Access control delegation for the Cloud

Nikos Fotiou, Apostolis Machas, George C. Polyzos, George Xylomenos

Mobile Multimedia Laboratory,
Athens University of Economics and Business

Why do enterprises fear the cloud?

pwc

“Uncertain ability to enforce provider security policies”

“[Lack of] effective models for managing and enforcing data access policies”

enisa

European Network and Information Security Agency

CSA cloud security alliance®

Interoperability requires complex APIs which increases chances of a security breach due to implementation errors

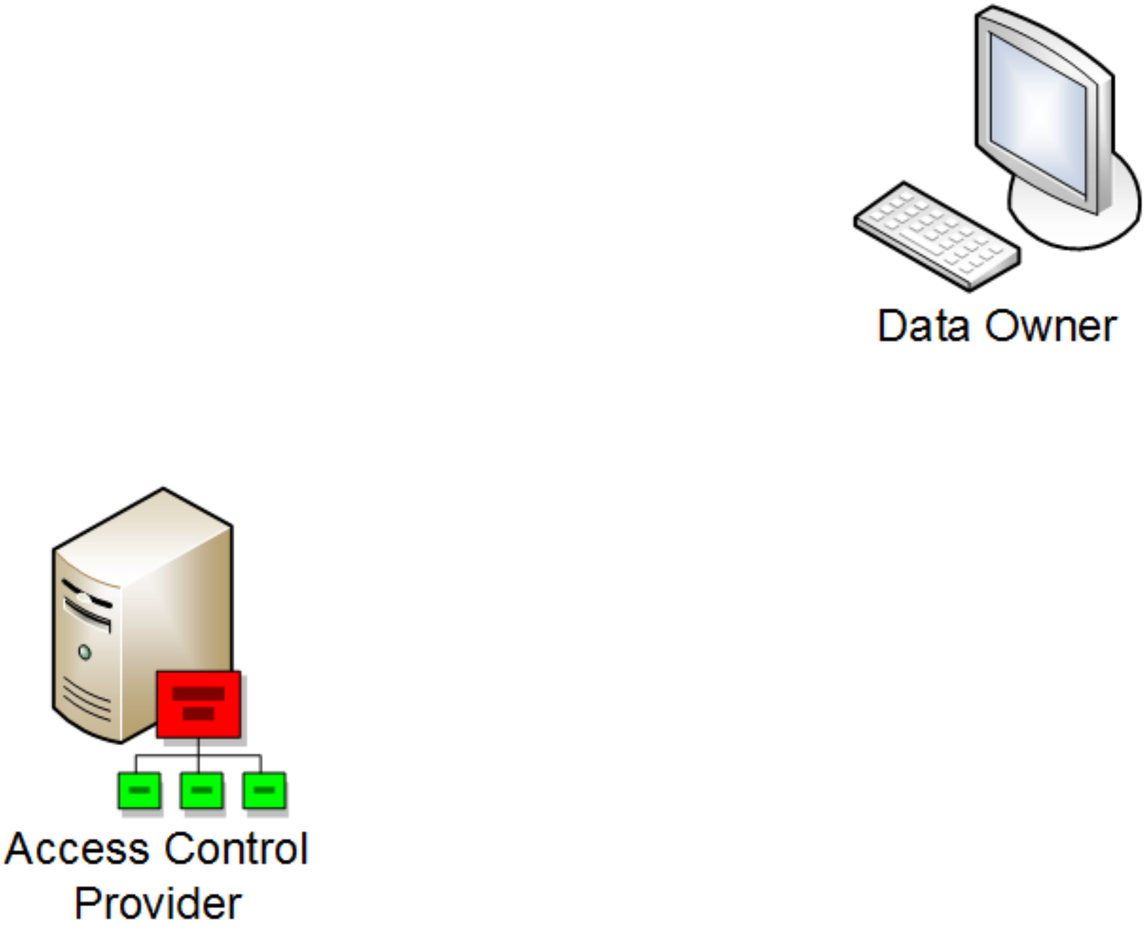
We need a solution that…

- Performs access control on outsourced data
- Requires minimum trust to cloud providers
- Protects user credentials
- Is easy to implement
- Enables migration to other cloud providers
- Provides privacy and prevents monitoring

A new approach

- Separate data storage from data access authorization
  - Cloud providers are concerned with data storage
  - Data access authorization performed by a trusted (not always third) party: the Access Control Provider

