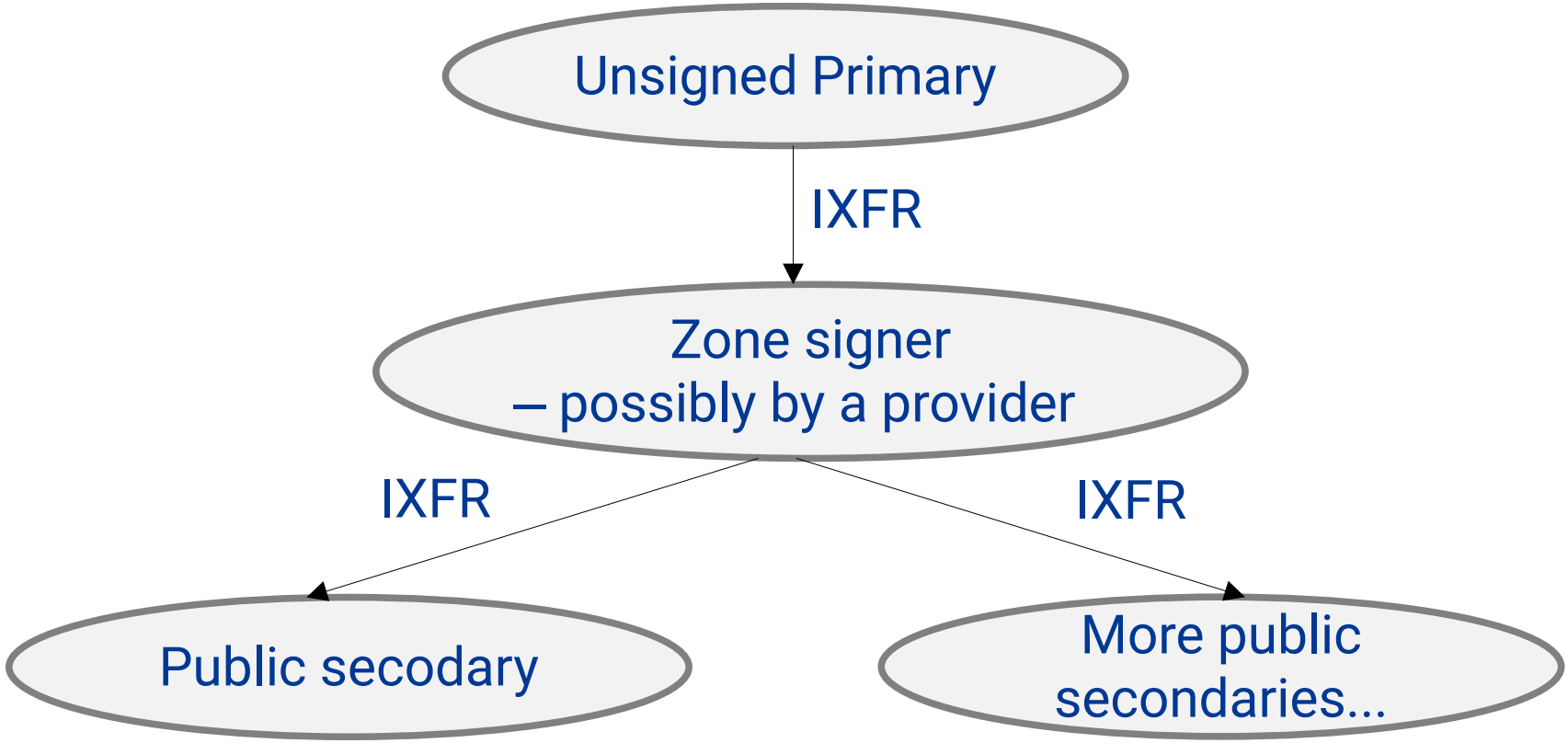
Single-provider Multi-signer: Overview of Scenarios

