UNIVERSITEIT VAN AMSTERDAM

# Ad Hoc Trust Associations with Trust Anchor Repositories

Stefan Roelofs

Research Project 2

1 July, 2009



# Agenda

- Research Questions
- DNSSEC
- Global Trust Hierarchy versus Island Based Concepts Comparison
- Future of TAR
- Network Resource Provisioning Concepts
- Using TAR in on-demand Network Resource Provisioning
- Conclusion

## Research Questions

- What are the differences between the original DNSSEC global trust model and the island based model with Trust Anchor Repositories?

- What models are currently developed and what could or should be future developments?

- How can the Trust Anchor Repositories be of use in multi-domain on-demand network resource provisioning?

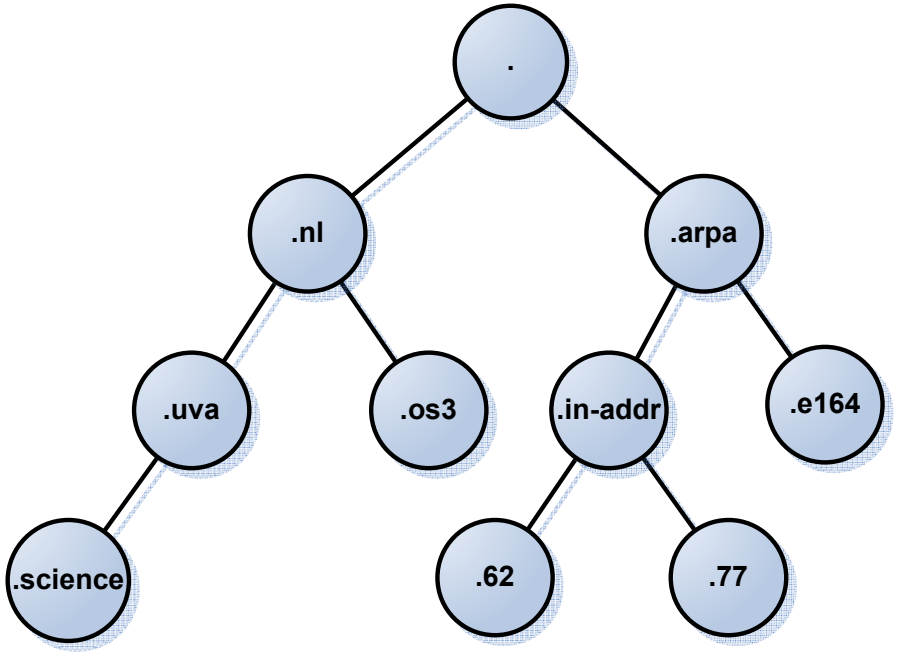
## DNSSEC

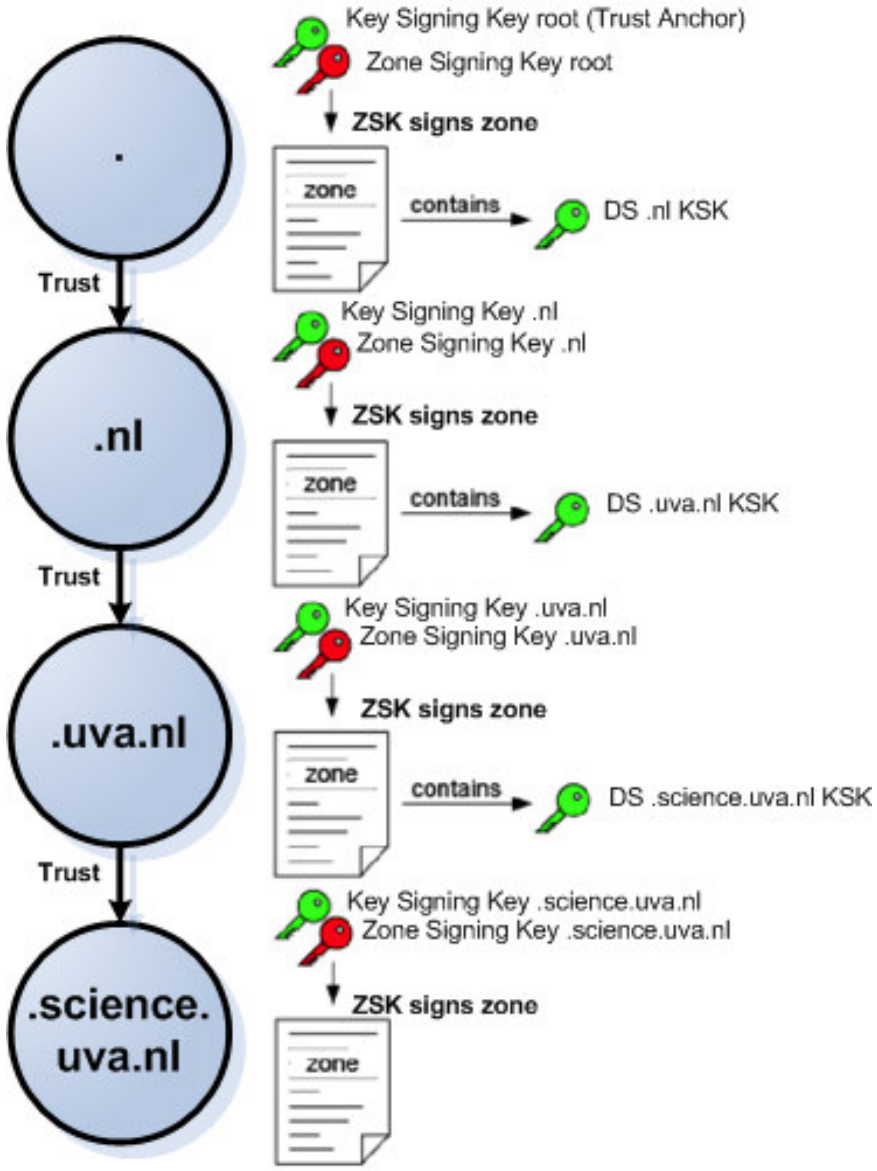
DNSSEC provides *origin authenticity, data integrity,* and *secure denial of existence* by using public-key cryptography

- *Origin authenticity:*
  Resolvers can verify that data has originated from authoritative sources.
- *Data integrity*
  Can also verify that responses are not modified in-flight
- *Secure denial of existence*
  When there is no data for a query, authoritative servers can provide a response that proves no data exists