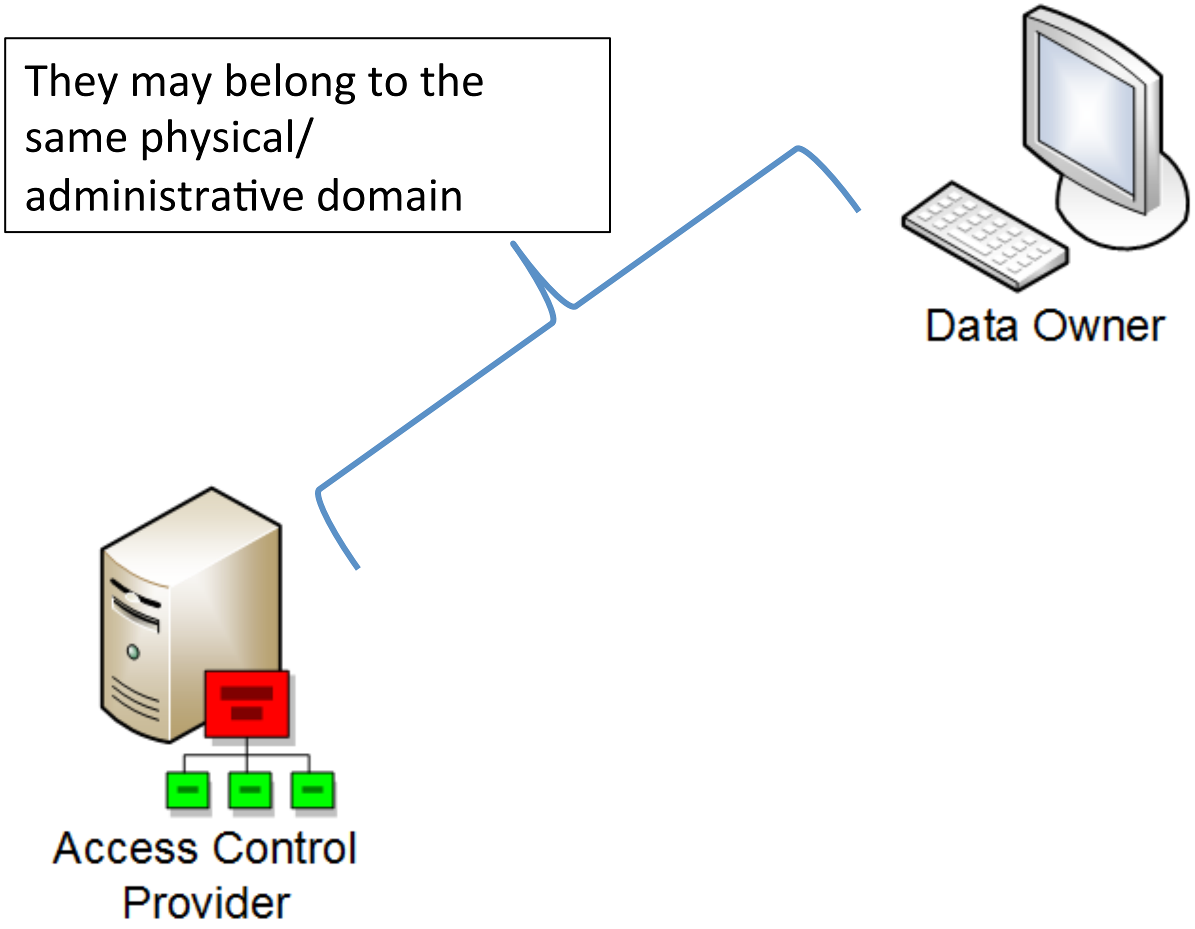
Scheme Overview



Data Owner

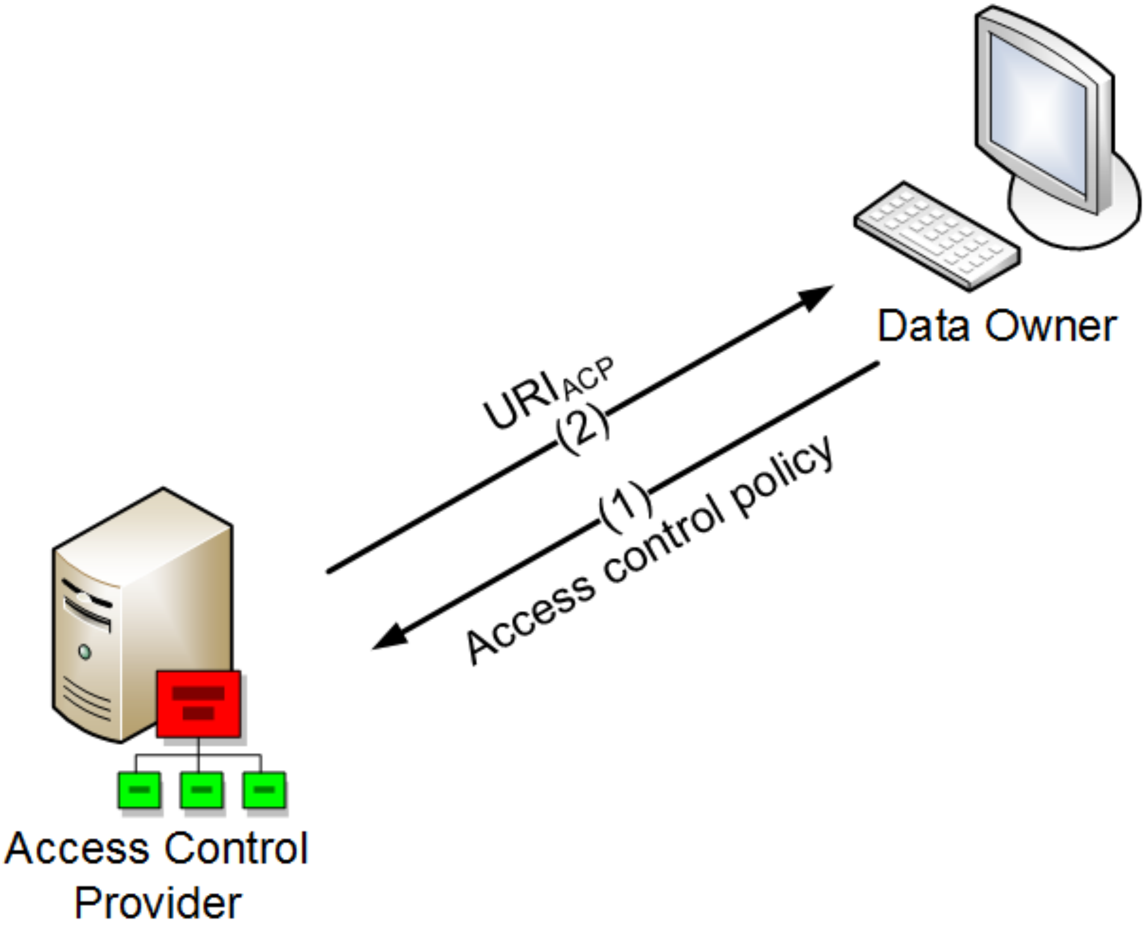
Access Control Provider

