A hybrid system for automatic exchanges of routing information

Stamatios Maritsas

University of Amsterdam
Informatics Institute
Master of Science in System and Network Engineering

supervised by

Stavros Konstantaras
s.konstantaras@uva.nl

George Thessalonikefs
george@nlnetlabs.nl

November 23, 2016

Border Gateway Protocol — BGP

Definition

BGP is the **de facto** inter-AS[1] routing protocol used on the Internet nowadays.

- Specified in RFC 4271 (BGP4)
- Peer-to-peer reachability discovery protocol
- Comes in two flavors, *iBGP* and *eBGP*

[1] Autonomous System (AS) = a connected group of IP prefixes having a single, consistent routing policy

Policies

Definition

Policies determine a set of rules on how routing and reachability information is exchanged between BGP routers.

- whom does an AS connect with
- which route prefixes are announced to others
- which route prefixes are accepted from others
- what are the desired preferences, etc.
- Categorization
  - Transit policies
  - Traffic engineering policies
  - Scalability policies
  - Security-related policies

Routing Policy Specification Language — RPSL

Definition

RPSL is a neutral-vendor, object-oriented language used to specify a routing policy in the IRR.

- defines 13 classes of objects
- `aut-num, route, as-set, route-set`

- Three-fold purpose
  - presentation of policies in IRR in an understandable format
  - description of policies in a more comfortable/solid way
  - can be converted into BGP configuration files
- Practical difficulties
  - complex policy descriptions due to its flexibility
  - level of accuracy of descriptions largely varies
  - adds an extra high-level configuration step

Internet Routing Registry — IRR

Definition

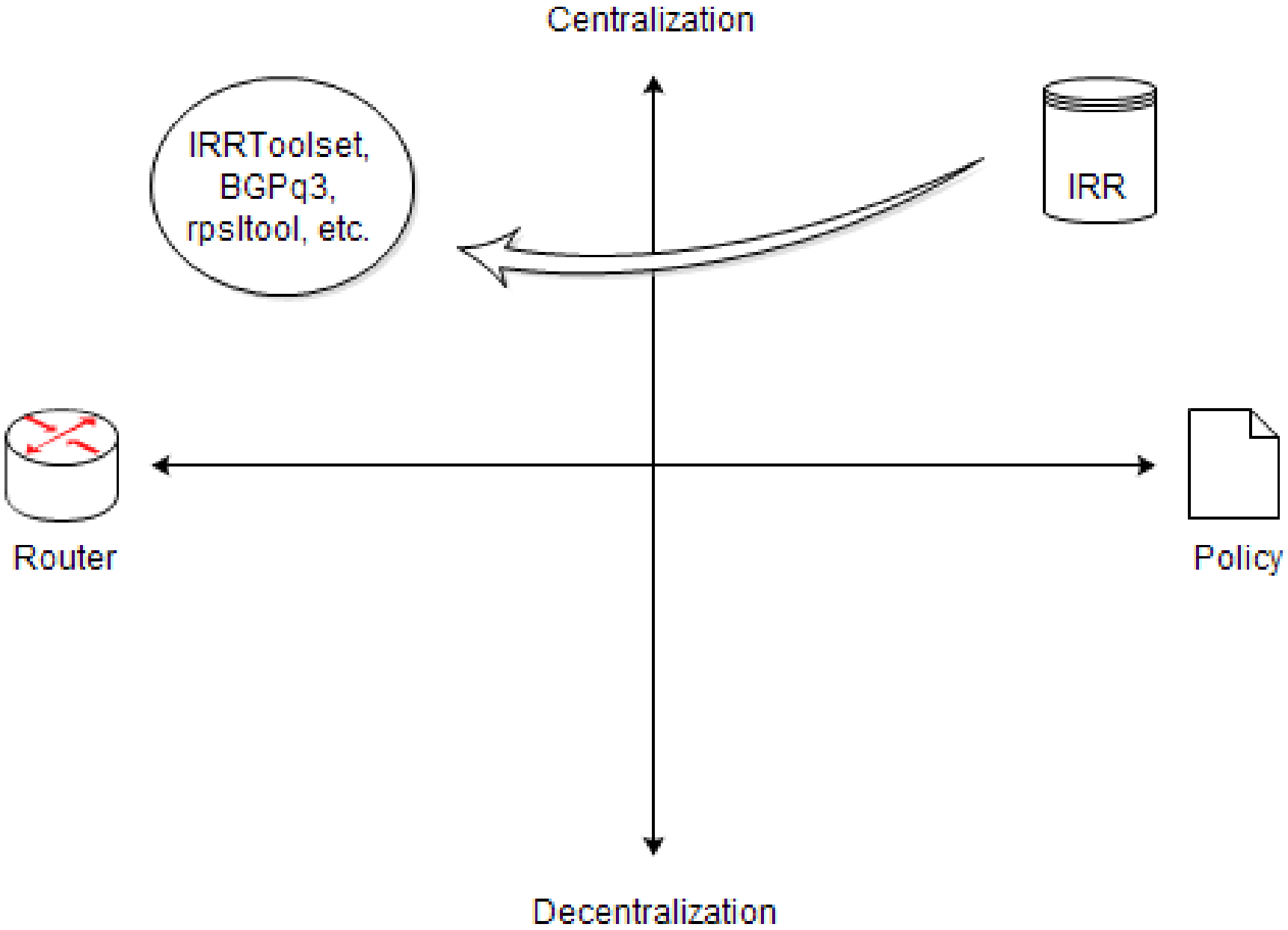
IRR is a distributed set of repositories used by many network operators to store their AS routing policy.