# Global Trust Hierarchy

- DNSSEC Model
- Public Key Infrastructures

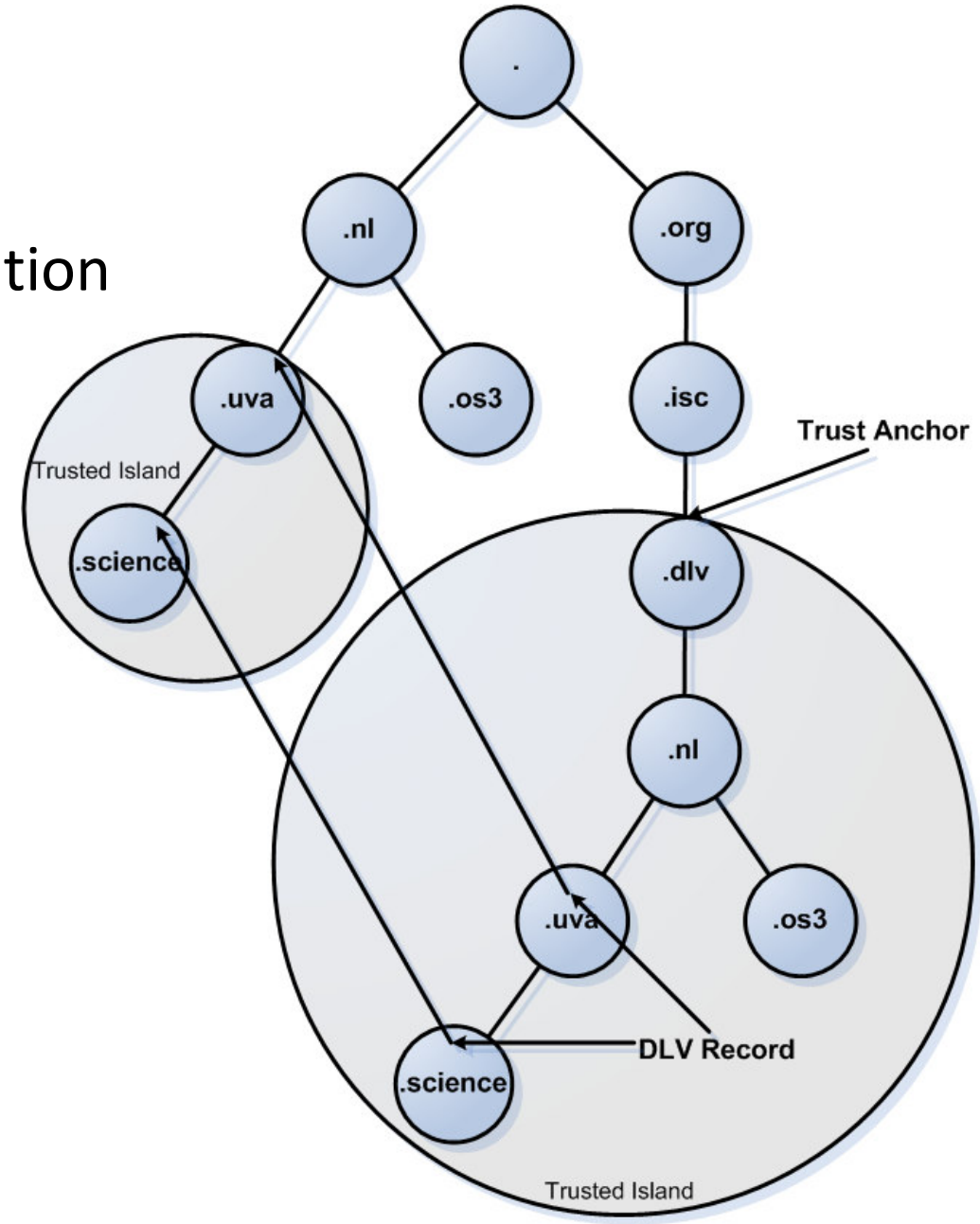



Picture partly derived from Surfnet

## Island Based Trust

- DNSSEC Look-aside Validation
- Manual TAR
- Automatic TAR





