



DNSKEY TRANSITION OBSERVATORY

Priya Ravichander <pravicha@masonlive.gmu.edu>

Eric Osterweil <eoster@gmu.edu>

Steve Crocker <steve@shinkuro.com>



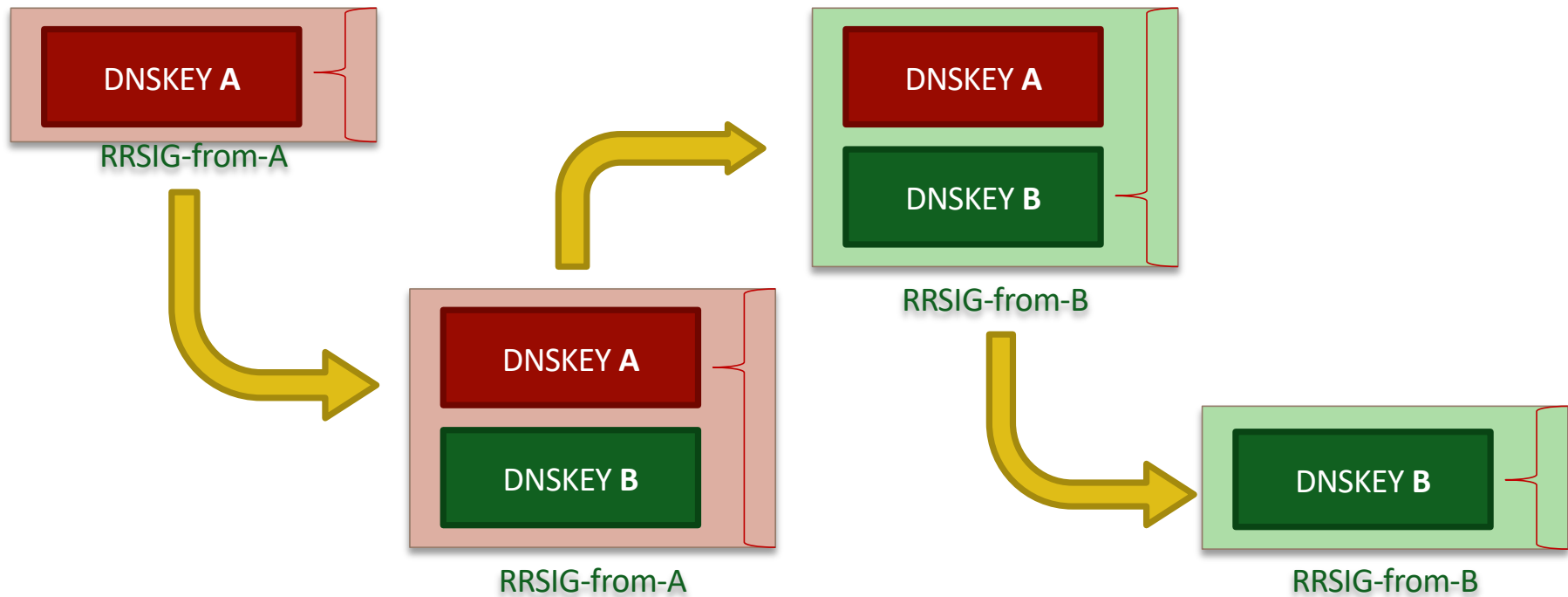
- When DNSSEC zones change their DNSKEYs, they *transition* from an existing set to a remaining set
 - A developing field of study
- This process can follow standards (such as RFC-7583 or RFC-5011), research papers [1], or no stated process at all!

