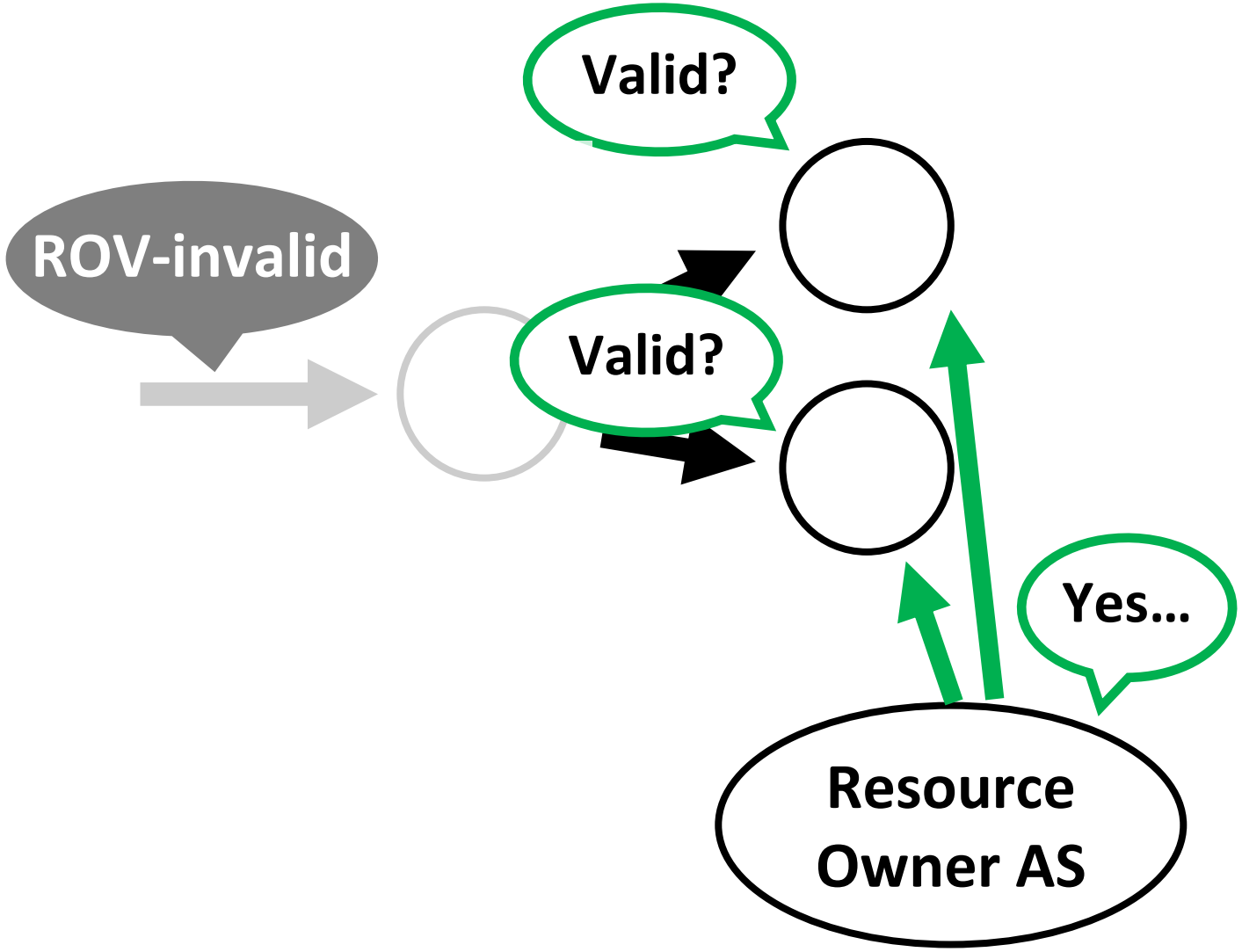
Interactivity Can Overwhelm Owners



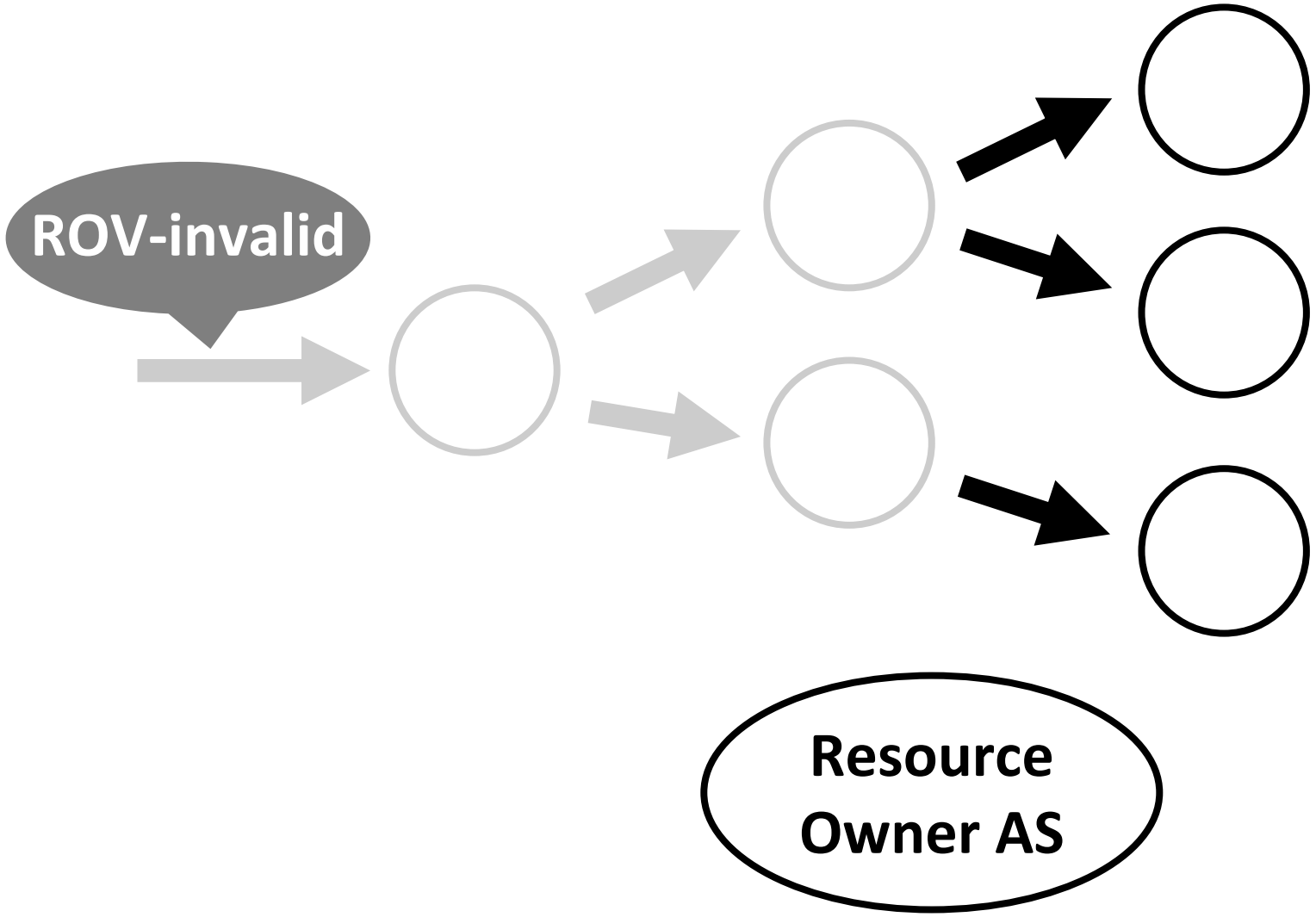
Interactivity Can Overwhelm Owners



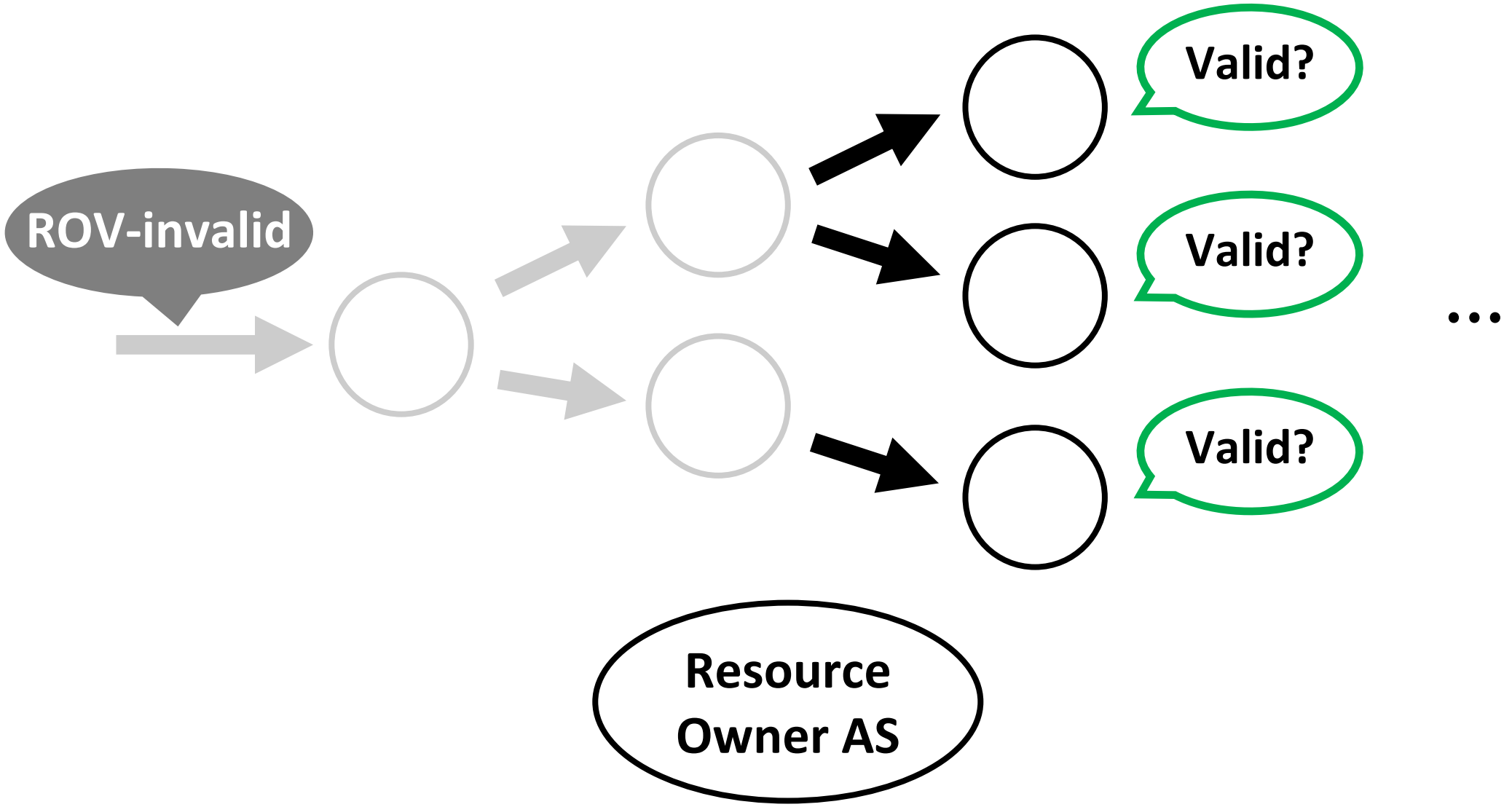
Interactivity Can Overwhelm Owners



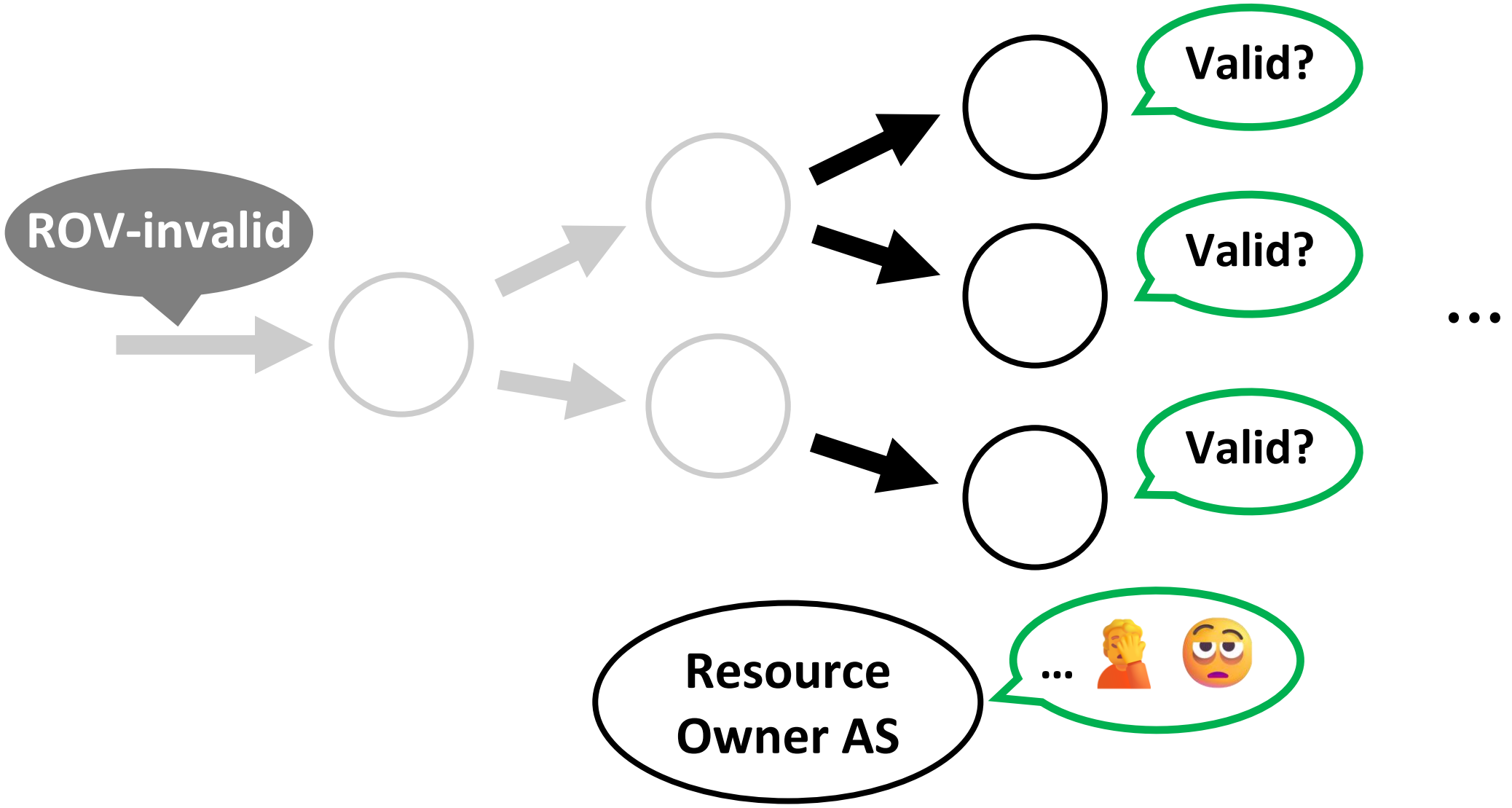
Interactivity Can Overwhelm Owners



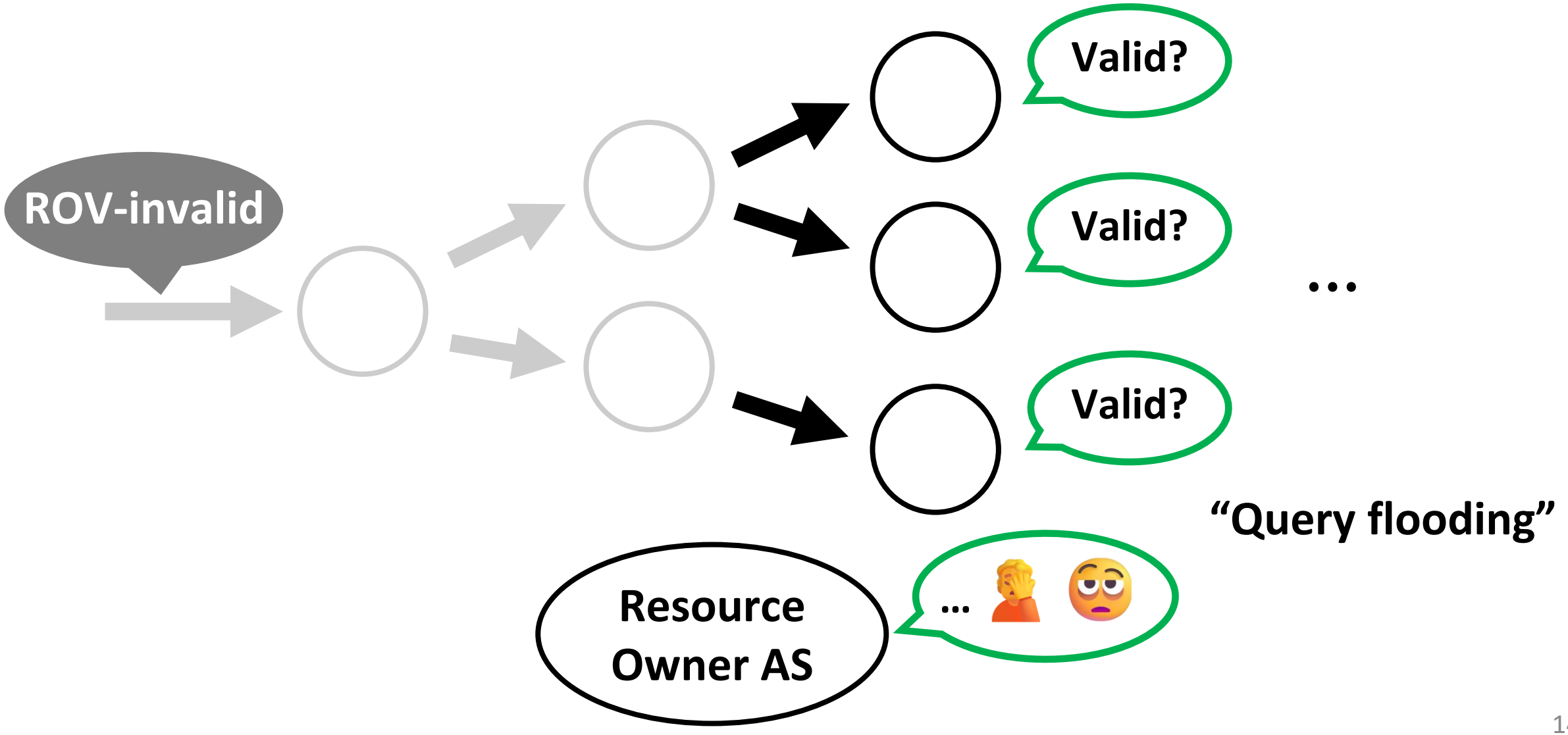
Interactivity Can Overwhelm Owners



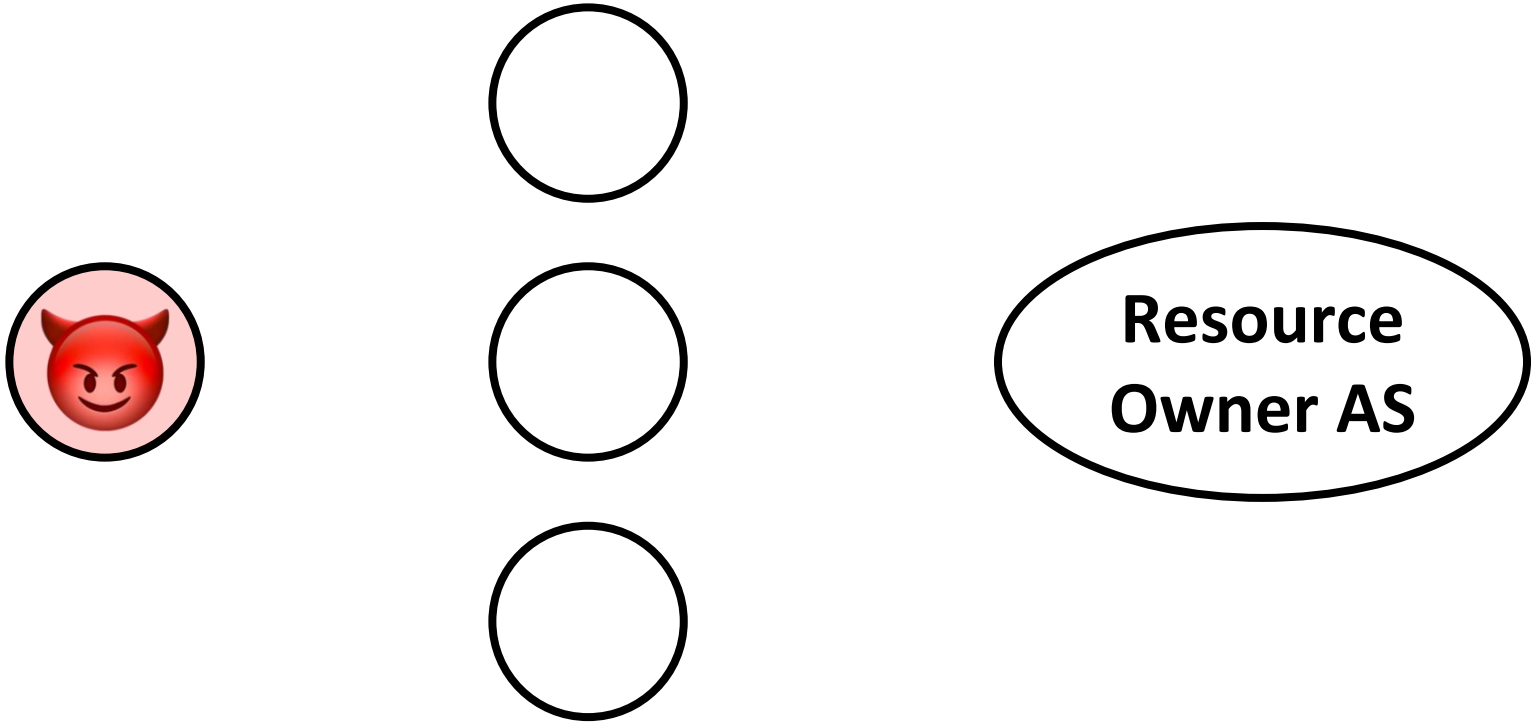
Interactivity Can Overwhelm Owners



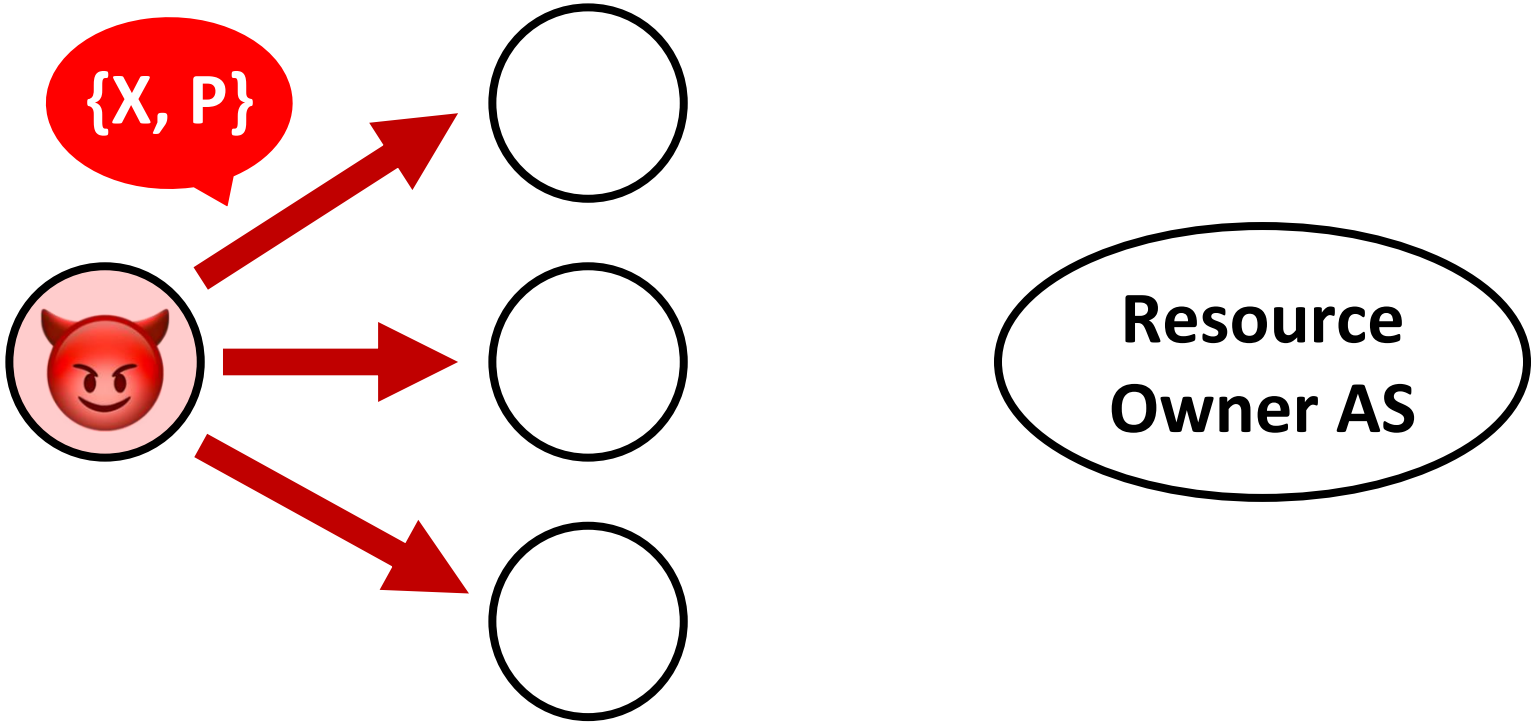
Interactivity Can Overwhelm Owners



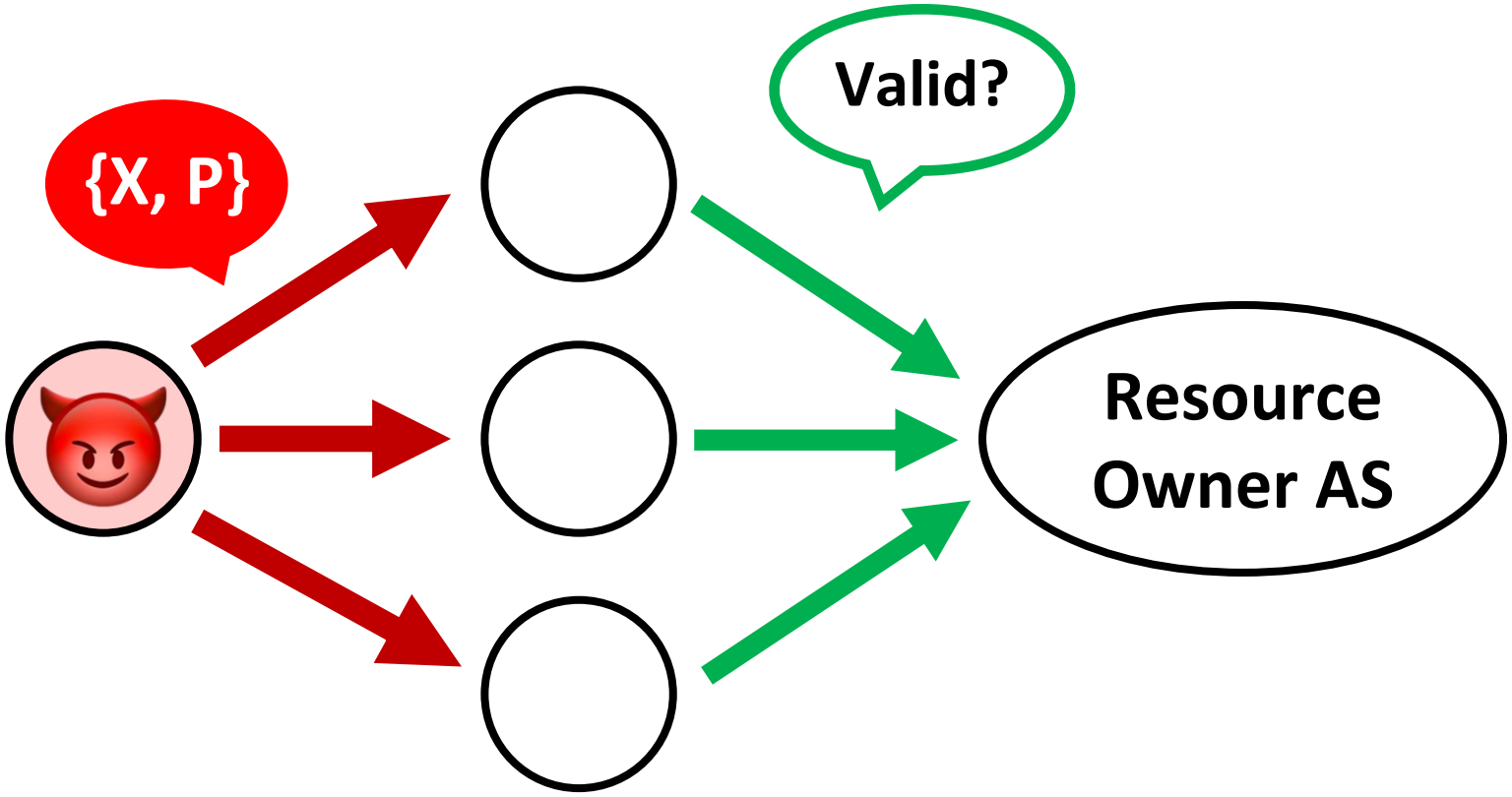
Interactivity Can Be Abused



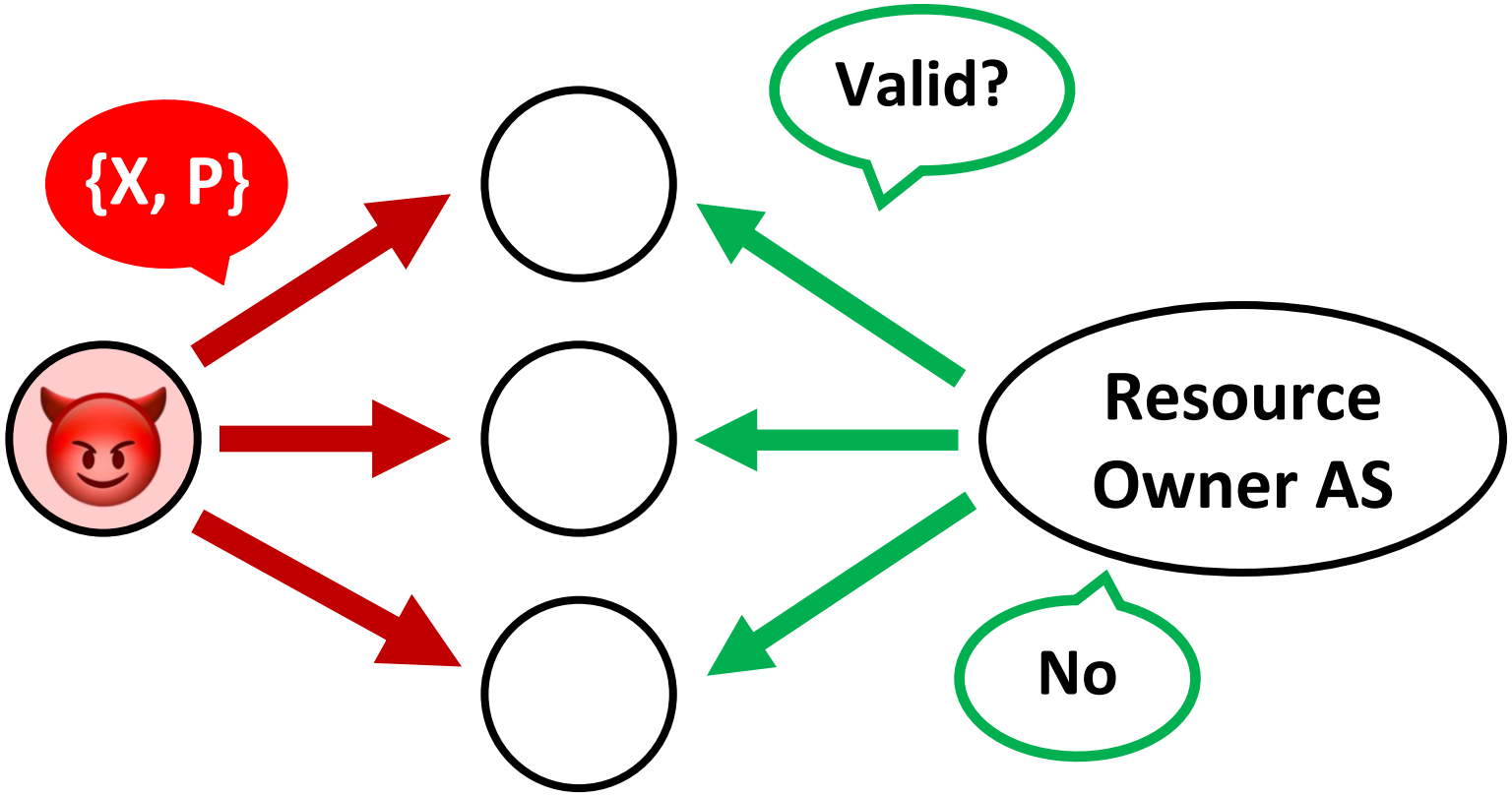
