

An introduction to .Net Services

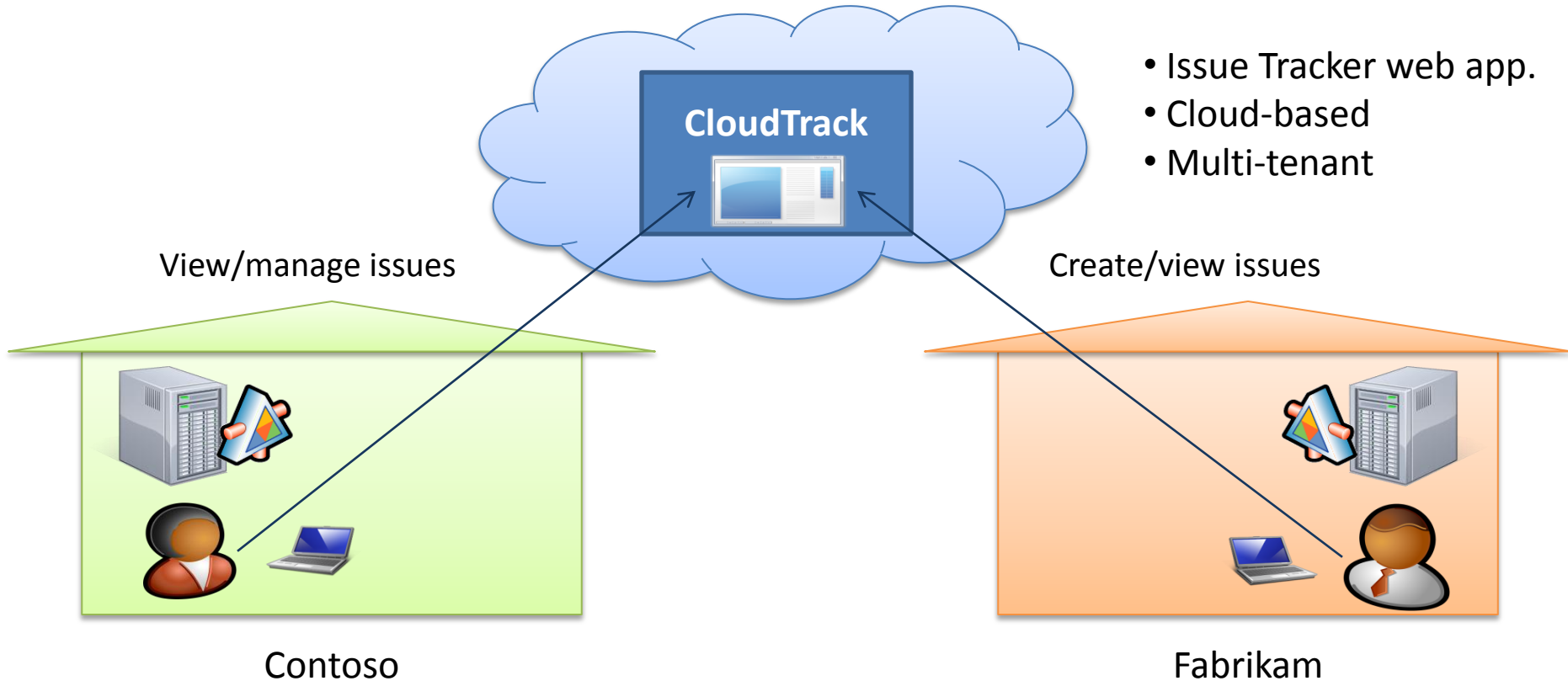
Pedro Félix

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

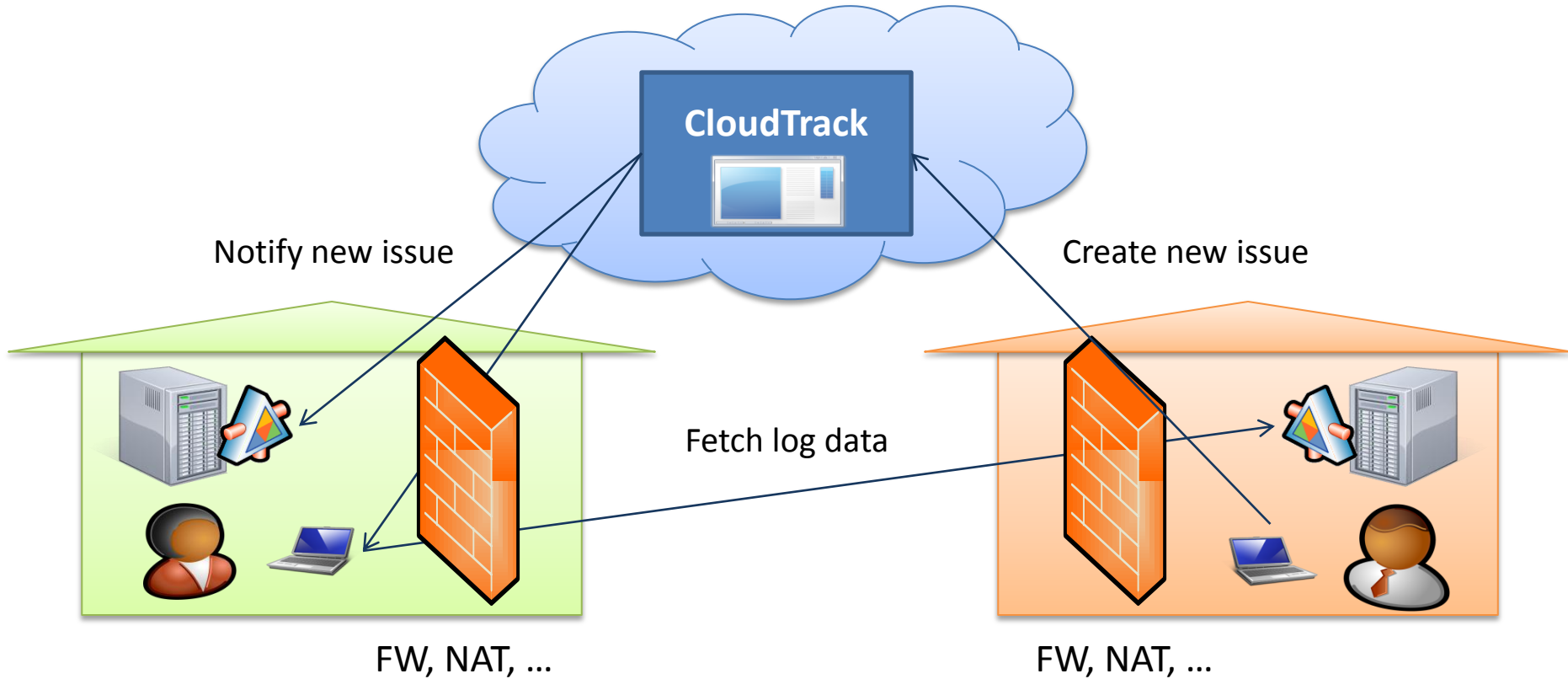
.NET Services

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

A Motivating Scenario