- Numbers
  - 26 both public and private routing registries in total
  - 5 Routing Internet Registries (RIRs) — 5 geographical regions
    - ★ AFRINIC, ARIN, APNIC, LACNIC, RIPE NCC
    - ★ Allocation of IP address space and ASNs
- Security considerations
  - out-of-date information
  - inconsistencies
  - no proper authorization/authentication
  - RFC 2725 (re-examine its applicability)

BGP security

- Early '90s
  - first standardization of BGP in RFC 1105, NOT security-oriented
  - small number of networks, trust in place
  - no need for security :)
- Nowadays
  - BGP4 (RFC 4271) is still NOT security-oriented
  - huge number of networks, NO trust in place
  - security has become mandatory
- Security solutions
  - many proposals, both *crypto-based* and *non-crypto based*
  - *crypto-based* difficult to be applied (excluding RPKI)
    - ★ require modifications to BGP messages structure
    - ★ high computational cost
  - BGP route filtering *(non crypto-based)*, most effective and widely deployed technique

Current state



Research Questions

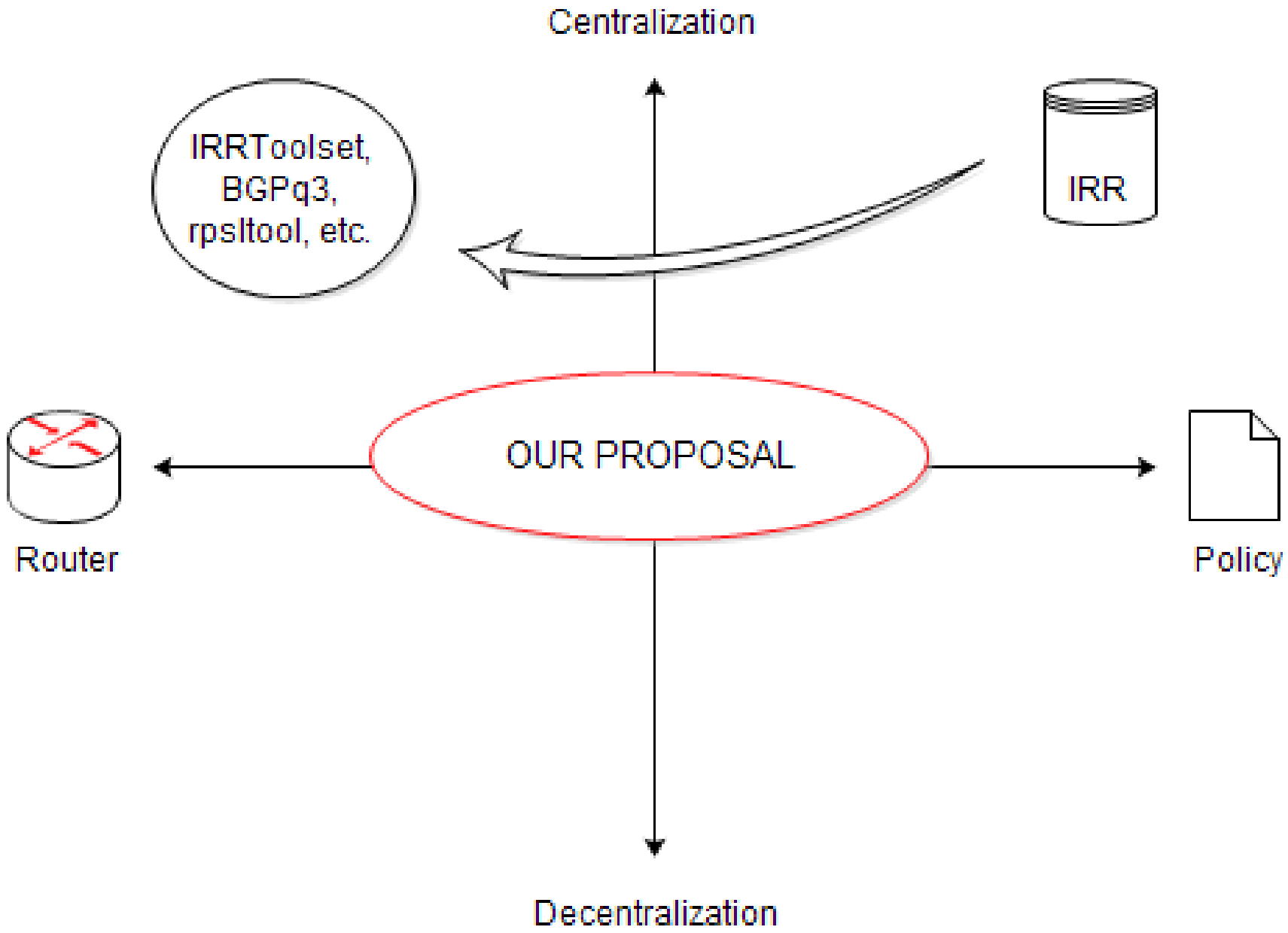
Main research question

Is it possible to design a hybrid system to automatically exchange routing policies for BGP configurations?