## Differences

- Governance: who controls the root
- Key management: key rollover
- Access: in-band or out-band
- Availability: load
- Partitioning of tree & complexity



## Future TAR concepts

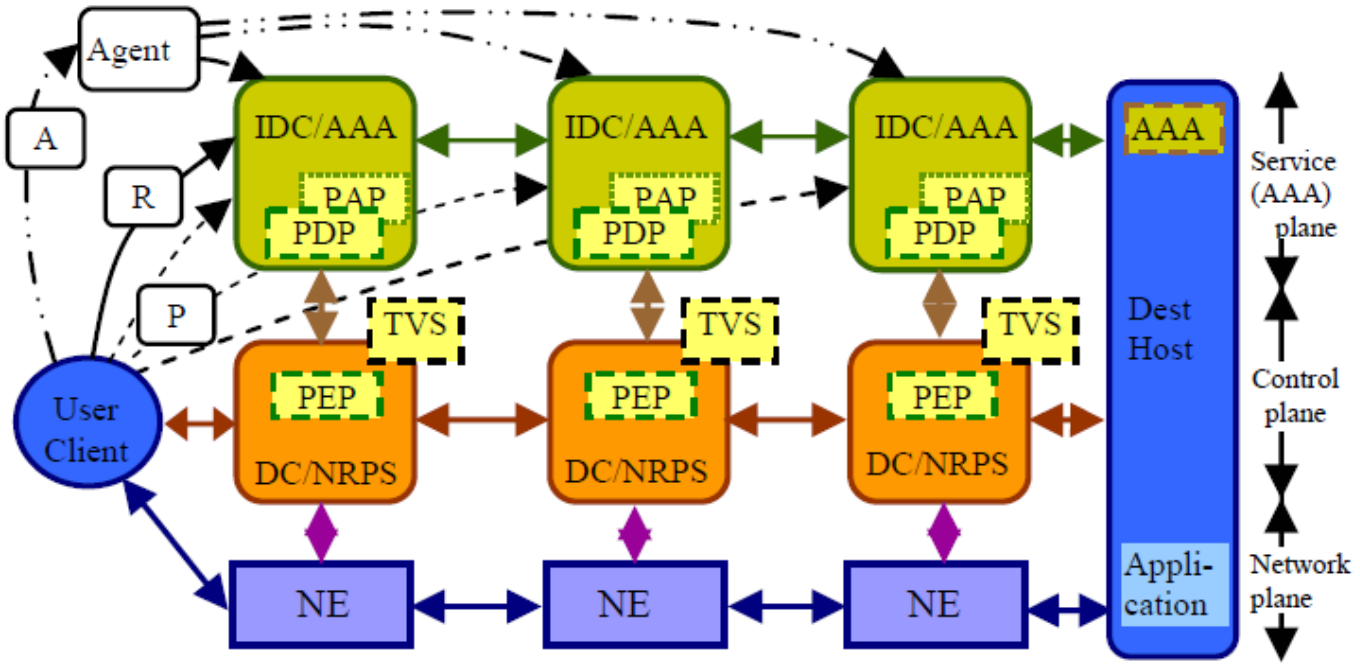
- Is there a future?

