An introduction to the Azure AppFabric

WebDay, Porto, Feb. 2, 2010

Pedro Félix

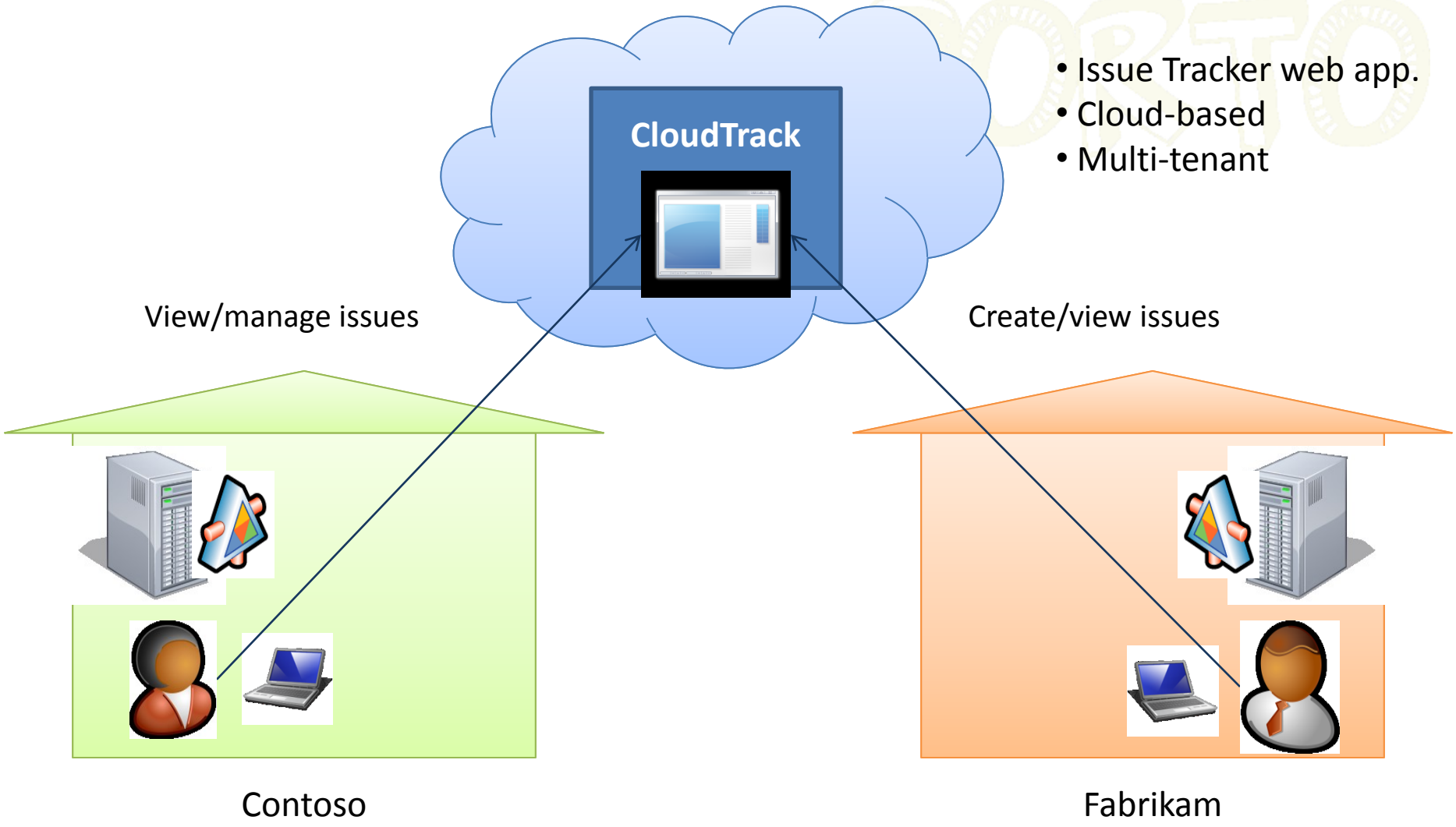
(**pedrofelix** *em* **cc.isel**.ipl.pt)

webday 2010

Azure AppFabric

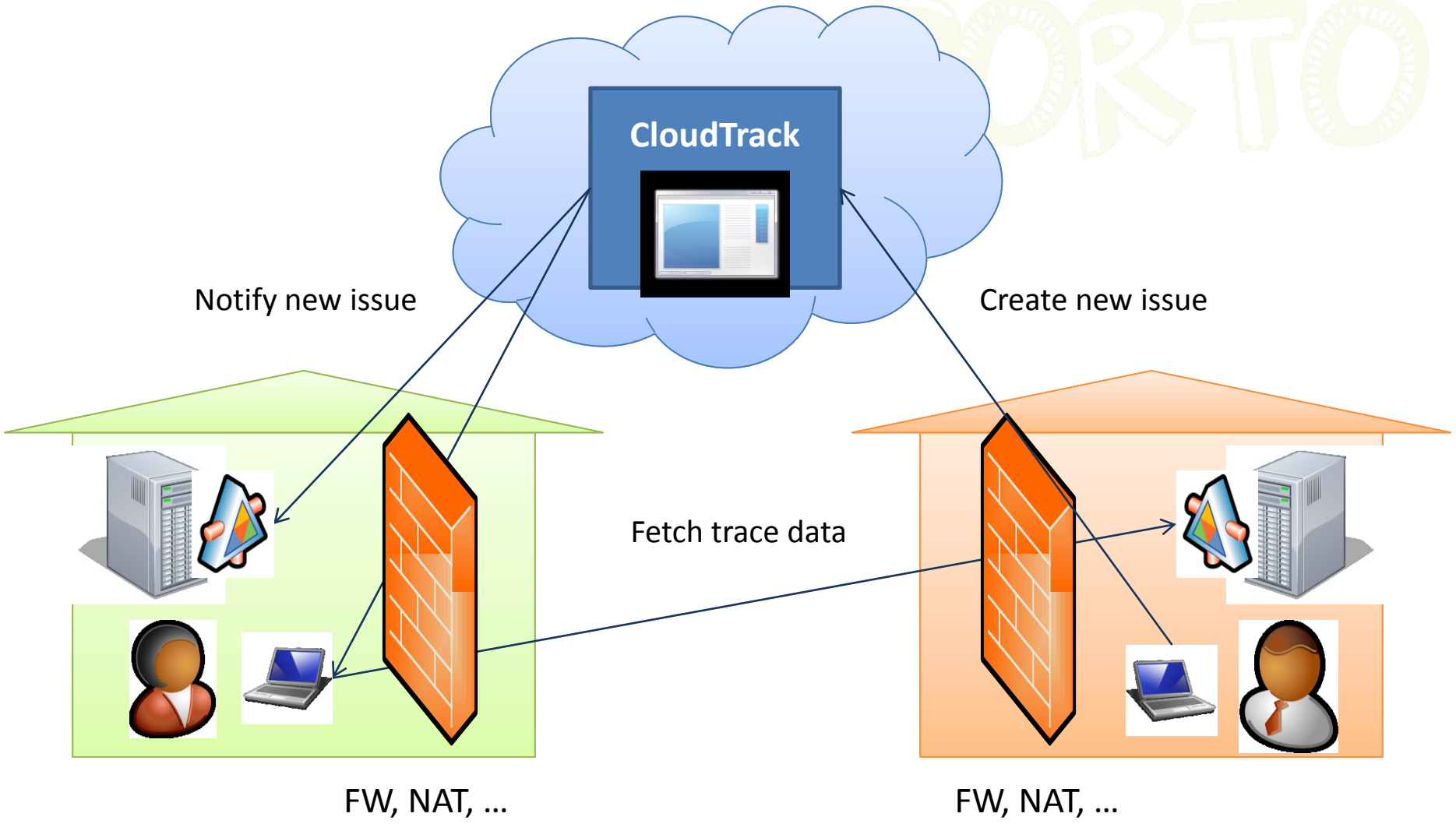
- Set of services
  - Service Bus (SB)
  - Access Control Service (ACS)
- Running in the cloud
  - Based on Windows Azure Platform
- Providing
  - SB : Service Connectivity, Addressability and Discoverability
  - ACS : Service Access Control