Scheme Overview

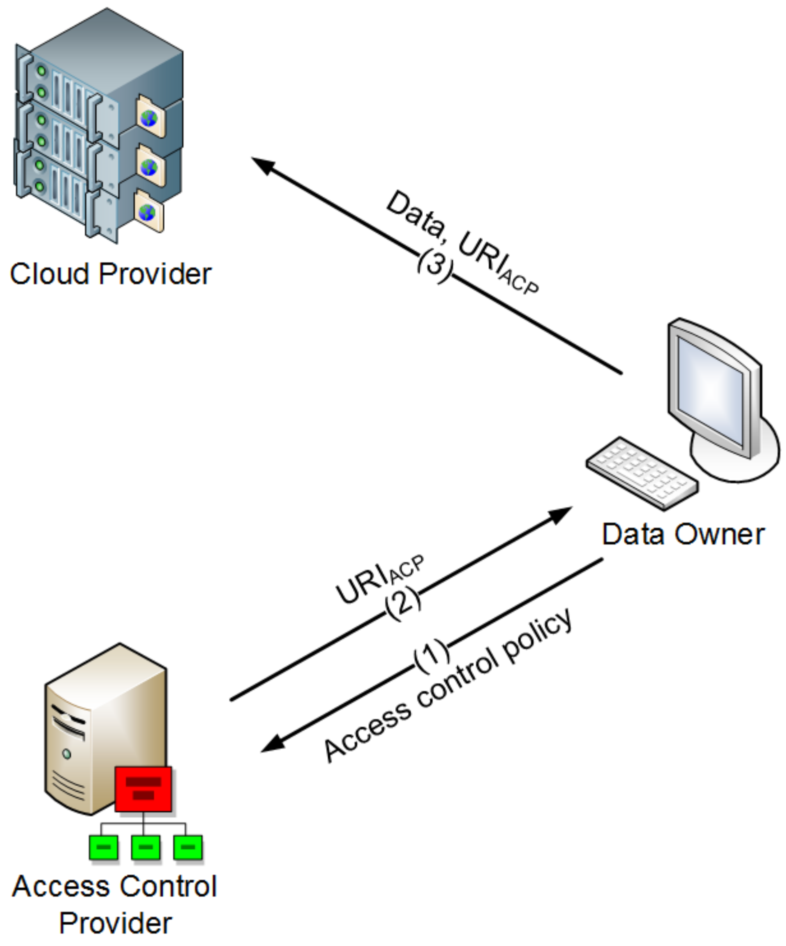


They may belong to the same physical/ administrative domain