BUT

- What are validating resolvers seeing?
- These processes are growing more complex (e.g., RFC-8901)
- The DNSKEY Transition Observatory will track resolver-side views of key transitions

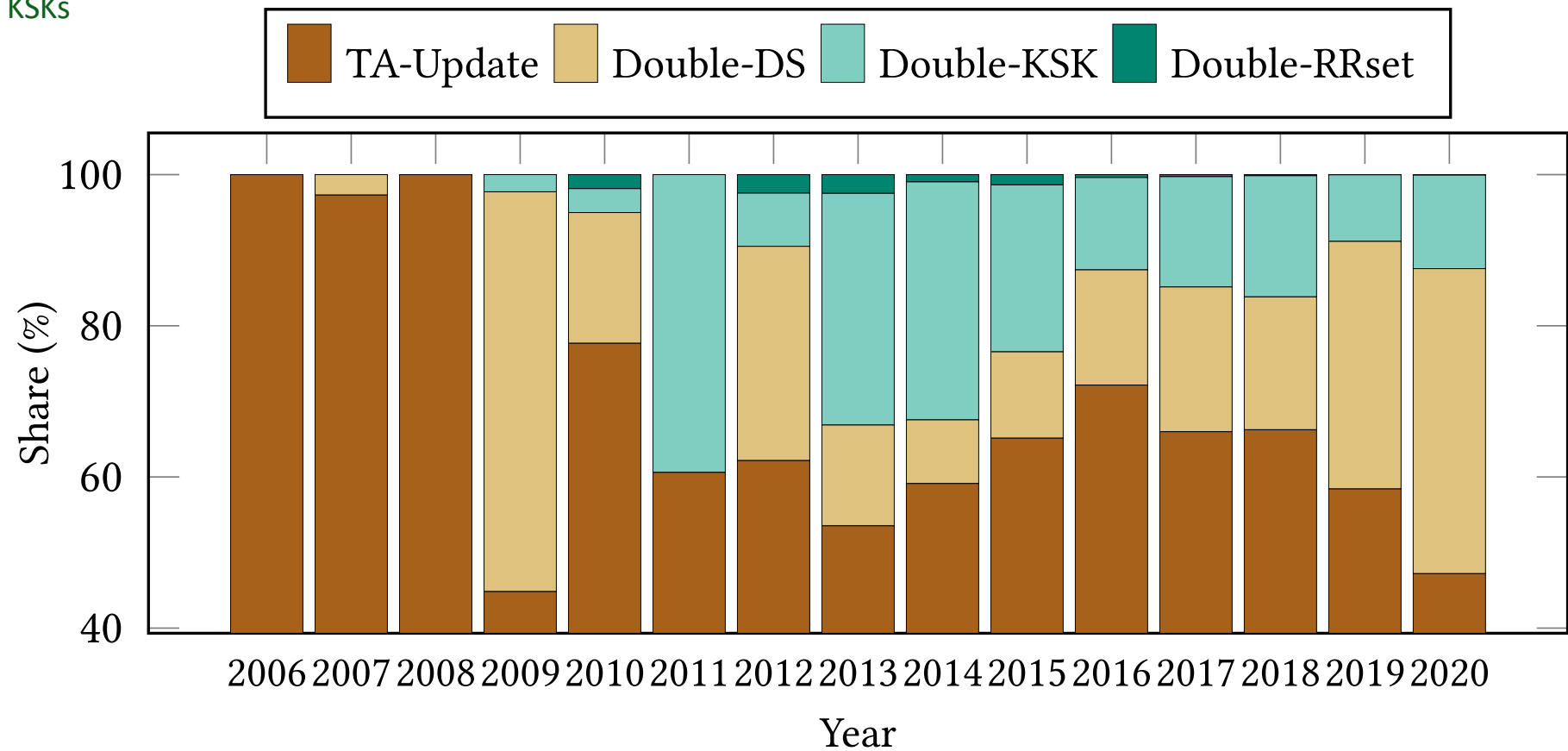
[1] Zheng Wang and Liyuan Xiao. Emergency key rollover in dnssec. In 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications, pages 598–604. IEEE, 2014.

