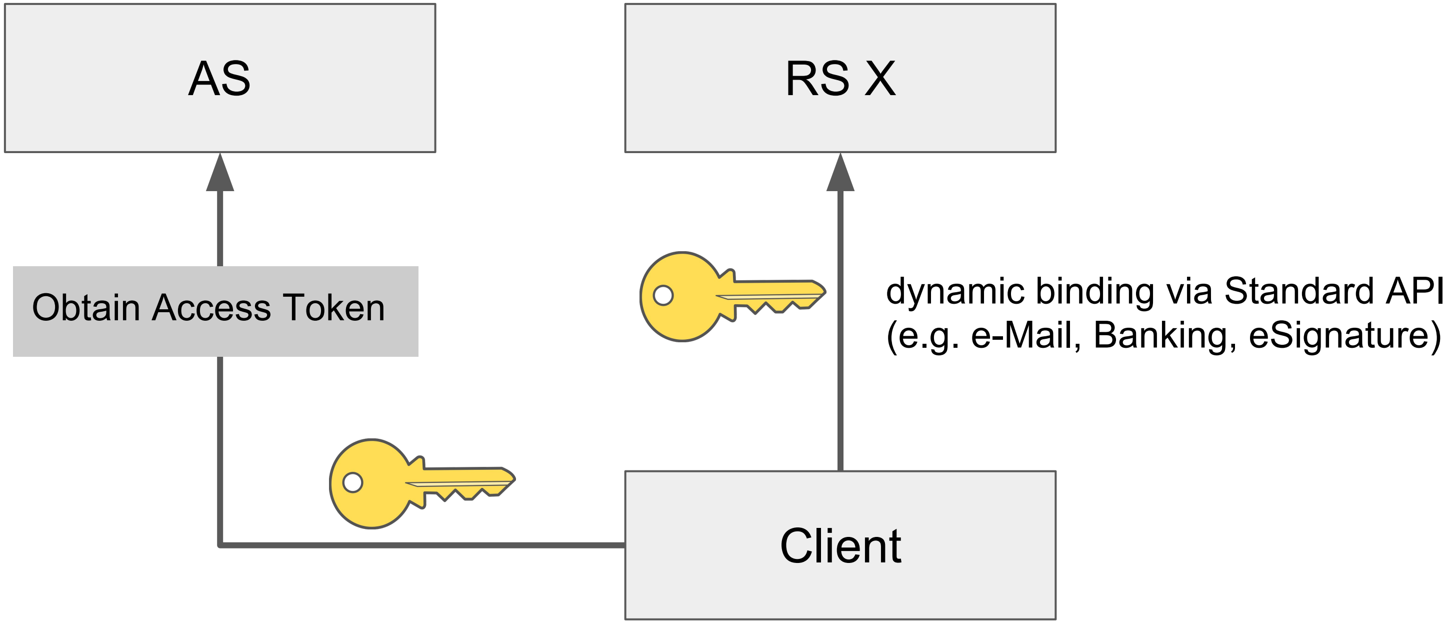
Access token phishing

John Bradley, Torsten Lodderstedt

OAuth Security Workshop
July 13&14 2017, ETH Zurich