Interactivity Can Be Abused



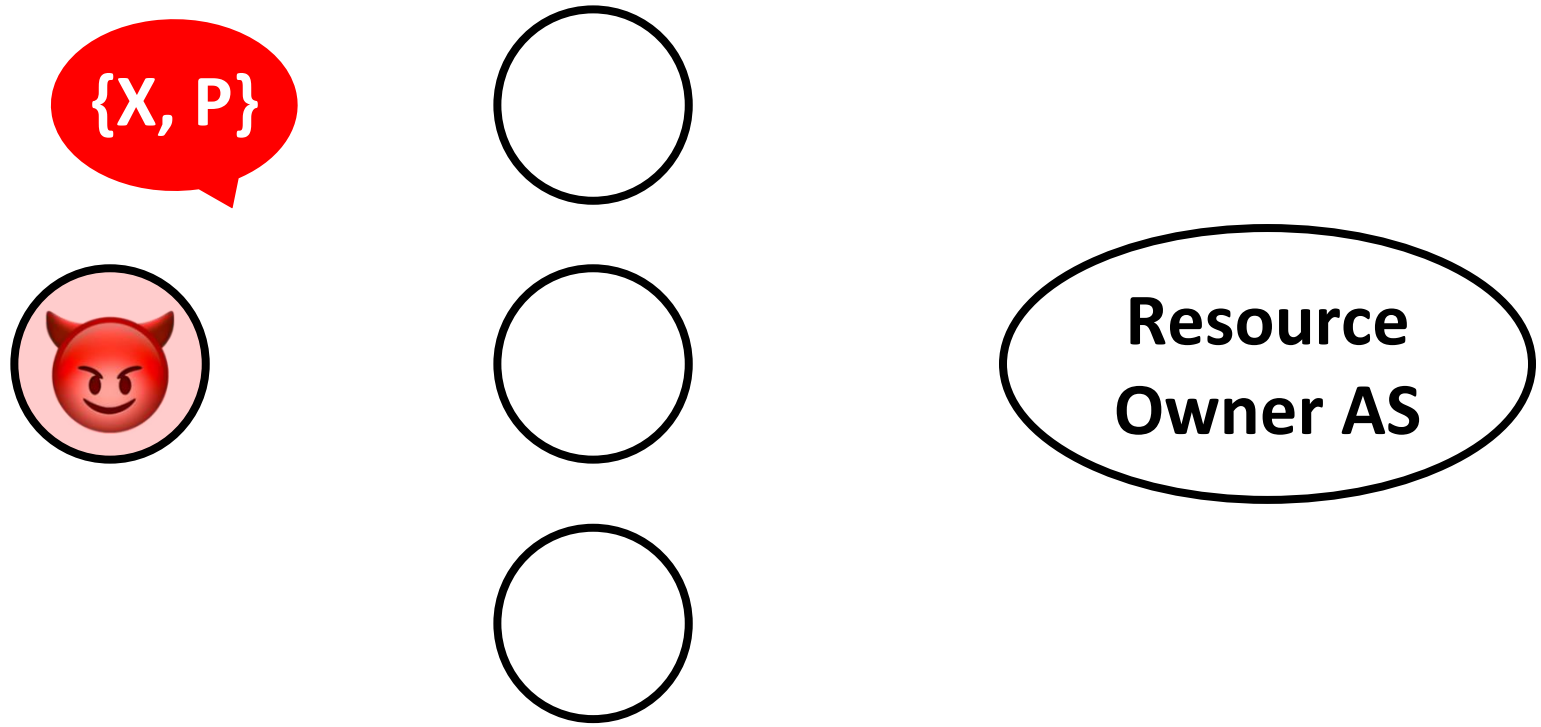
Interactivity Can Be Abused



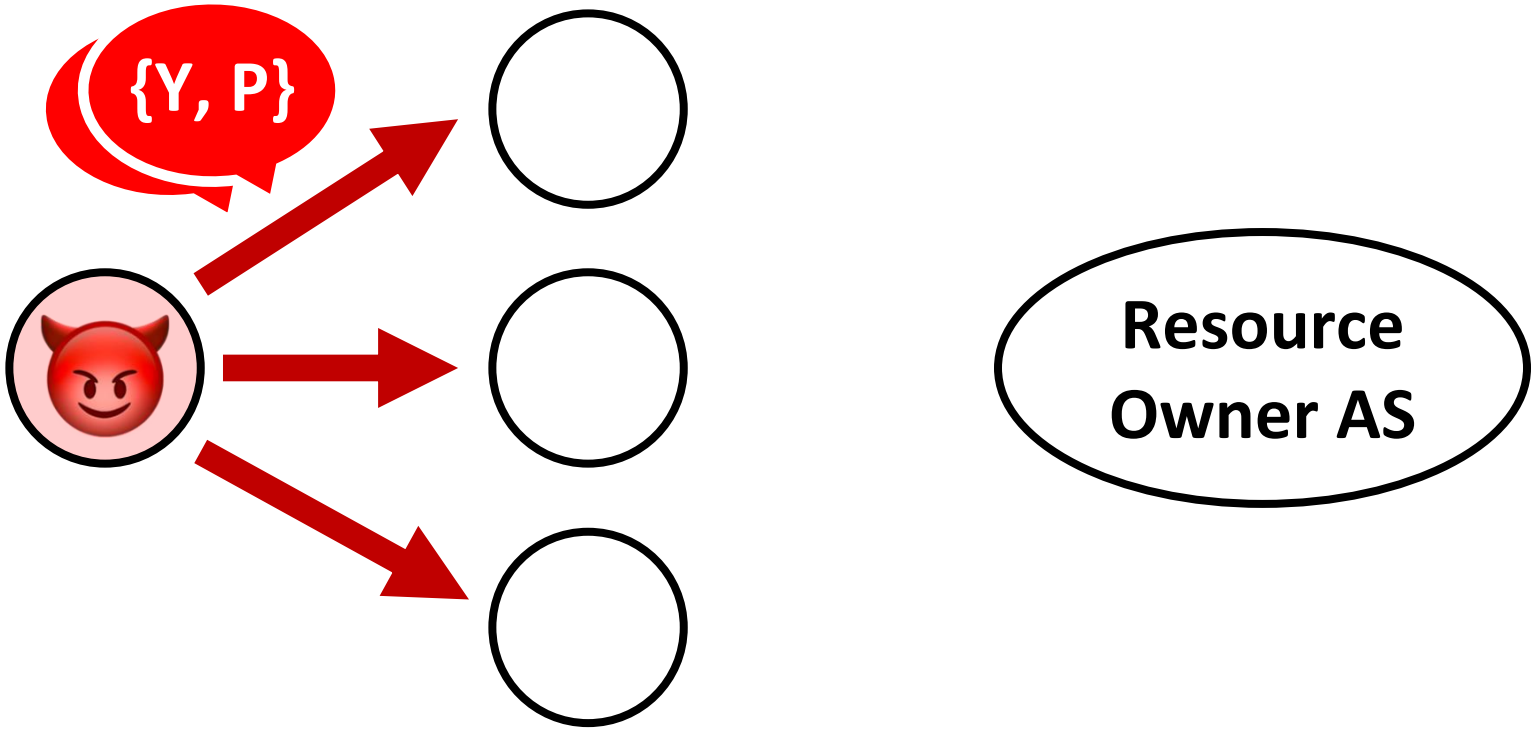
Interactivity Can Be Abused



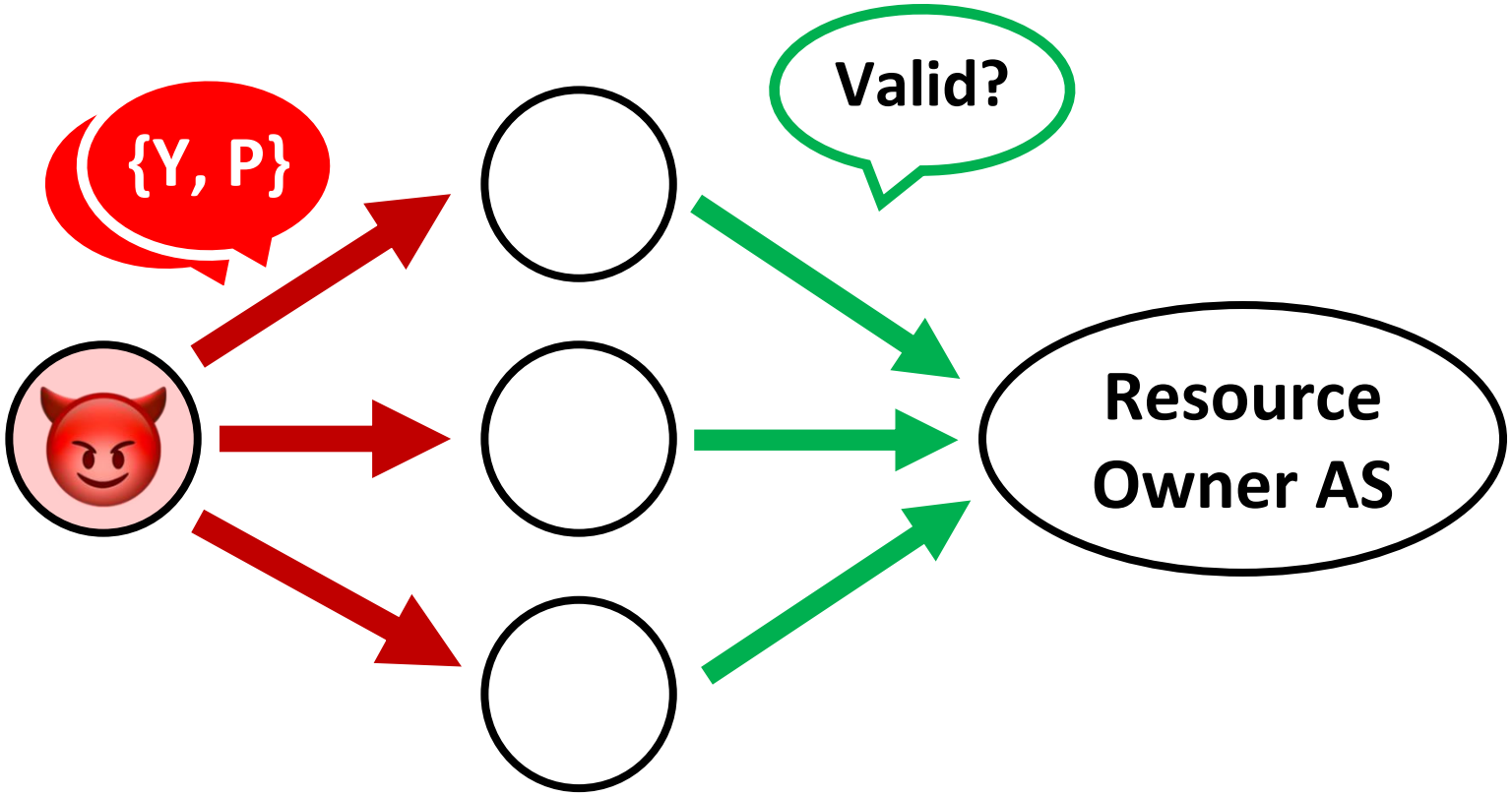
Interactivity Can Be Abused



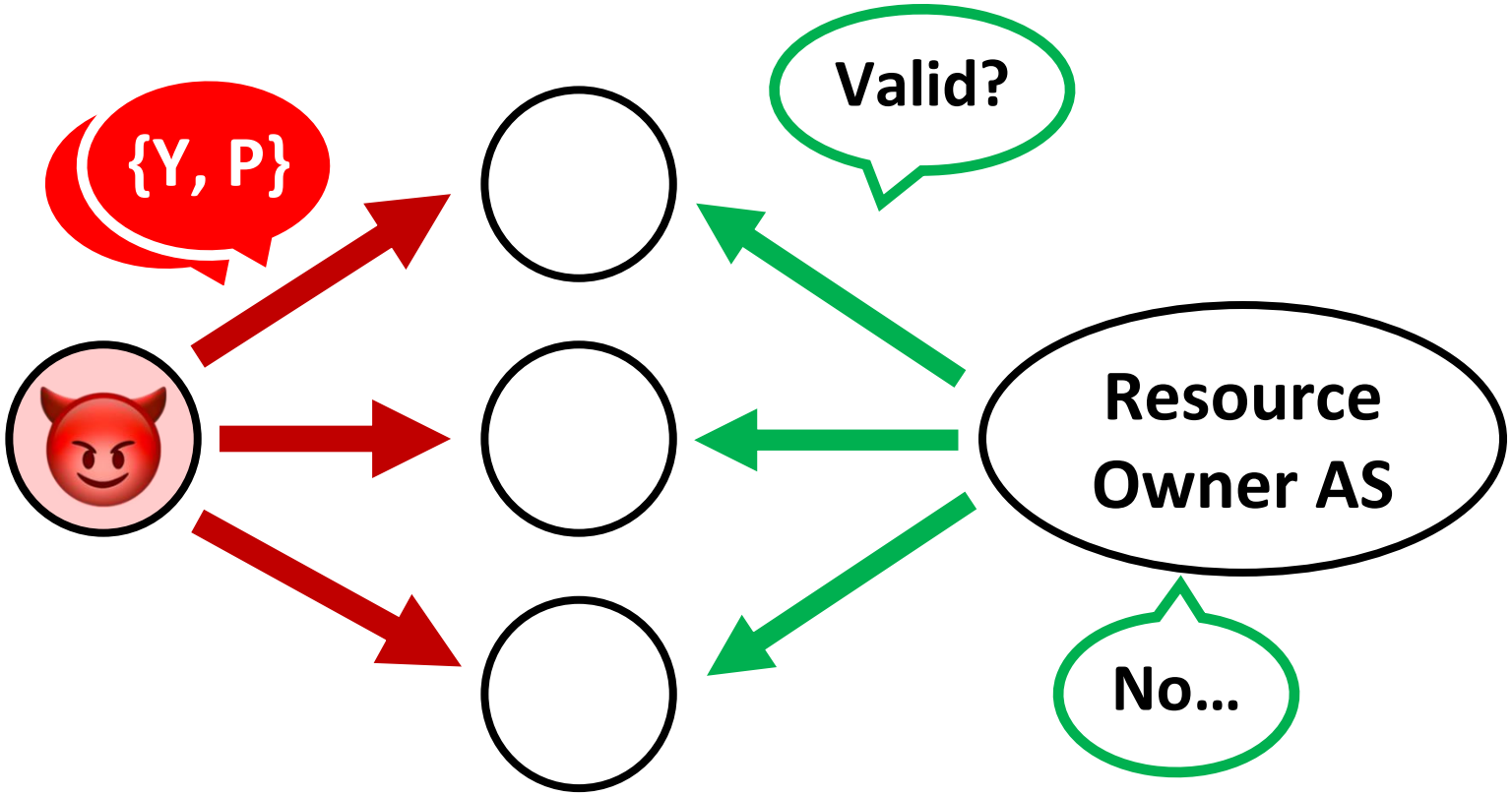
Interactivity Can Be Abused



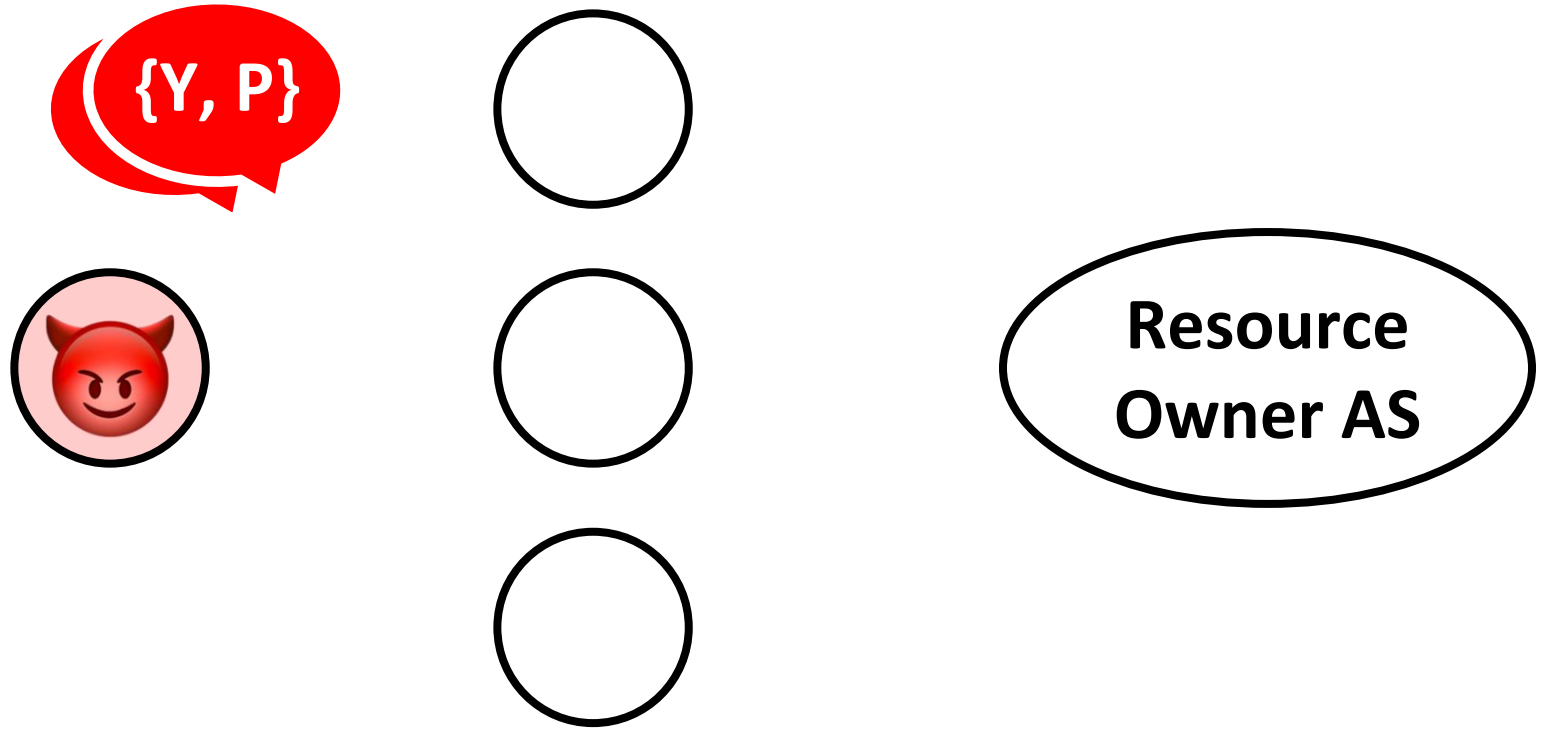
Interactivity Can Be Abused



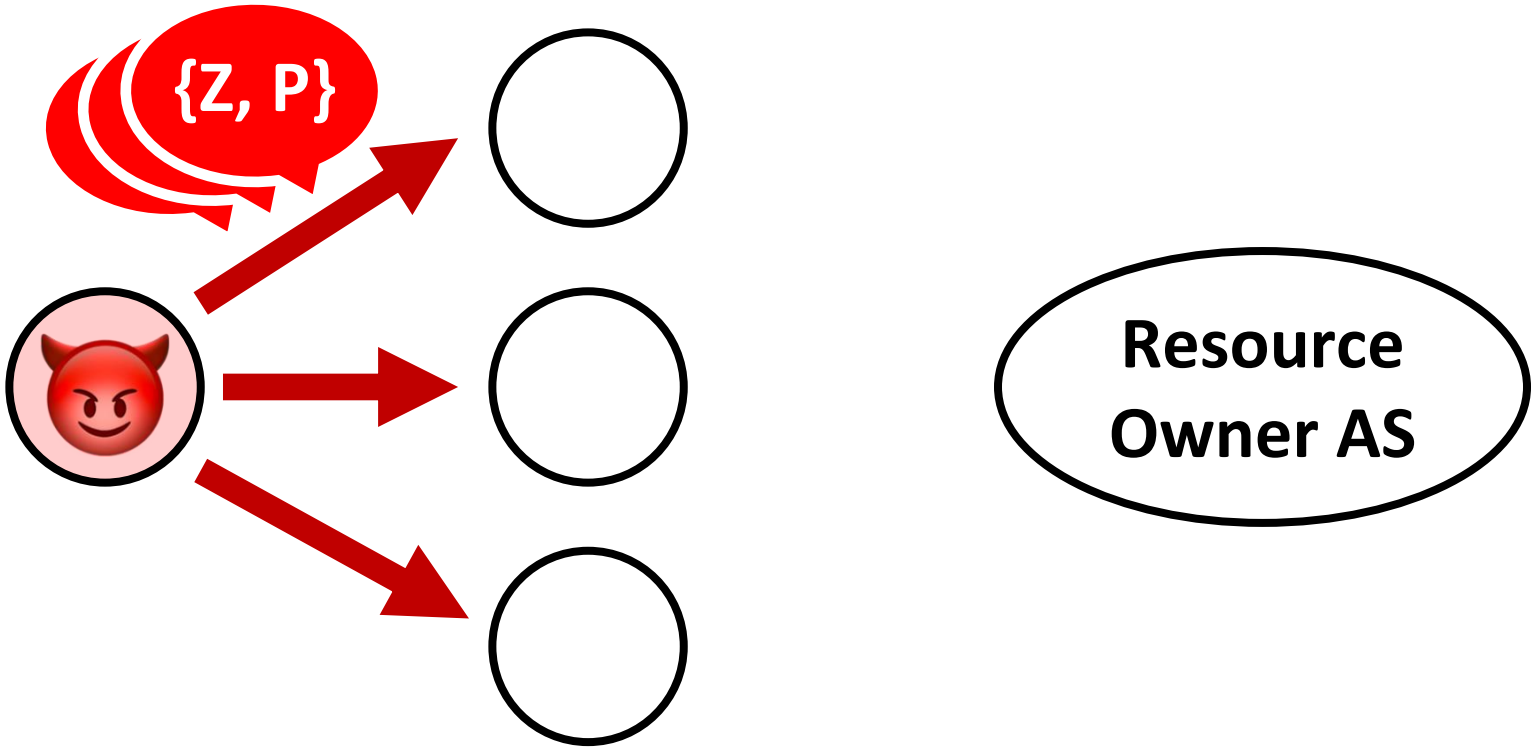
Interactivity Can Be Abused



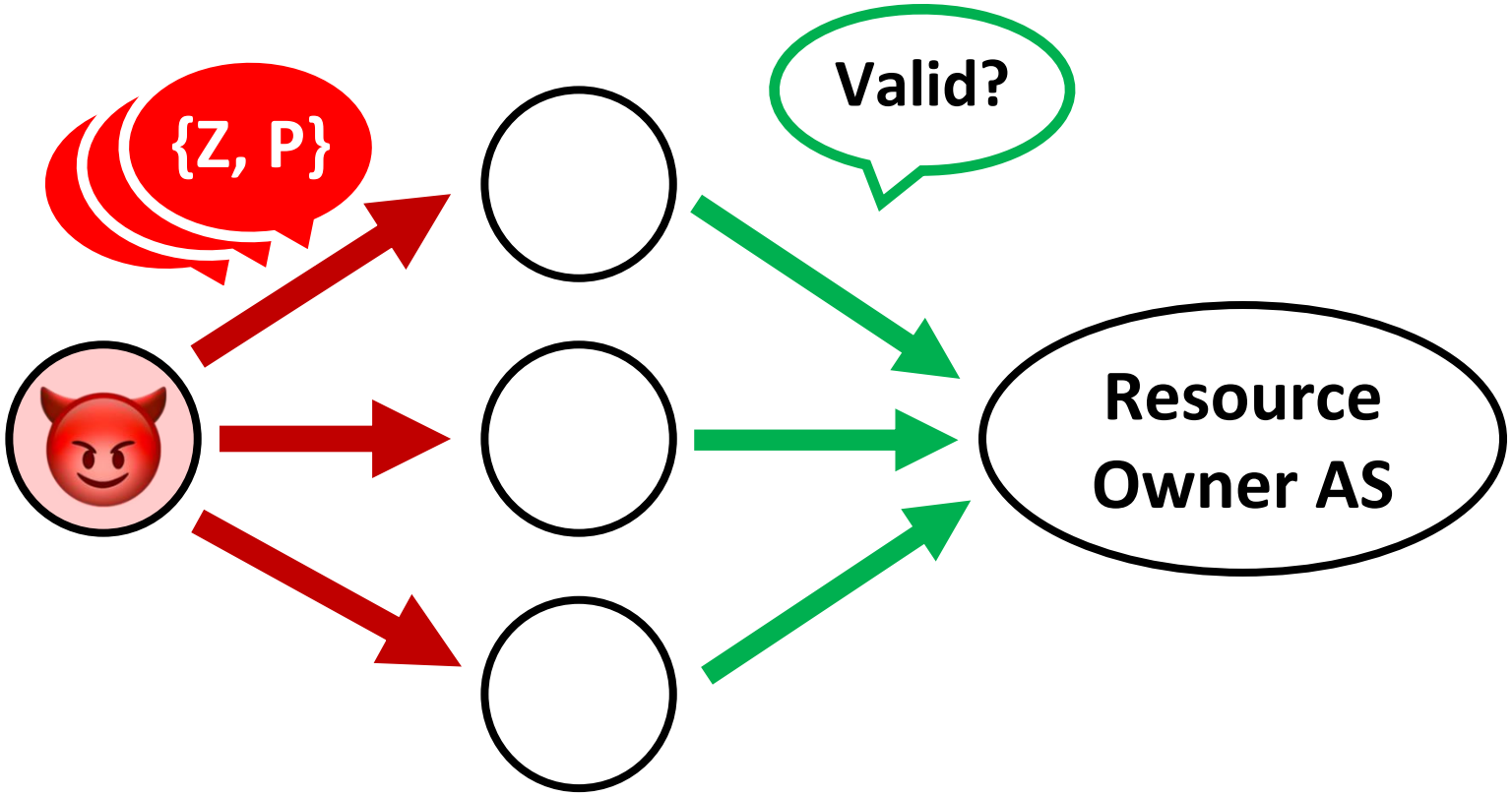
Interactivity Can Be Abused



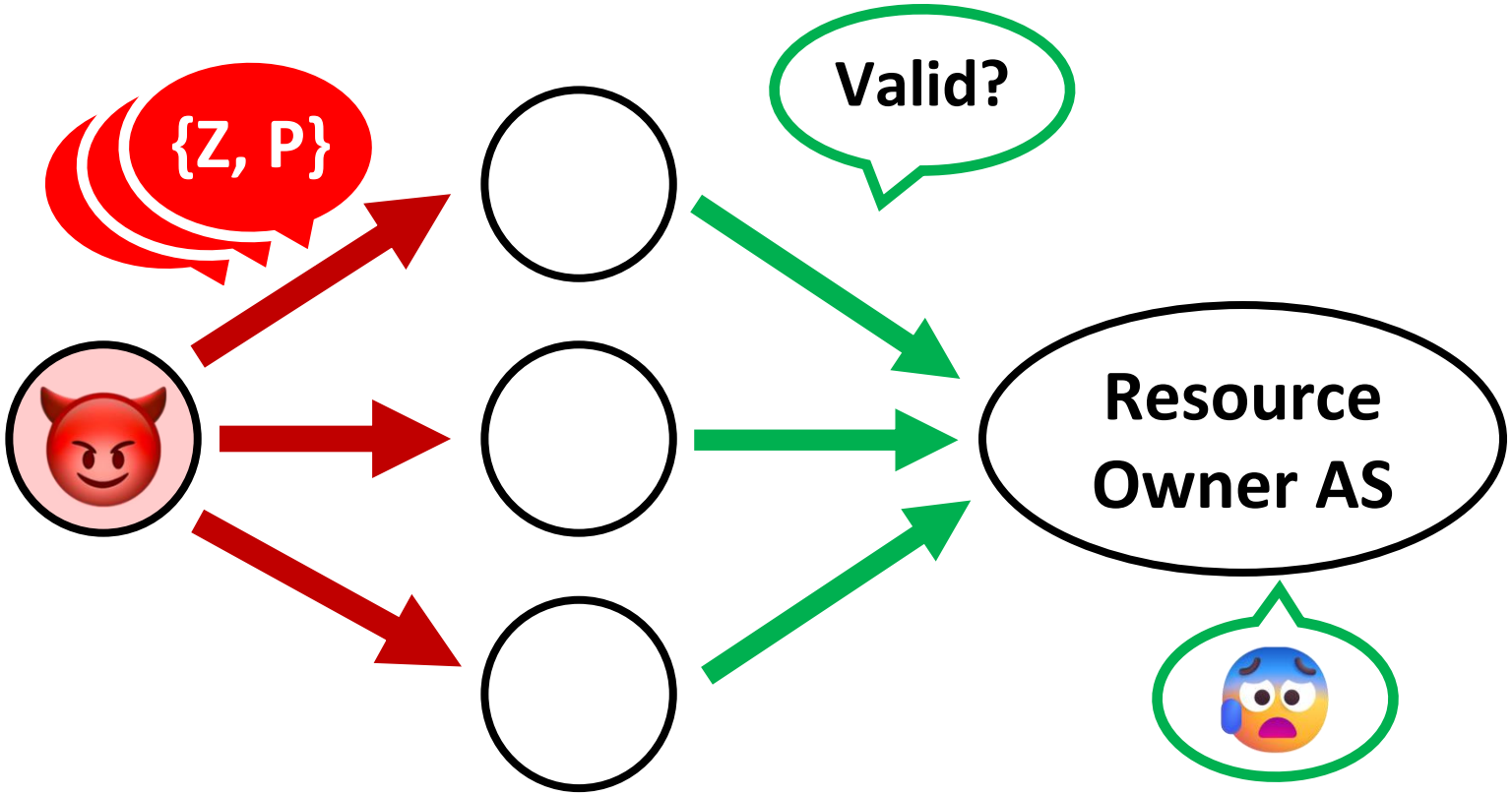
Interactivity Can Be Abused



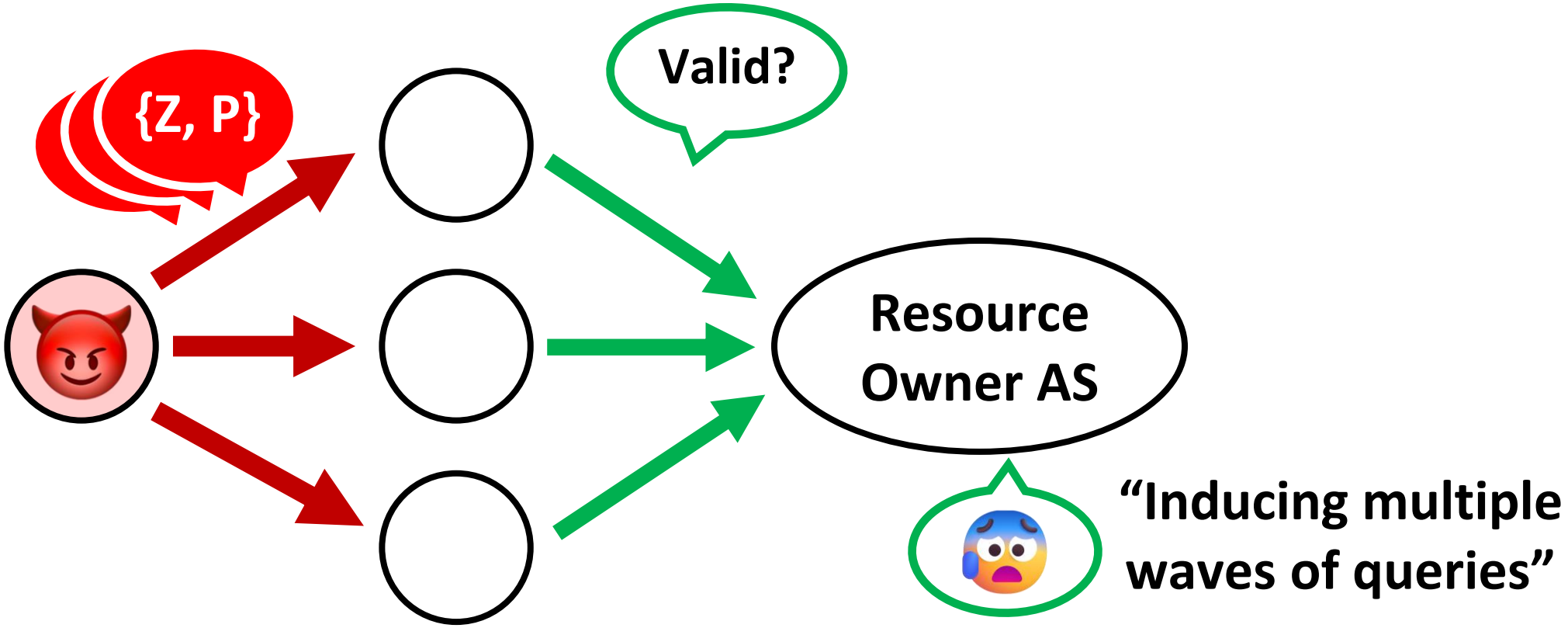