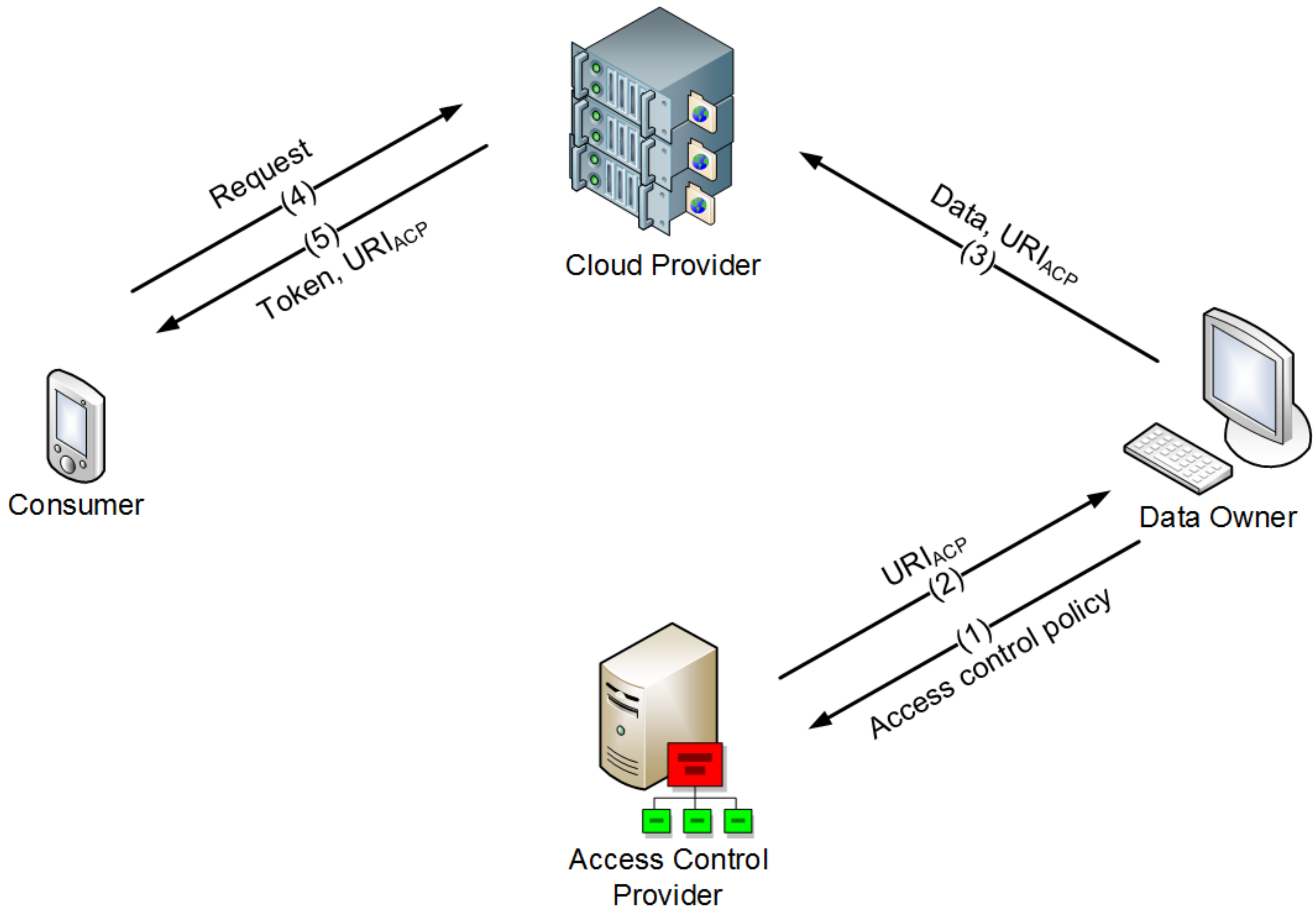
Scheme Overview



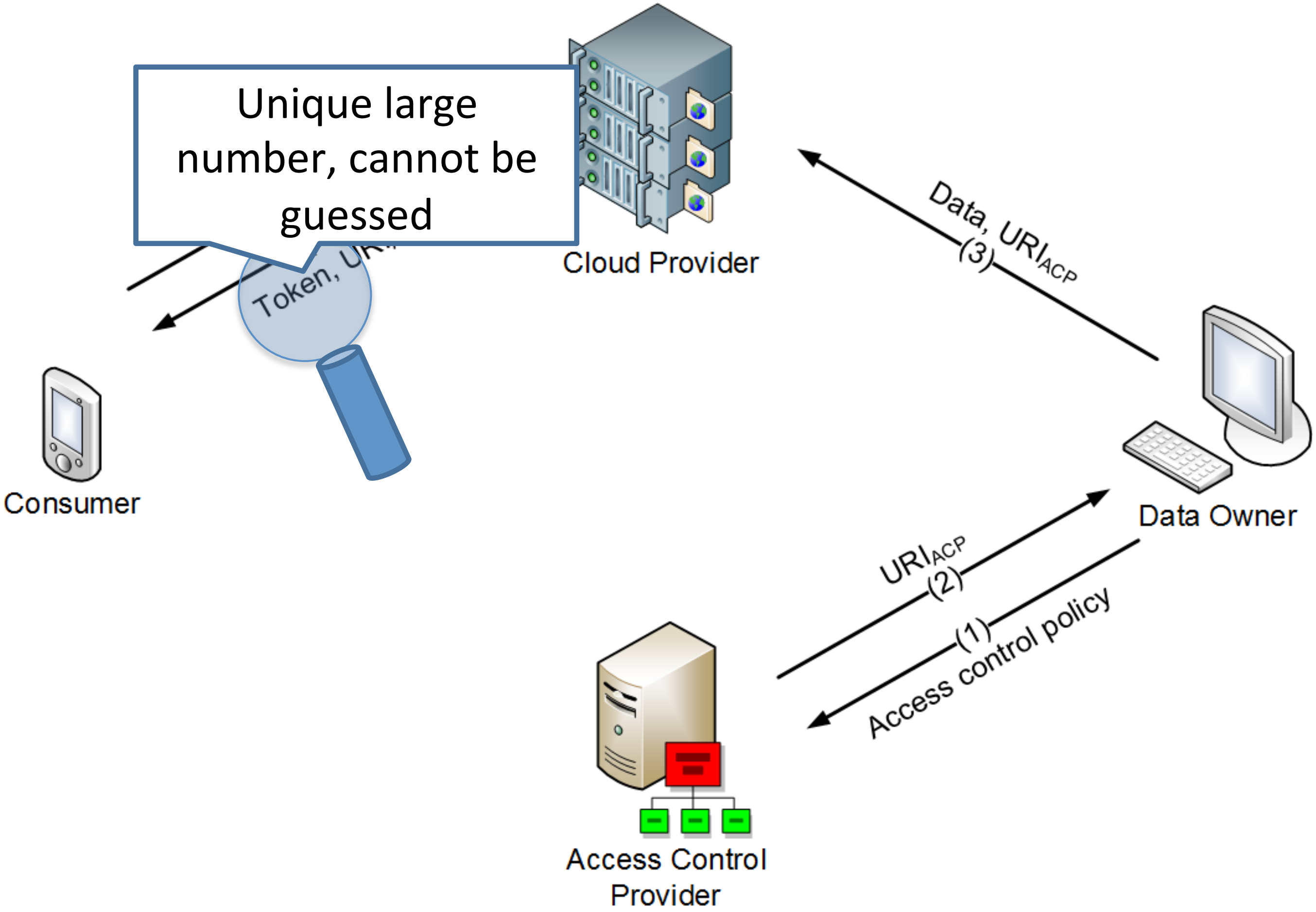
Scheme Overview