*Proposed models by the NIST:*

- Global TAR: to support global DNSSEC deployment
- Community of Interest (COI) TAR: research networks, contractors, outsourcing parties
- Enterprise TAR: for multiple internal namespaces

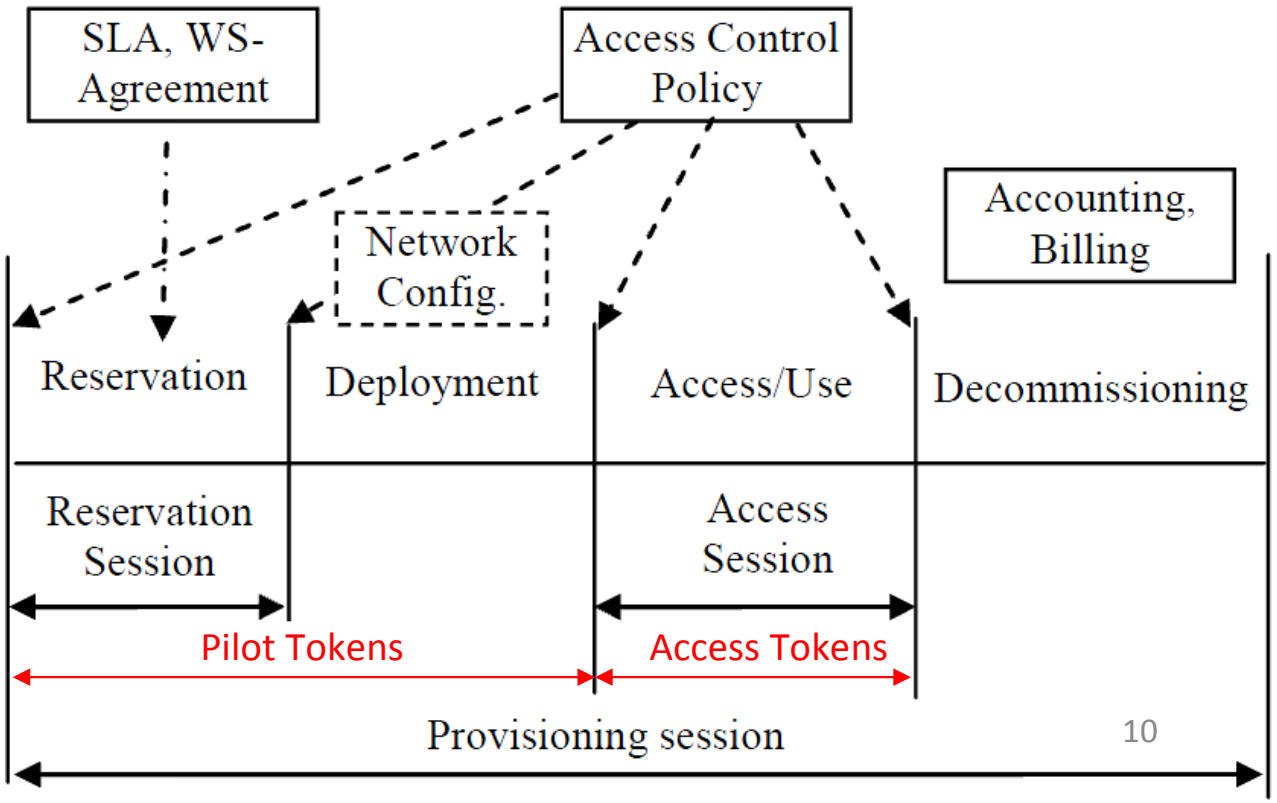
# Network Resource Provisioning (NRP) Model

- Allocate network resources as a virtualized resource like computation
- Authorization infrastructure for NRP extends generic AAA infrastructure