Interactivity Can Be Abused



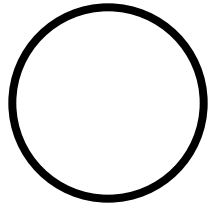
Interactivity Can Be Abused

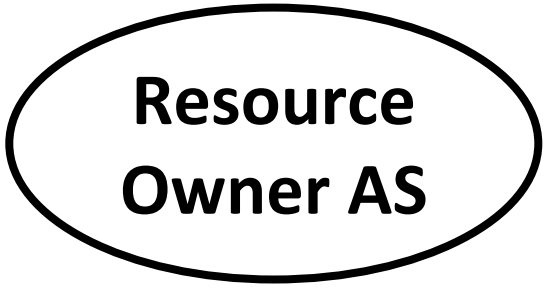


Interactivity Can Be Abused

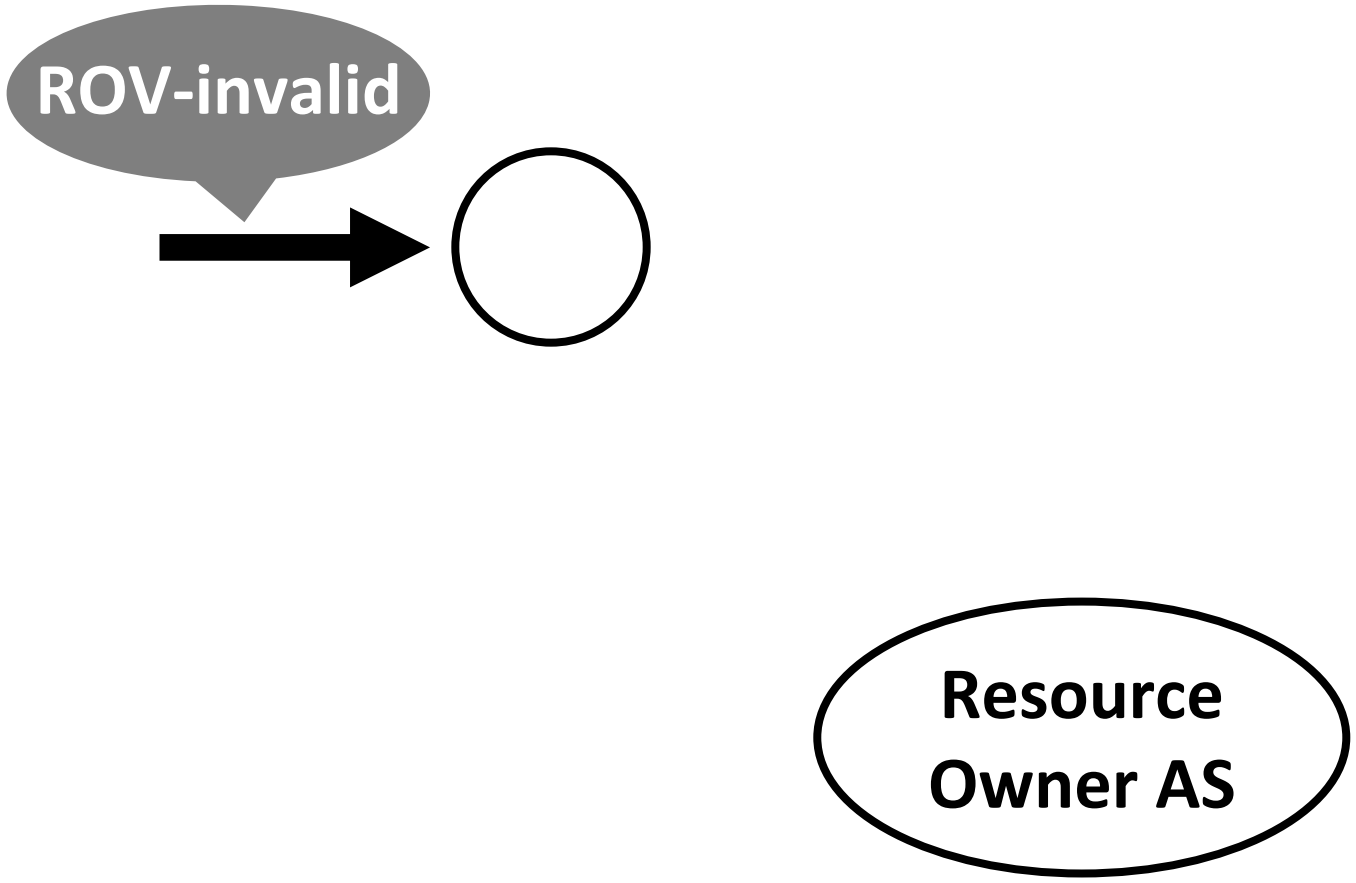


iROV Prevents Query Flooding and Abuse

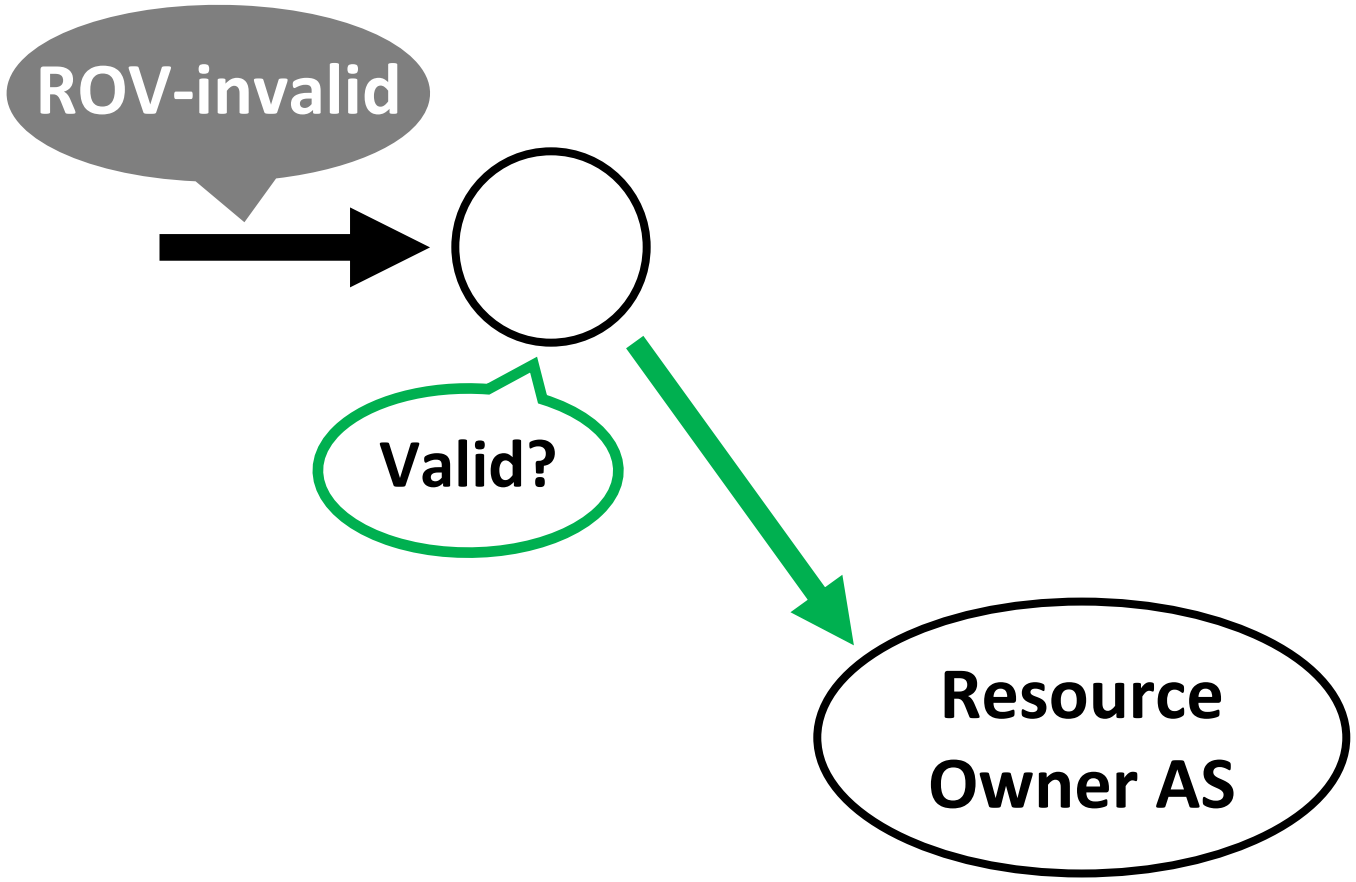




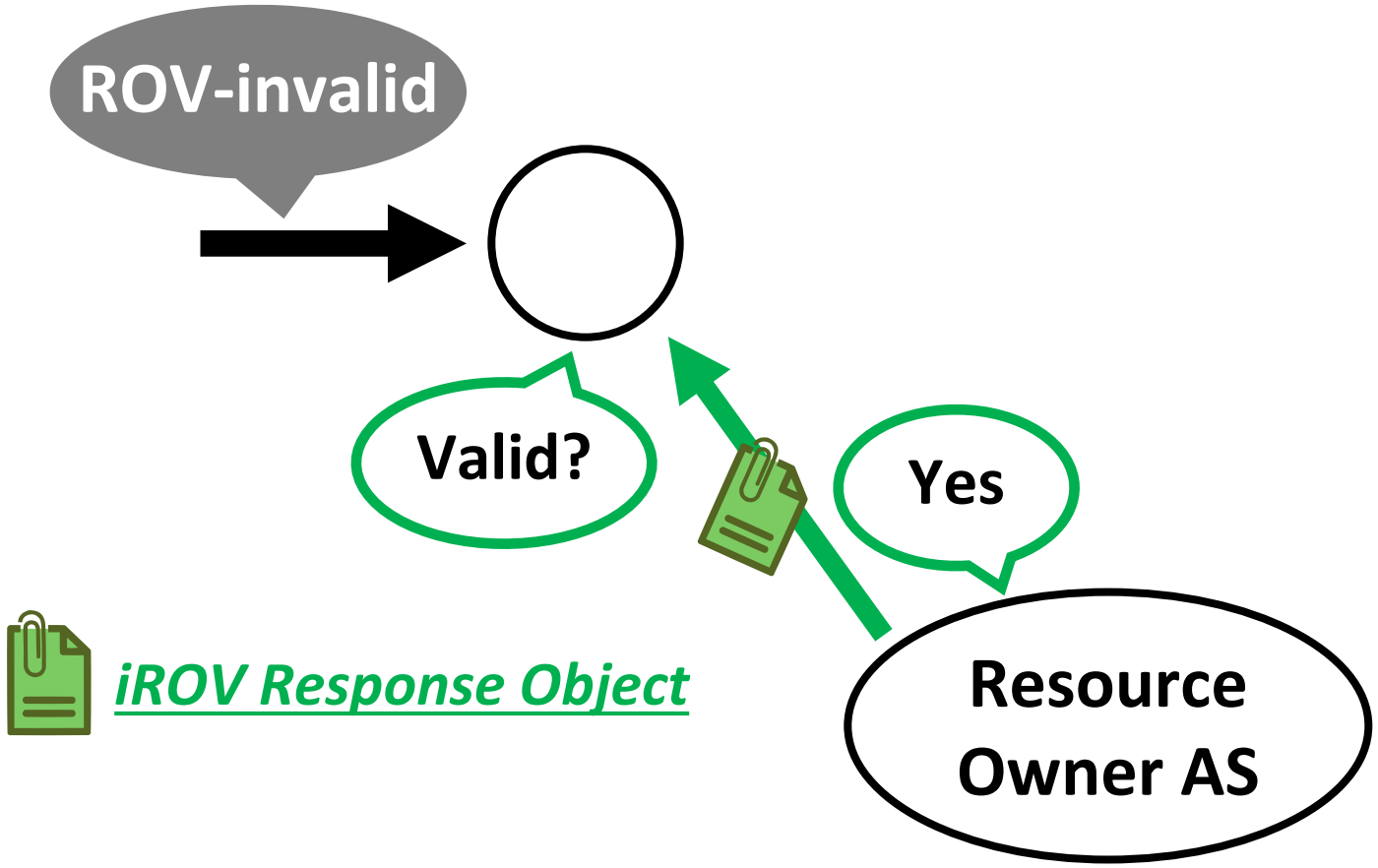
iROV Prevents Query Flooding and Abuse



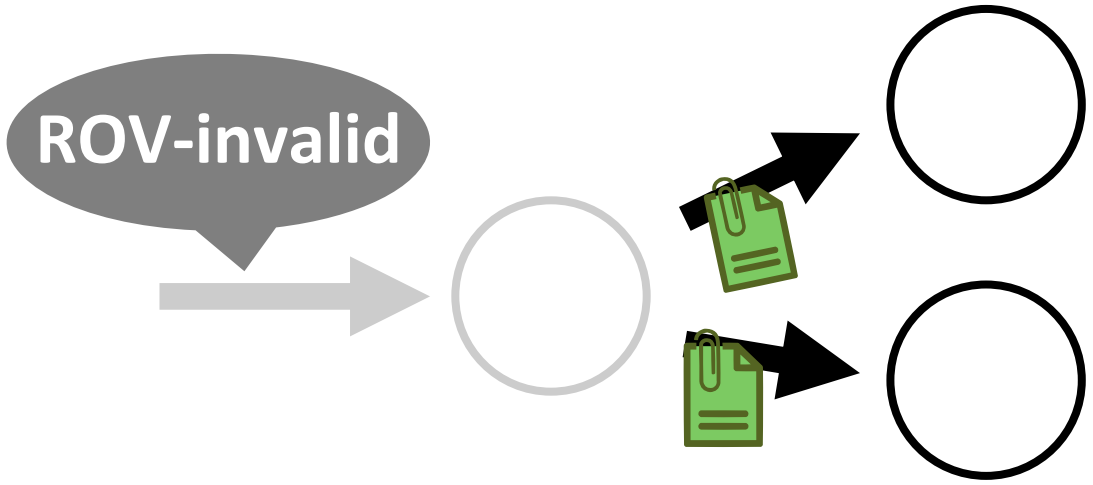
iROV Prevents Query Flooding and Abuse



iROV Prevents Query Flooding and Abuse



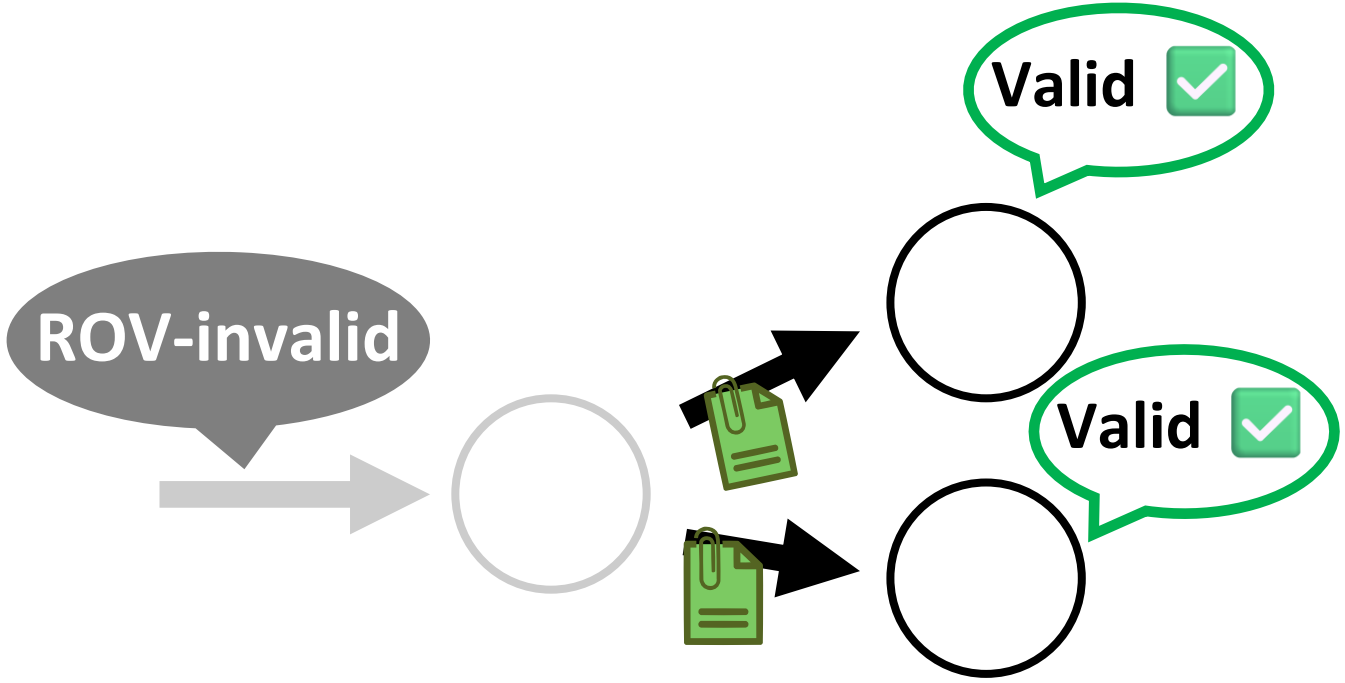
iROV Prevents Query Flooding and Abuse



iROV Response Object

Resource Owner AS