A Motivating Scenario



- Issue Tracker web app.
- Cloud-based
- Multi-tenant

Connectivity challenges

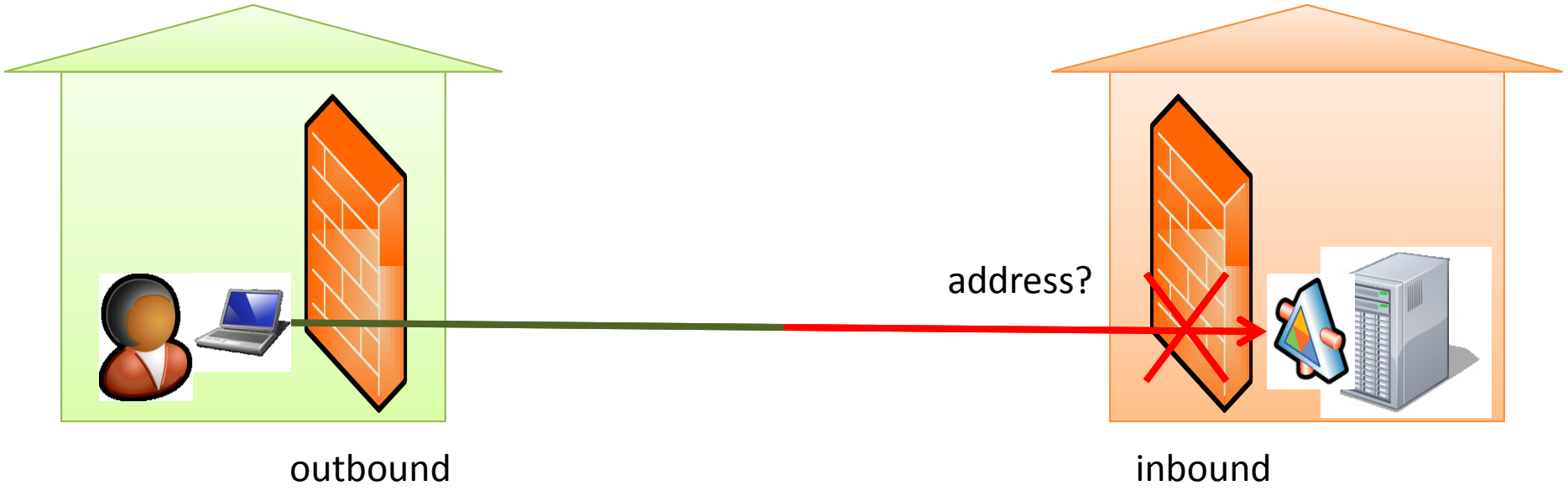


Challenges

- Addressability and discoverability
  - Private addresses and Network Address Translation (NAT)
  - Dynamic addresses (e.g. ISP)

- Connectivity
  - Firewalls (denial of inbound connections)
  - Event distribution
  - Transient connectivity

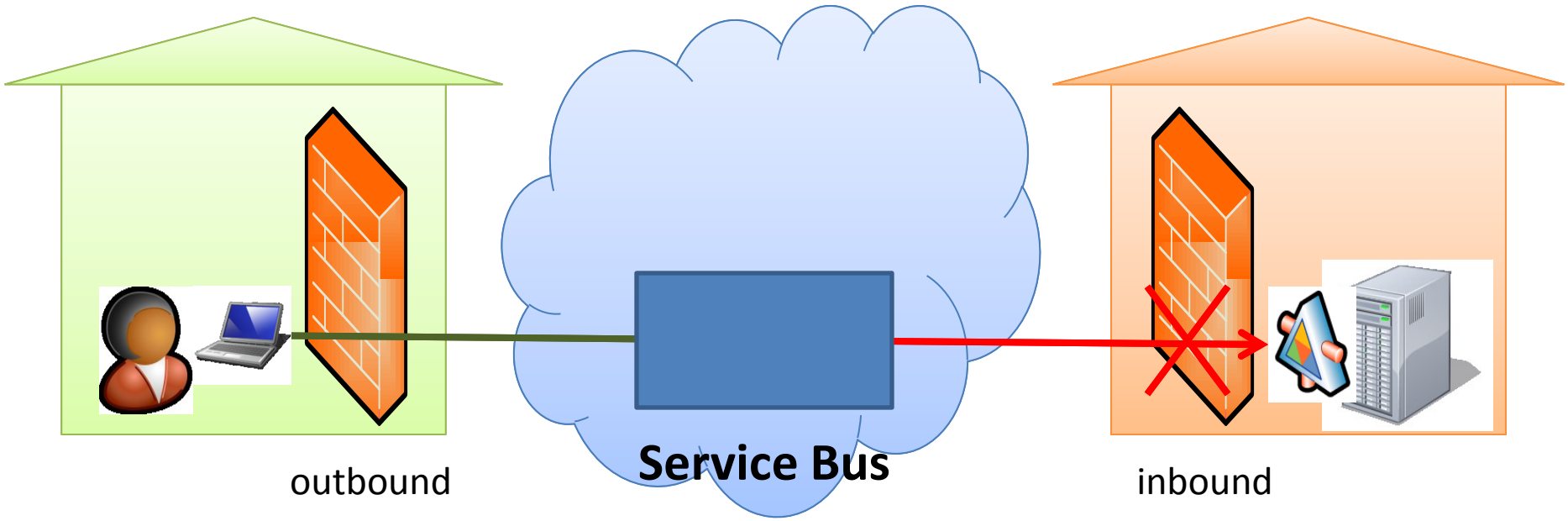
Service Bus



Service Bus

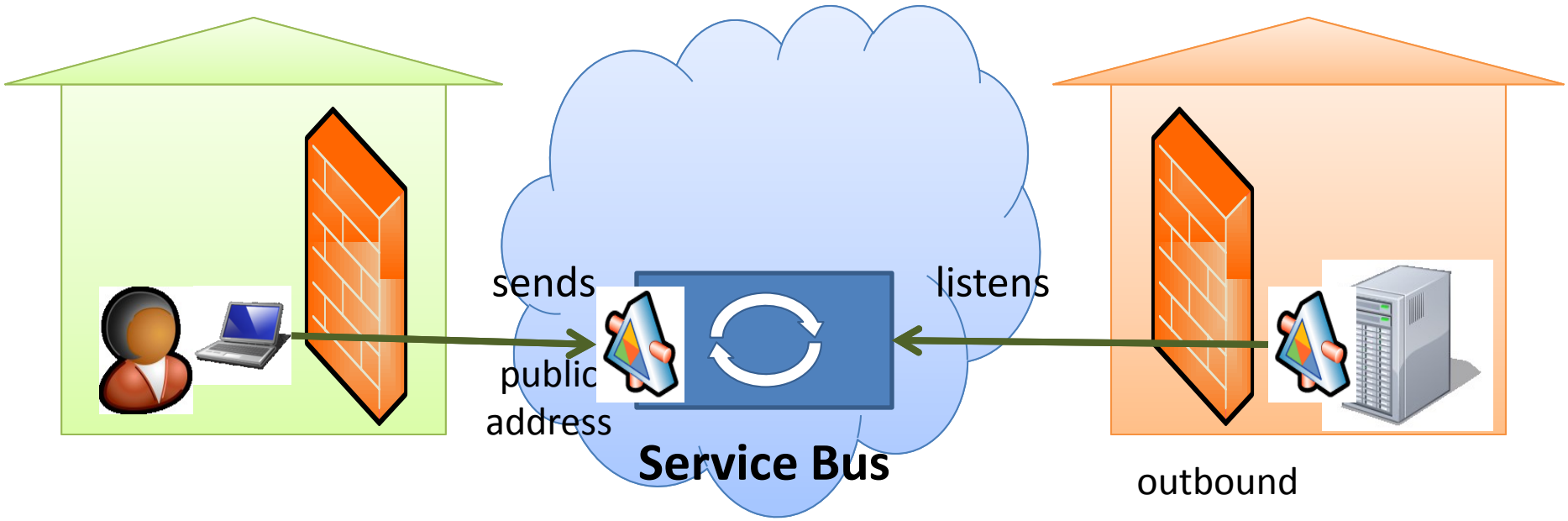
"All problems in computer science can be solved by another level of indirection"