Sub-research questions

- Which would be the benefits by designing a hybrid approach?
- What is the potential of this hybrid system in terms of scalability and efficiency?
- What security aspects should this hybrid system employ?

Where does our project land?

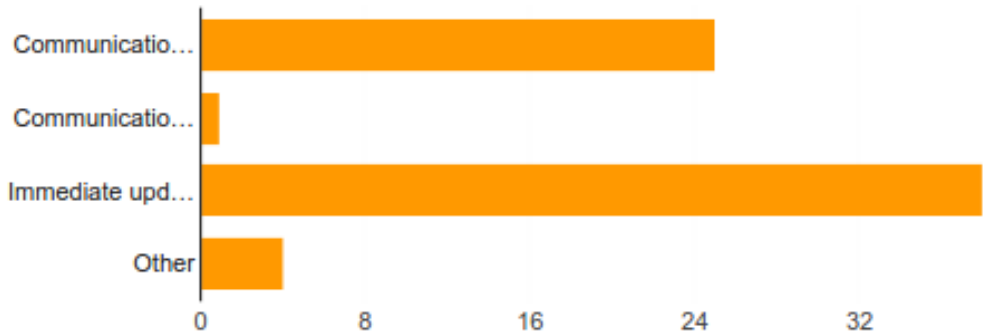


Methodology

- Literature study, theoretical knowledge
  - articles
  - RFCs
  - etc.
- Meetings, practical knowledge
  - supervisors
  - a few network operators (mostly of small ISPs)
- Questionnaire, practical knowledge
  - 2 questions concerning BGP update policy
  - 19 network operators mailing lists
  - statistical sample = 55 responses, only an indication :(
  - more than one answer to every question

Questionnaire (1/2)

How do you inform all the involving members that a change has been made to your routing policy?

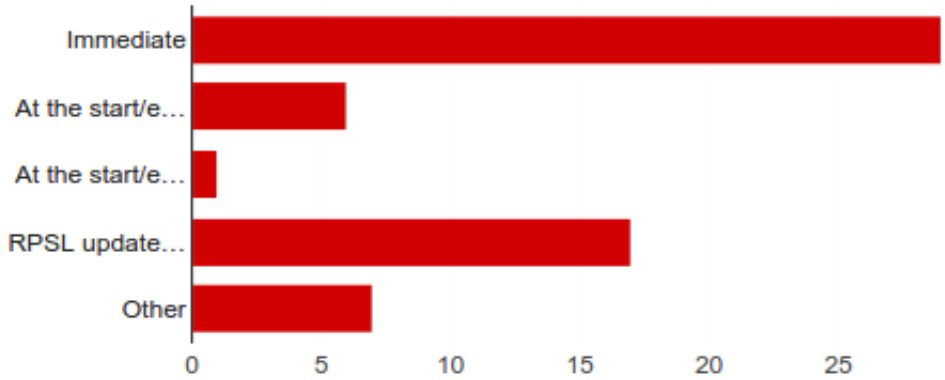


Communication via e-mail	**25**	45.5%
Communication via phone, or fax	**1**	1.8%
Immediate update of RPSL policy in RIR	**38**	69.1%
Other	**4**	7.3%

- Q1 indicates a need for an automatic way to exchange policies

Questionnaire (2/2)

What is the time between a policy change and the actual RPSL update inside RIR?



Immediate	**29**	52.7%
At the start/end of the week	**6**	10.9%
At the start/end of the month	**1**	1.8%
RPSL update is irrelevant to the policy change	**17**	30.9%
Other	**7**	12.7%

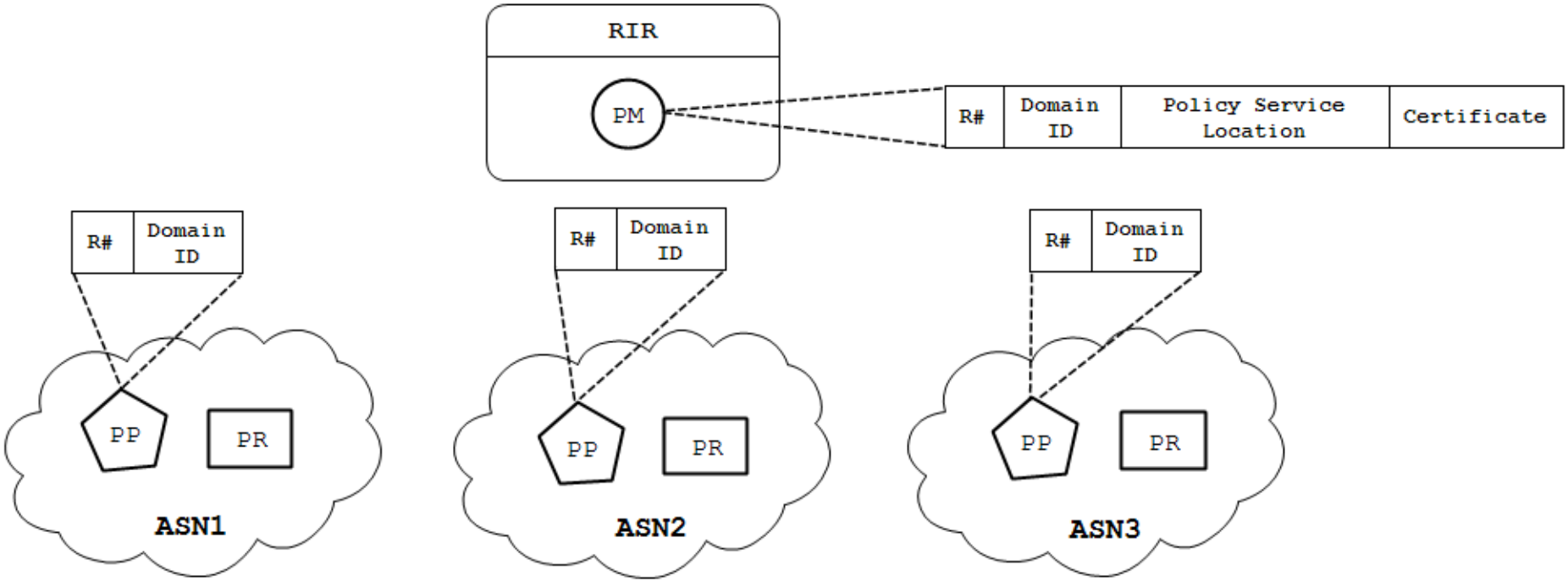
- Q2 indicates a need for an automatic way to exchange policies
- Q2 slightly indicates RPSL's difficulty to be adopted (17 / 55, 30.9%)