• 22. 5. 2024

CZ.NIC | SPRÁVCE DOMÉNY CZ

Typical signer setup

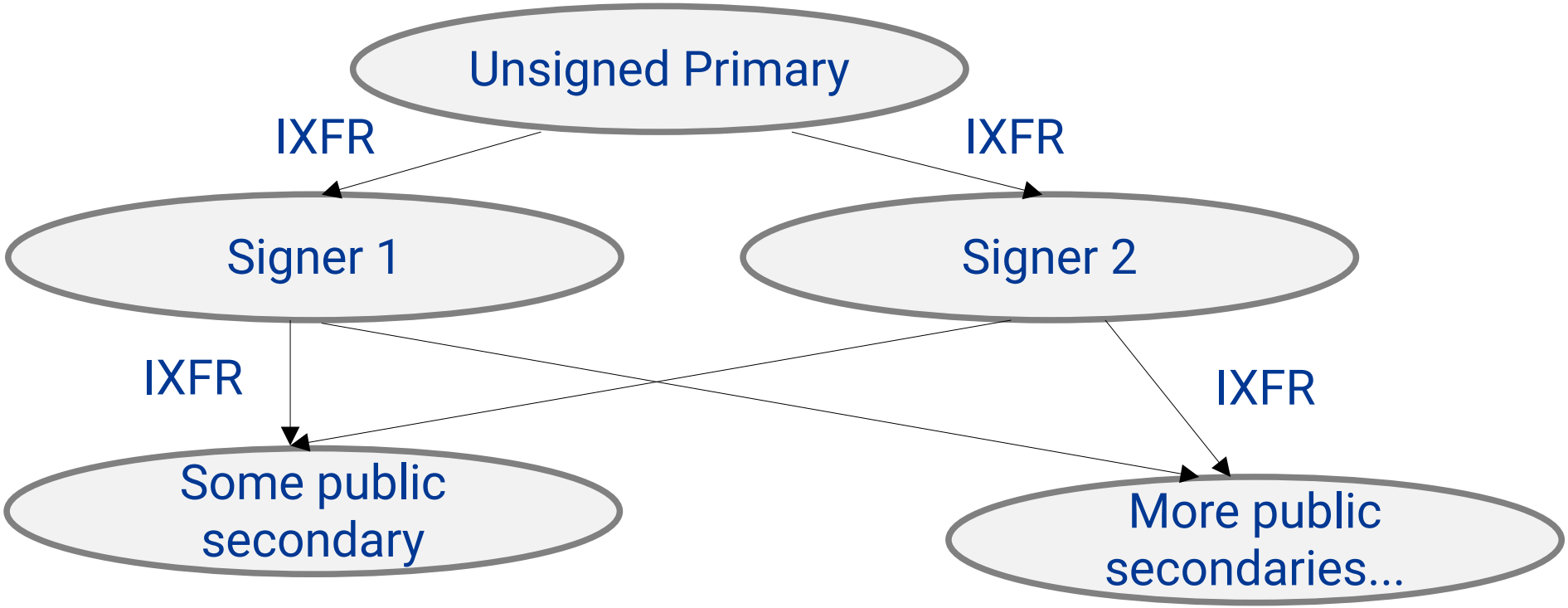


Multi-provider multi-signer

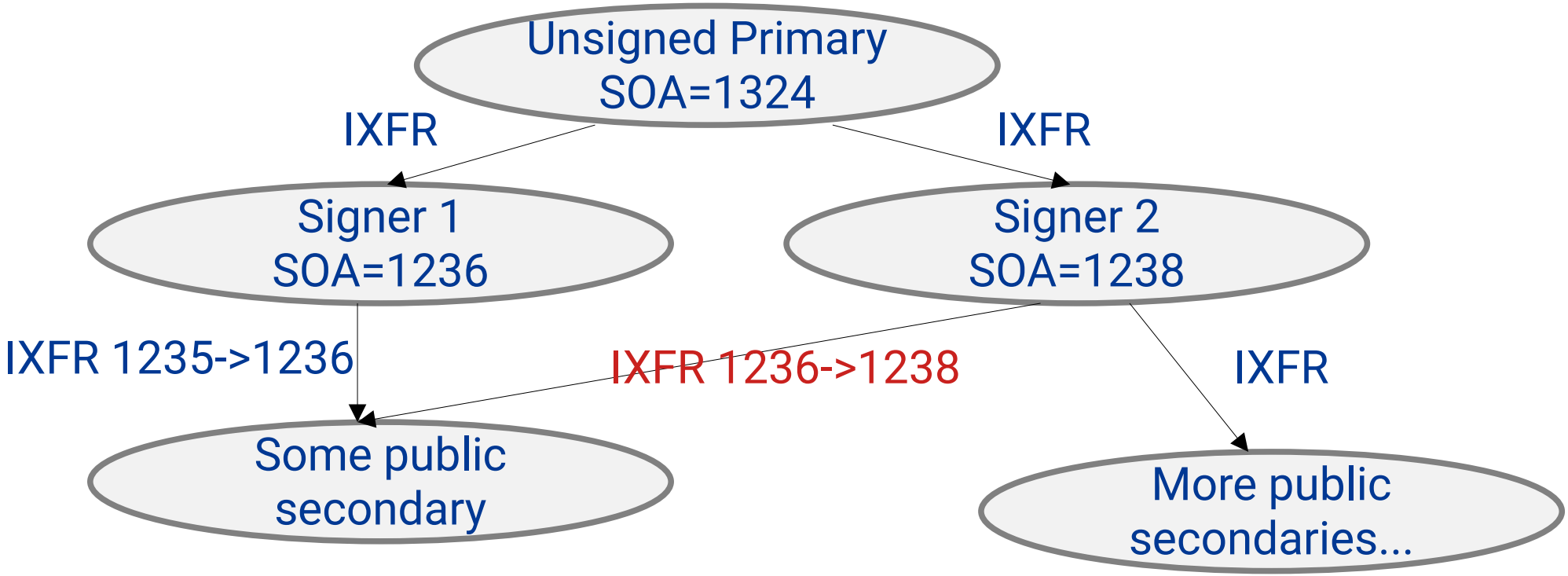
- Smooth DNSSEC-provider transition
- MUSIC project
  - in development