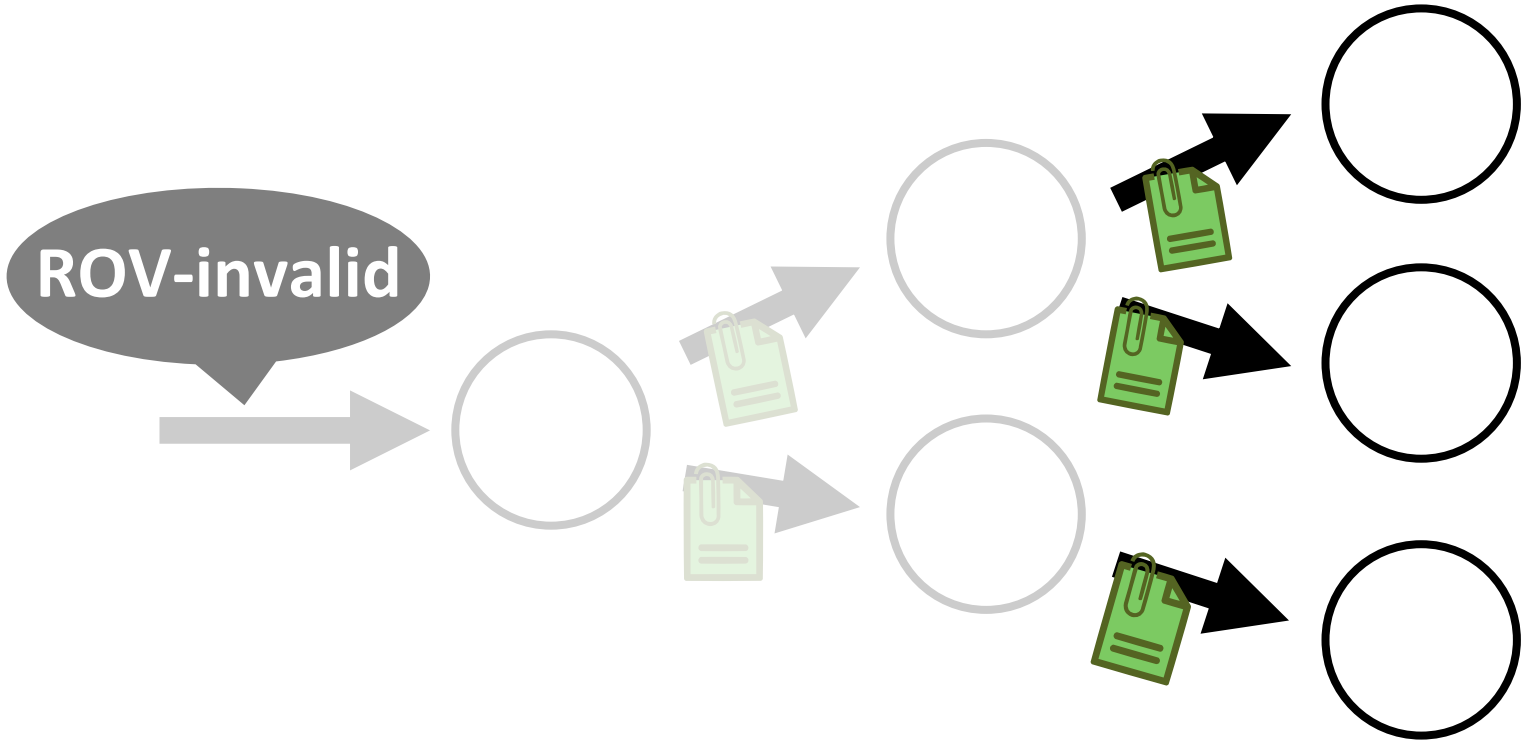
iROV Prevents Query Flooding and Abuse



iROV Response Object

Resource Owner AS

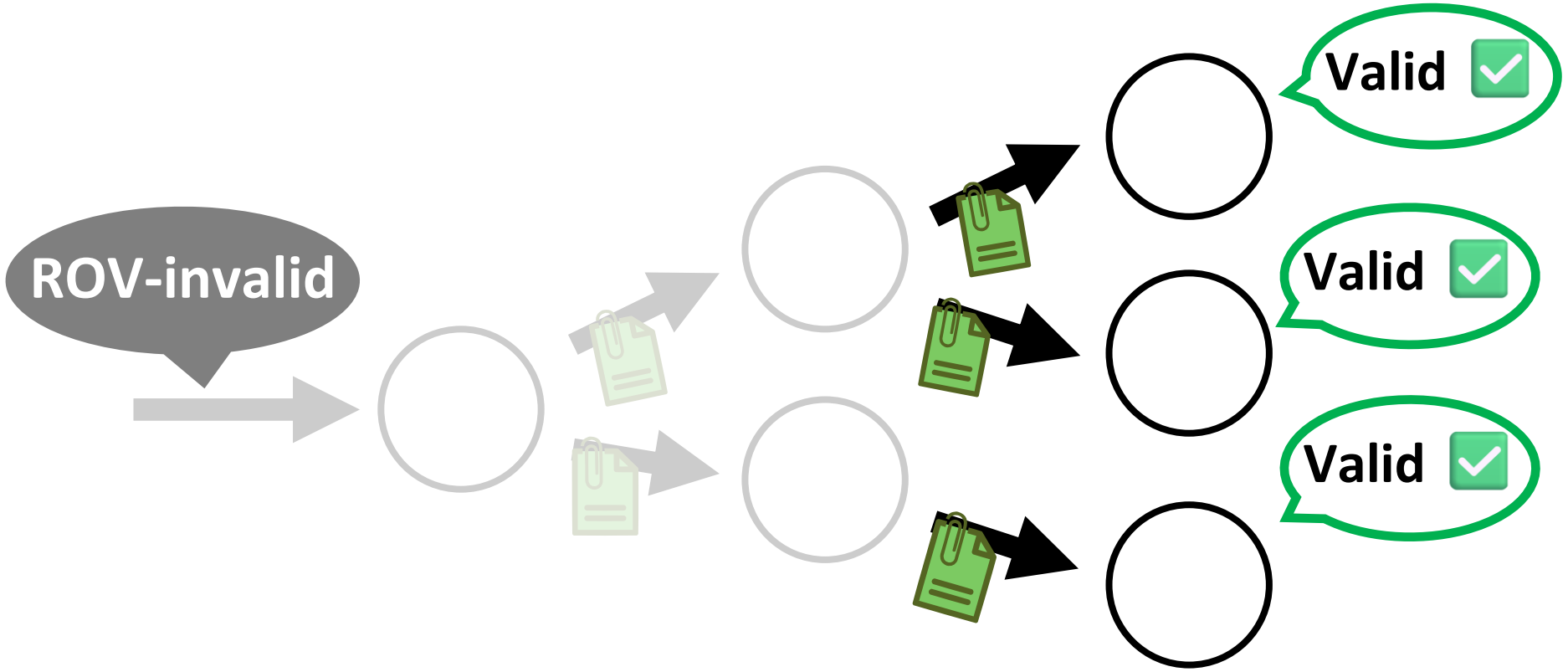
iROV Prevents Query Flooding and Abuse



iROV Response Object

Resource Owner AS

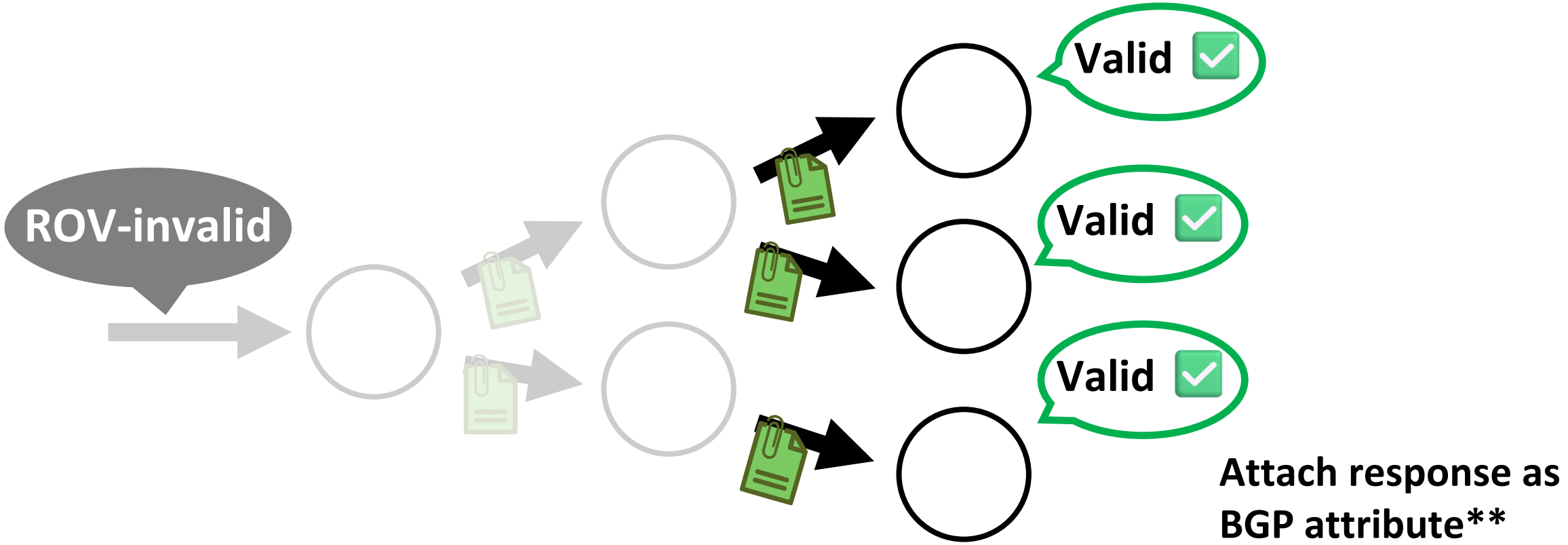
iROV Prevents Query Flooding and Abuse



iROV Response Object

Resource Owner AS

iROV Prevents Query Flooding and Abuse

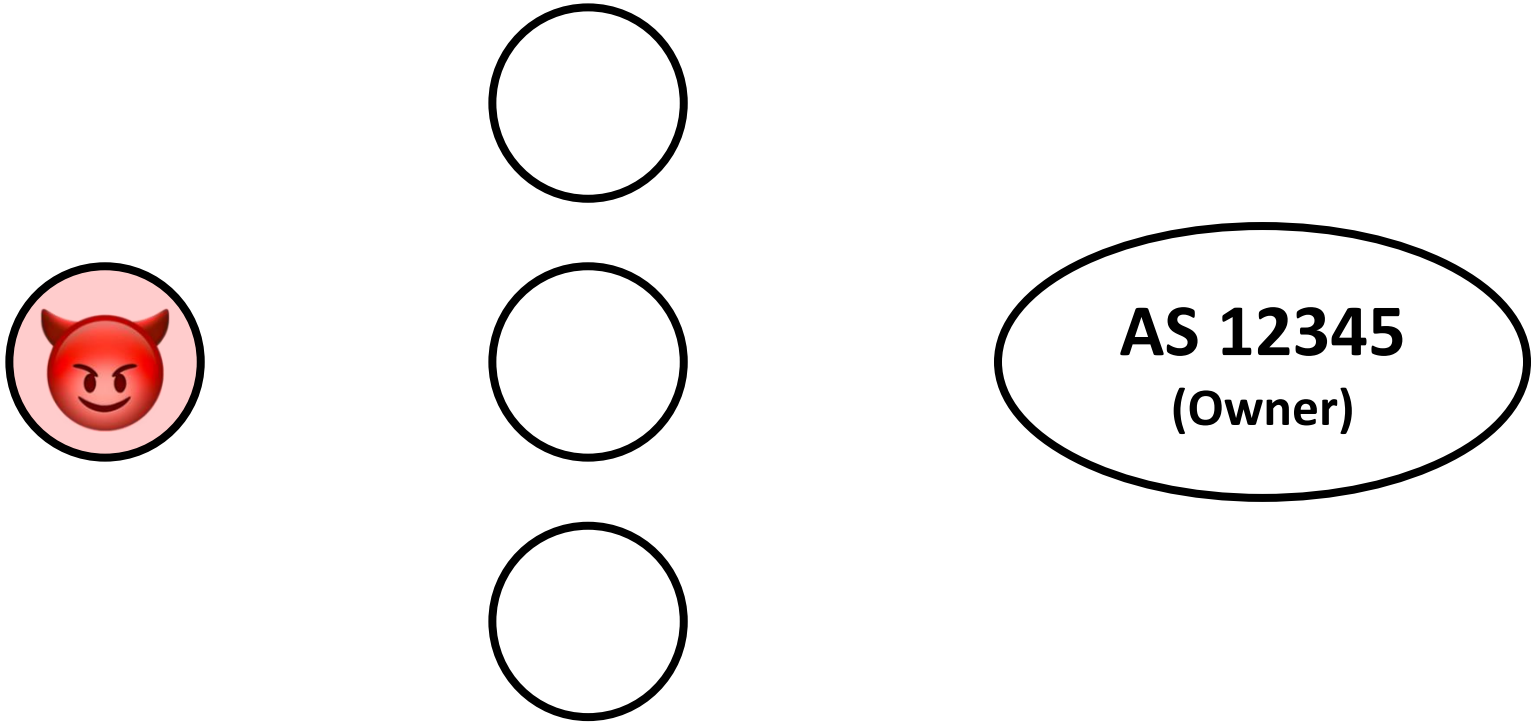


iROV Response Object

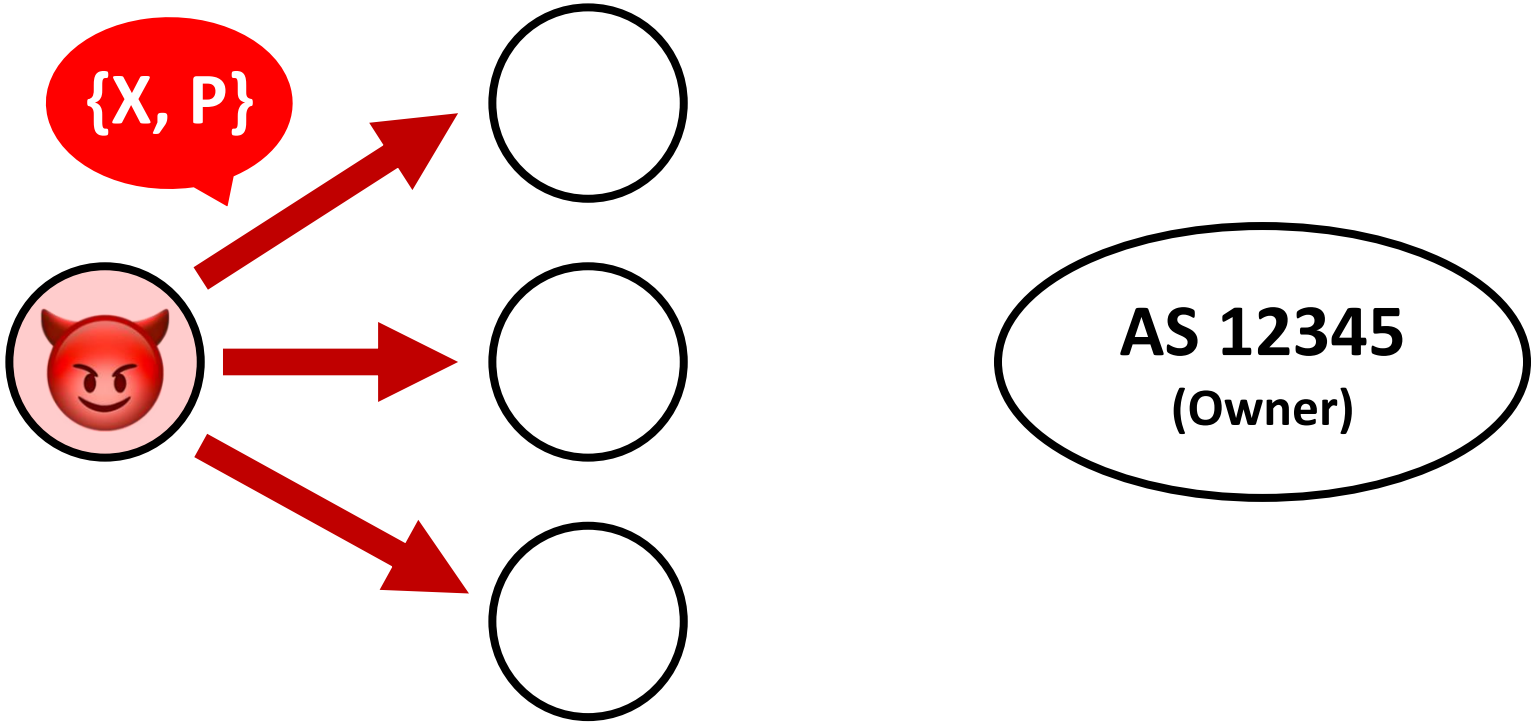
Resource Owner AS

Attribute is set as **optional and transitive such that non-ROV ASes will propagate attribute even if they do not recognize it