Decision making (1/3)

- Requirements
  - Decentralization of policy information
  - Mapping between domains [2]- policy service locations
  - Vendor-neutrality of routing policy language
  - Security (authorization & authentication)
  - Support for *Policy Views* (privacy)

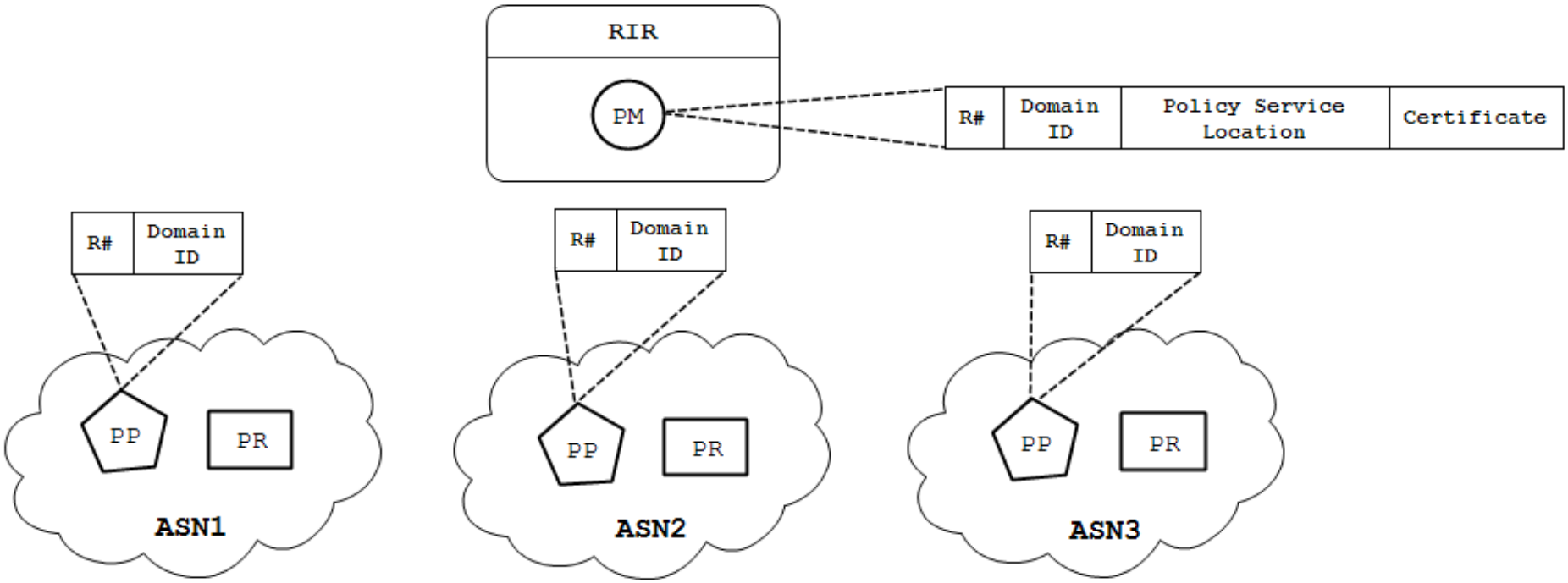
[2] For brevity, *domain == administrative domain or AS*

Decision making (2/3)



- Hybrid system model — Inspired by [1] [UvA+TUDelft, 2015]
  - need for both centralization & decentralization
  - 3 components
    - ★ Policy Mapper (PM) - centralized part
    - ★ Policy Provider (PP) - distributed part
    - ★ Policy Requester (PR) - distributed part