## Stages & Session Management

- Stages: reservation, deployment, access/use, decommissioning
- Access Tokens (all planes) & Pilot Tokens (control plane)
- PTT3: carry security information context during reservation (forward)
- PTT4: set-up TVS infrastructure during deployment (backward)



## Stages & Session Management

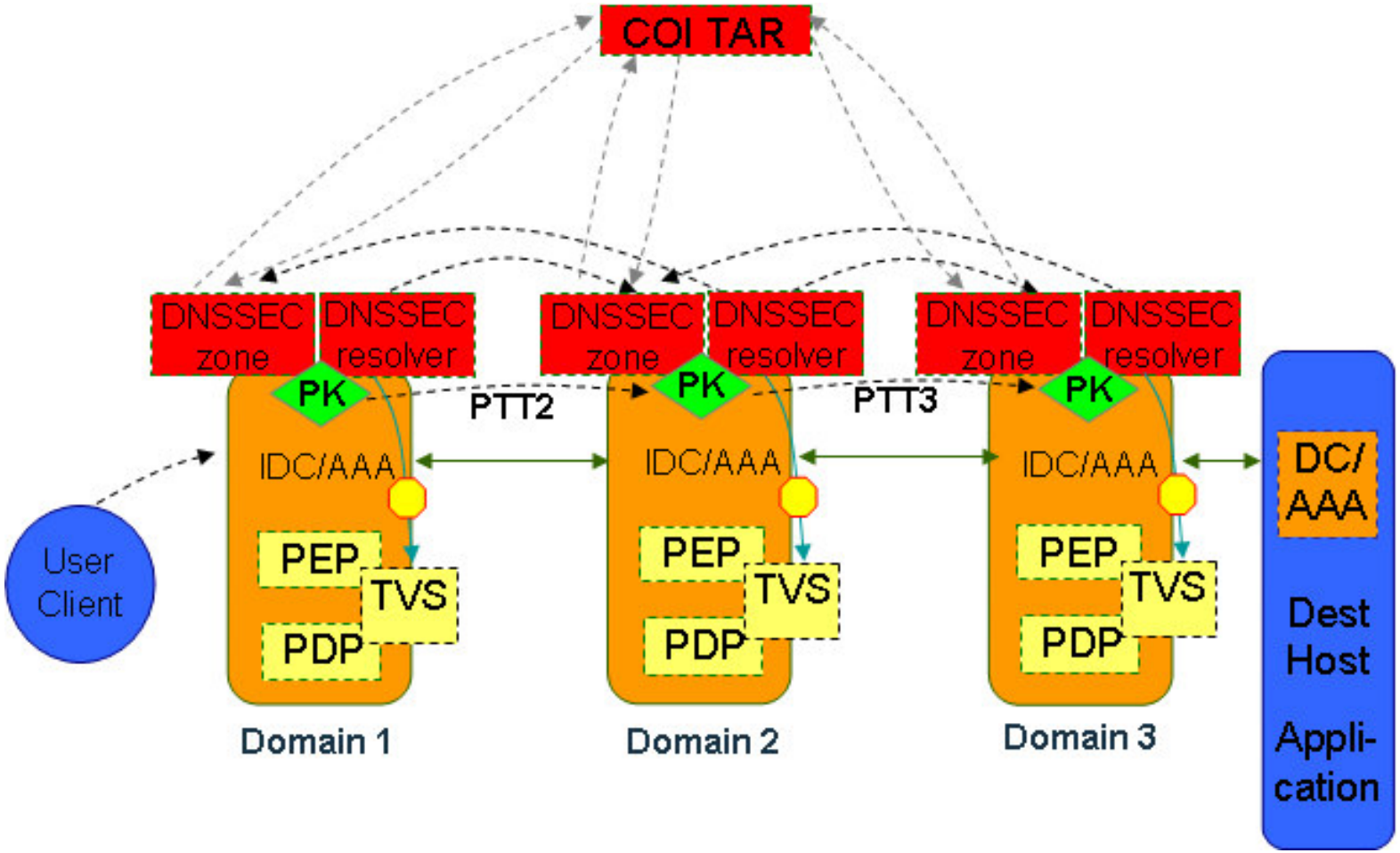
- Authentication using TokenKey and TokenValue
  - TokenKey
    *HMAC(GRI, tb_secret)*
  - TokenValue
    *HMAC(GRI, TokenKey) – access tokens*
    *HMAC(concat(DomainId, GRI, TokenId), TokenKey) – PTT2/PTT3*
- Current implementation uses shared secret
- Shared secret: tb_secret: (token builder) 3DES hard-coded