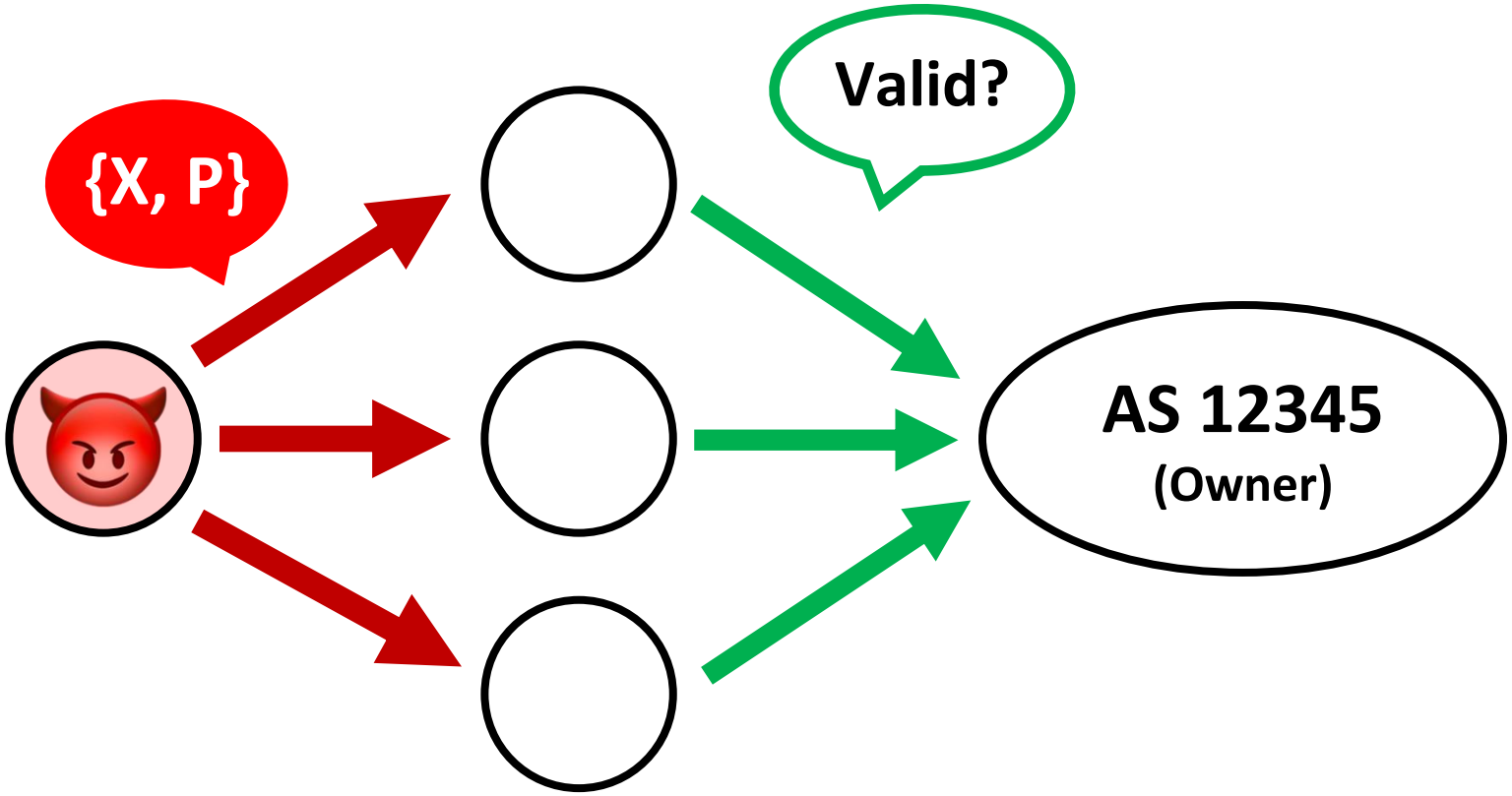
iROV Prevents Query Flooding and Abuse



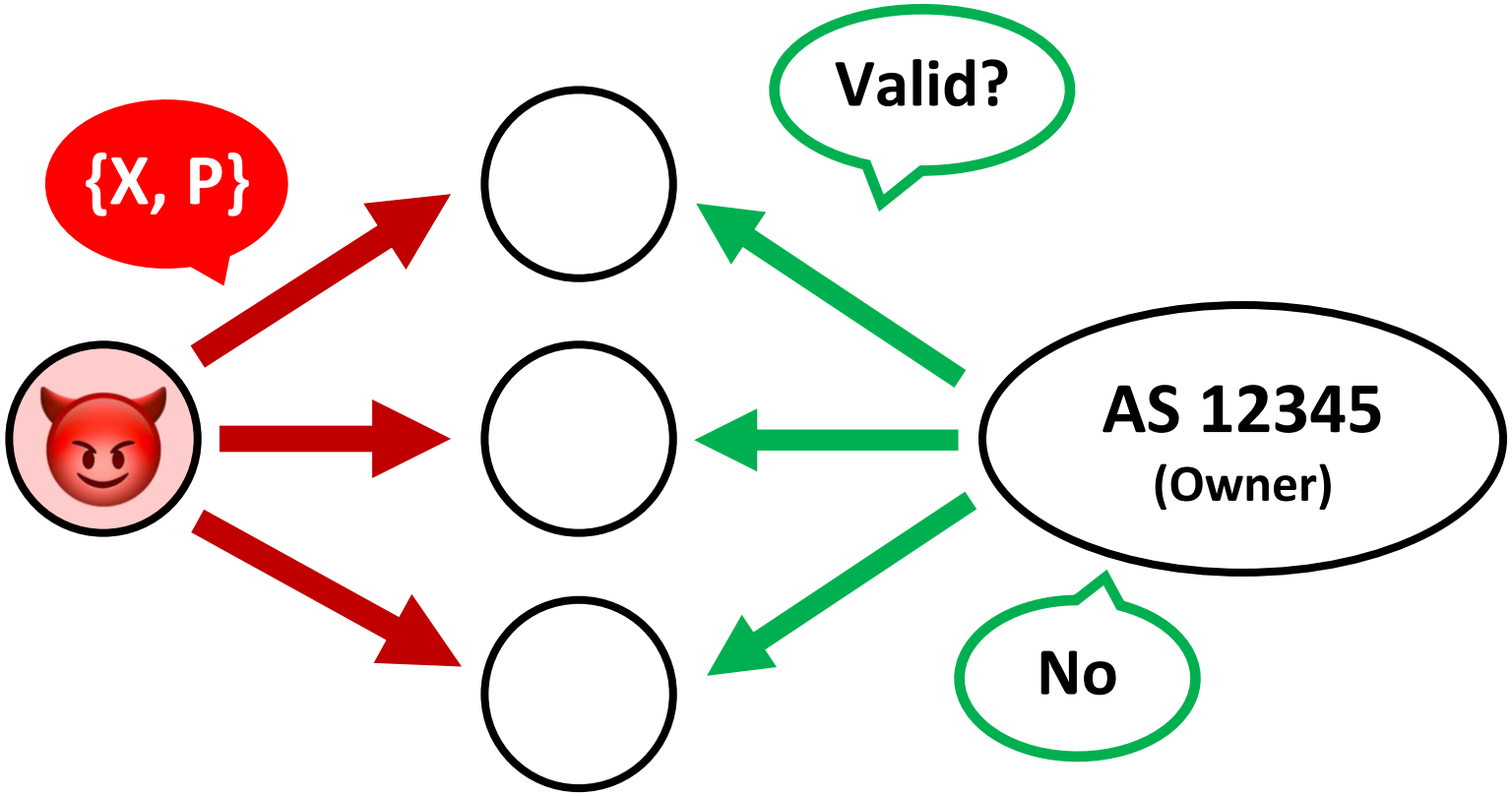
iROV Prevents Query Flooding and Abuse



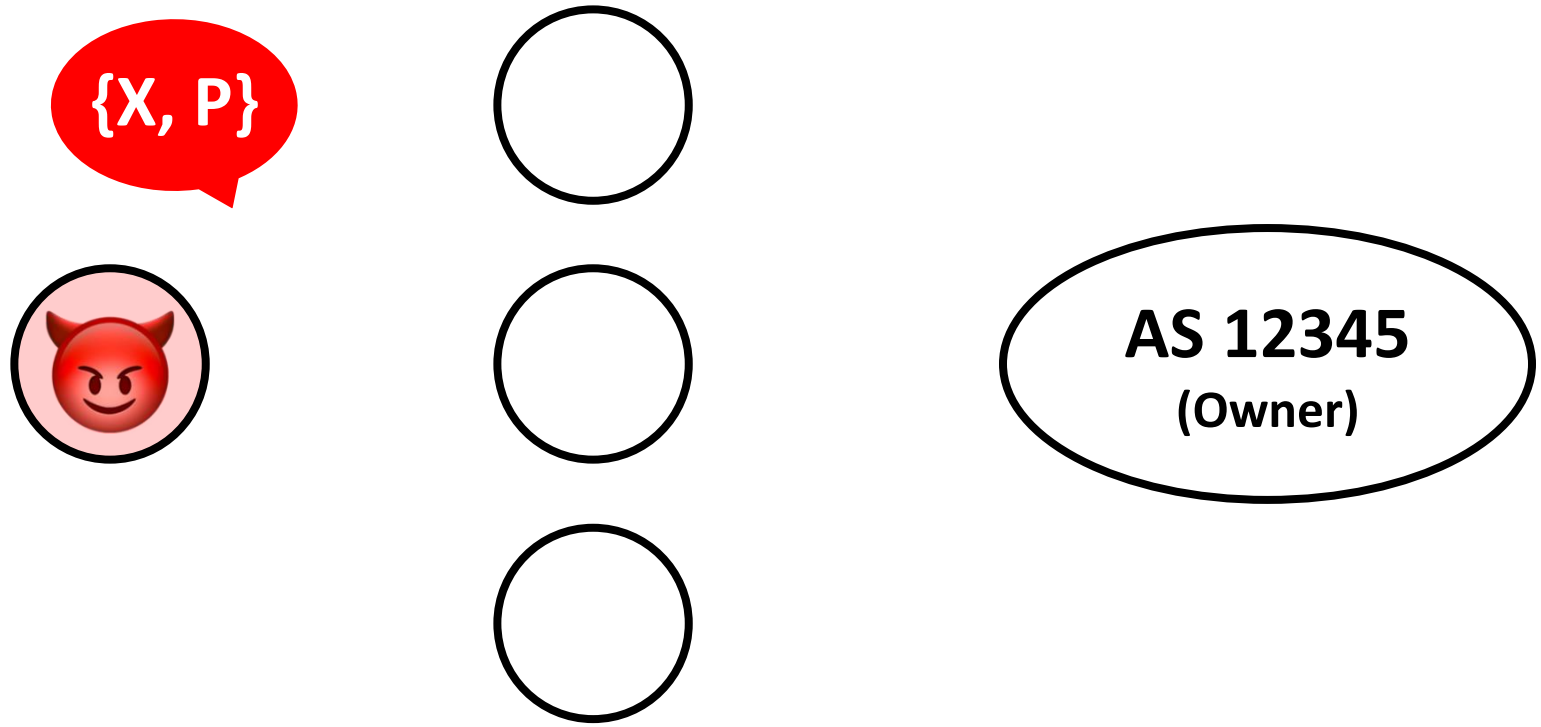
iROV Prevents Query Flooding and Abuse



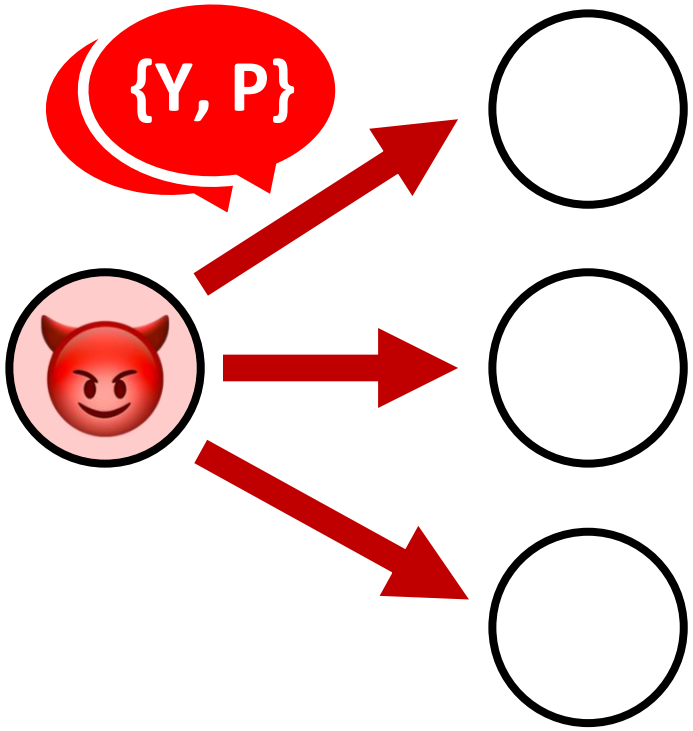
iROV Prevents Query Flooding and Abuse

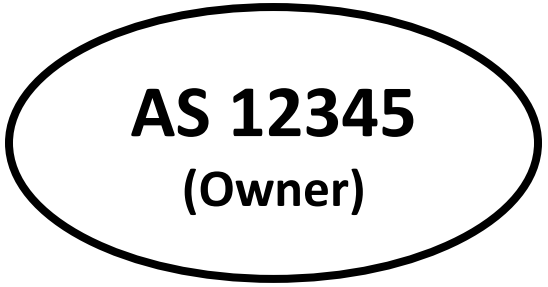


iROV Prevents Query Flooding and Abuse

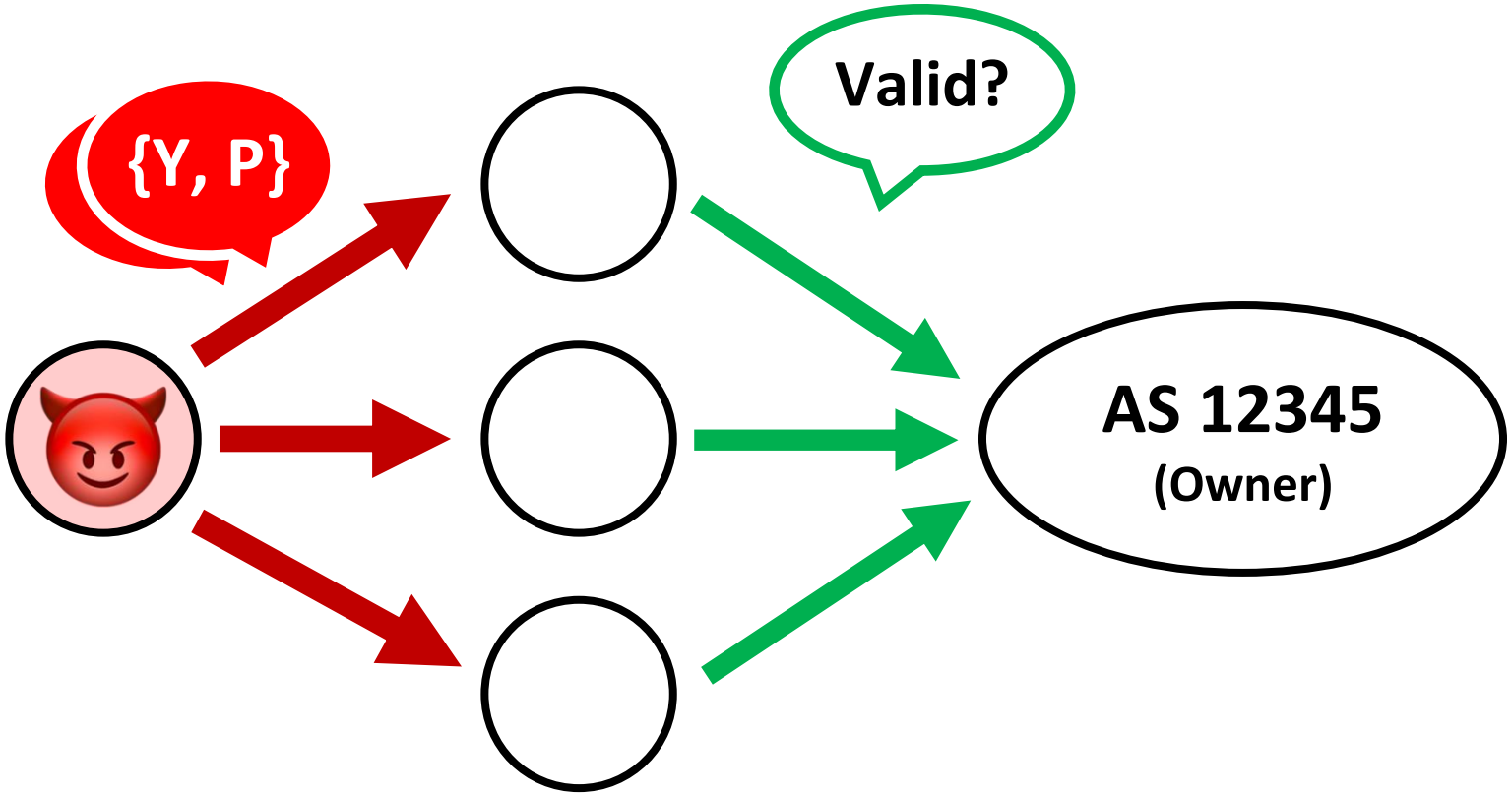


iROV Prevents Query Flooding and Abuse

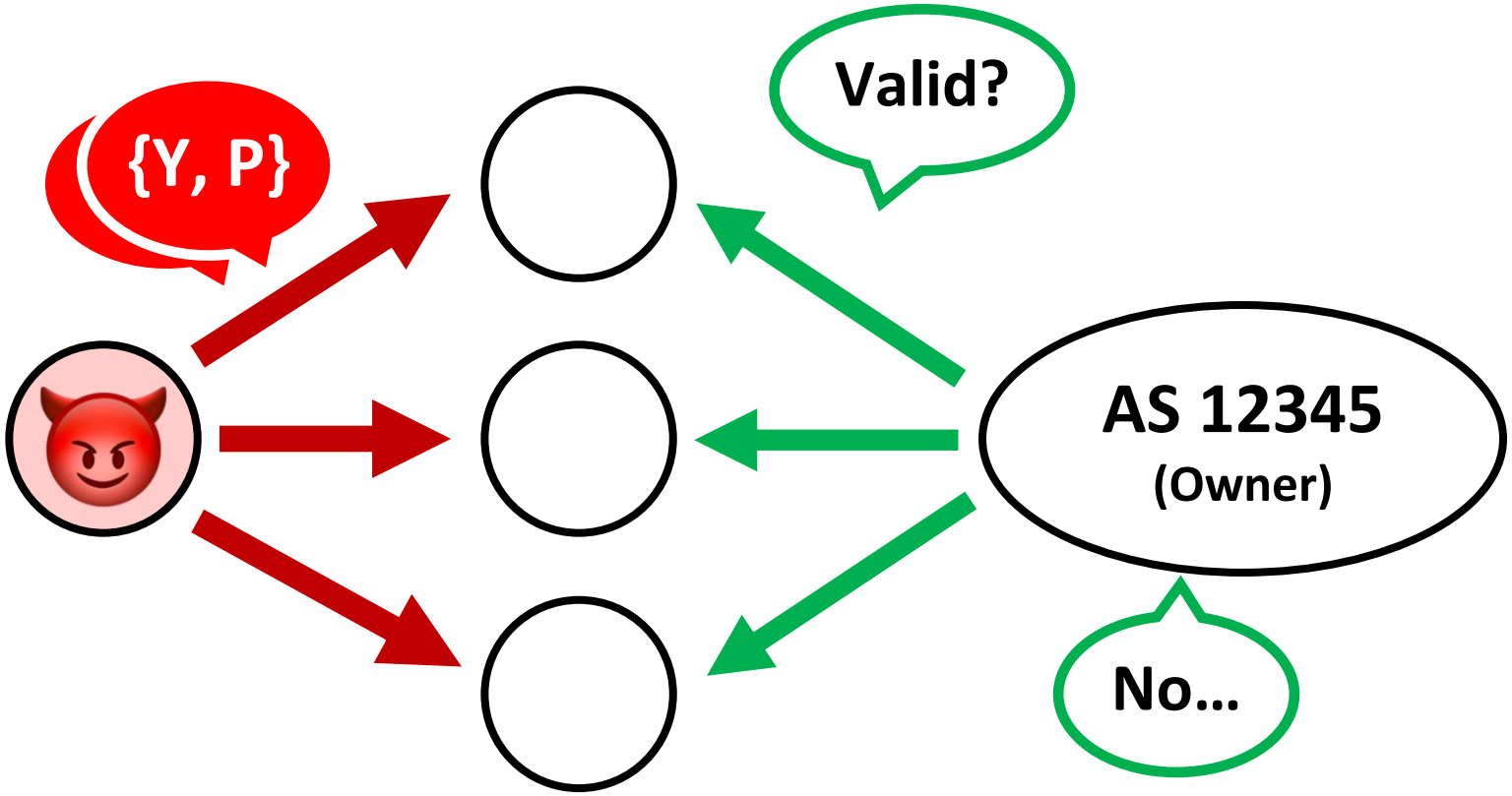




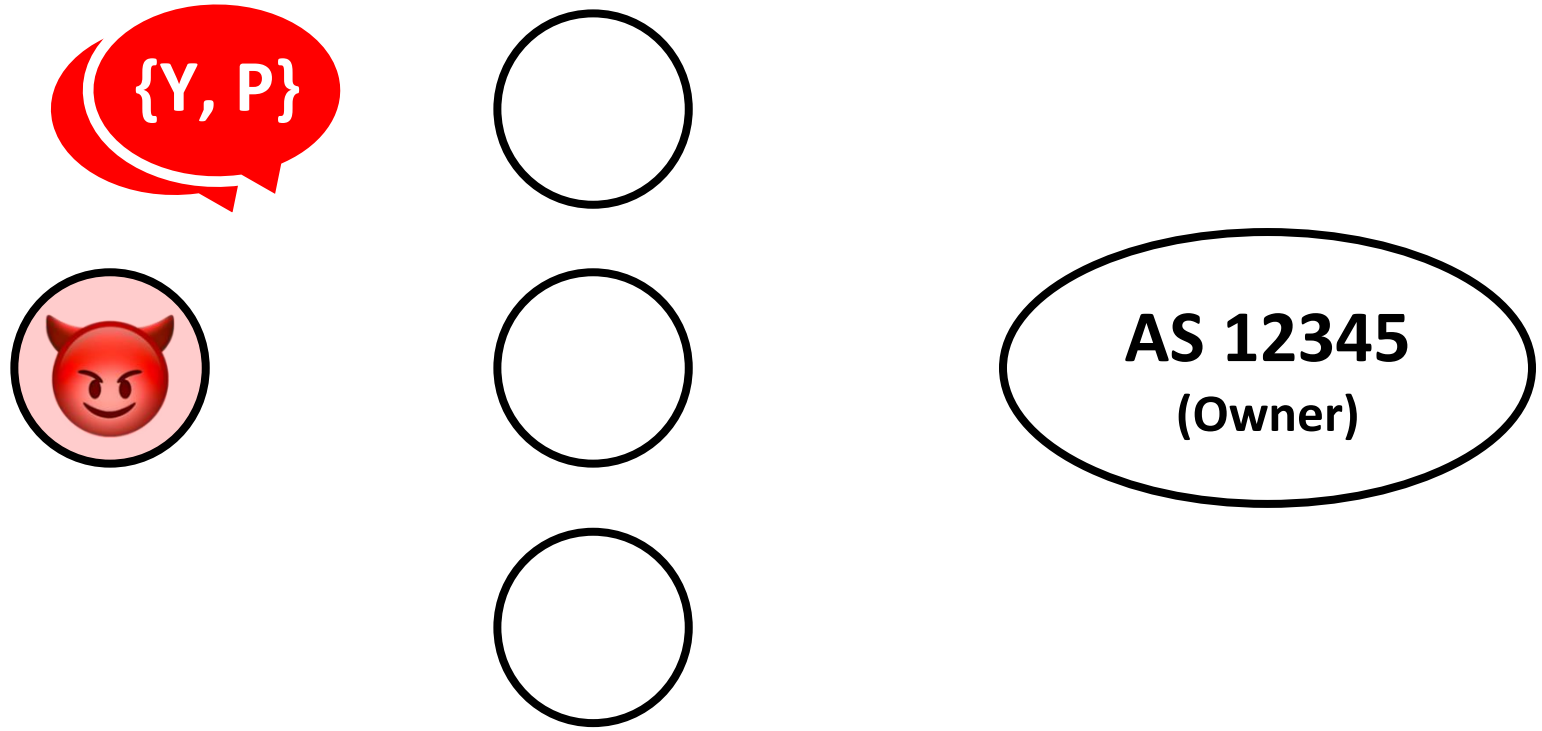
iROV Prevents Query Flooding and Abuse



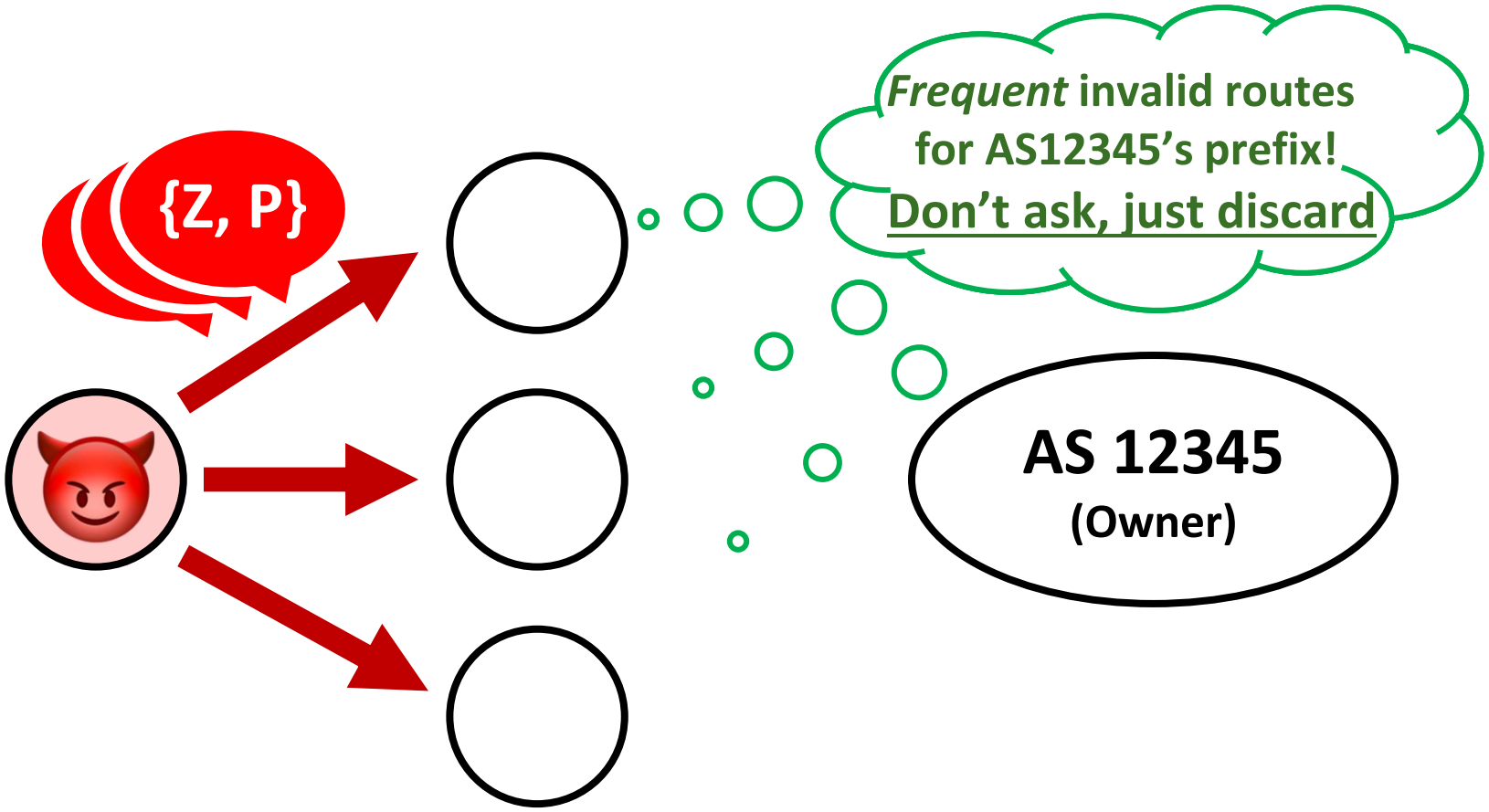
iROV Prevents Query Flooding and Abuse



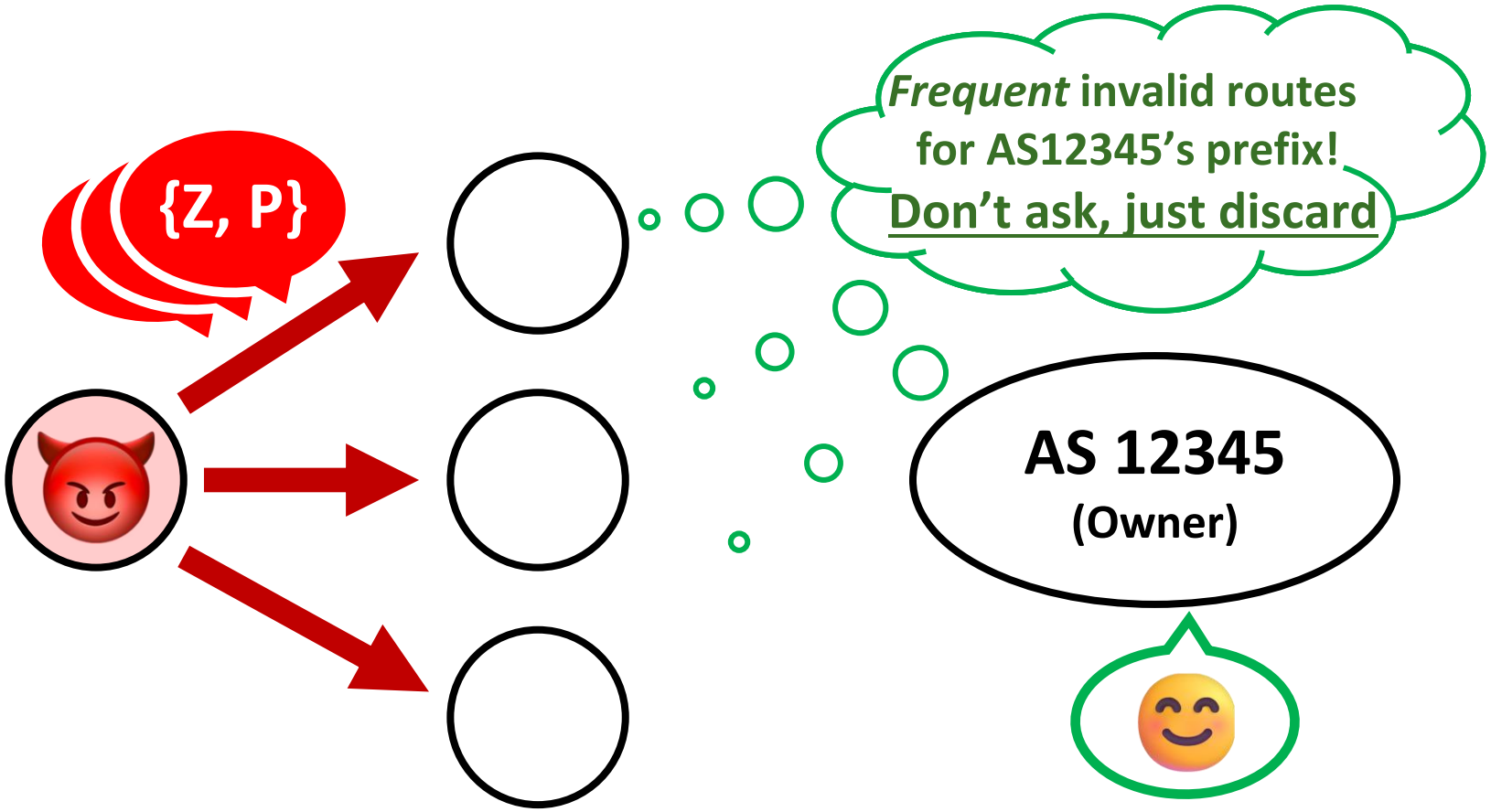
iROV Prevents Query Flooding and Abuse



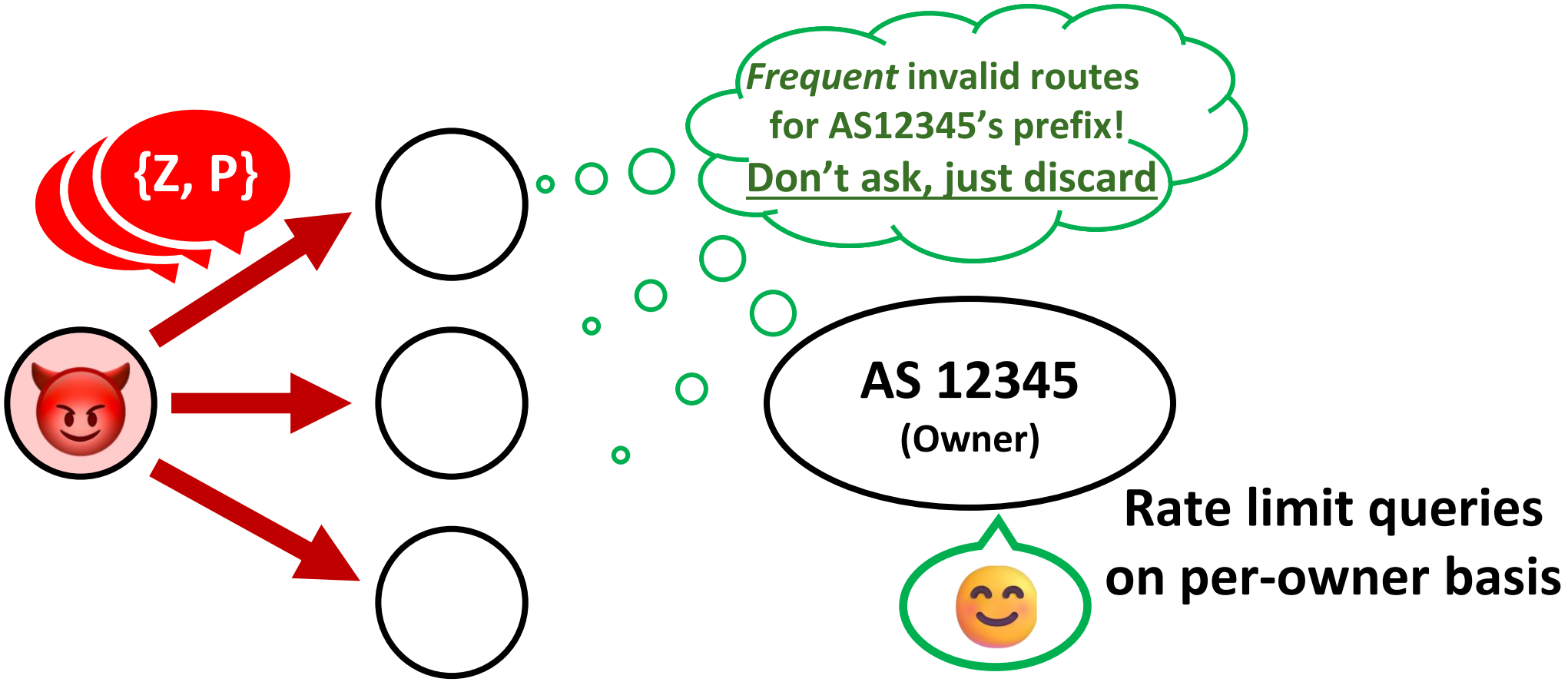
iROV Prevents Query Flooding and Abuse



iROV Prevents Query Flooding and Abuse



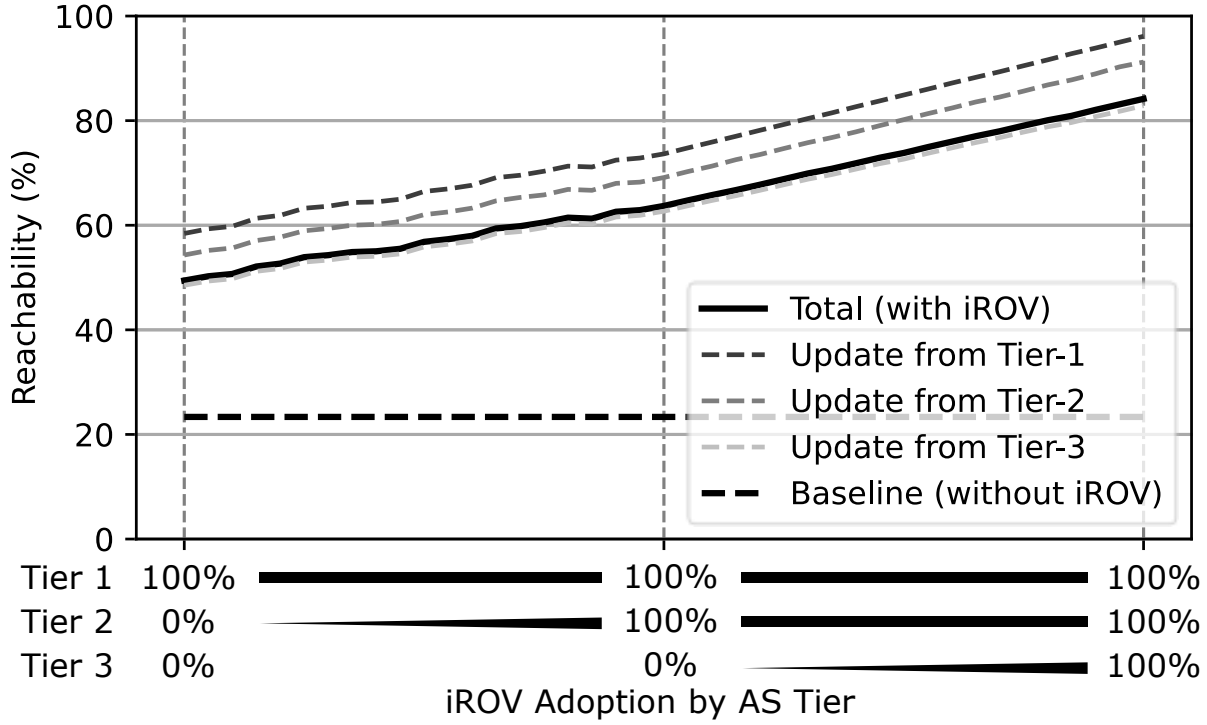
iROV Prevents Query Flooding and Abuse



iROV Is Effective Even In Partial Adoption