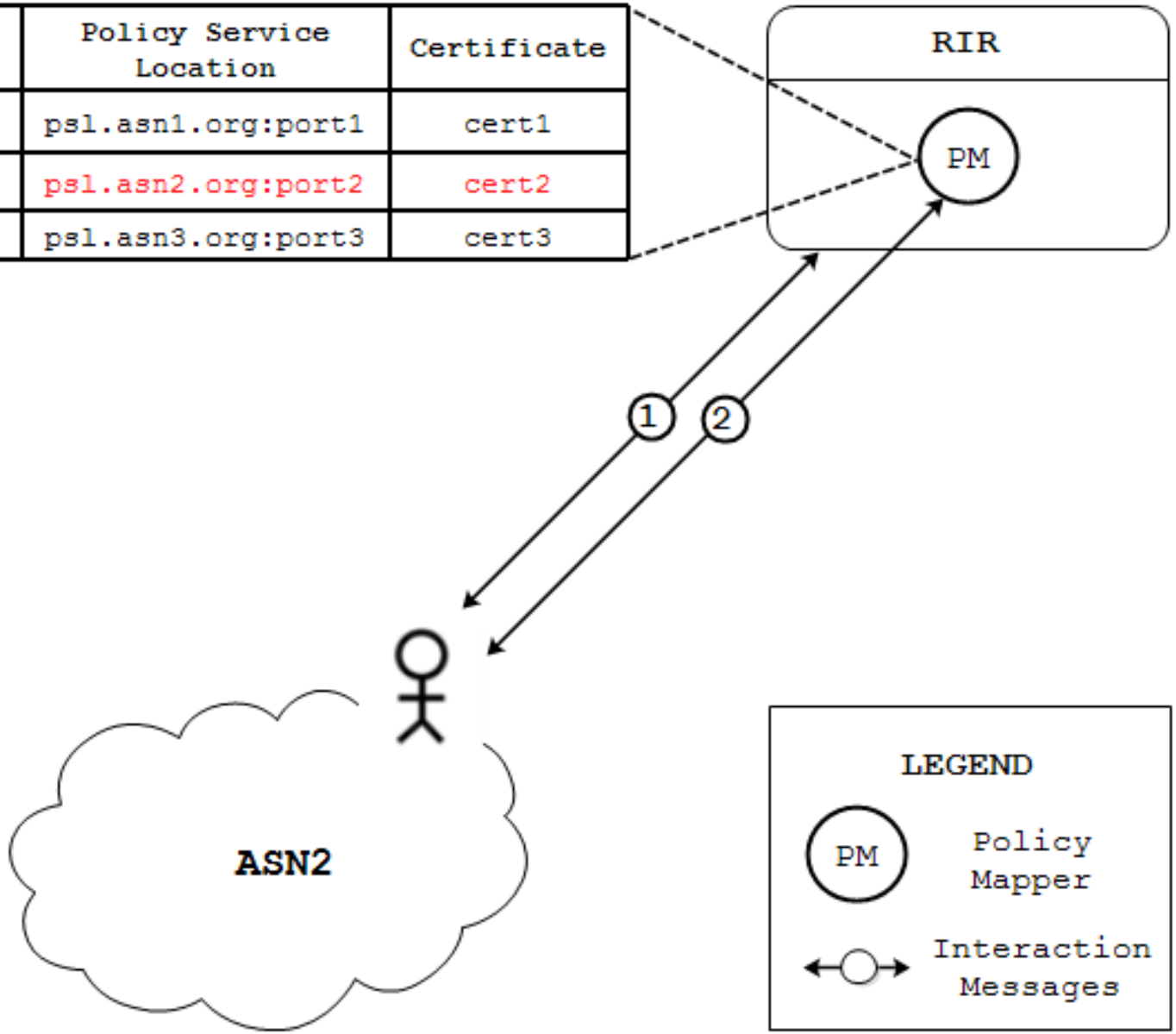
Decision making (3/3)