## Proposed Modifications

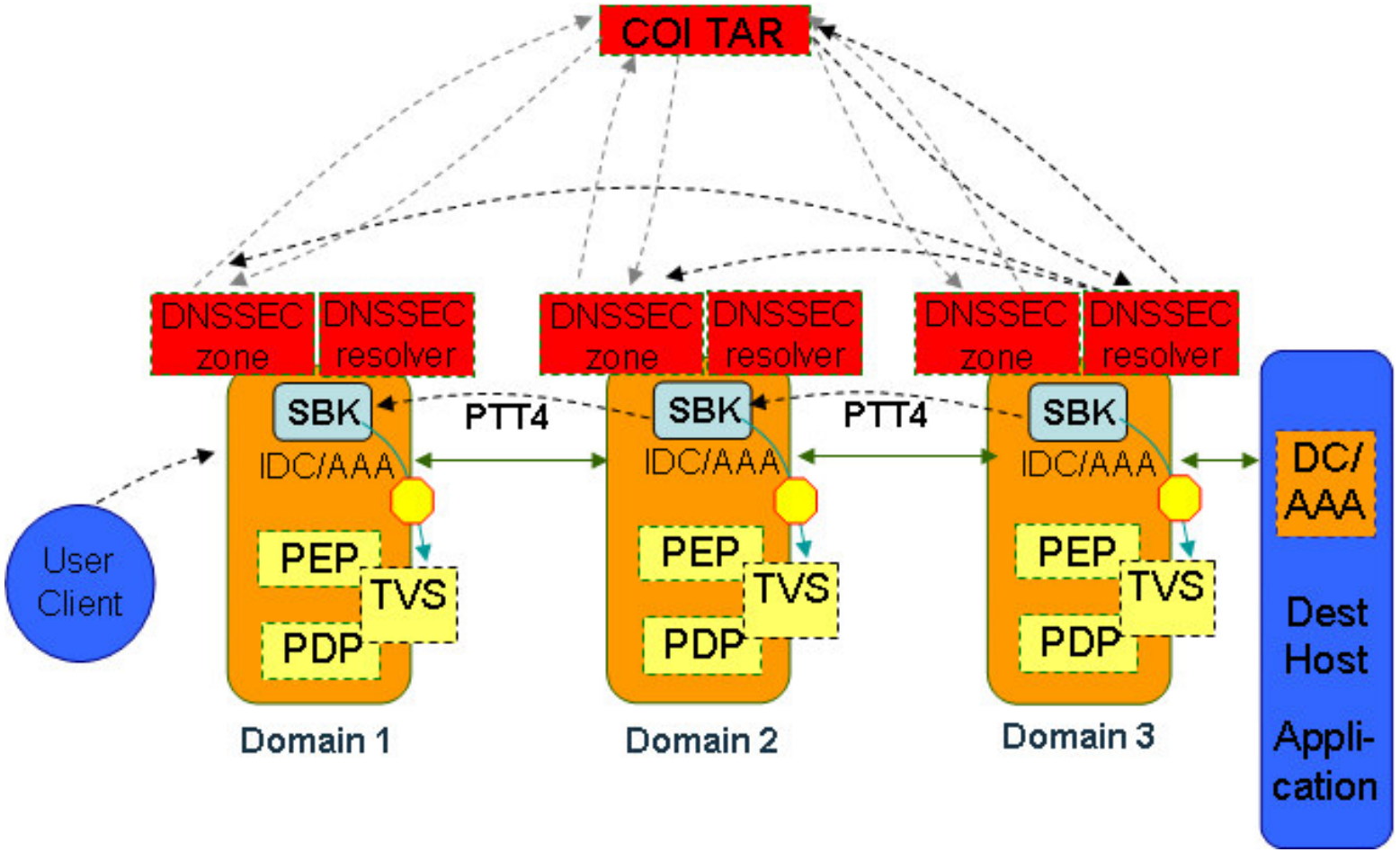
- Session Based Key (SBK) to replace tb_secret
- Moving to PKI infrastructure using DNSSEC ZSK
  - *TokenValue = SIG(SHA1(concat(DomainId, GRI, TokenId))) – PTT 2/3/4*
  - *TokenKey = HMAC(GRI, SBK) – Access Token*
- Community of Interest (COI) TAR collecting domain trust anchors (e.g. established between European partners)