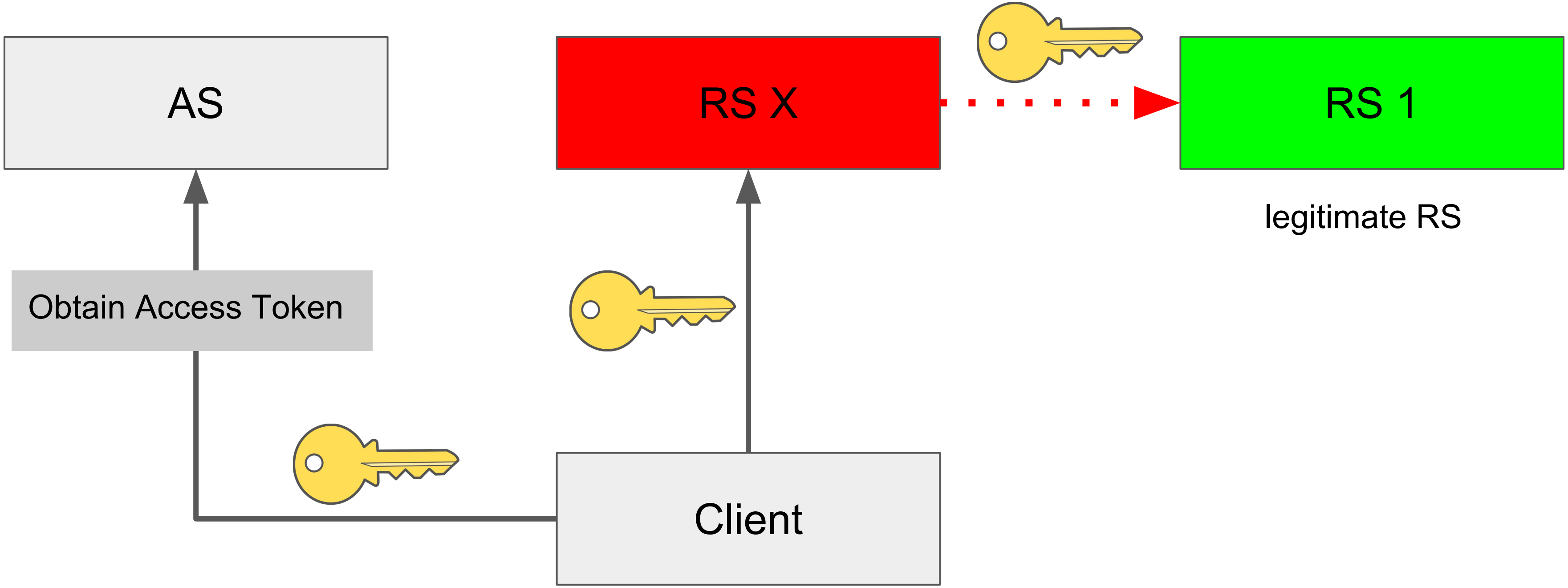
What’s the setup?



dynamic binding via Standard API
(e.g. e-Mail, Banking, eSignature)

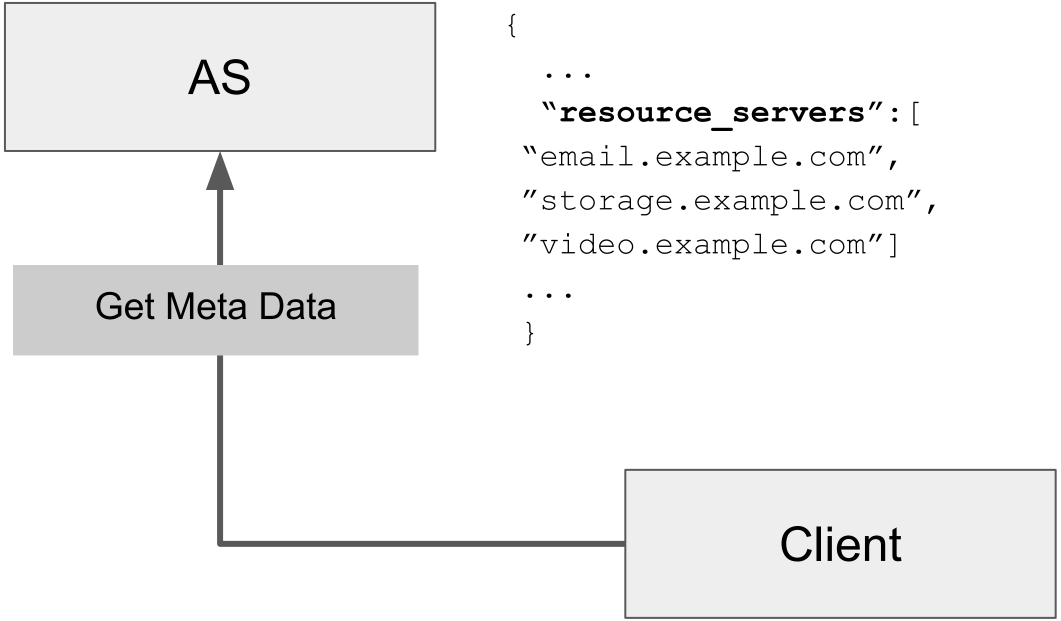
What if ...