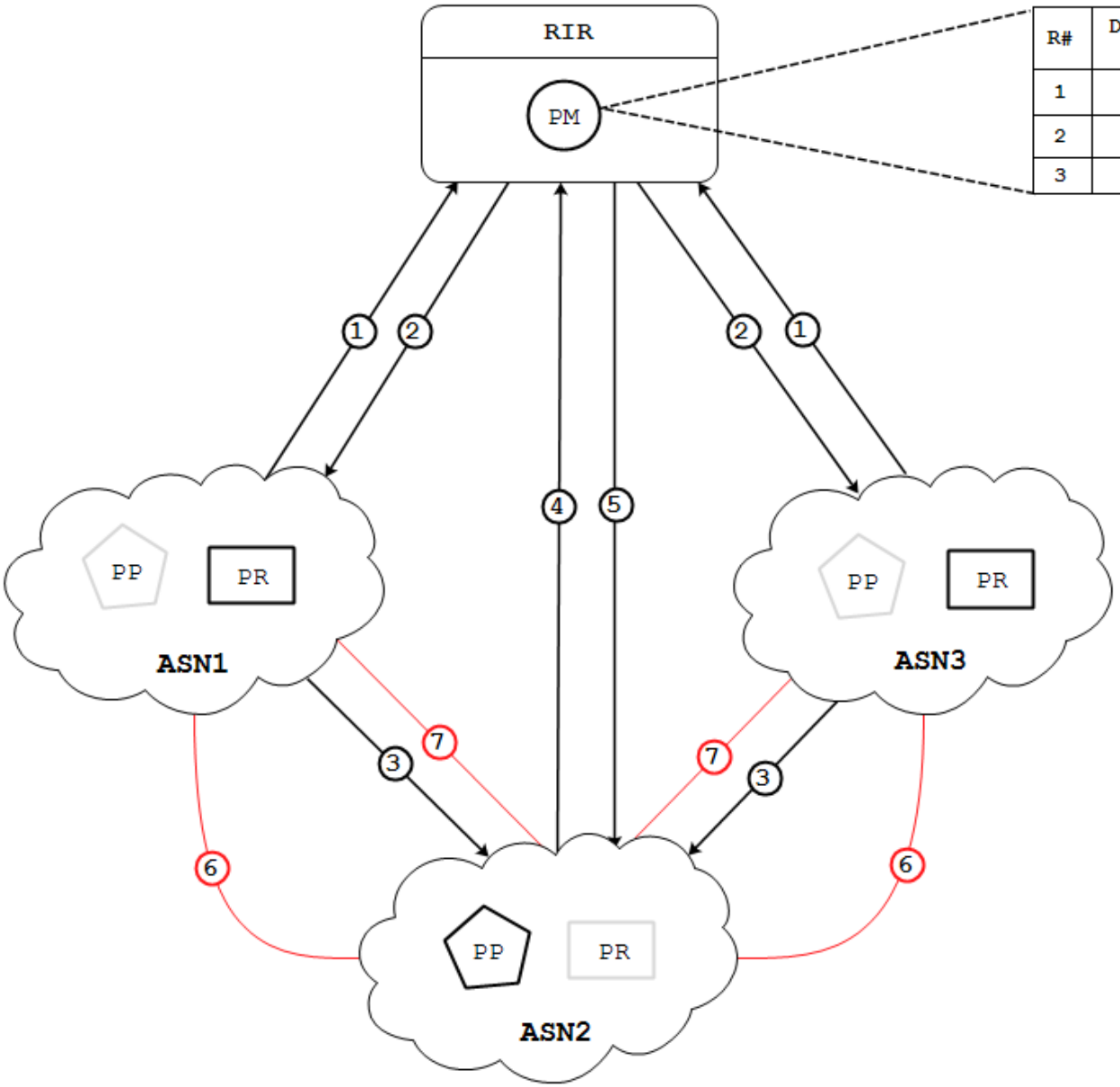
- Security aspects
  - PM acts as a Trusted Third Party (TTP) & accessible by both PRs and PPs
  - One public/private key-pair per domain, used to create a self-signed certificate and share it with PM
  - PRs & PPs communicate using their self-signed certificates over TLS (mutual authentication)

Registration to Policy Mapper

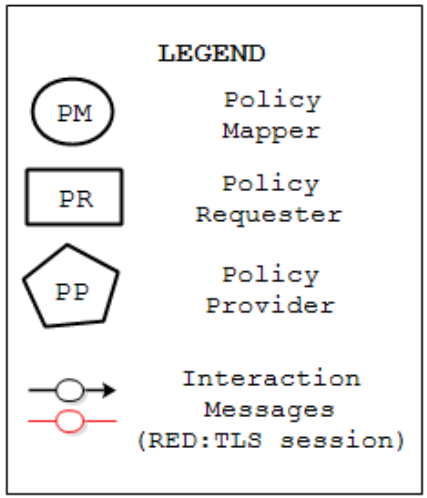
R#	Domain ID	Policy Service Location	Certificate
1	ASN1	psl.asn1.org:port1	cert1
2	ASN2	psl.asn2.org:port2	cert2
3	ASN3	psl.asn3.org:port3	cert3