I.
Common multi-signer considerations

Multi-signer is multi-primary



Multi-signer is multi-primary

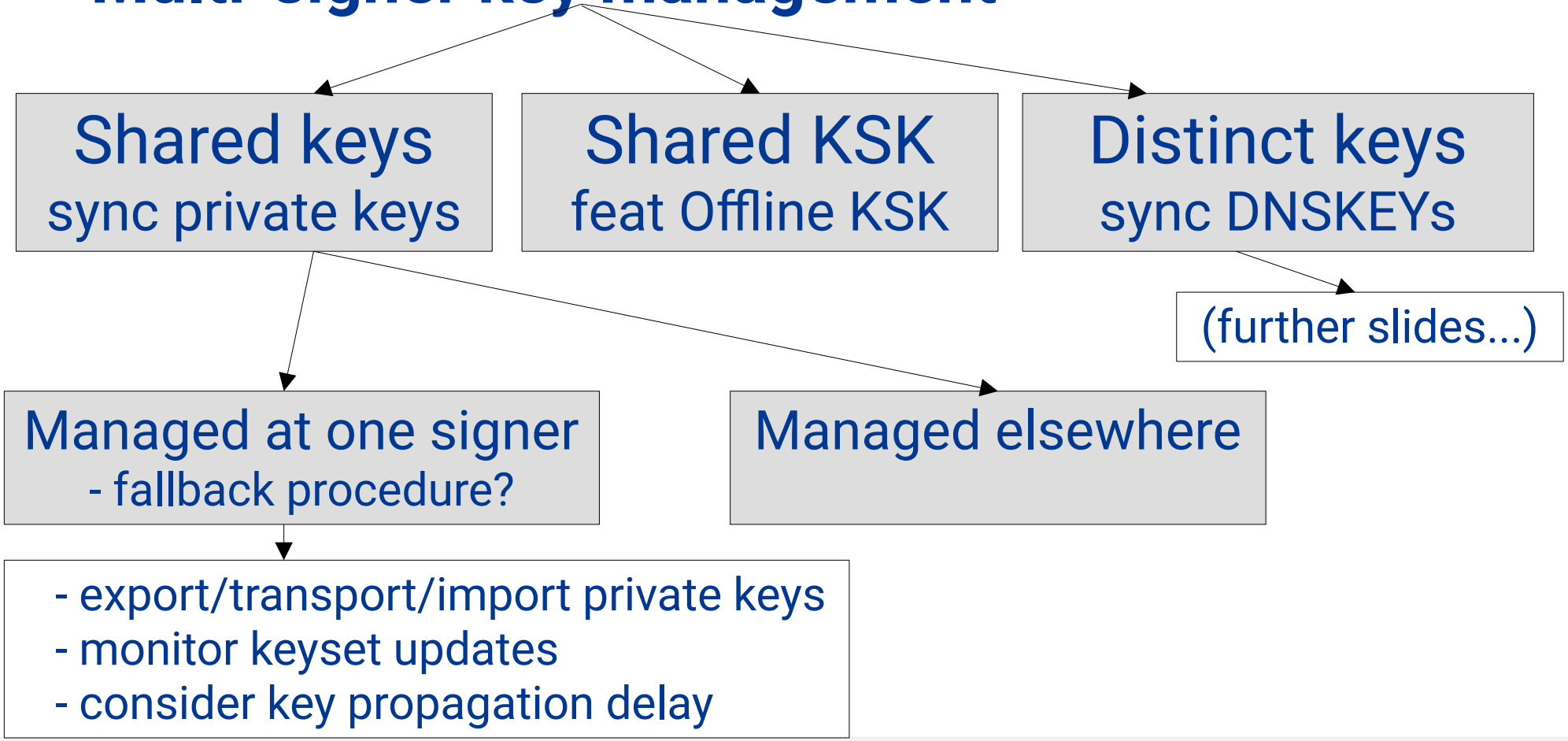


Preventing Interchanged IXFR

- Disable IXFR (only if desperate)
- Prevent equal SOA serial (serial-modulo)
  - configurable on signers
- Prevent roaming between primaries
  - configurable on secondaries
  - master-pinning, not trivial but nice

II.
Various multi-signer setups
...and goals

Multi-signer key management



DNSKEY synchronization

- Each signer's „own“ and „foreign“ DNSKEYs
  - Large DNSKEY RRSet
- Synchronization
  - Initial
  - Key roll-overs
- CDS+CDNSKEYs either all or none

DNSKEY synchronization 2

- DDNS or whatever
- Either to all others
  - potential cycling issues if > 2
- Or to common primary
  - IXFR issues: additions of own DNSKEYs

Recommendations

- Automate, Automate, Automate
  - Keep monitoring
- Event-triggered tools
- Roll-over timing reflects sync delay
- Guidelines:

  https://www.knot-dns.cz/docs/latest/singlehtml/index.html#dnssec-multi-signer

- QUESTIONS ?

Libor Peltan, CZ.NIC