KEY TRANSITIONS: SIMPLE... IN THEORY



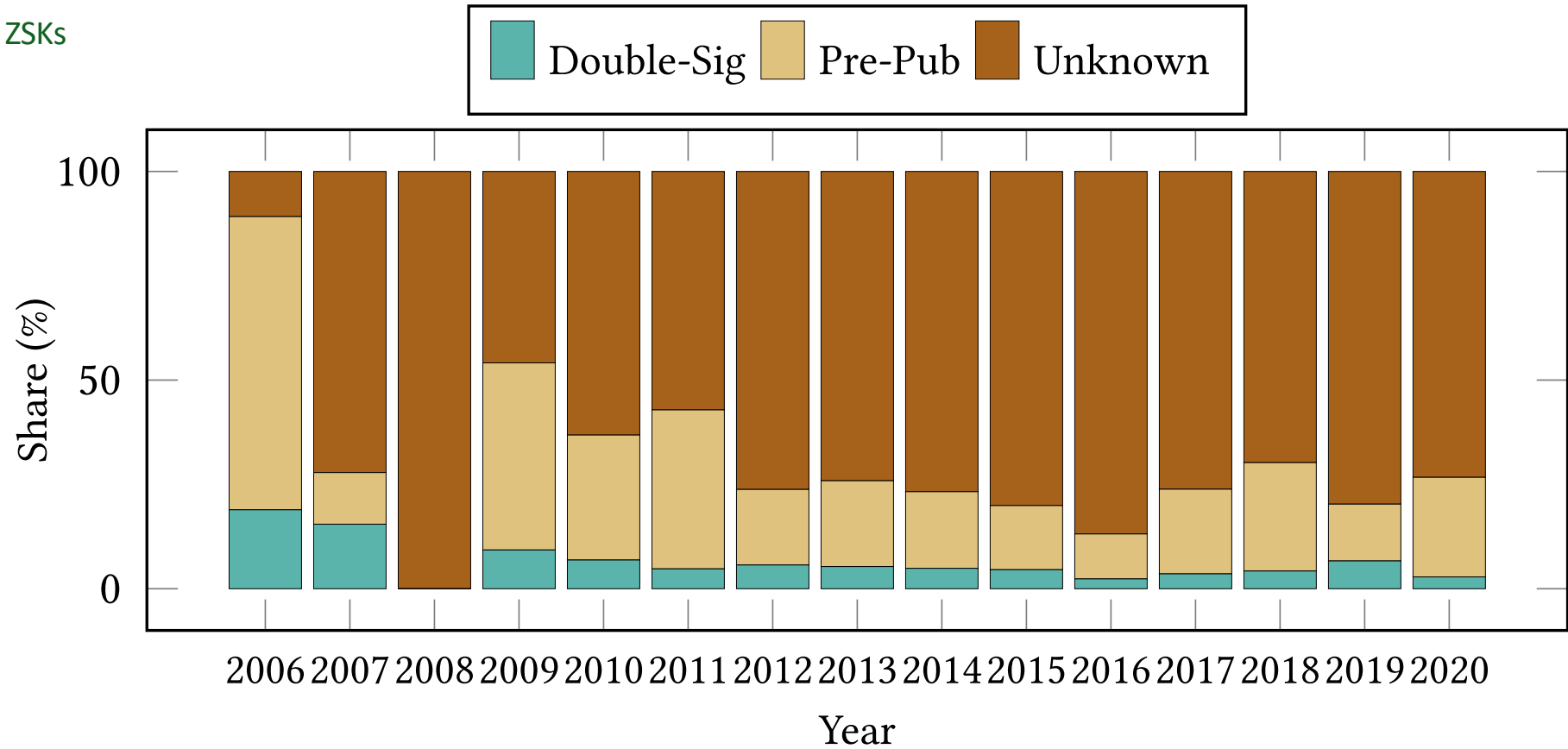
BUT, IN PRACTICE WE HAVE SEEN A LOT OF “INNOVATION”