Butler Lampson



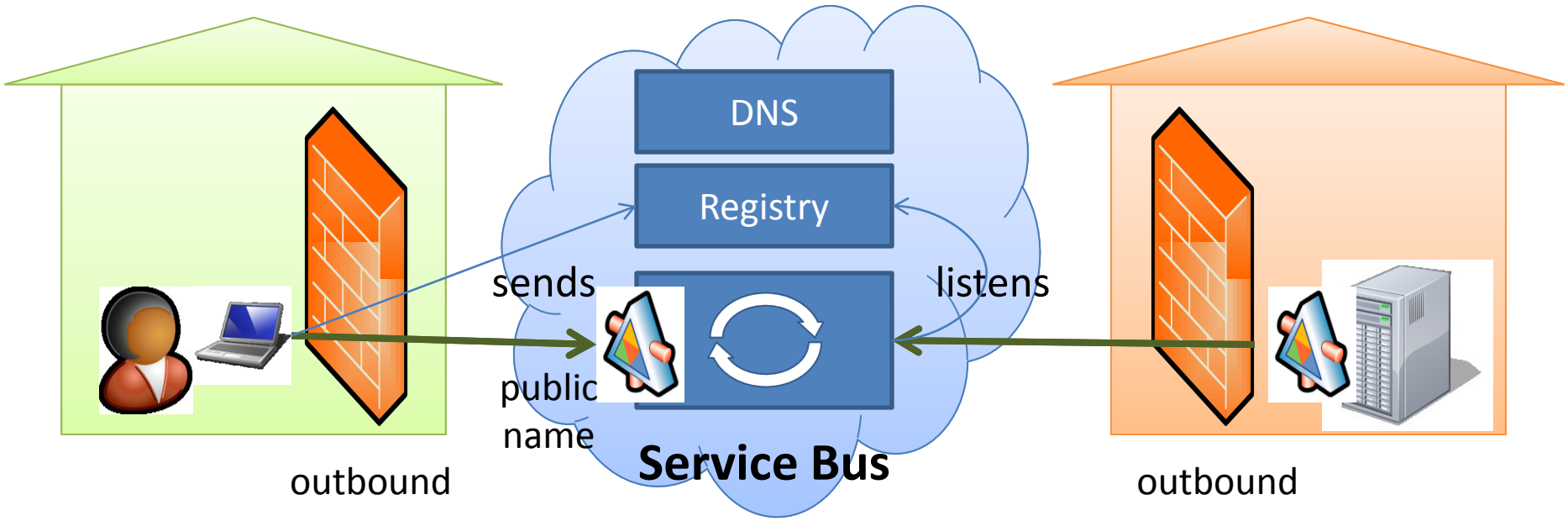
Connectivity and addressability

- Relay
  - Service "listens" on the SB via outbound connection
  - Client "sends" to the SB
  - SB relays between client and service



Naming and discovery

- Naming
  - Service is exposed via a public name
  - Local DNS binds these public names to IP addresses
  - Local registry describes available public names

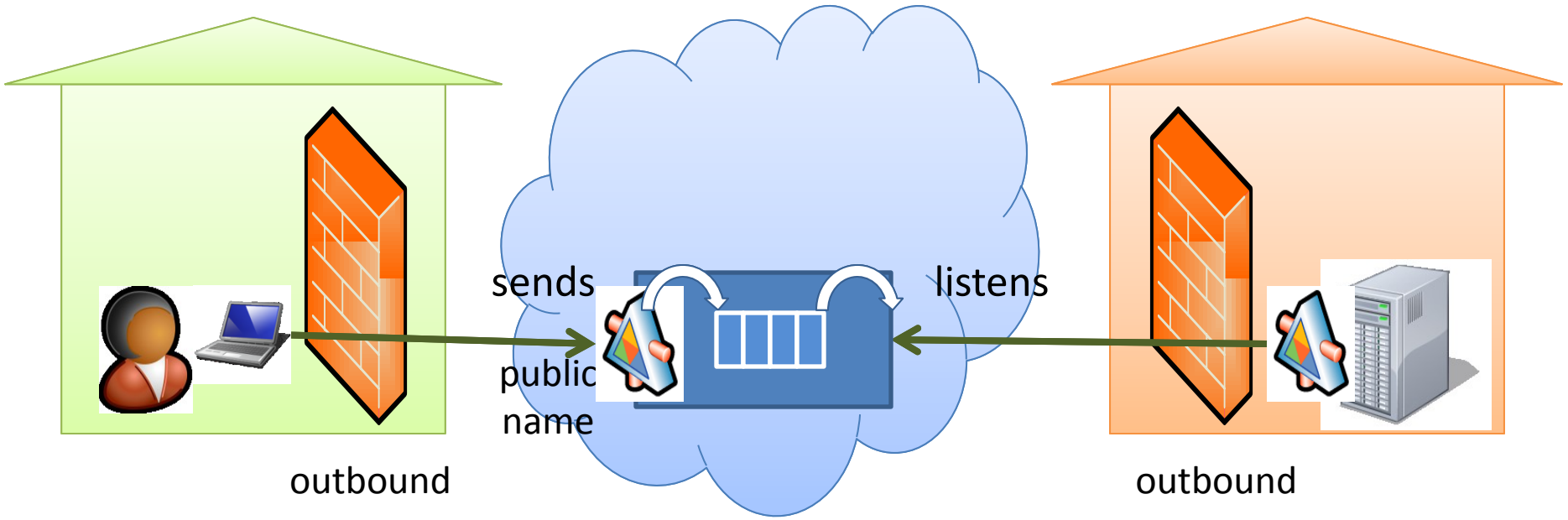


Naming and discovery

- Naming
  - Public service namespaces
  - One Azure project – multiple service namespaces
  - **{scheme}**://**{namespace}**.servicebus.windows.net/**{relpath}**
- Registry
  - Mapping between URIs and services
  - Readable via HTTP+ATOM