Scheme Overview

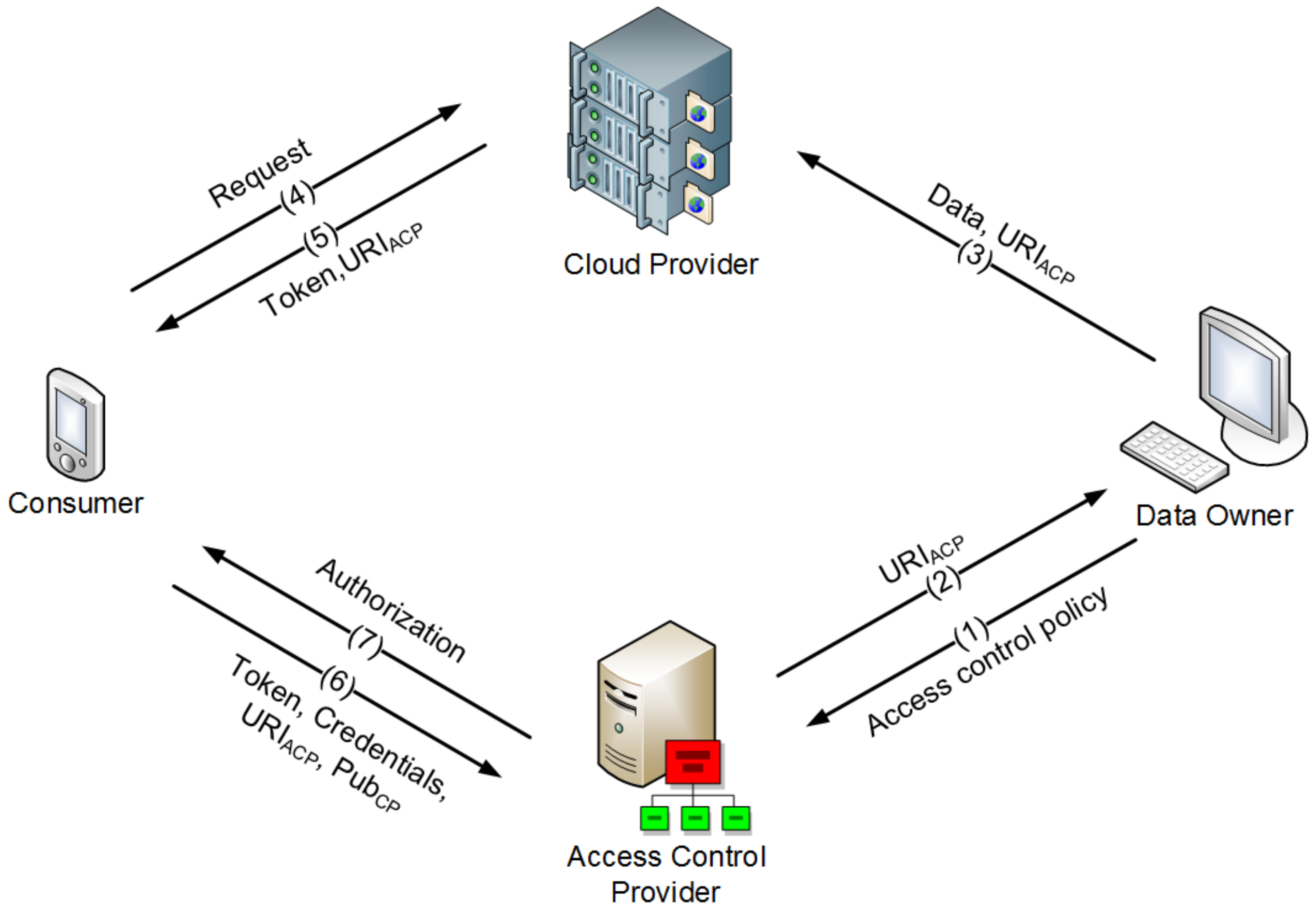


Scheme Overview

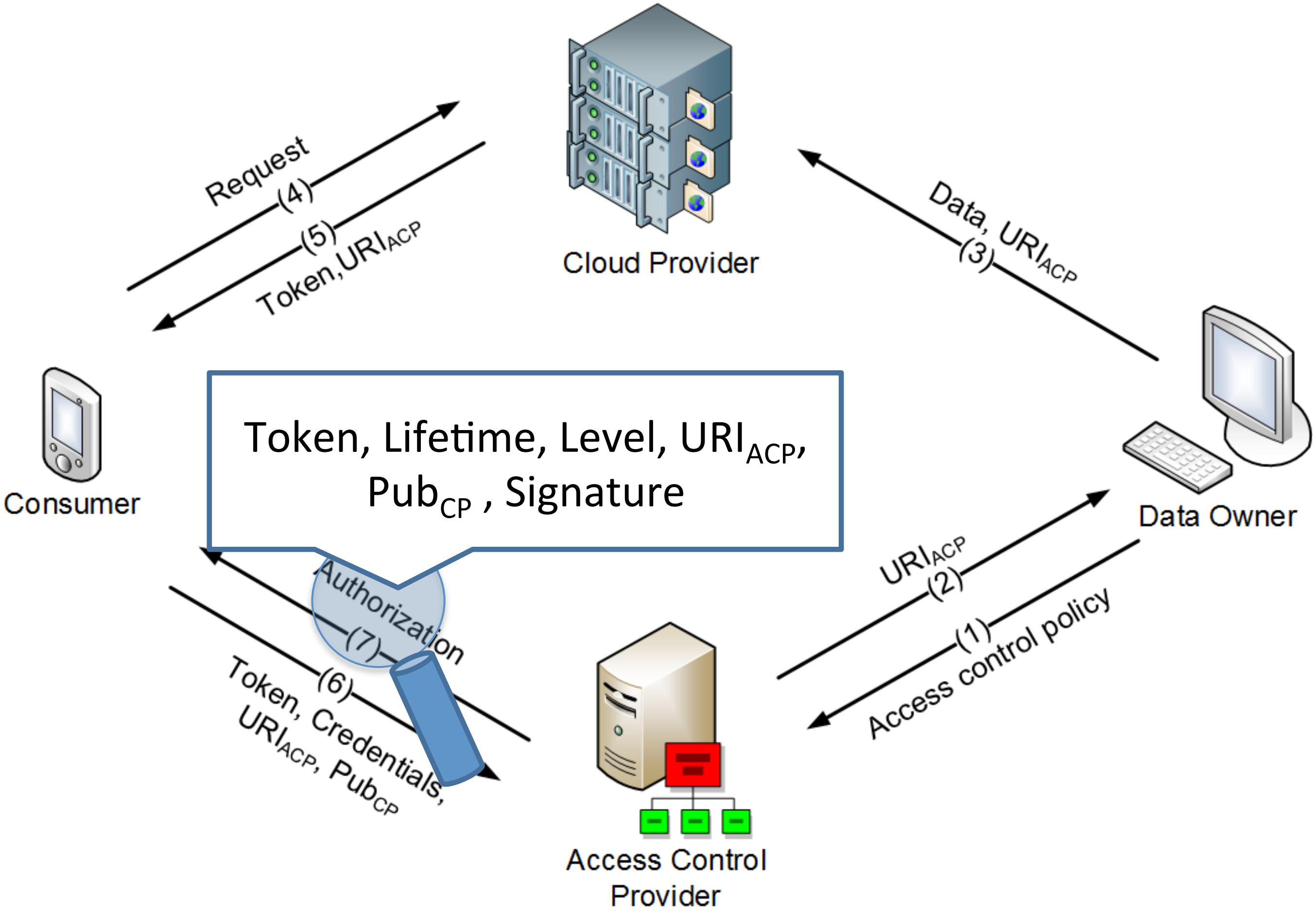