Policy retrieval

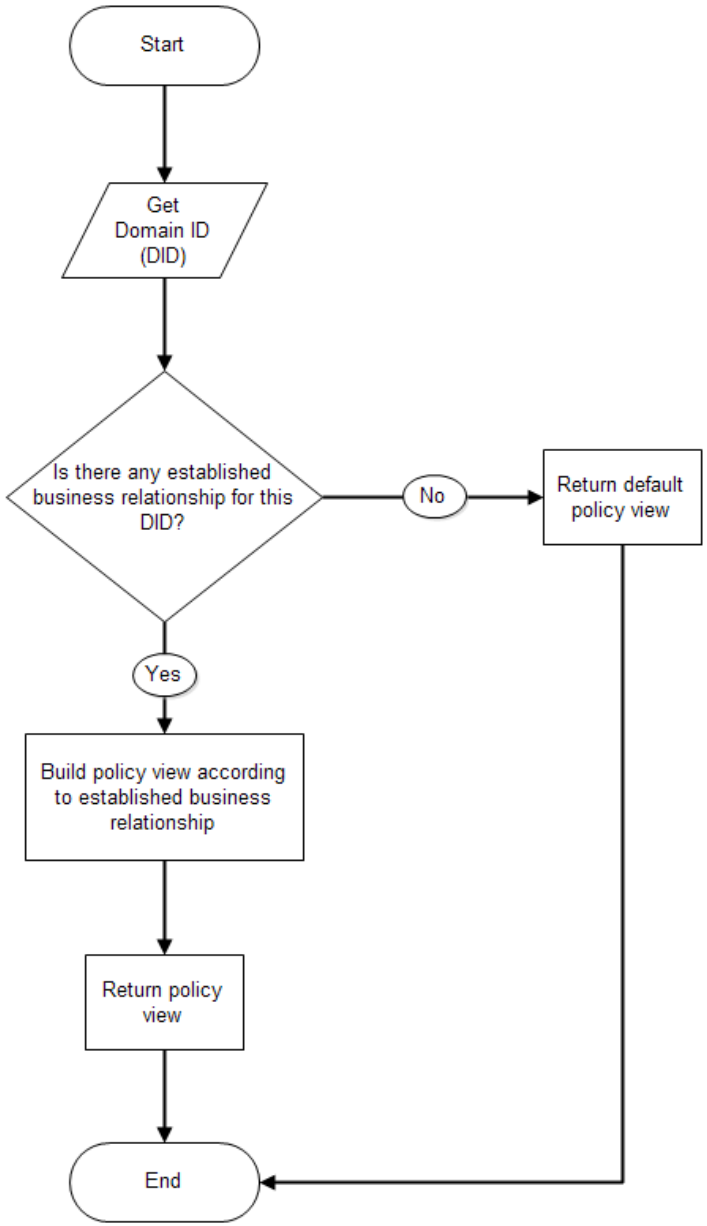


R#	Domain ID	Policy Service Location	Certificate
1	ASN1	psl.asn1.org:port1	cert1
2	ASN2	psl.asn2.org:port2	cert2
3	ASN3	psl.asn3.org:port3	cert3