Extensively propagating urgent route changes

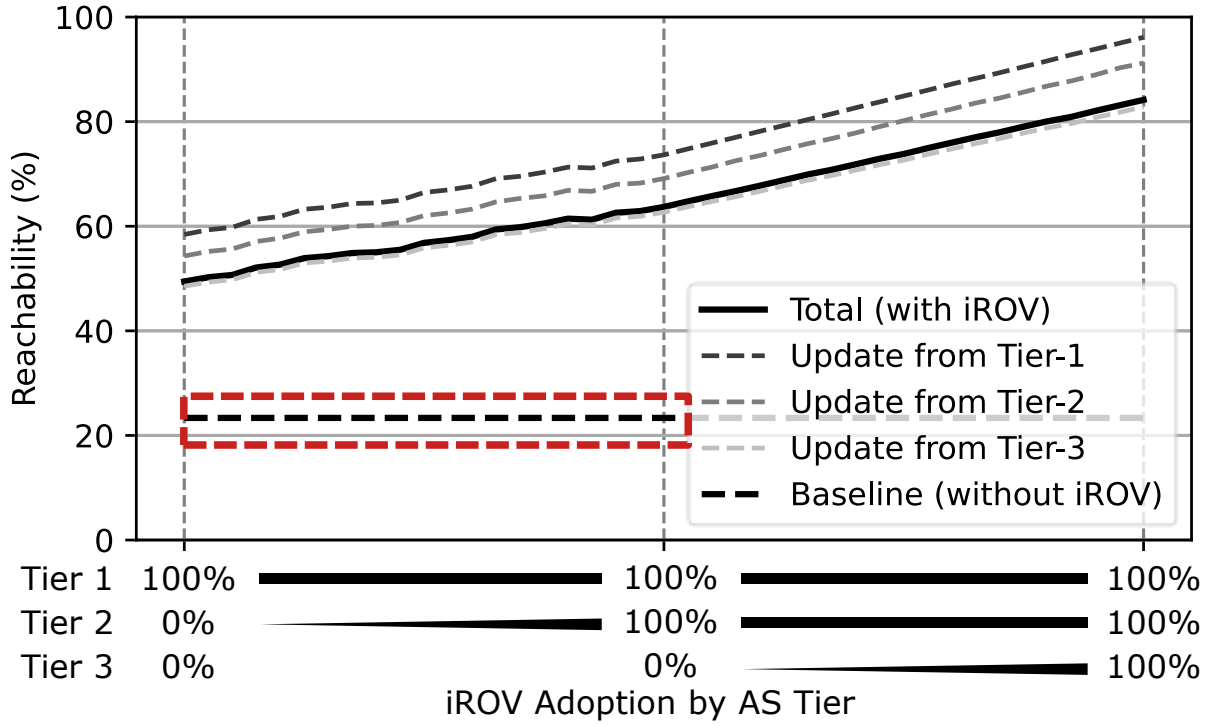
Per an extensive BGP Simulation based on Sep. 2025 CAIDA AS Relationship Dataset



iROV Is Effective Even In Partial Adoption

Extensively propagating urgent route changes

Per an extensive BGP Simulation based on Sep. 2025 CAIDA AS Relationship Dataset

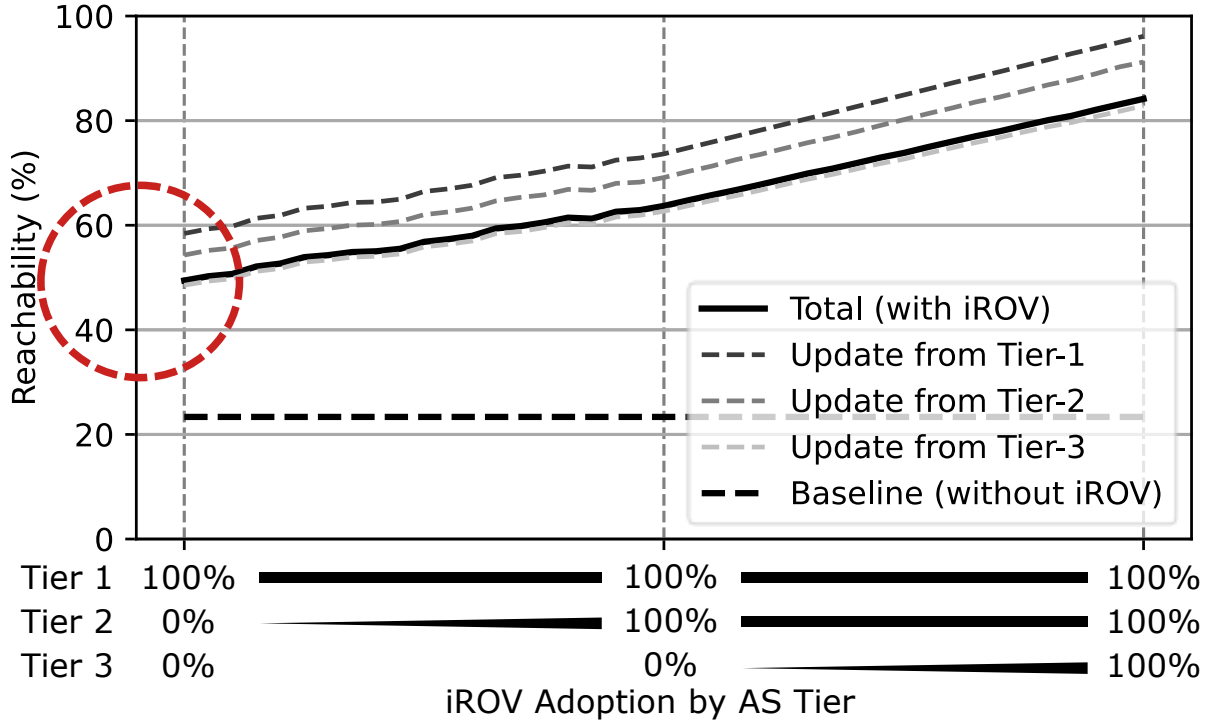


- Baseline urgent route change: reaches **23%** of ASes (No iROV deployed)

iROV Is Effective Even In Partial Adoption

Extensively propagating urgent route changes

Per an extensive BGP Simulation based on Sep. 2025 CAIDA AS Relationship Dataset

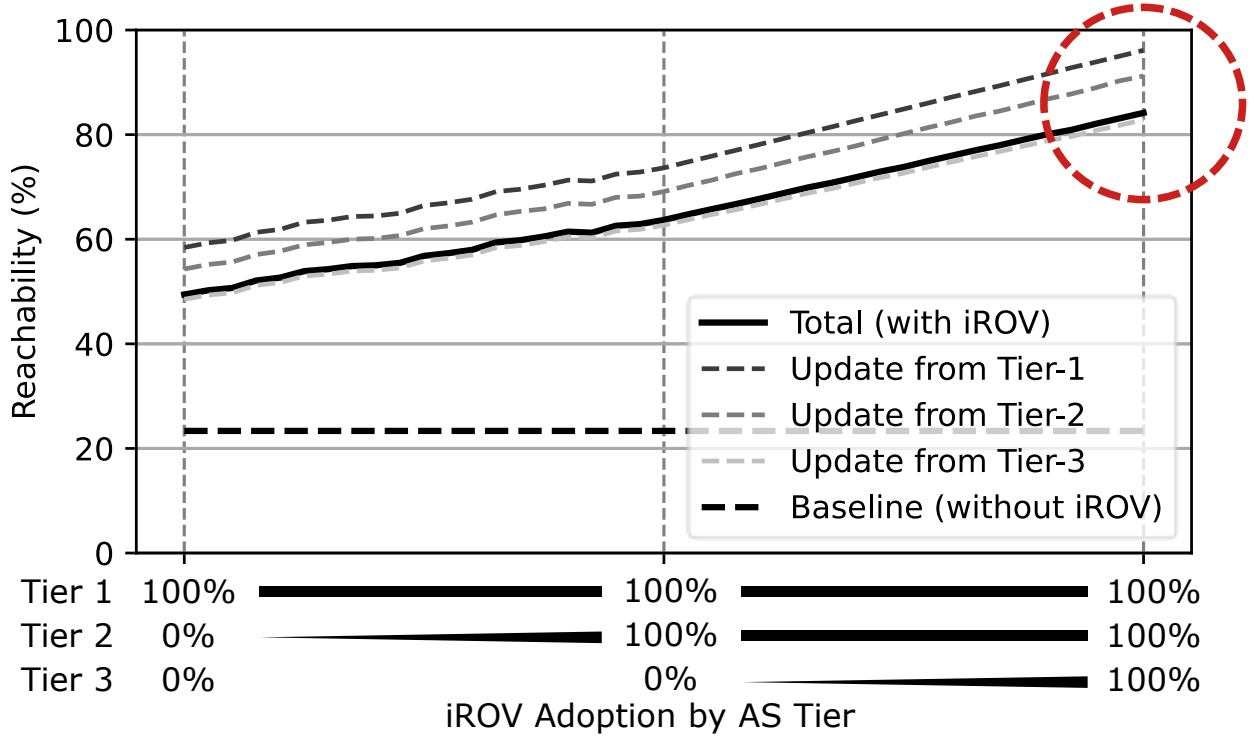


- Early tier-1 only adoption: reaches **49%** of ASes (**> 2x reachability** for early partial adoption)

iROV Is Effective Even In Partial Adoption

Extensively propagating urgent route changes

Per an extensive BGP Simulation based on Sep. 2025 CAIDA AS Relationship Dataset

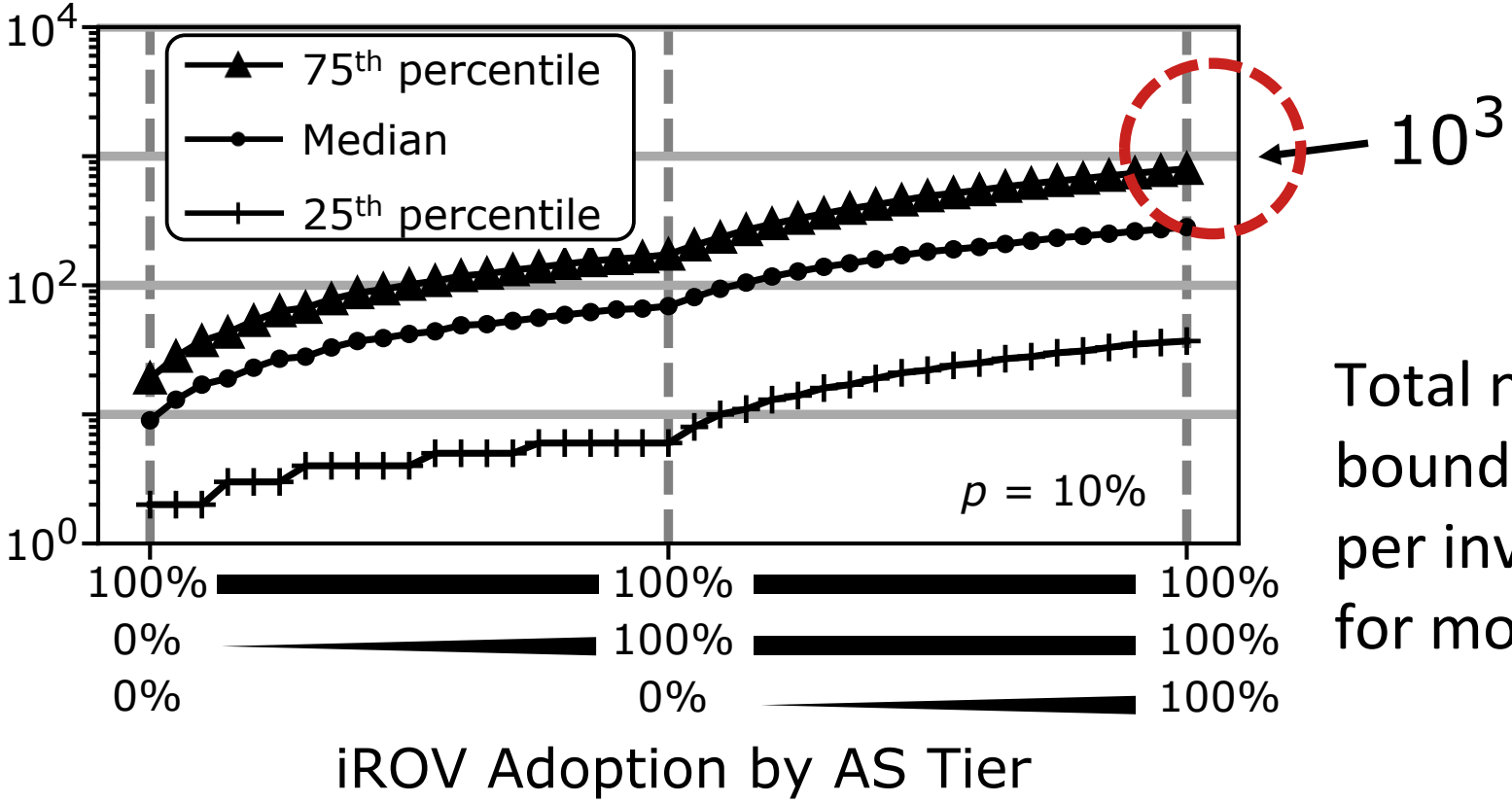


- Full adoption: nearly **90%** of Ases (**Near full eventual reachability**)