Unique large number, cannot be guessed

Scheme Overview

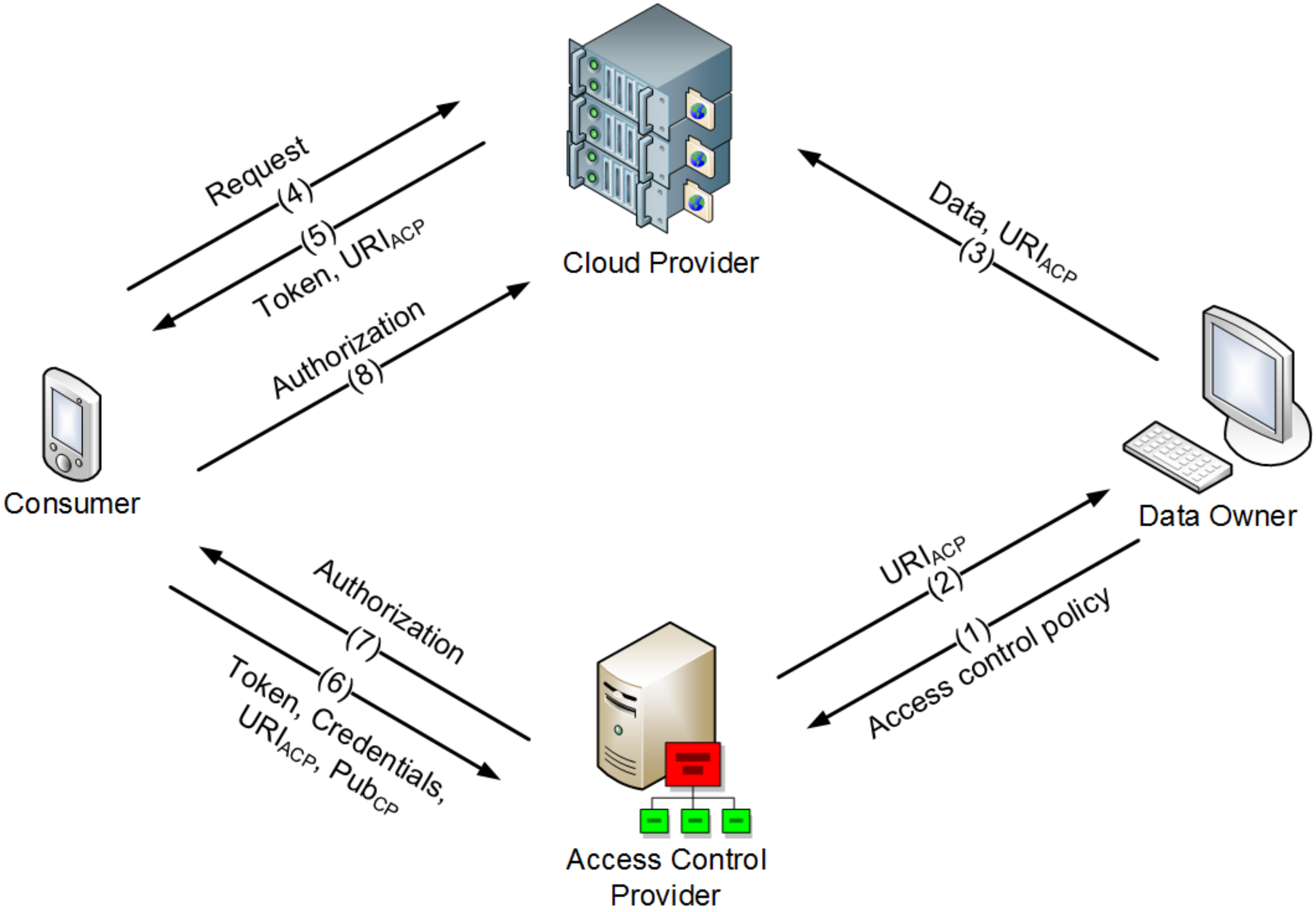


Scheme Overview