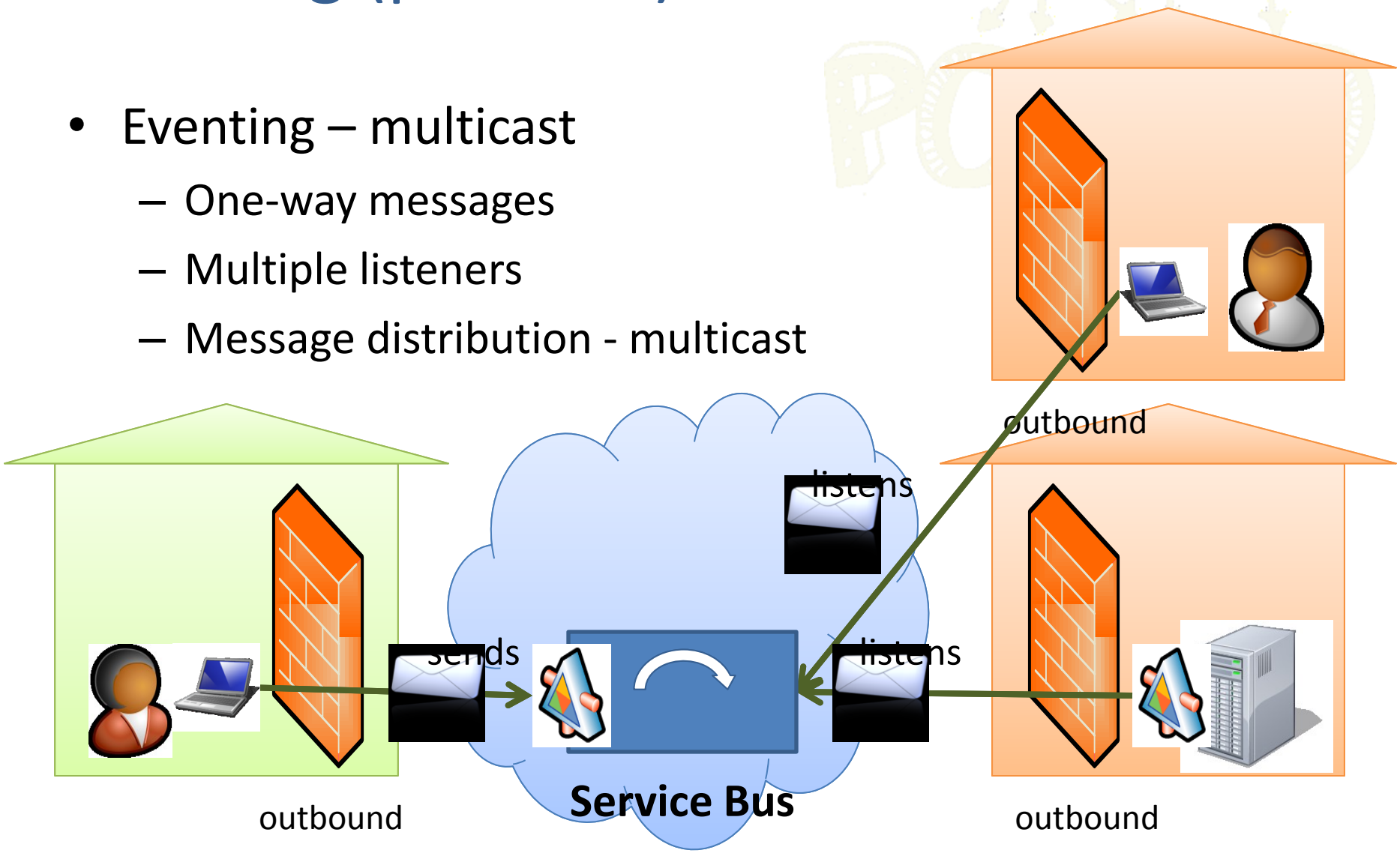
Buffering

- Buffering
  - One-way messaging
  - Temporal decoupling



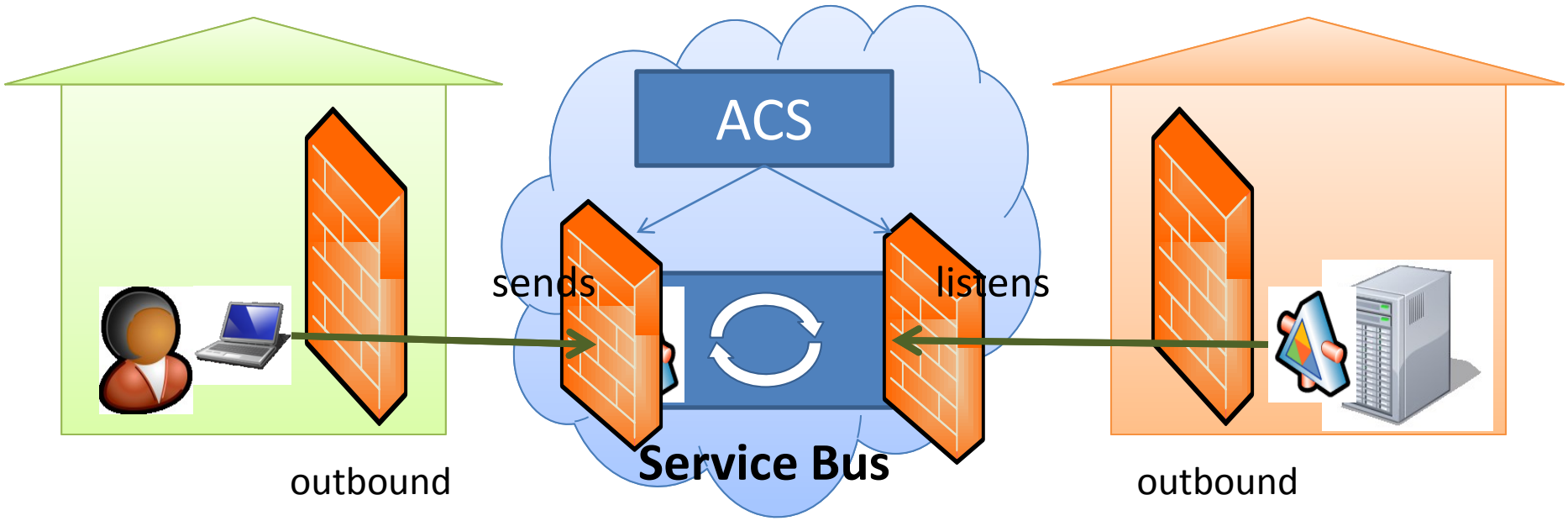
Eventing (pub-sub)

- Eventing – multicast
  - One-way messages
  - Multiple listeners
  - Message distribution - multicast



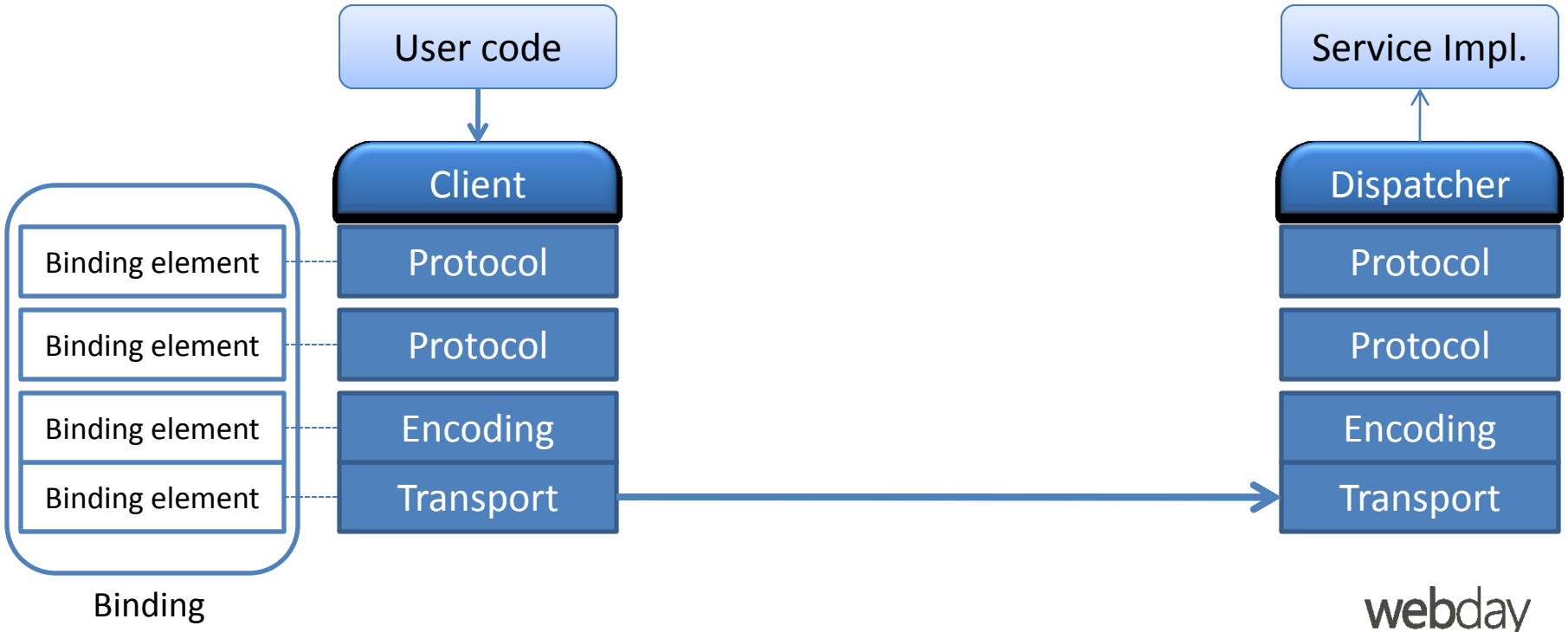
Security

- Access Control
  - Both “listen” and “send” subject to access control
  - Programmable authorization policy, defined by ACS
- Isolation – SB is the DMZ