KSKs



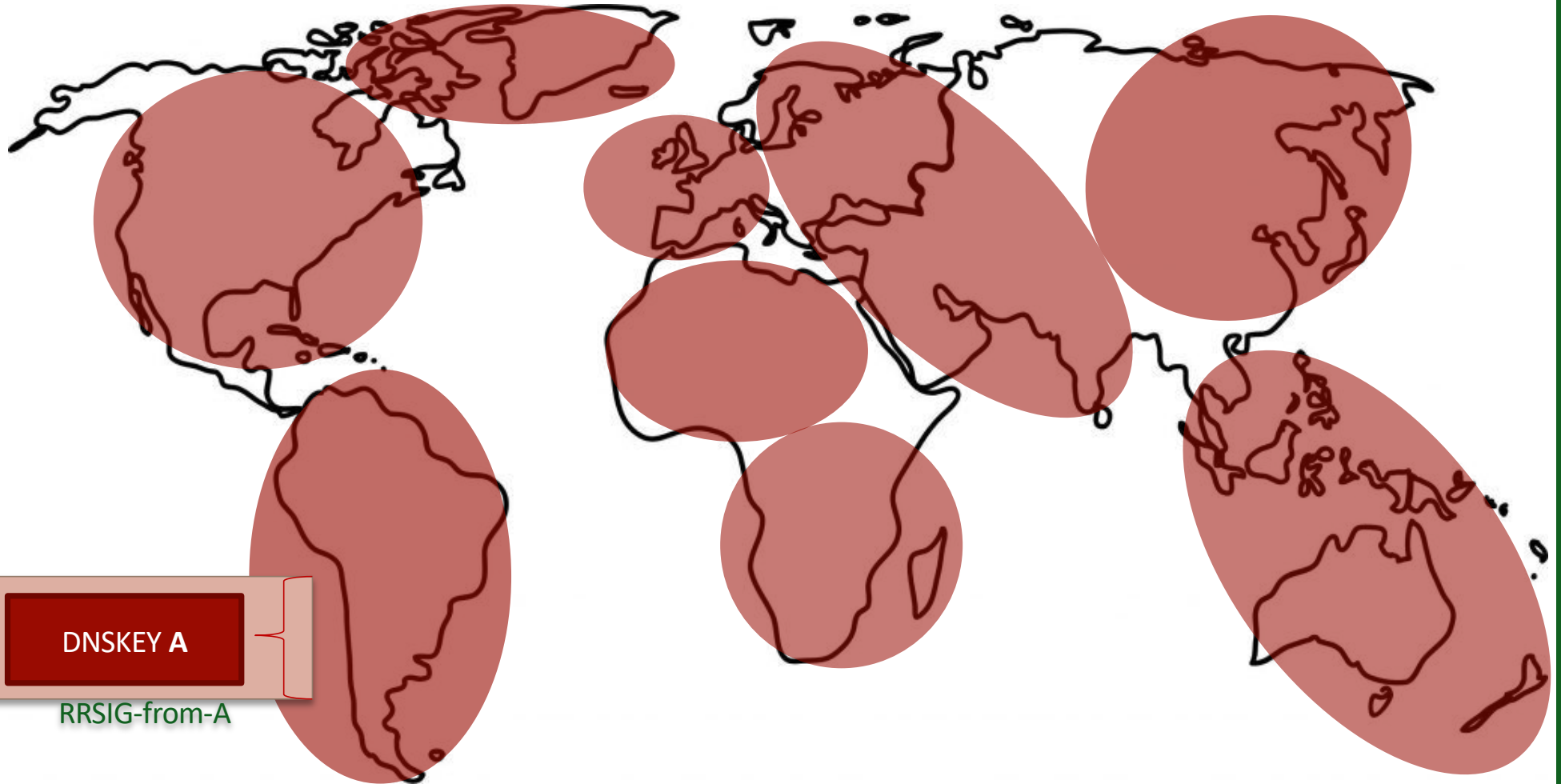
BUT, IN PRACTICE WE HAVE SEEN A LOT OF INNOVATION

ZSKs



BUT, WHAT DO RESOLVERS SEE?