… RS X is a bad guy?



What can we do?

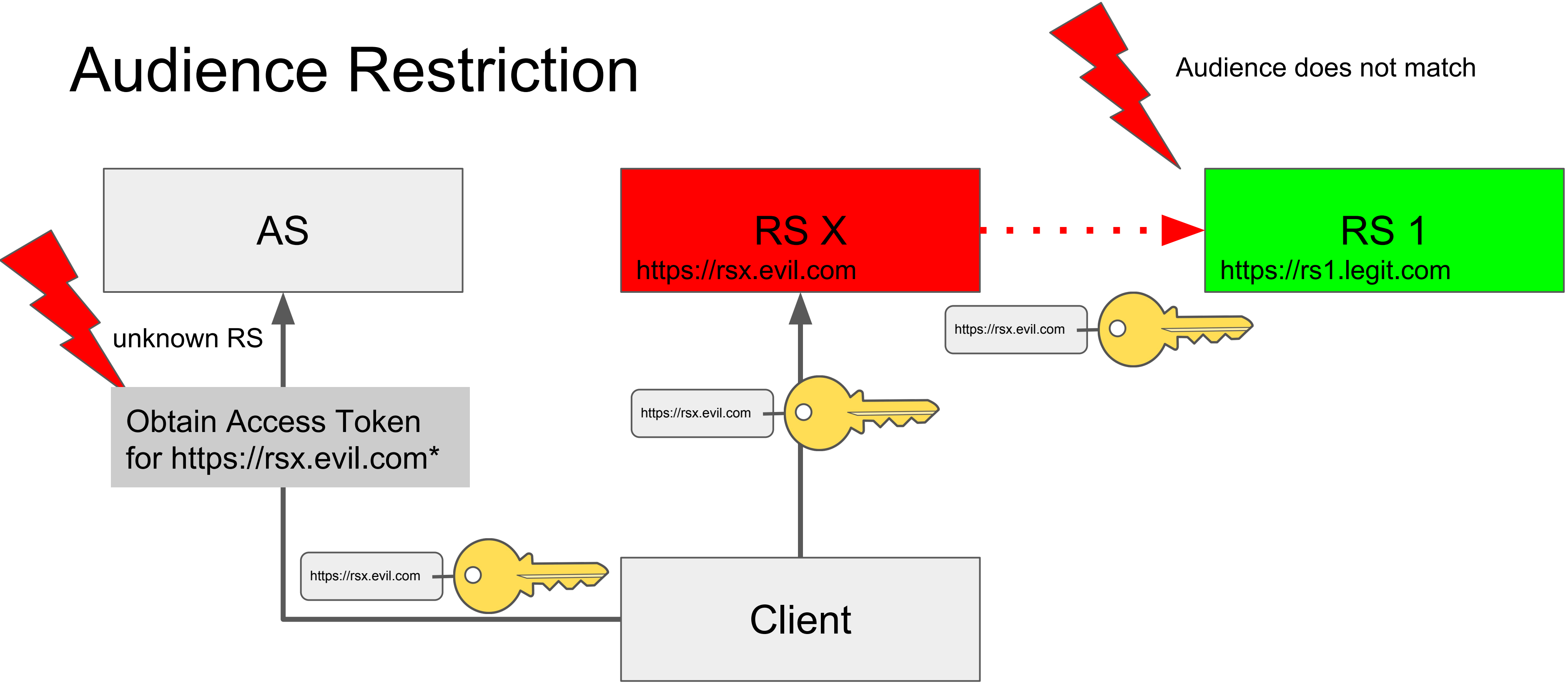
What if the client would know upfront which places it is safe to send access tokens to?



```
{
   ...
   “resource_servers”:[
 “email.example.com”,
 ”storage.example.com”,
 ”video.example.com”]
 ...
 }
```