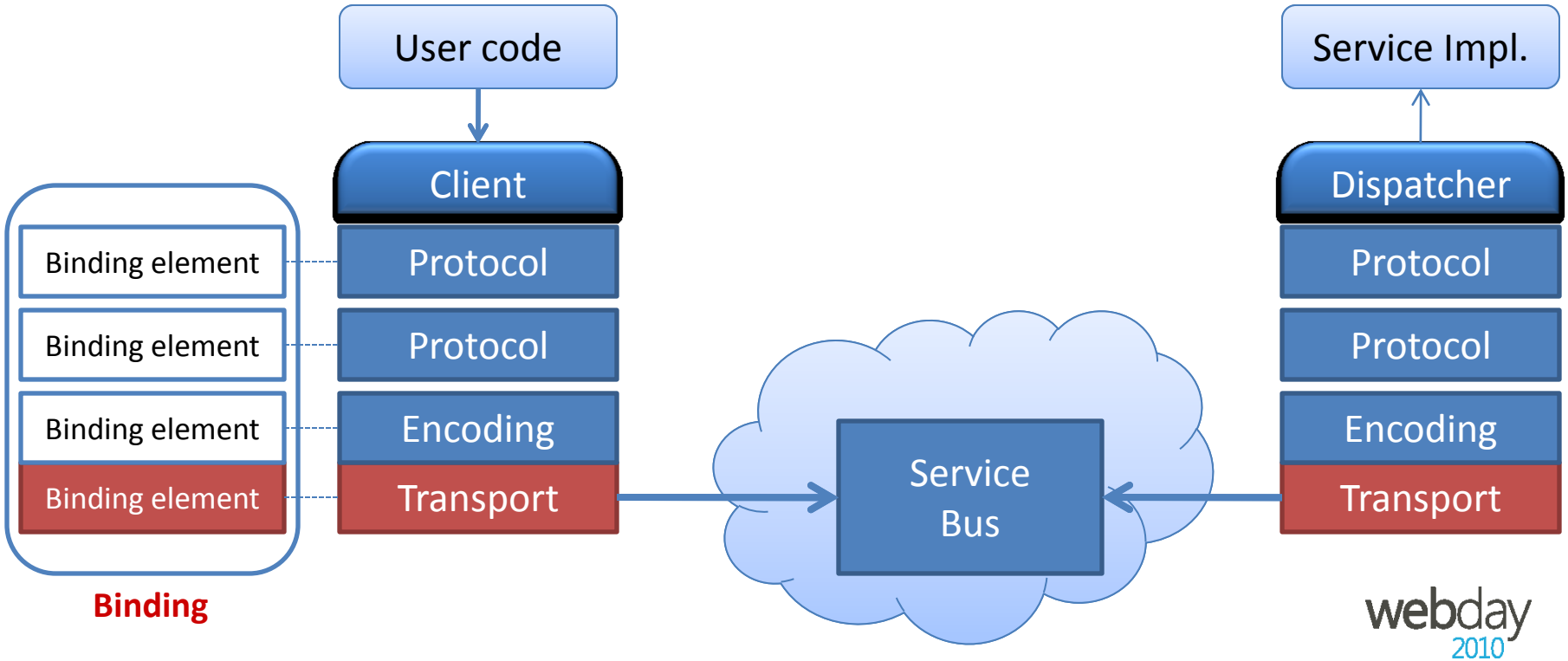
WCF architecture

- Channel stack with transport and protocol channels
- Channels described by binding elements
- One binding contains several binding elements



WCF and SB

- New bindings
  - New transport channels and binding elements
- New behaviors



Bindings

- **WebHttpRelayBinding**
  - HTTP (Web programming model)
  - Client interoperability
- **BasicHttpRelayBinding** e **WS2007HttpRelayBinding**
  - SOAP over HTTP (basic profile | WS-*)
  - Client interoperability
- **NetTcpRelayBinding**
  - Similar to **NetTcpBinding** (request-response and duplex)
- **NetOnewayRelayBinding** e **NetEventRelayBinding**
  - One- way w/buffering and multicast

Binding elements

- **Http(s)RelayTransportBindingElement**
- **TcpRelayTransportBindingElement**
- **RelayedOnewayTransportBindingElement**

Demo

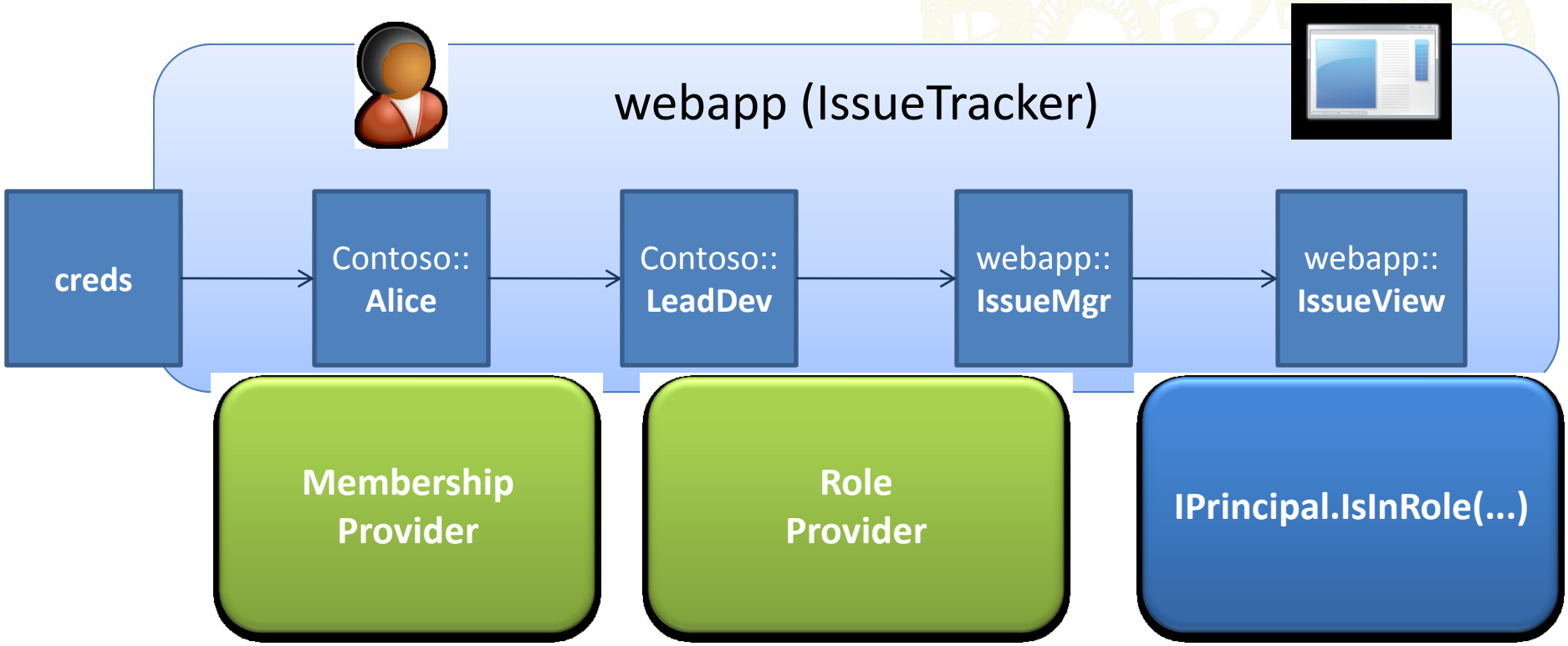
http://**demos-pfelix**.servicebus.windows.net/**webday**