iROV Incurs Minimal Overhead

Effectively bounding owner-side query pressure

Per an extensive BGP Simulation based on Sep. 2025 CAIDA AS Relationship Dataset

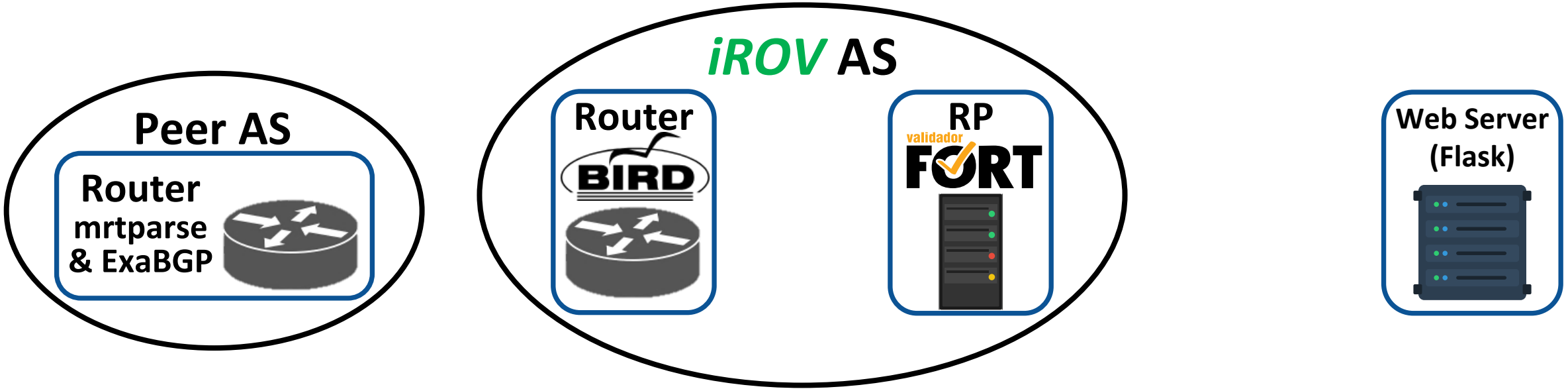


Total number of queries is bounded to **~1,000** per invalid announcement for most cases

iROV Incurs Minimal Overhead

Negligible performance overhead: prototype implementation

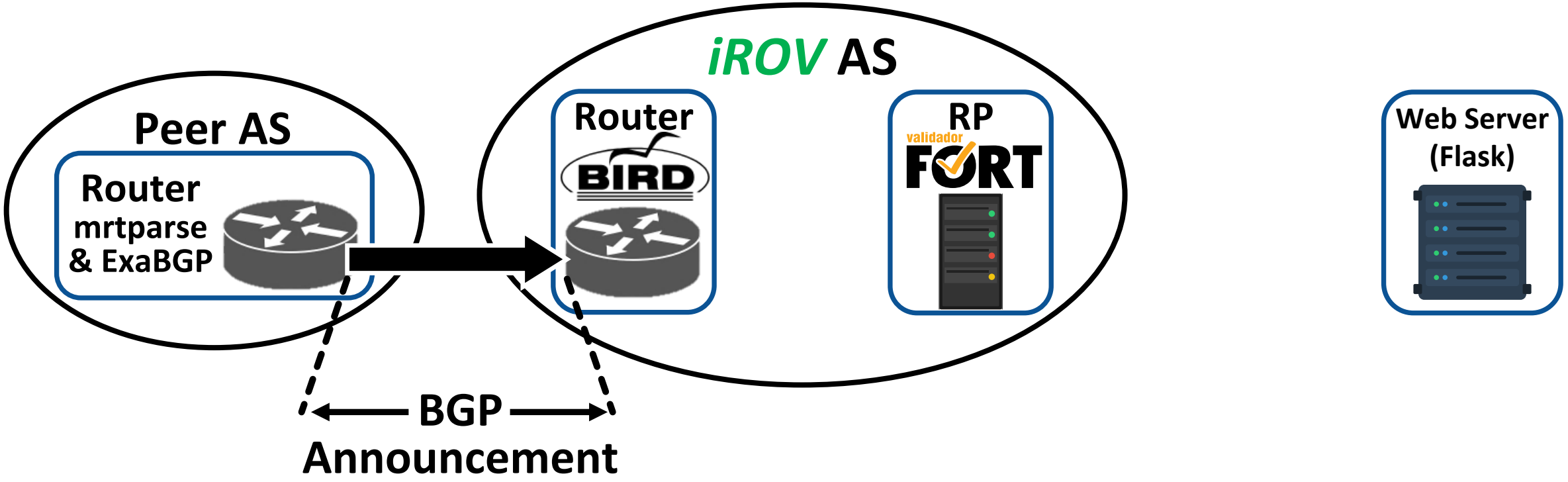
Modified BIRD (router) and FORT Validator (RP)



iROV Incurs Minimal Overhead

Negligible performance overhead: prototype implementation

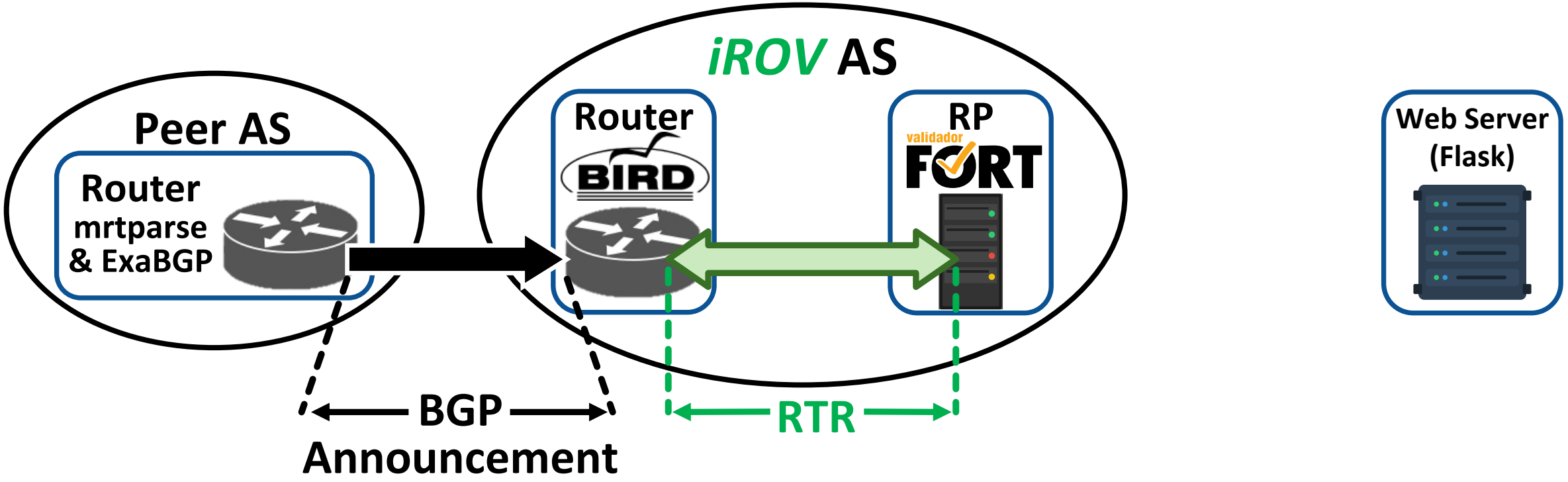
Modified BIRD (router) and FORT Validator (RP)



iROV Incurs Minimal Overhead

Negligible performance overhead: prototype implementation

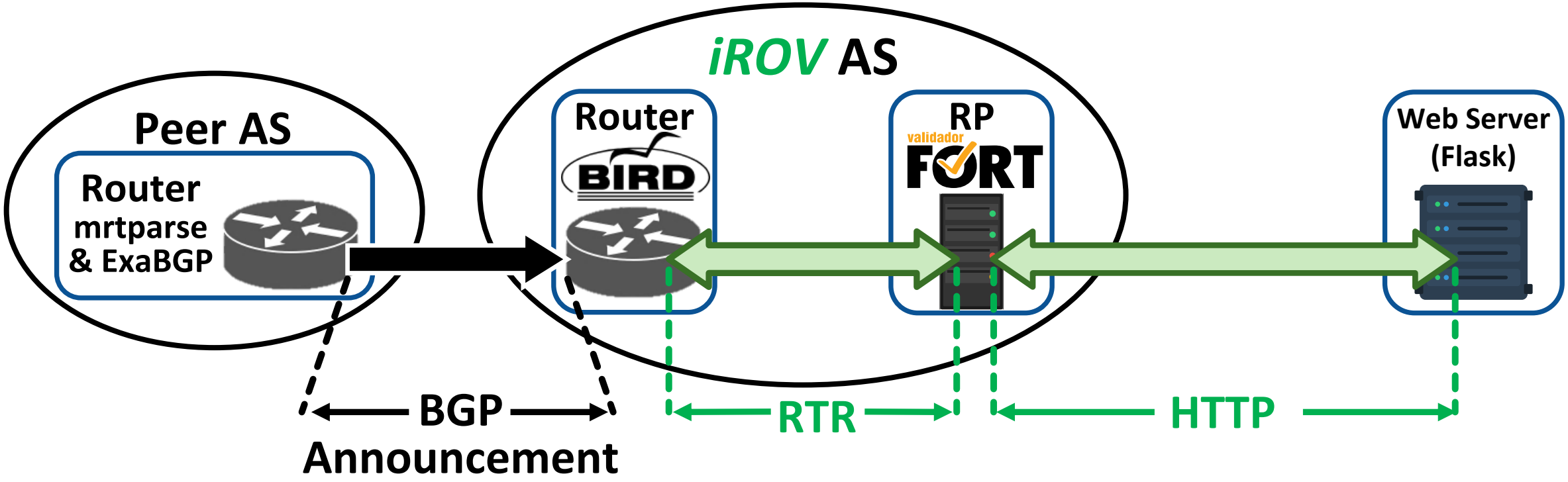
Modified BIRD (router) and FORT Validator (RP)



iROV Incurs Minimal Overhead

Negligible performance overhead: prototype implementation

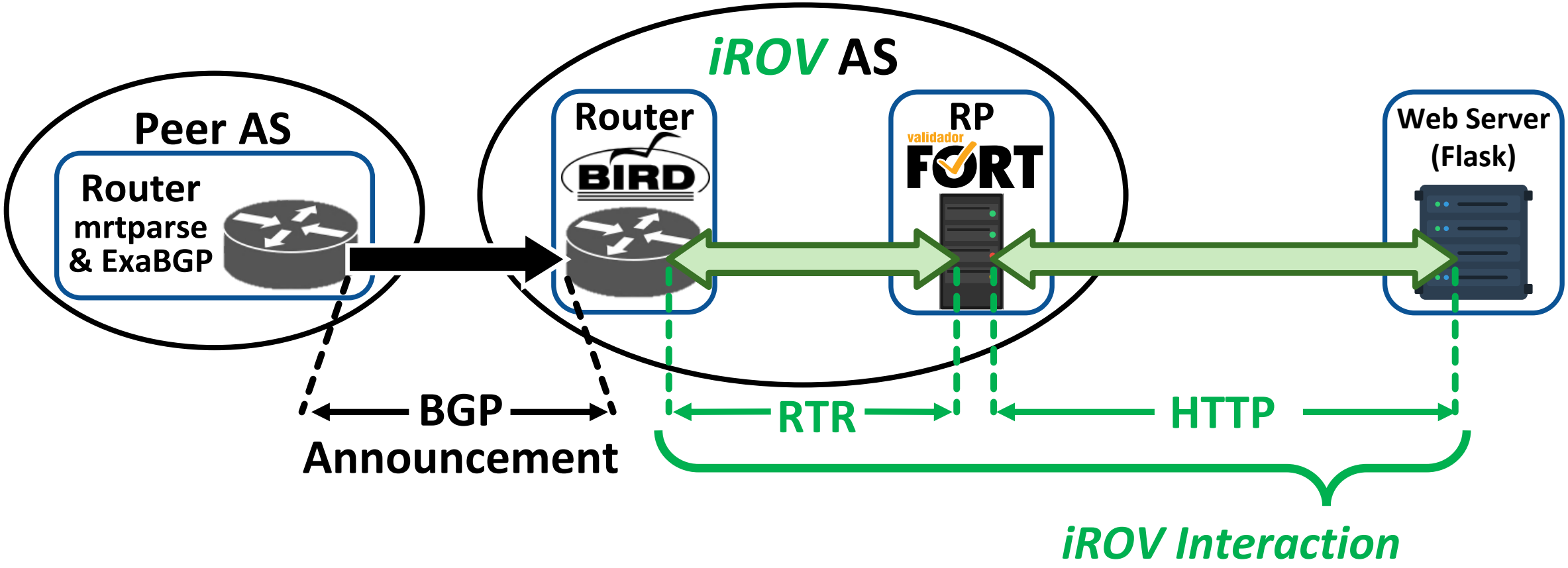
Modified BIRD (router) and FORT Validator (RP)



iROV Incurs Minimal Overhead

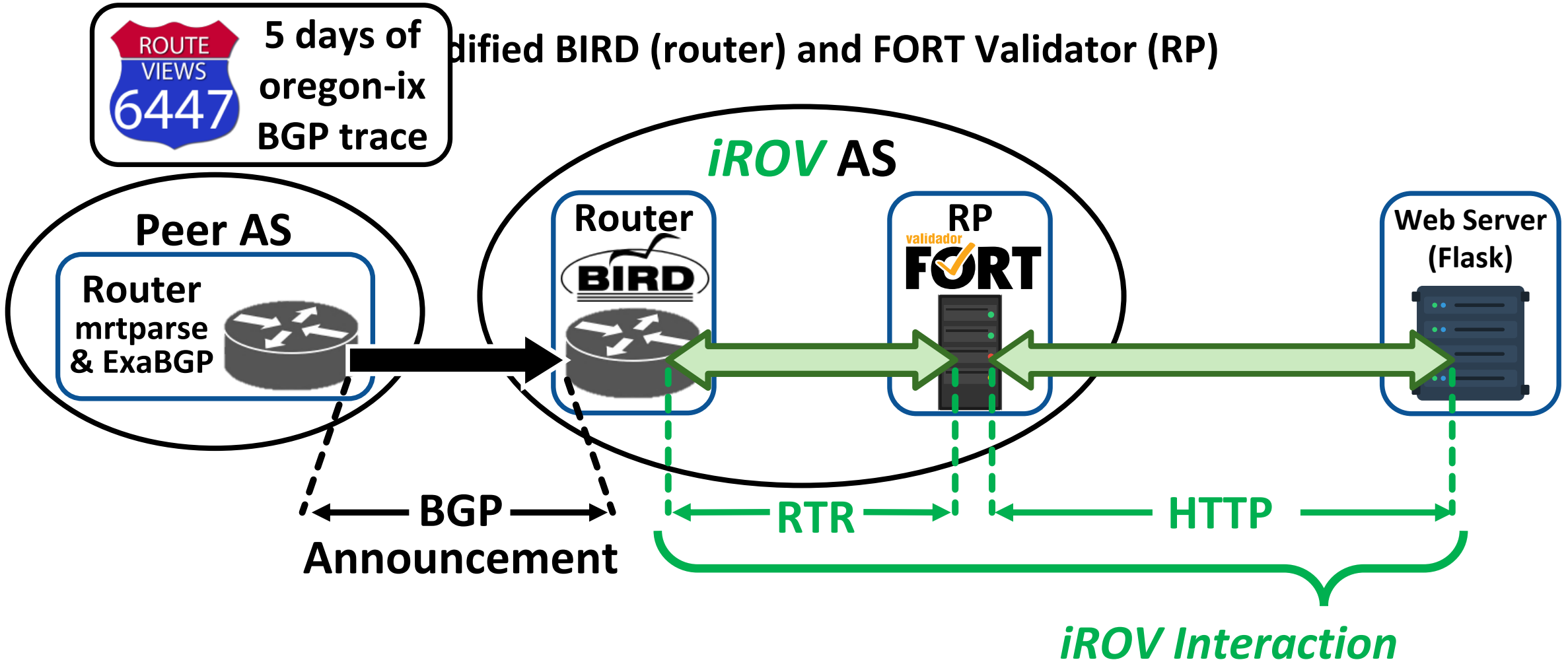
Negligible performance overhead: prototype implementation

Modified BIRD (router) and FORT Validator (RP)