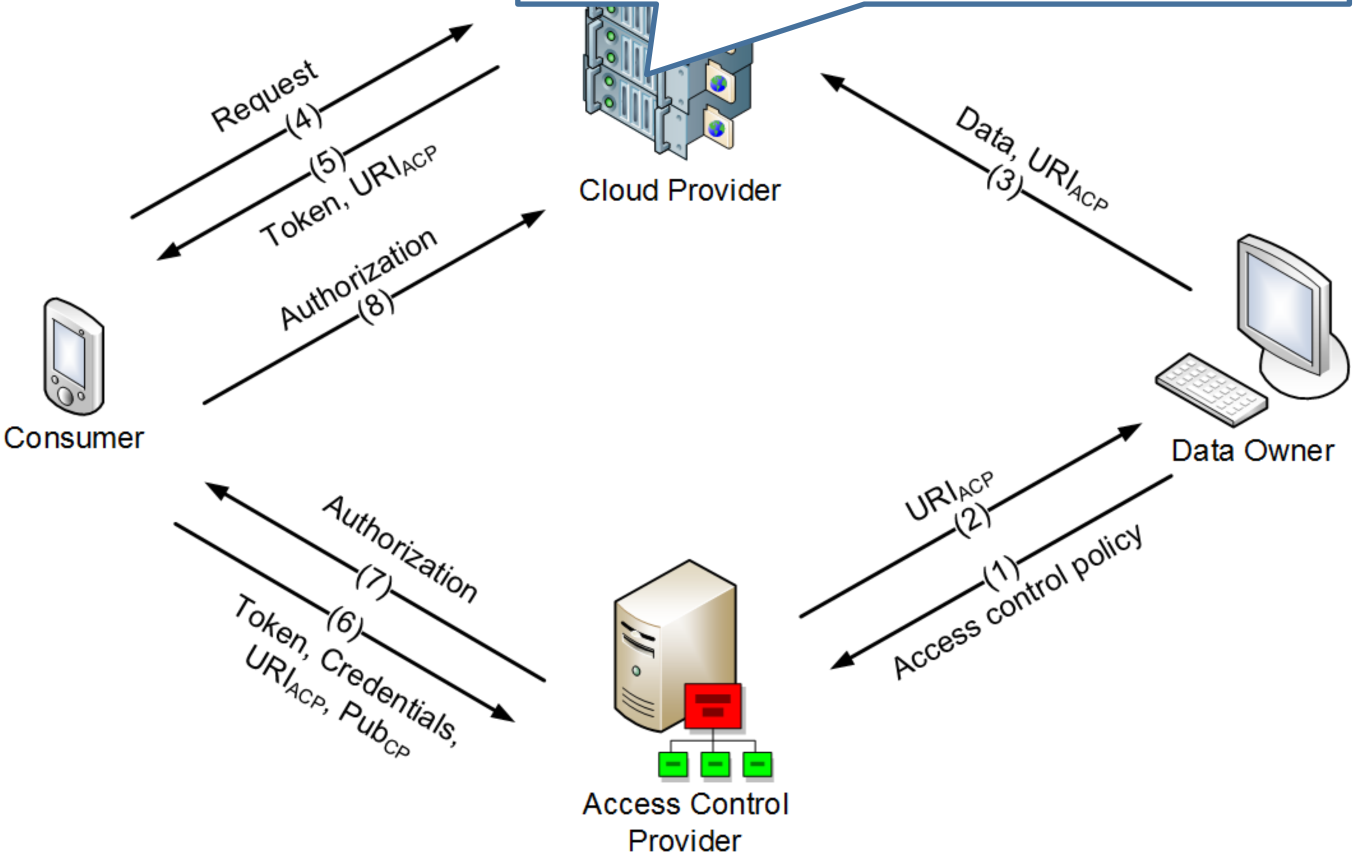
Token, Lifetime, Level, $\mathrm{URI}_{\mathrm{ACP}}$, $\mathrm{Pub}_{\mathrm{CP}}$, Signature

