



---

# Response Identity in Session Initiation Protocol

draft-cao-sip-response-identity-00

Feng Cao

Cullen Jennings

# Agenda

---

- ⊖ Introduction
  - ⊖ Scope
  - ⊖ Requirements
- ⊖ SIP Response Identity
  - ⊖ Overview
  - ⊖ Open Issues
- ⊖ Summary

# Introduction: Scope

---

- ⊖ Why response identity?
  - ⊖ Cannot rely on the existing header fields, such as “To:”, “Reply-to:” and “Contact:”, in all the scenarios
  - ⊖ Need response identity as early as possible
    - ♣ Provide response identity in non-dialog session
    - ♣ Provide proxy’s identity for confirming certain response codes
    - ♣ Prevent response identity spoofing as early as possible
  
- ⊖ Scope of this response identity draft
  - ⊖ Provide response identity inside response message with the security mechanism for verifying the integrity of response identity.

# Introduction: Requirement

---

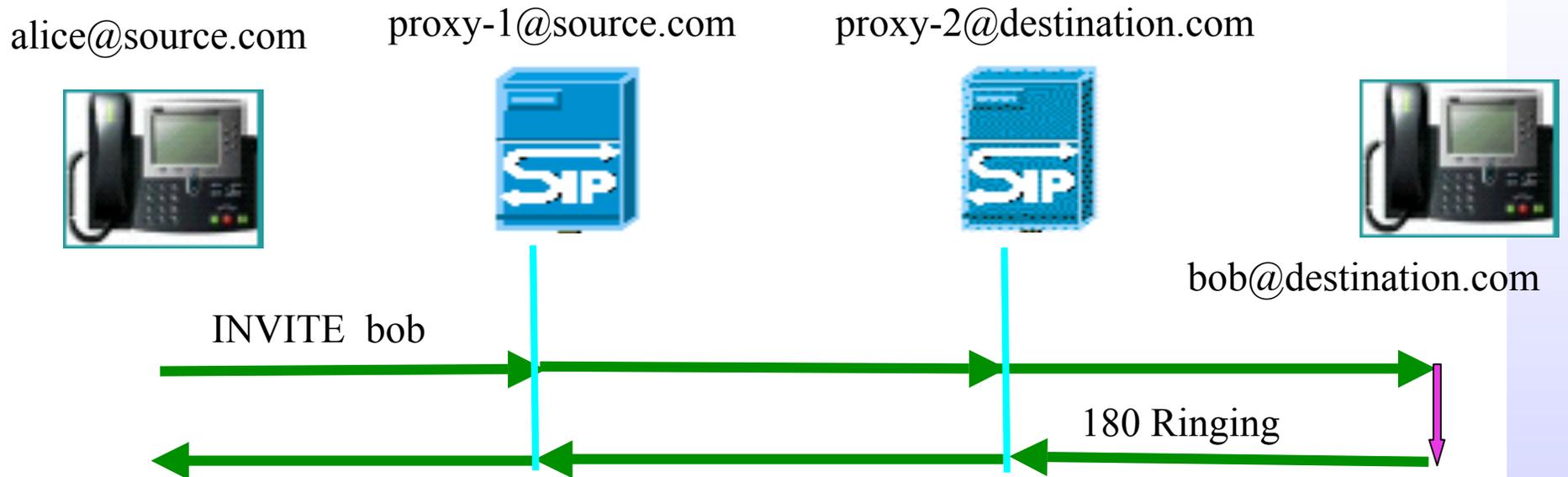
- ⊖ The mechanism must be backward compatible
- ⊖ The identity must be clearly specified in the header by the responder (or its proxy)
- ⊖ The identities of both UAs and proxies must be covered
- ⊖ The integrity of SIP response must be partially covered along with the responder's identity
- ⊖ The enforcement of providing response identity must be provided through the originator's request.
- ⊖ Open question: Anonymity of response identity?

# Enforcement of Response Identity

---

- ⊖ UAC (or its proxy) should be able to ask for response identity
  - ⊖ Required: responder-id
  - ⊖ Open question: can any intermediate proxy ask for it?
  