Access Control Service

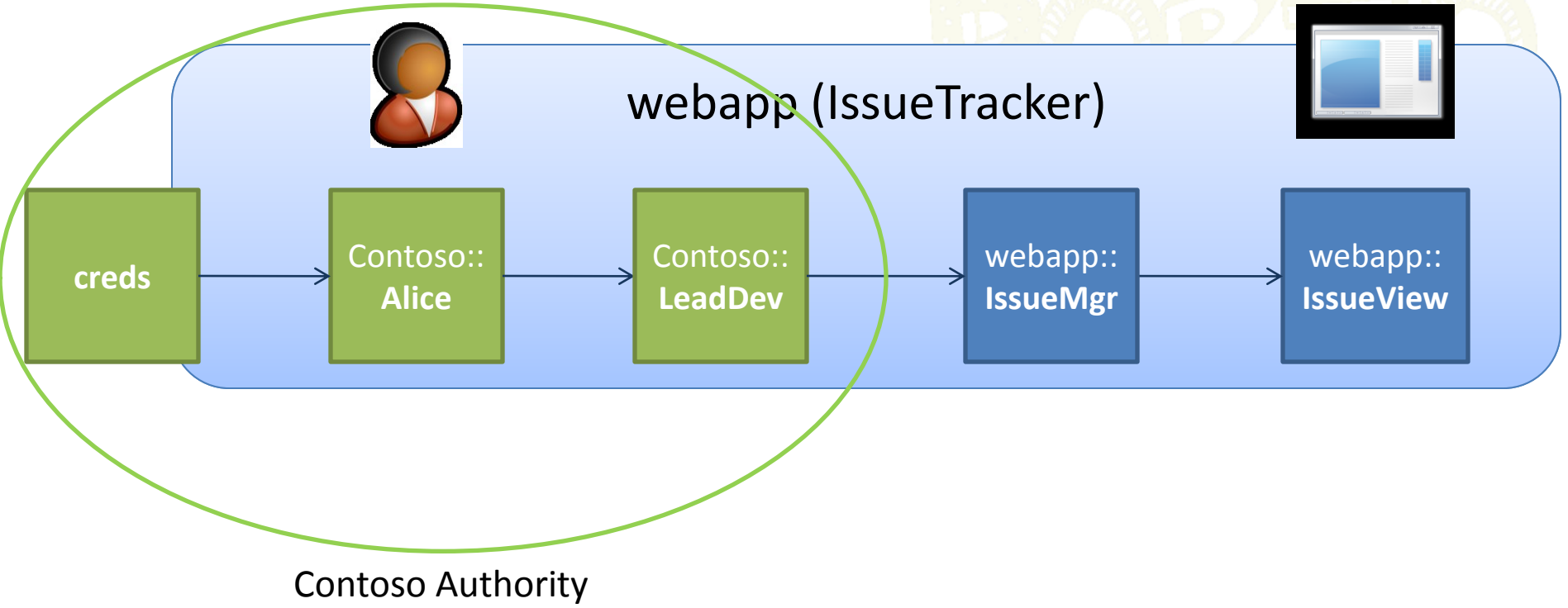
- Identity and access control
- Distributed systems
  - Decentralized authority
  - Heterogeneous technologies
- Claims-based model
- SB integration