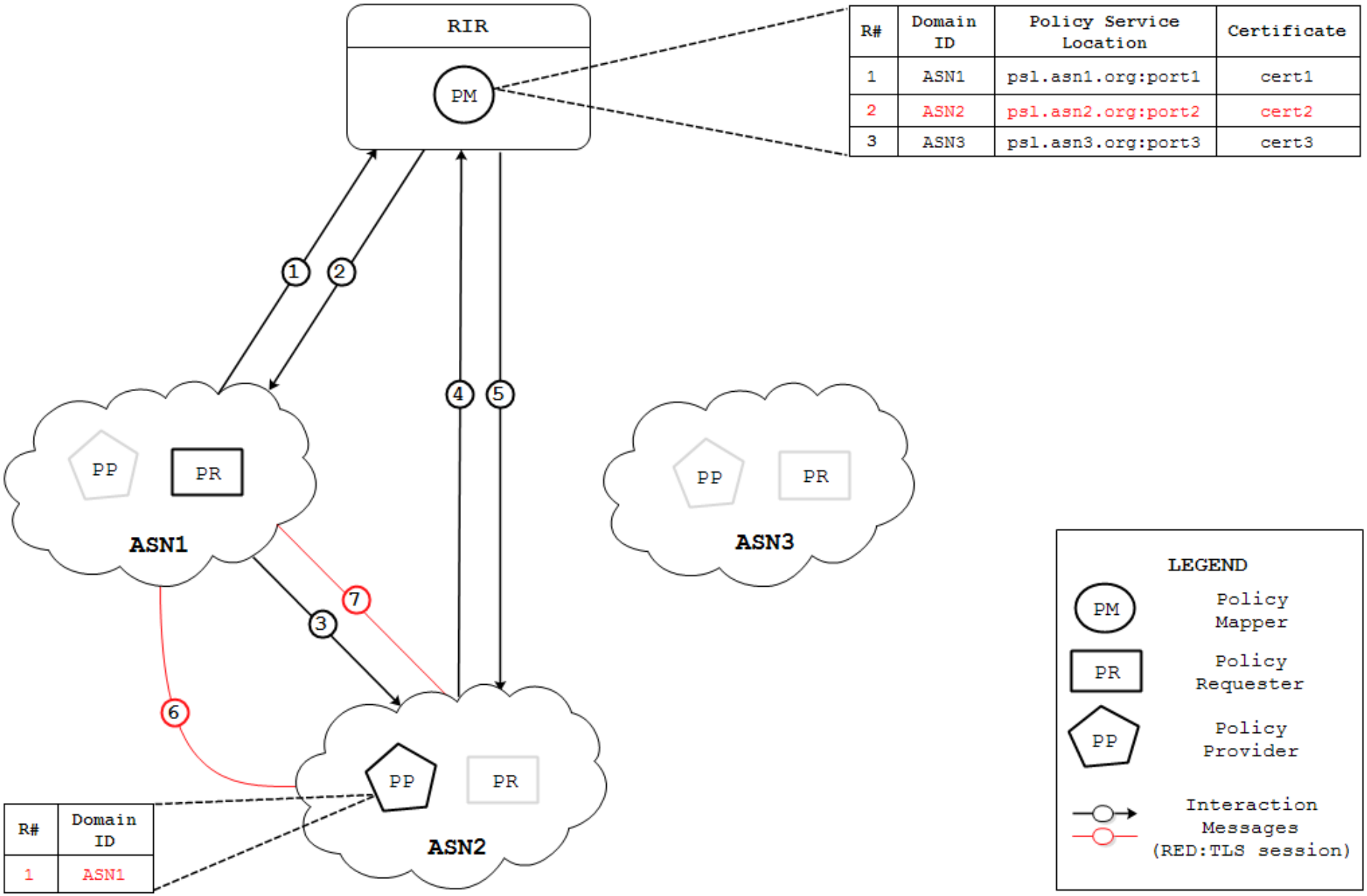


Policy view

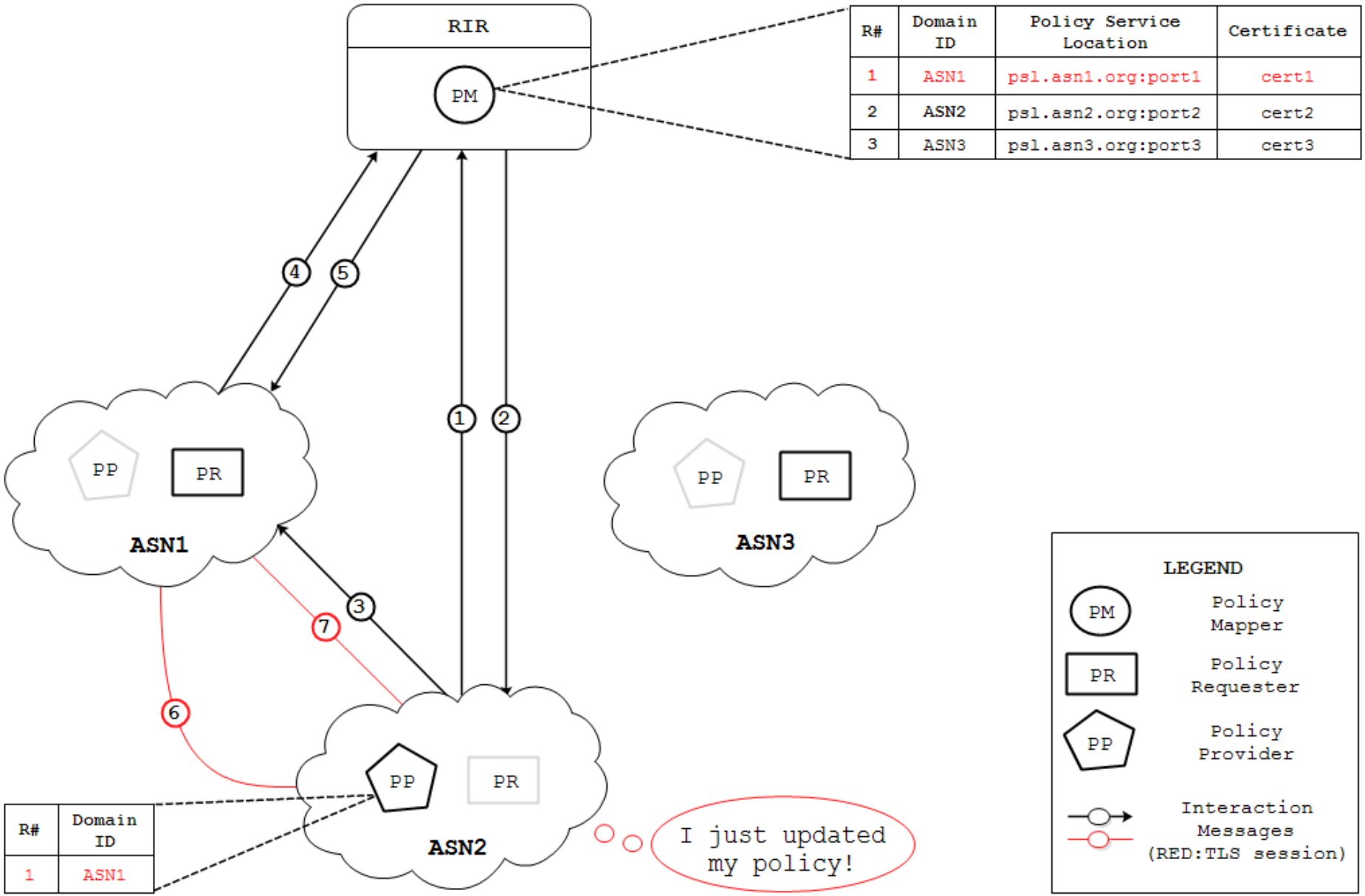
- Innovative idea
- Discrete piece of main policy information
- Different *policy views* for different requesters



Registration to Policy Provider



Policy update & notification



Discussion

- Scalability
  - hybrid model offers scalability
  - innovative system proposal
- Implementation ideas
  - Security
    - ★ RPKI, authorization but NOT authentication (RFC 6480)
    - ★ HTTPS, need for client certificates as well
  - Policy language
    - ★ only RPSL in place
    - ★ need for a structure-based, human-readable language that provides one-to-one correlation between router configurations and policies

Conclusion

- Decentralization of policies is possible! :)
- Simplicity of architecture
- Components simple and well-defined
- Room for extra services and extension of system capabilities
- Contribute to BGP security by supporting the correctness and effectiveness of BGP filters
  - policy views preserve the confidentiality of data
  - ISPs more motivated to keep their policy information accurate and up to date

Further work

- Proof of concept
- Large scale scenario
- RPSL alternatives
  - Routing Documentation Language (RDL) [3]
  - YAML Ain't Markup Language
- Correctness of policy information
  - Comparison of the *policy view* received with the local policy

[3] part of Extendible Next Generation Routing Information Toolkit (ENGRIT) project and kicked off on 2014 [2]

References

Ralph Koning, Miroslav Zivkovic, Stavros Konstantaras, Paola Grosso, Cees de Laat (UvA) and Farabi Iqbal (TUDelft) (2015)

Architecture for Exchanging Topology Information in Multi-domain Environments

Per Gregers Bilse and Benno Overeinder, IEPG Meeting, IETF 89, London, UK, March 2014

Presentation: "A programmatic approach to generating router configurations"

http://www.iepg.org/2014-03-02-ietf89/rdl-IEPG-89.pdf

Thank you for your attention! :)
Questions?