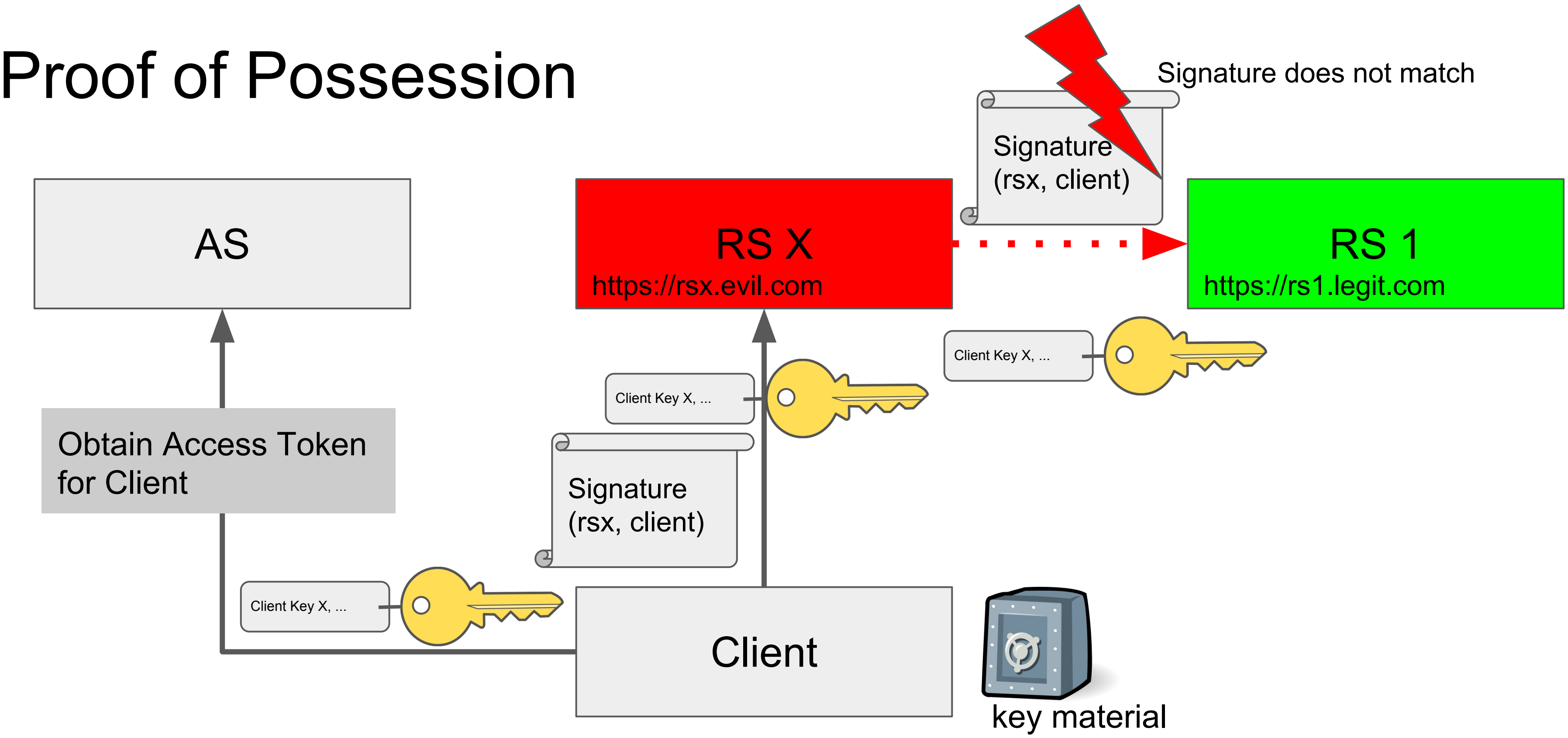
puts the burden of security checks to clients

Audience Restriction



* e.g. using https://tools.ietf.org/html/draft-campbell-oauth-resource-indicators

Proof of Possession



Signature does not match

AS

RS X

https://rsx.evil.com

RS 1

https://rs1.legit.com

Signature (rsx, client)

Client Key X, ...

Obtain Access Token for Client

Client Key X, ...

Signature (rsx, client)

Client Key X, ...

Client

key material

Proof Posession (Existing Proposals)

- Transport
  - Token Binding - draft-ietf-oauth-token-binding
  - MTLS - draft-ietf-oauth-mtls
- Application
  - Signed Request - draft-ietf-oauth-signed-http-request
  - J-POP - draft-sakimura-oauth-jpop

What do you think?