Identity and Authorization

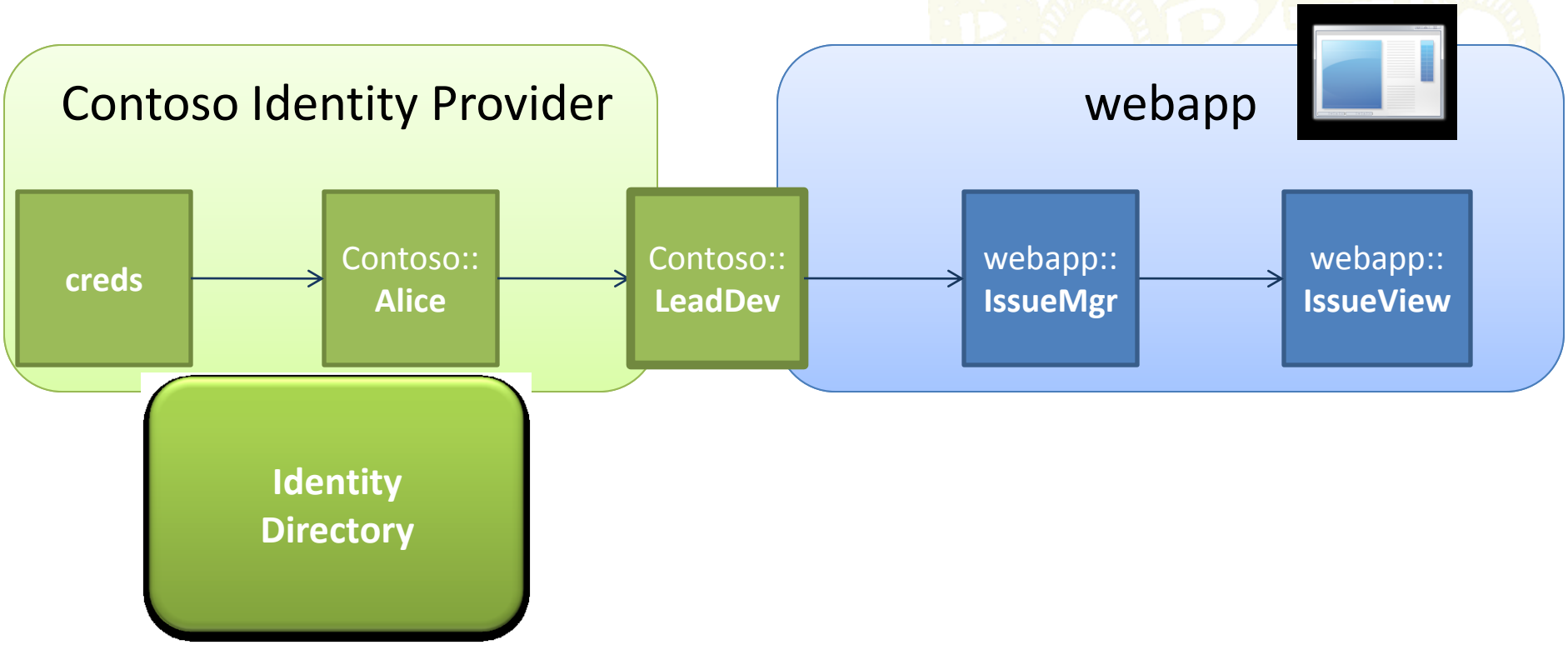
Centralized Solution



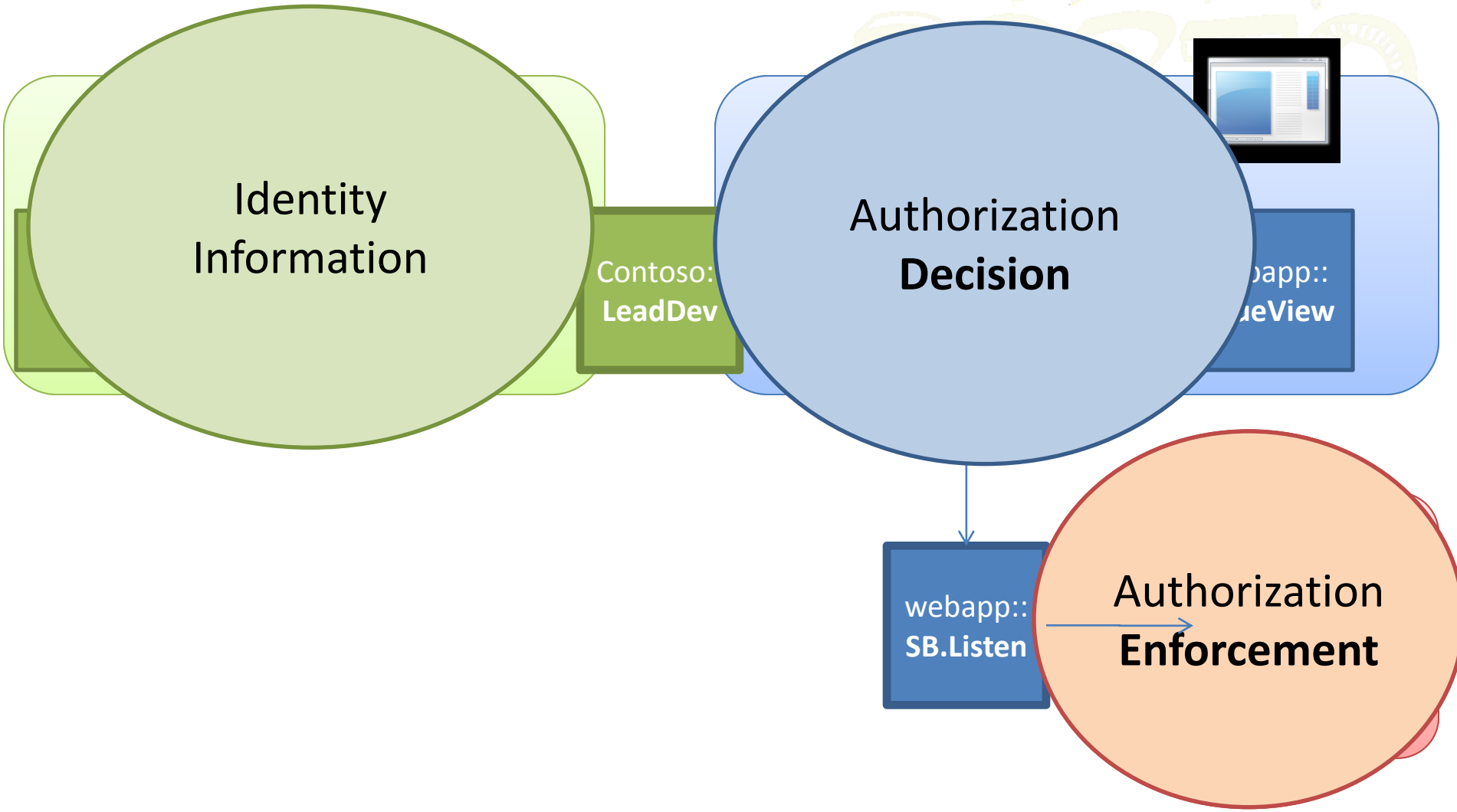
Decentralized Authority



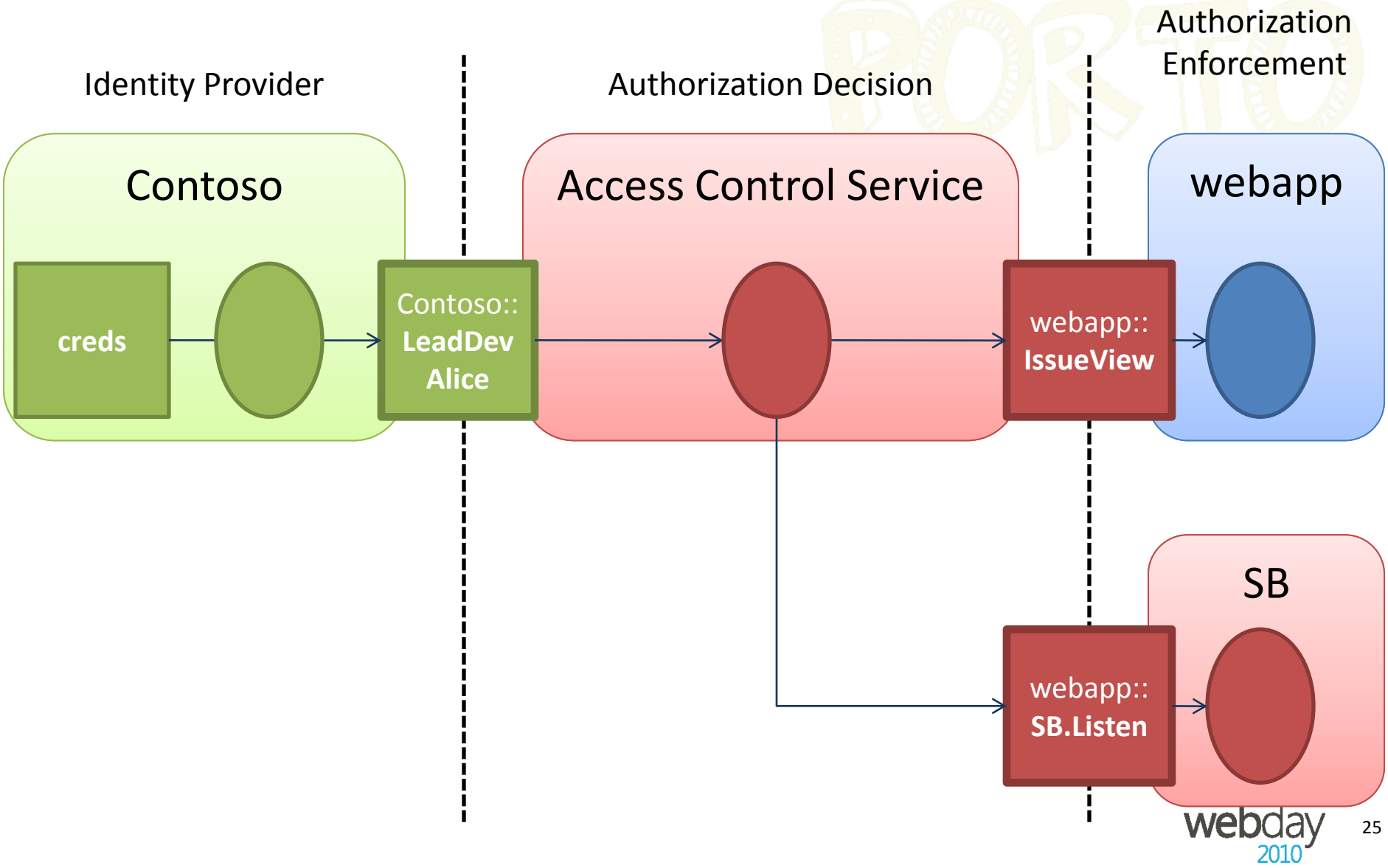
Decentralized Authority



Decision ≠ Enforcement



Access Control Service



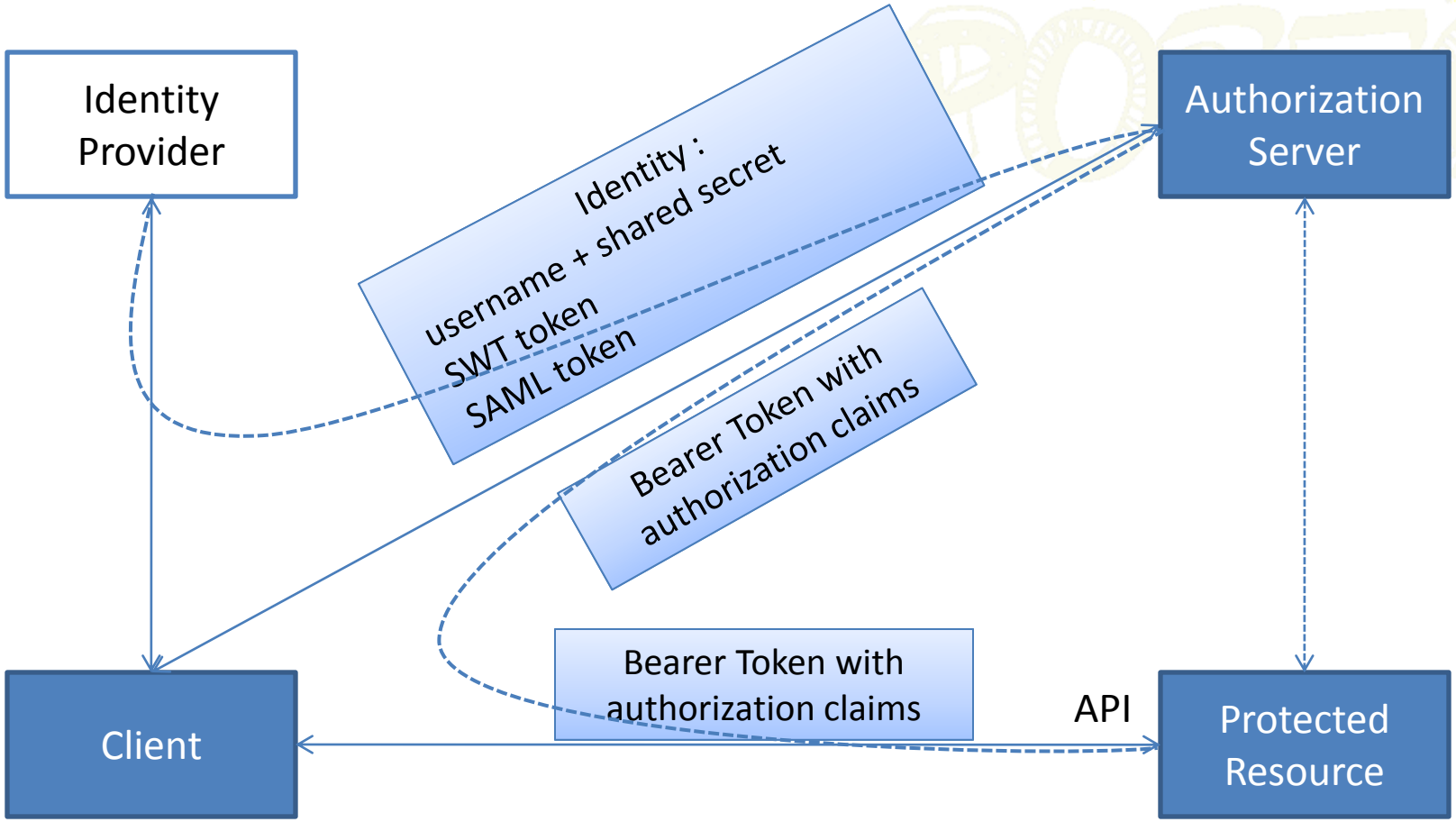
Access Control Service

- Claims-based Identity and Access Control
- Claims transformer ("claims in, claims out")
  - Consumes claims from federated issuers
  - Provides claims to applications and services
- Rule based issuance policy
  - Rule: **If has** claim1 **then output** claim2
- *Not* an identity provider
  - Does not manage user's identities

Protocols and technologies

- AppFabric 1.0
  - OAuth WRAP (Web Resource Authorization Protocol)
  - Simple Web Token
- Future (and past)?
  - WS-Federation – “passive” (browser based) federation
  - WS-Trust – “active” (SOAP based) federation
  - LiveID integration

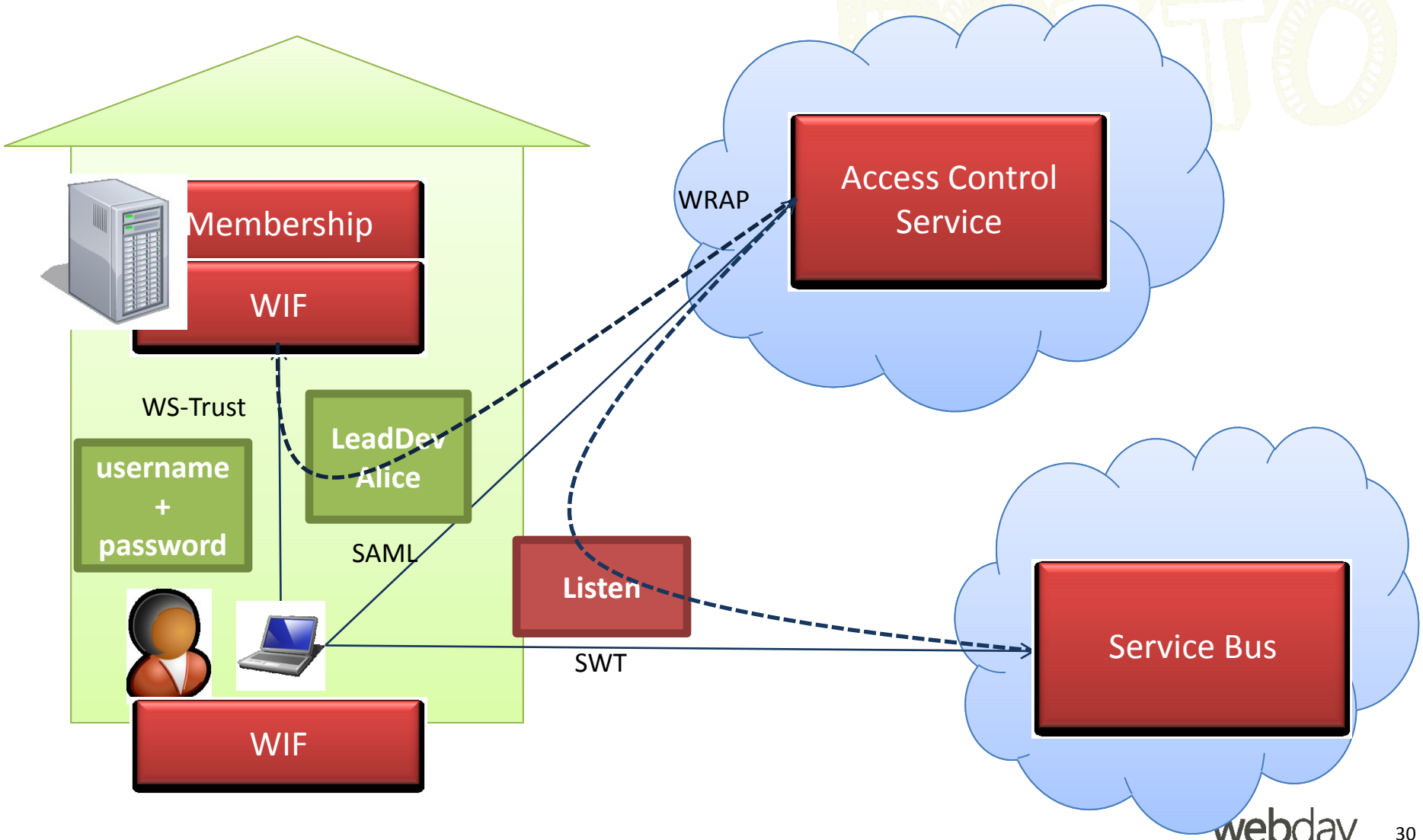
WRAP


Identity Provider
Authorization Server
Identity :
username + shared secret
SWT token
SAML token
Bearer Token with authorization claims
Bearer Token with authorization claims
Client
API
Protected Resource

WRAP and SWT

- Simple Web Token (SWT)
  - Form encoded name-value pairs
  - HMAC-SHA-256 symmetric signature
- WRAP token request
  - HTTP POST
  - username+password or authentication assertion (e.g. SAML)
- WRAP protected client call
  - HTTP header (Authorization: WRAP **access_token** = "…")
  - GET or POST parameter (**wrap_access_token** = "…")

Demo


Membership
WIF
WS-Trust
username
+
password
LeadDev
Alice
SAML
WIF
WRAP
Access Control
Service
Listen
SWT
Service Bus

Finally …

- Service Bus
  - Connectivity
  - Addressability and discoverability
  - Eventing
  - Buffering
- Access Control Service
  - Authorization Decision Point
    - For Service Bus
    - For other services, both cloud or on-premises
  - Flexible claims based policy