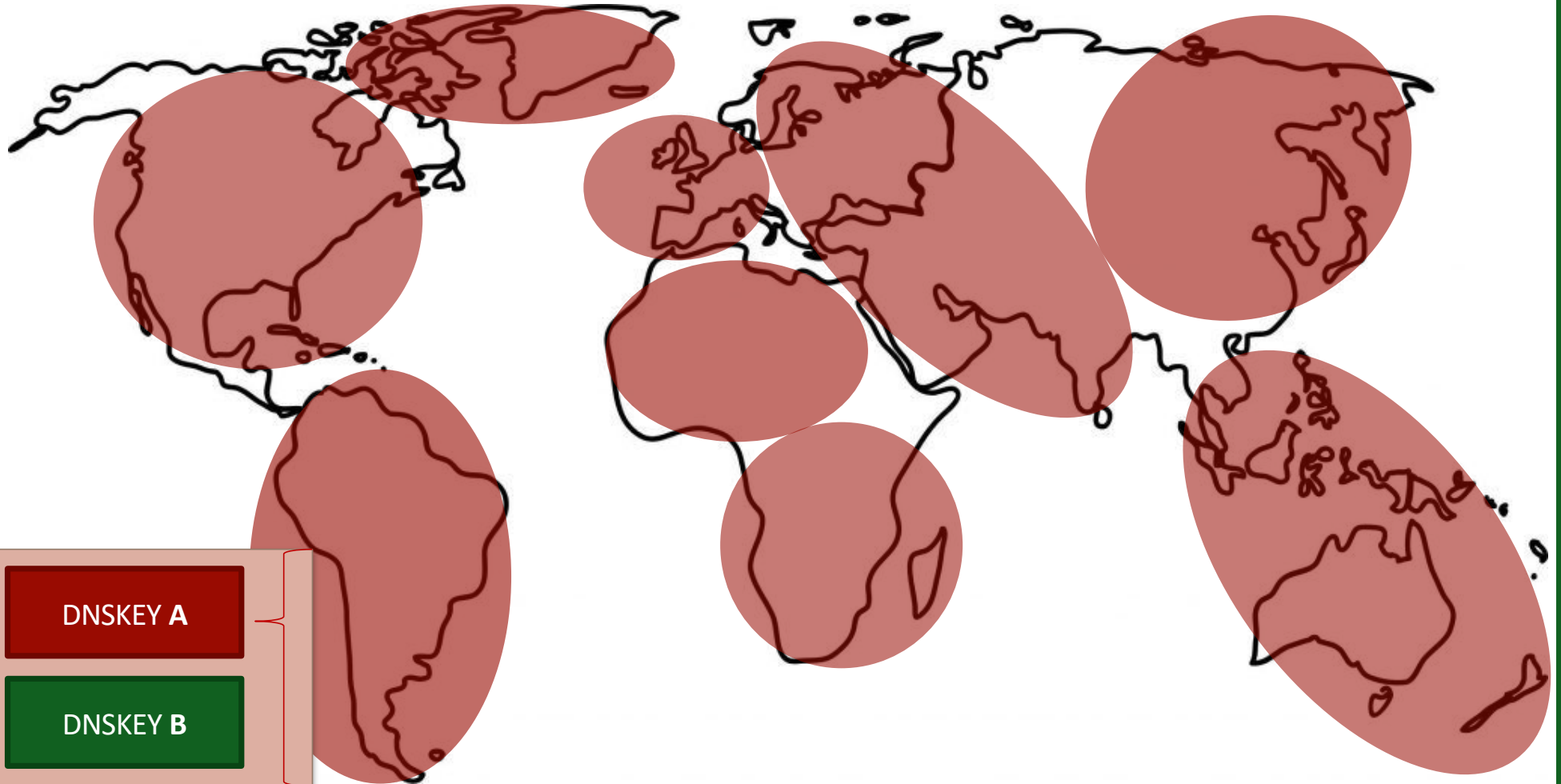
- When a zone transitions from an existing key (DNSKEY A) to a new key (DNSKEY B), when do resolvers see the change?
- Many details can complicate this
 - Timing
 - Caching
 - Multiple signing providers/operators
 - etc.
- Will transitions be regional?
- Will they converge, and how long will that take?
- We need a distributed monitor (an *observatory*) to monitor the global/distributed evolution