Scheme Overview

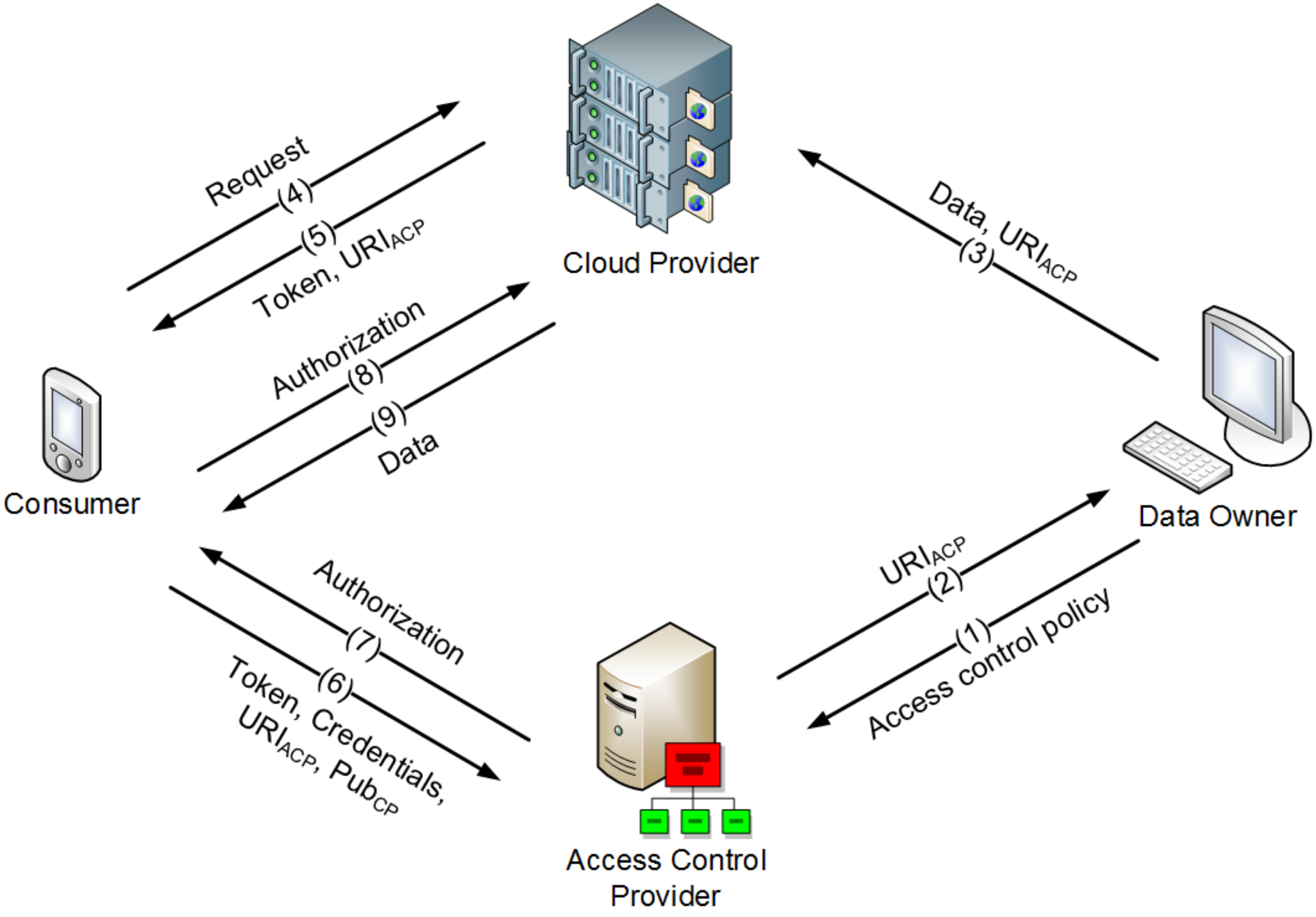


Schen

- Verify signature
- Check if URI_{ACP}, Pub_{CP} are correct
- Check lifetime
- Check level



Scheme Overview



Revisiting our requirements

- ✓ Performs access control on outsourced data
- ✓ Requires minimum trust on cloud providers
  - The cloud provider is only trusted to respect the decision of the ACP
  - Relaxed form of existing trust relationships
- ✓ Protects user credentials
- ✓ Easy to implement, allows migration
  - Data can be copied-pasted
- ✓ Provides privacy
  - The cloud provider learns nothing about users

…And some additional benefits

- Policies are reusable
  - The Content Provider does not know how policies work (useful for e.g. for B2B applications)
- Policies can be modified without the involvement of the cloud providers
- ACPs create the potentials of a new market

Why not OpenID or OAuth?

- OpenID
  - Identity Provider checks user credentials
  - But the Cloud Provider checks the policy
  - The Cloud Provider knows who the user is
- Oauth
  - Identity Manager verifies user attributes
  - But the Cloud Provider checks policy attributes
  - The Cloud Provider knows the user attributes

Attacks deflected

- Attack scenarios by Wang et al., SSP 2012
- Switching policy from legal A to illegal B
  - The ACP includes the policy in the signature
- Cloud provider B seeing data in provider A
  - The ACP includes B's key in the signature
- Pretending to be another user of the system
  - The CP knows who asked for each token
  - This worked on facebook and twitter…

Implementation

- On top of Swift (object storage system)
  - Component in Swift pipeline
  - Uses HTTPS for communication

Middleware for

Google Drive

amazon web services™ | S3

Thank you

xgeorge@aueb.gr