- ⊖ Responder (UAS or proxy) should be able to decline to disclose the response identity
  - ⊖ Warning: 380 Response Identity Cannot be Revealed
  - ⊖ Open question: the exact behavior and the consequence?

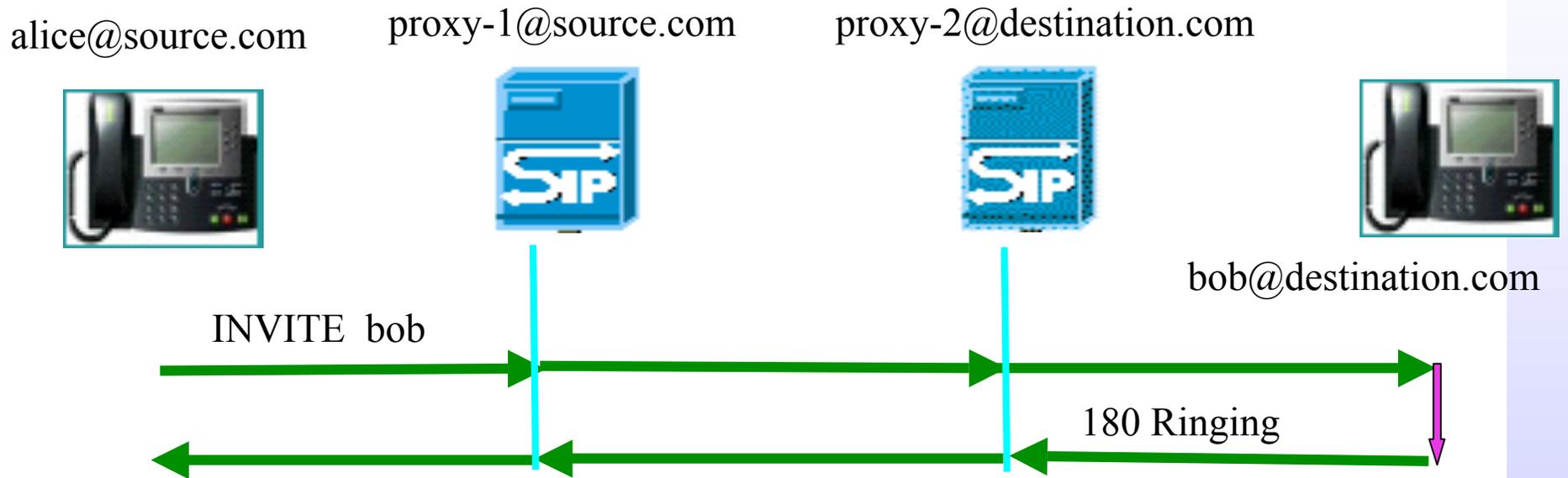
# DAS-based Approach



*Responder: claimer=bob@destination.com; verify-method=DAS;*  
*Responder-Info: https://www.destination.com/certs; algo=rsa-sha1*  
*Identify: akfjiqiowrgnavnvnnfa2o3fafanfjkfjakfjalkf203urjafskjfaf*  
*Jprqiyupirequqpiruskfka*

**Note:** *Domain-based Authentication Service (DAS)*

# AIB-based Approach



*Responder: claimer=bob@destination.com;*  
*verify-method=AIB;*

*Responder-Info: https://www.destination.com/certs; algo=rsa-sha1*

# Open Questions

---

- θ Is AIB needed?
  - ⊖ Advantage: Anonymity can be achieved
  - ⊖ Disadvantage:
    - ♣ Complexity and processing delay
    - ♣ end-to-middle security
  
- θ the new response code?
  - ⊖ 403 'Failed Responder Identity'
  
- θ The behavior and consequence for dealing with the enforcement?
  - ⊖ Warning: 380 Response Identity Cannot be Revealed

# Summary

---

- ⊖ Scope and requirement for response identity
- ⊖ Some solutions are provided
- ⊖ Open questions
- ⊖ Next Step?