DNSKEY A

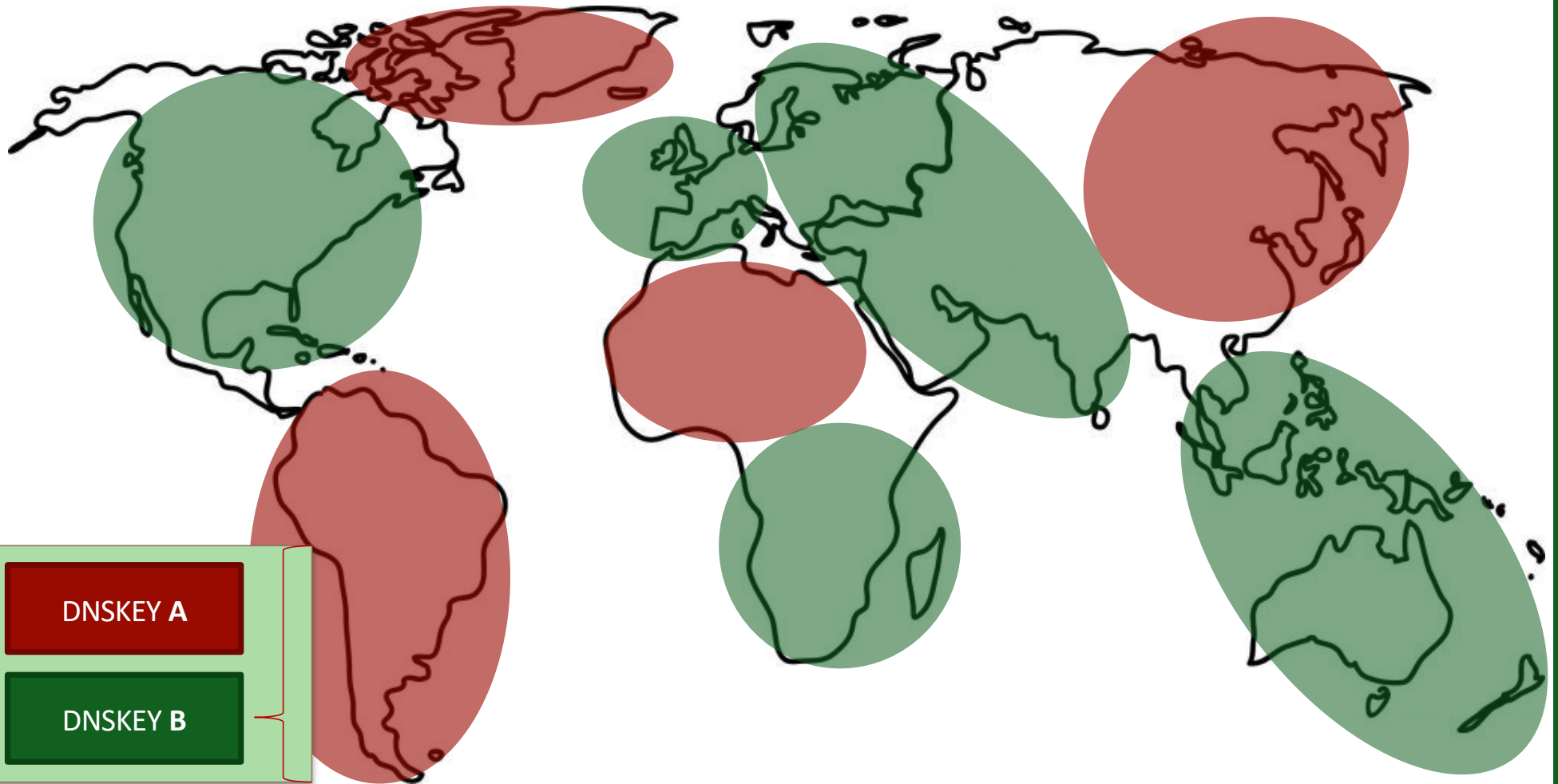
RRSIG-from-A

GLOBAL RESOLVER OBSERVATORY



RRSIG-from-A

GLOBAL RESOLVER OBSERVATORY

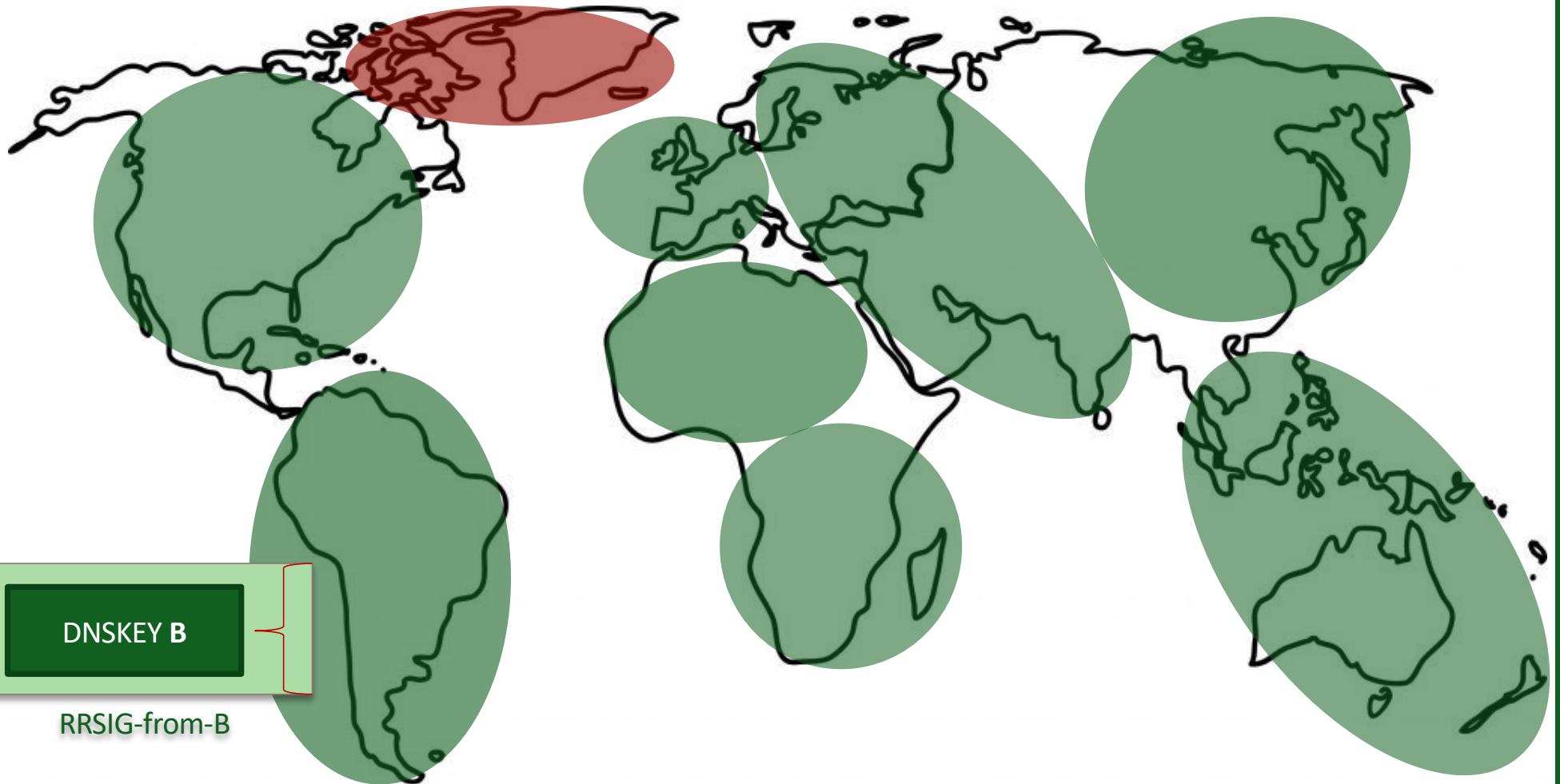


DNSKEY A

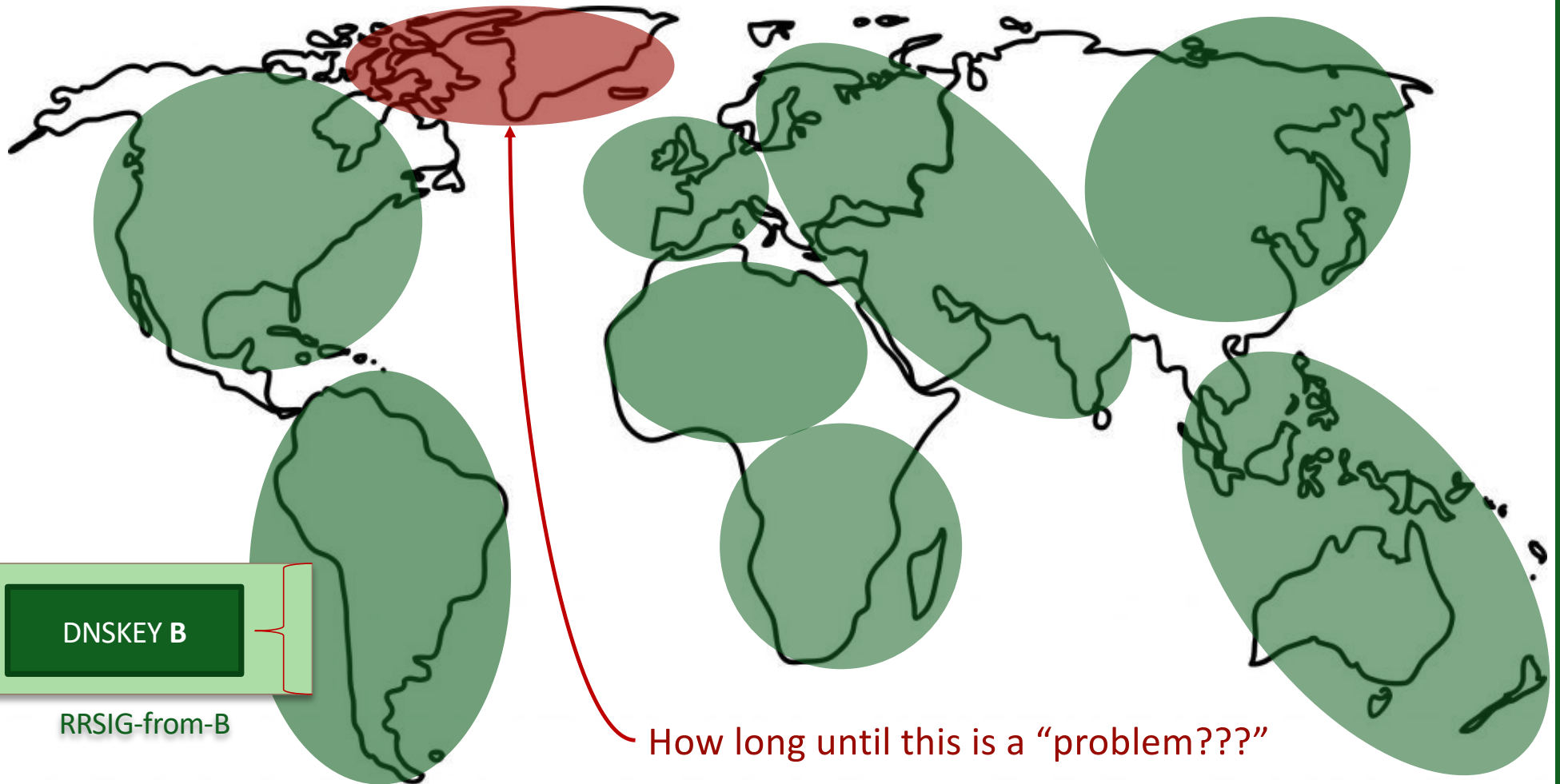
DNSKEY B

RRSIG-from-B

GLOBAL RESOLVER OBSERVATORY



GLOBAL RESOLVER OBSERVATORY



- The transition observatory will track transitions in real-time
- The sets of transitions and procedures will each lead to different acceptance criteria, such as
 - What is a valid state?
 - How long should transitions take?
 - What, if anything, has gone wrong?
 - etc.
- Aggregate analyses will be disseminated and fed-back into operational forums (like this one)

THANK YOU

The background is a solid dark green. On the left side, there are stylized, light green shapes that resemble a mountain range or a series of overlapping leaves. On the right side, there are several curved, light green shapes that look like stylized leaves or petals, arranged in a fan-like pattern.