- PTT4: deployment of Session Based Key (SBK) generated at destination host

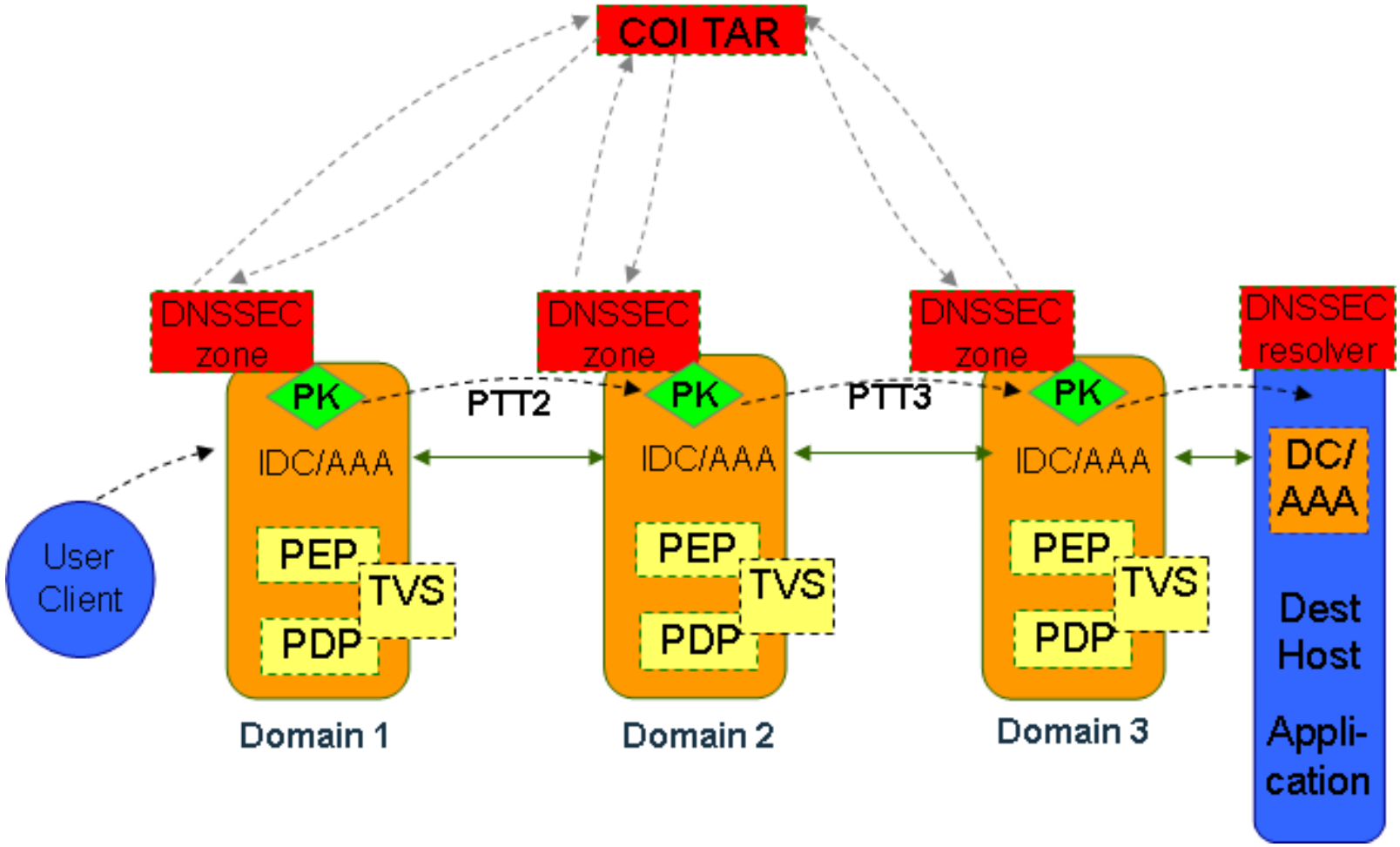
# Scenario 1: Reservation Stage



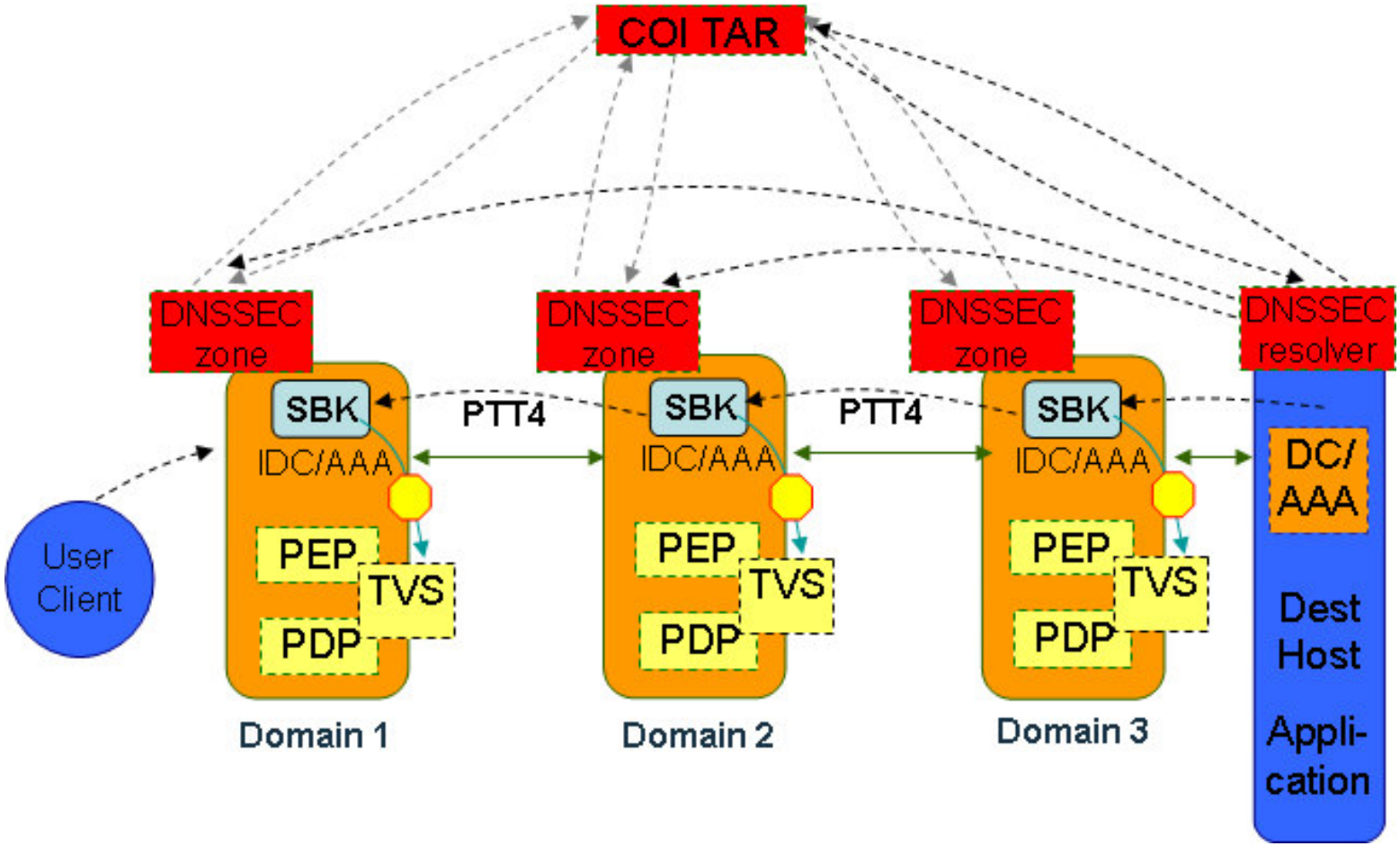
# Scenario 1: Deployment Stage



# Scenario 2: Reservation Stage



# Scenario 2: Deployment Stage



## Conclusion

- What are the differences between the original DNSSEC global trust model and the island based model with Trust Anchor Repositories?

*Governance issues, different key management, access (in-band/out-of-band), availability, partitioning of tree (weak spots).*

- What models are currently developed and what could or should be future developments?

*Community of Interest (COI) for research community.*

## Conclusion

- How can the Trust Anchor Repositories be of use in multi-domain on-demand network resource provisioning?

*Moving to PKI with deployment of encrypted SBK for use in access stage and signed pilot tokens.*

## Future Work

- Developing the communication protocol and API to allow NRP AAA system to interact with TAR



# Thank you for your attention!

# Questions?