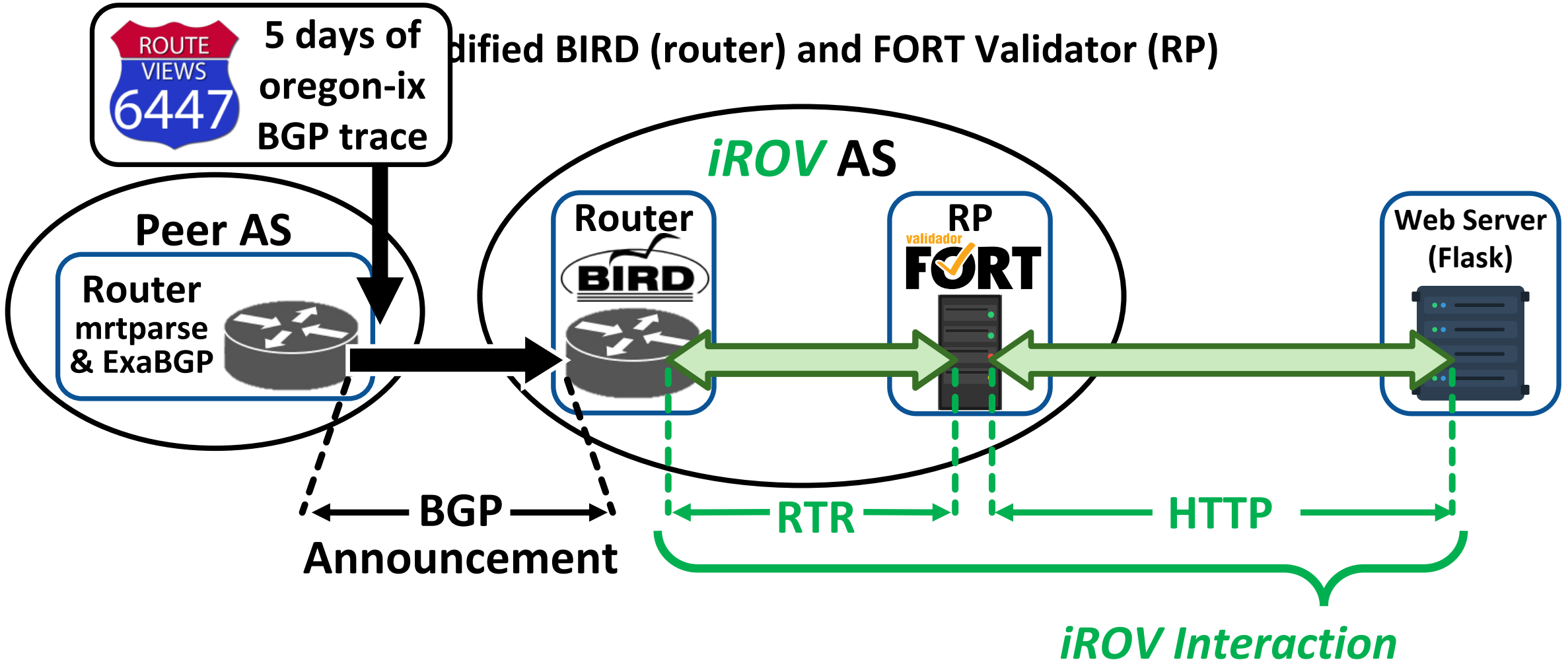
iROV Incurs Minimal Overhead

Negligible performance overhead: prototype implementation



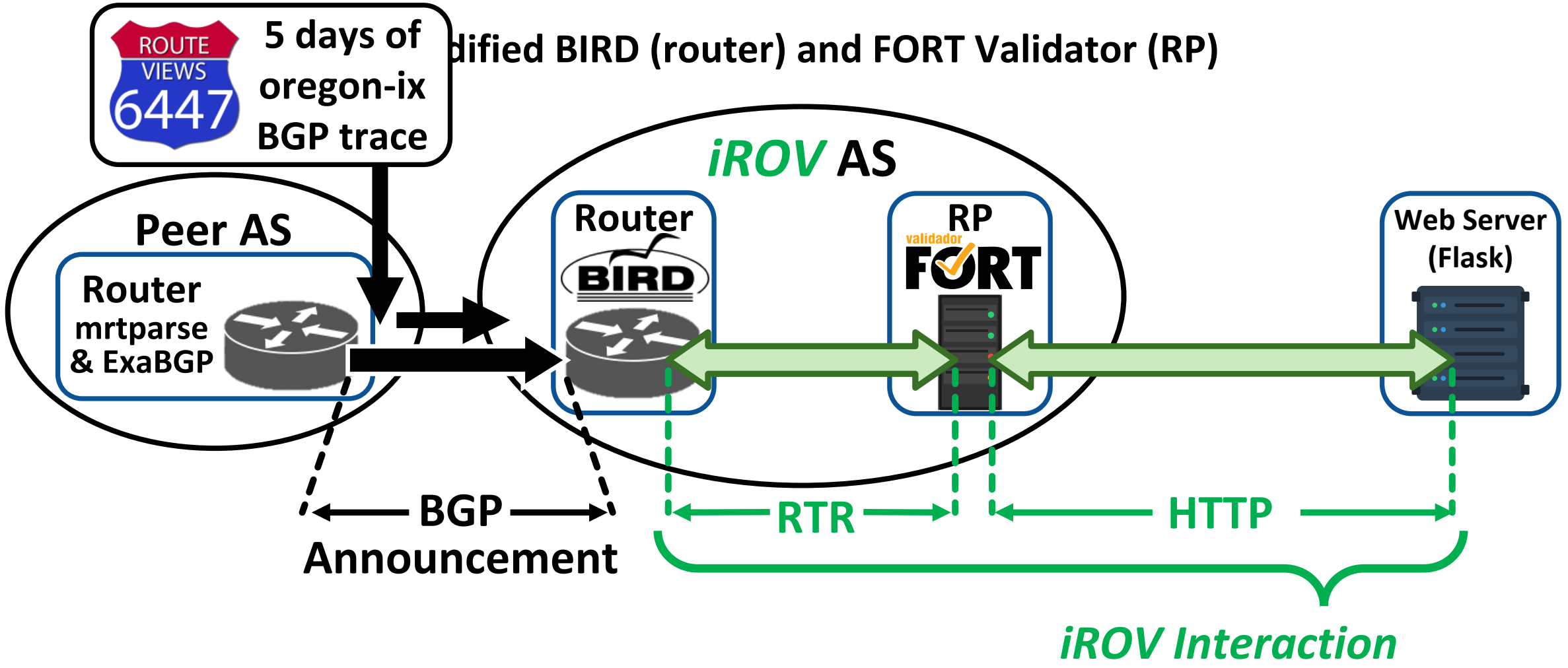
iROV Incurs Minimal Overhead

Negligible performance overhead: prototype implementation



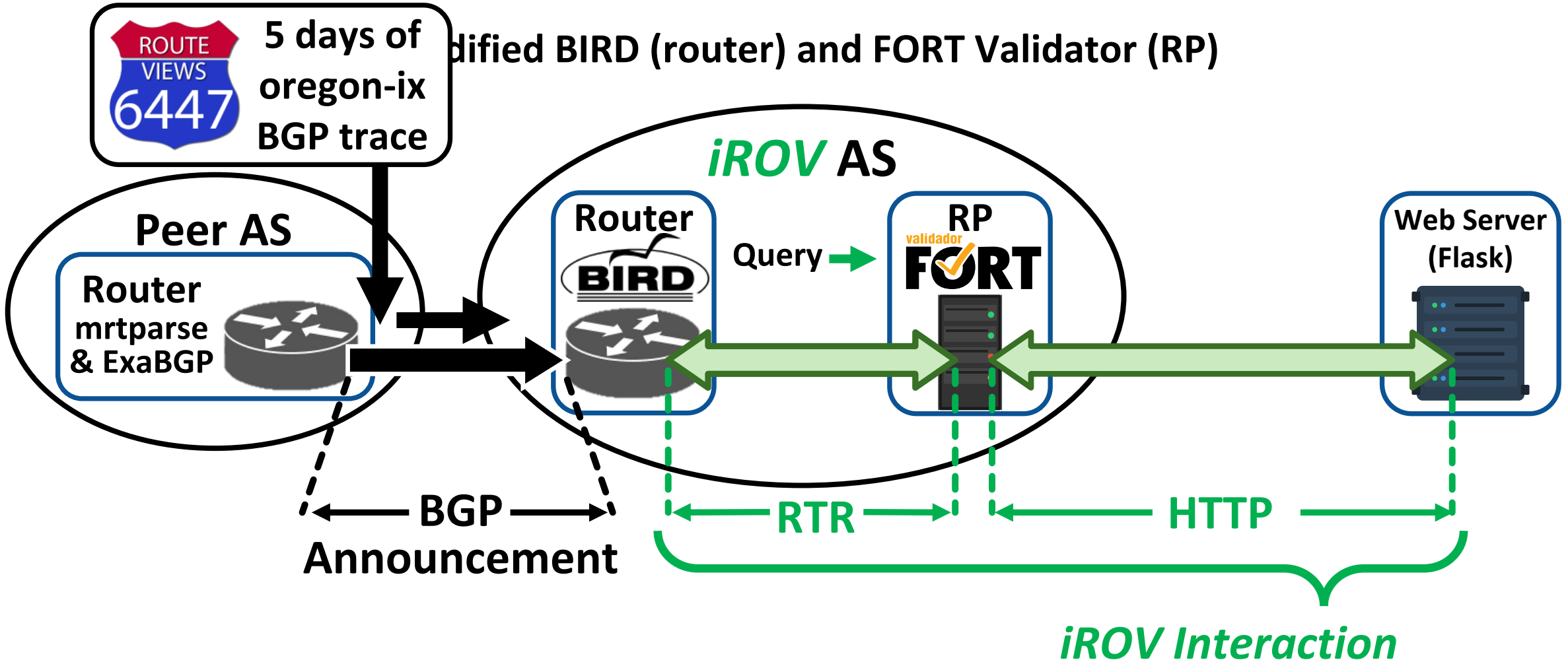
iROV Incurs Minimal Overhead

Negligible performance overhead: prototype implementation



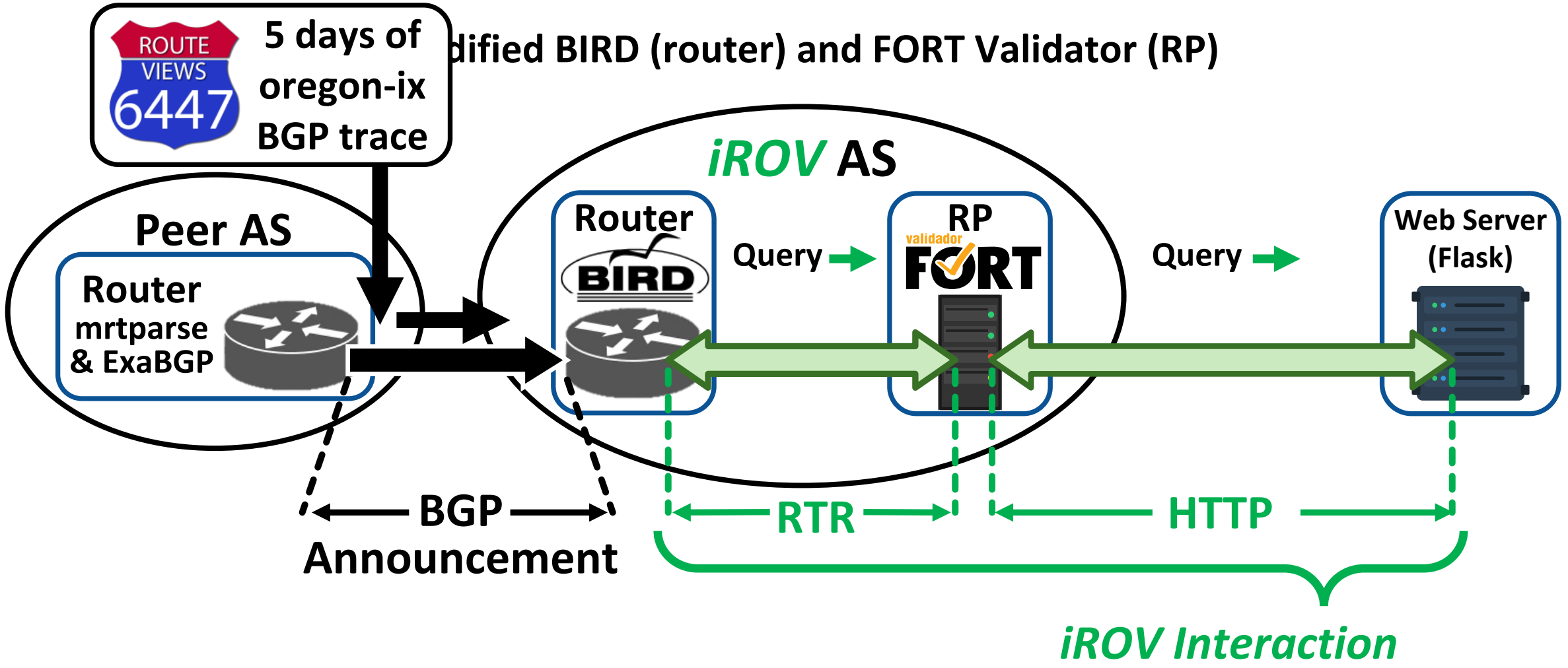
iROV Incurs Minimal Overhead

Negligible performance overhead: prototype implementation



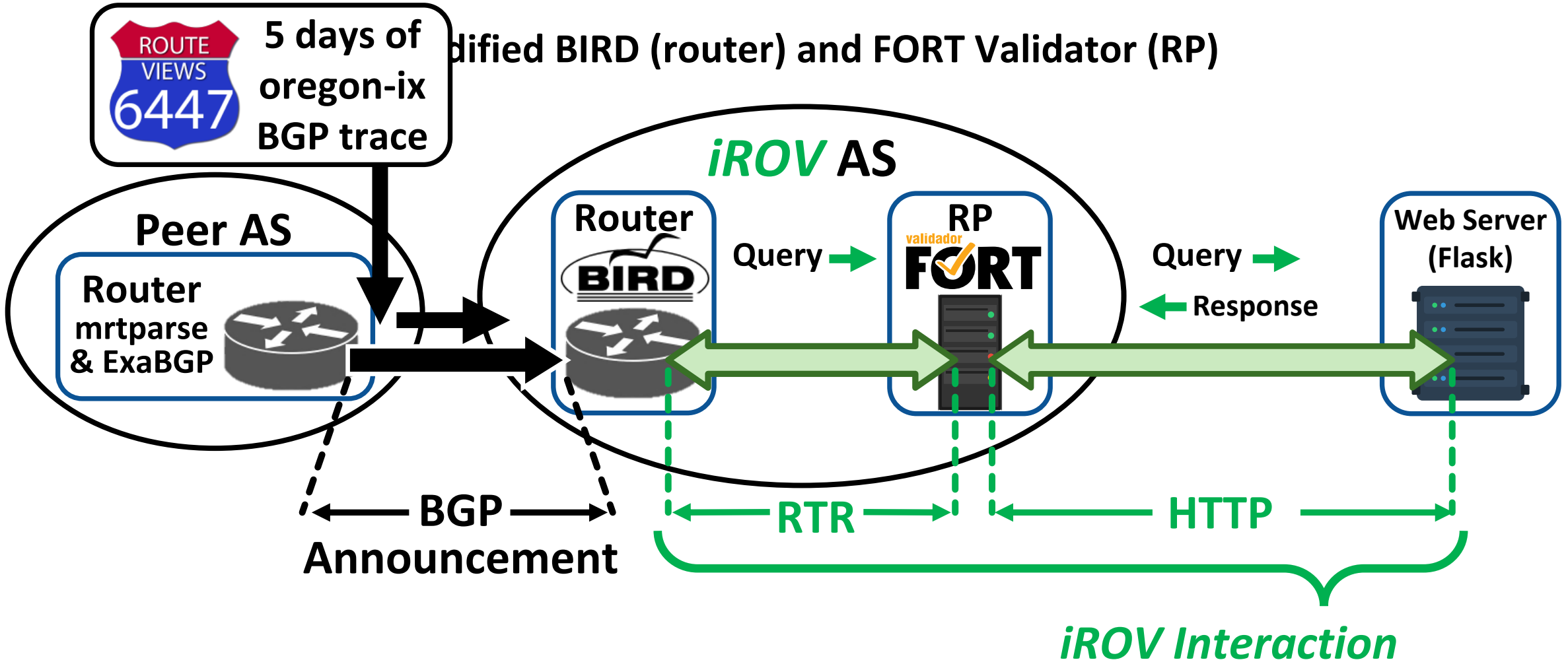
iROV Incurs Minimal Overhead

Negligible performance overhead: prototype implementation



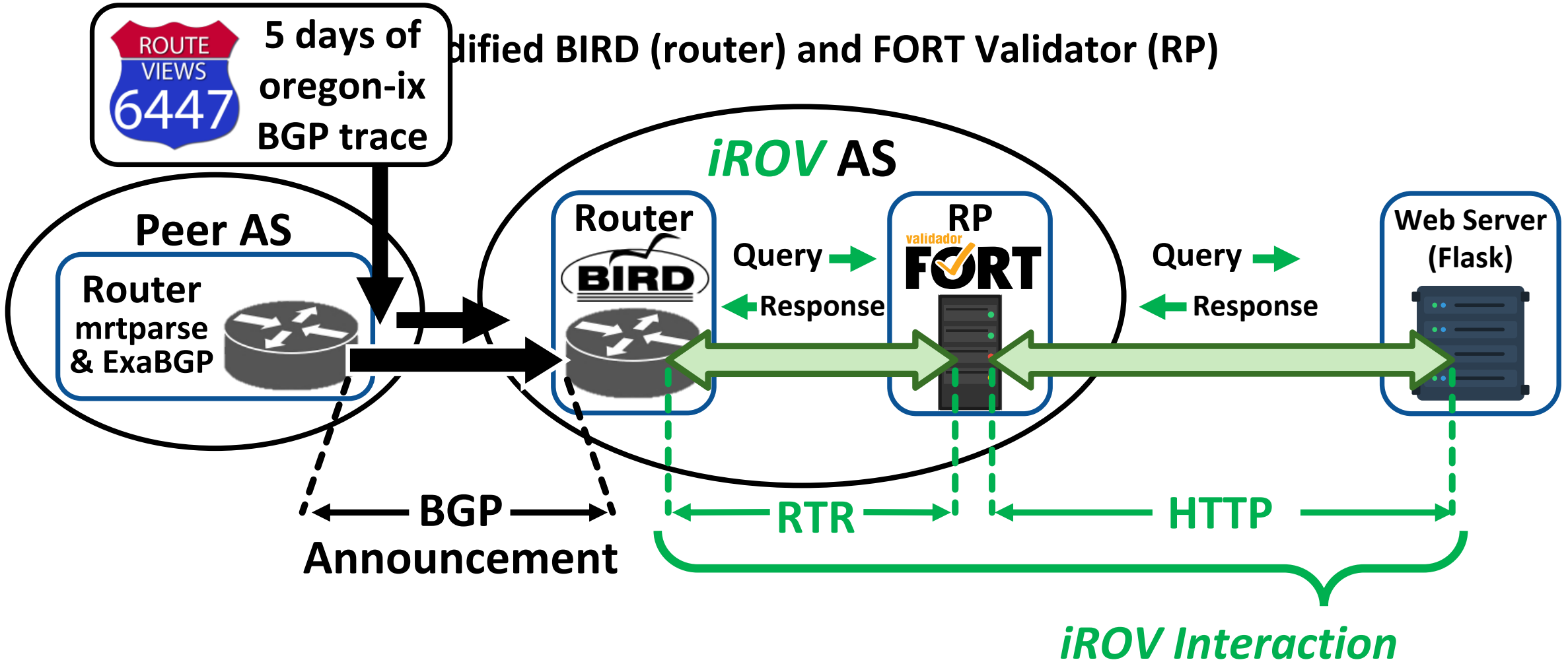
iROV Incurs Minimal Overhead

Negligible performance overhead: prototype implementation



iROV Incurs Minimal Overhead

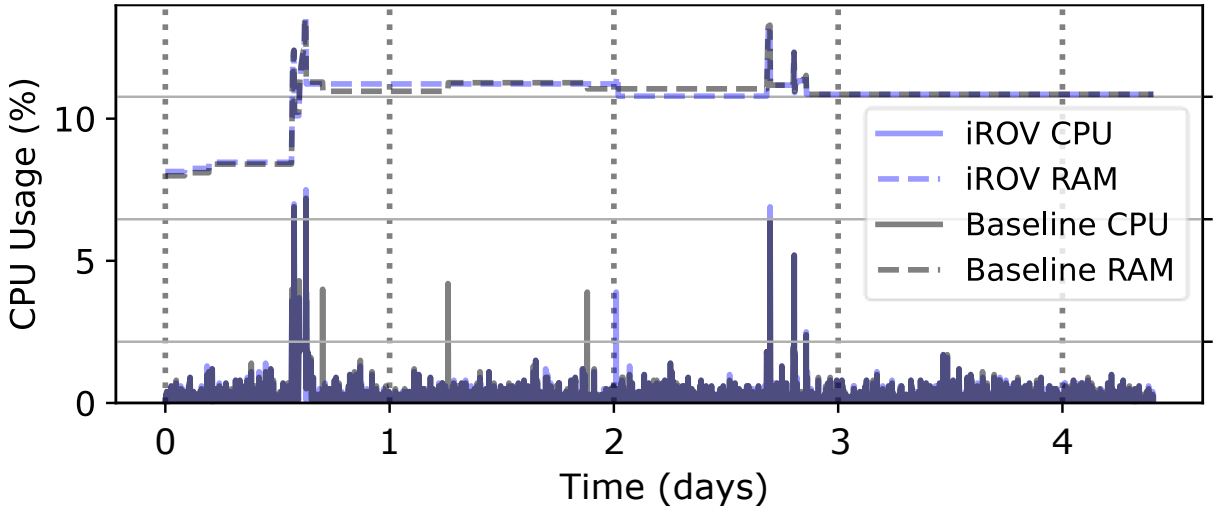
Negligible performance overhead: prototype implementation



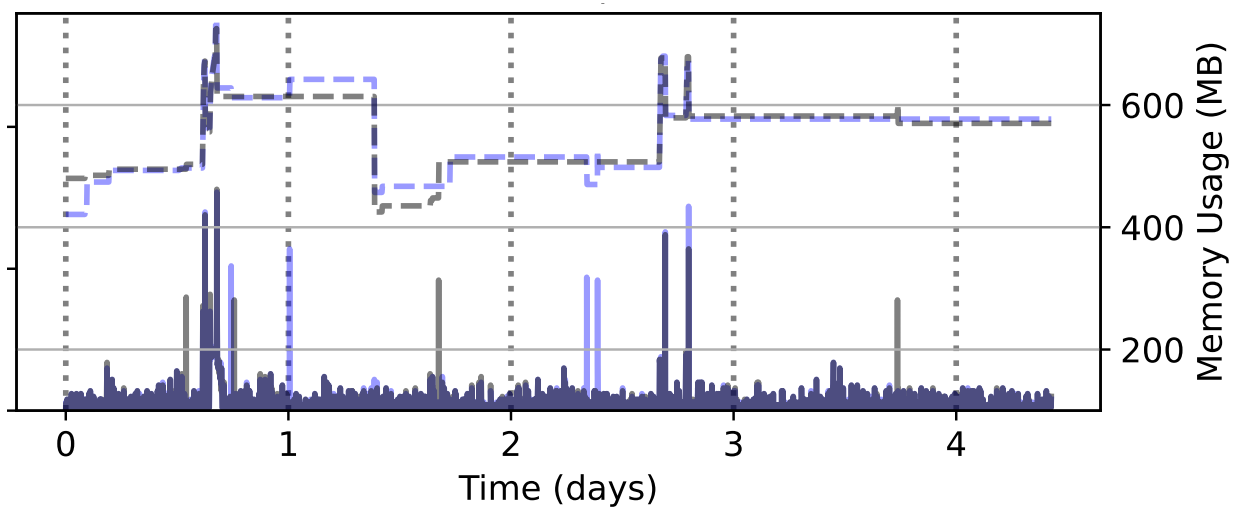
iROV Incurs Minimal Overhead

Negligible performance overhead: prototype implementation

Per prototype implementation and evaluation under real-world BGP trace
(~5 days of Route-Views2.oregon-ix.net)



(a) Initial-inquiry mode

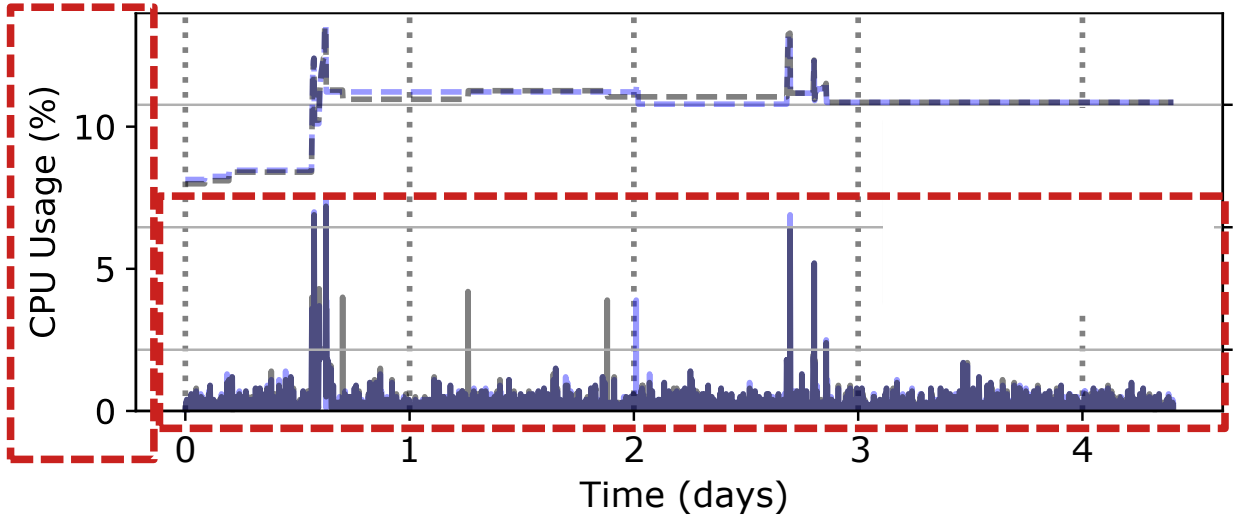


(b) Read-stapled mode

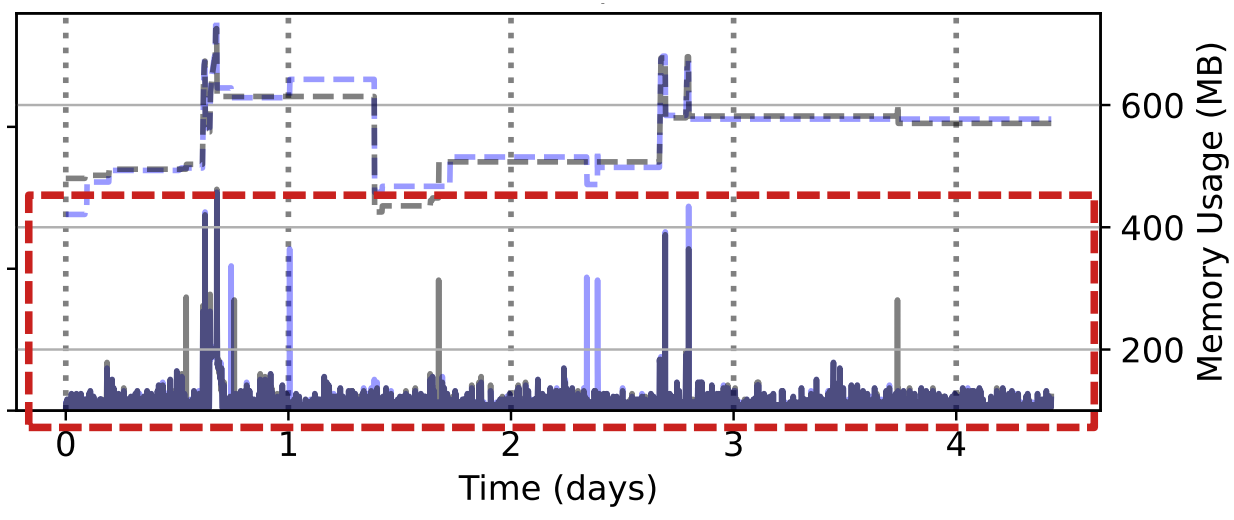
iROV Incurs Minimal Overhead

Negligible performance overhead: prototype implementation

Per prototype implementation and evaluation under real-world BGP trace
(~5 days of Route-Views2.oregon-ix.net)



(a) Initial-inquiry mode

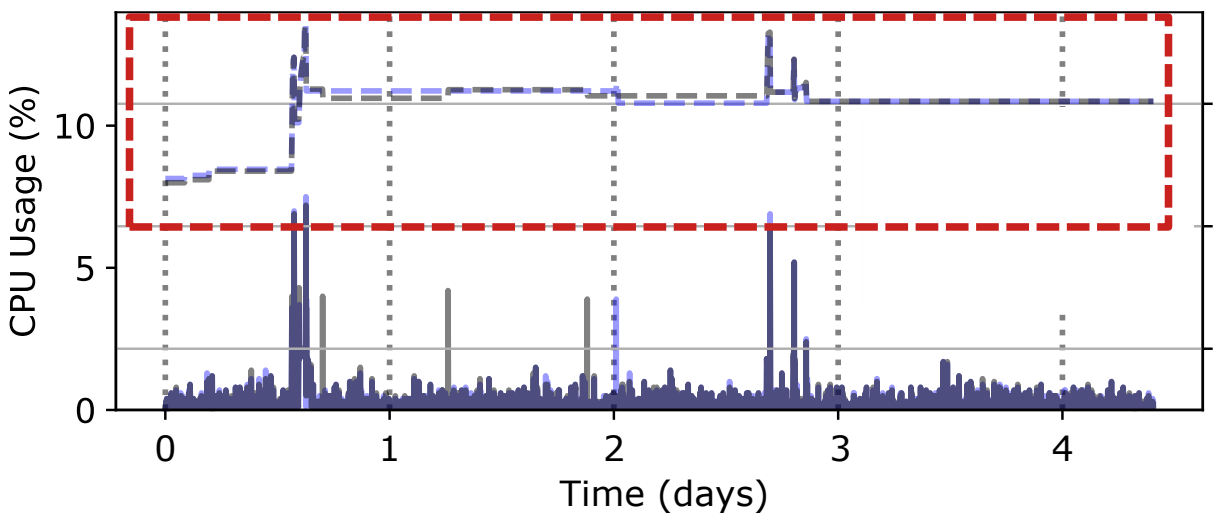


(b) Read-stapled mode

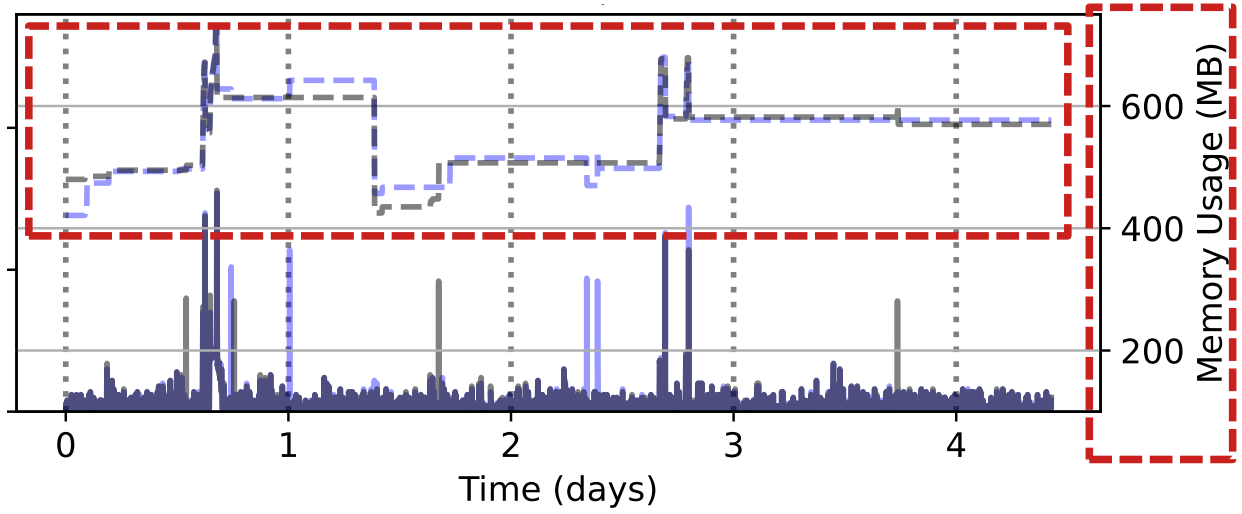
iROV Incurs Minimal Overhead

Negligible performance overhead: prototype implementation

Per prototype implementation and evaluation under real-world BGP trace
(~5 days of Route-Views2.oregon-ix.net)



(a) Initial-inquiry mode



(b) Read-stapled mode

Conclusion

- RPKI ROV's silent-drop model creates critical operational challenges (**Lack of visibility** into incidents, **incompatibility** with DDoS defense)
- iROV solves these challenges via ***interactivity***
- iROV also addresses challenges inherent to interactivity itself, ensuring **safety** and **efficacy** from the earliest stages of adoption
- iROV prototype demonstrates **minimal performance overhead**

Thank you