Connectivity challenges

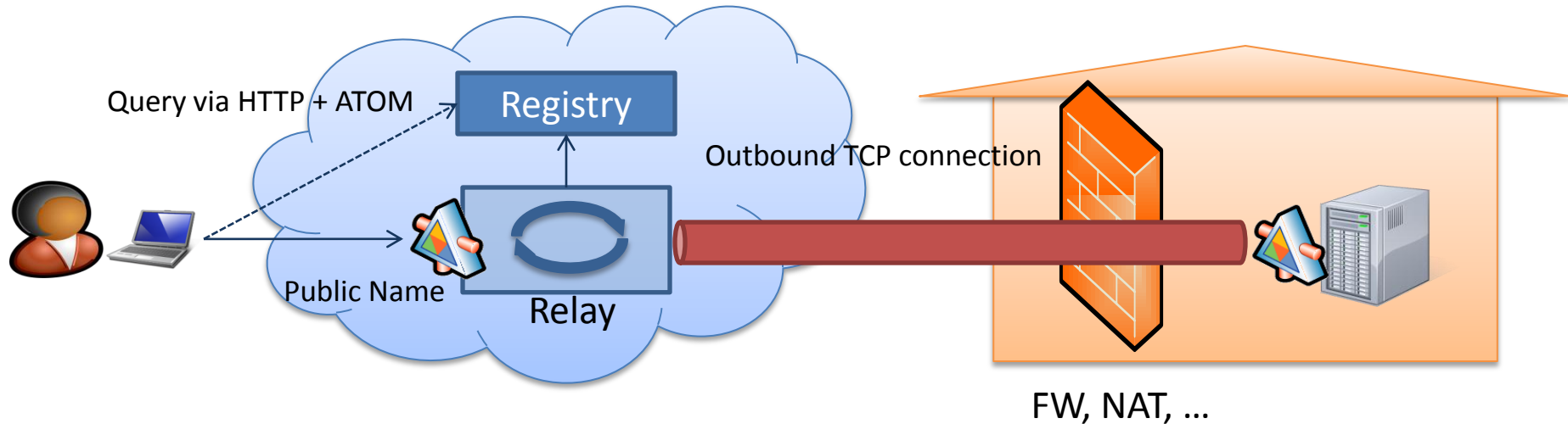


Connectivity Challenges

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

Service Bus Relay

- Connectivity - public *projection* of private endpoints
- Addressability and discoverability



Service Bus

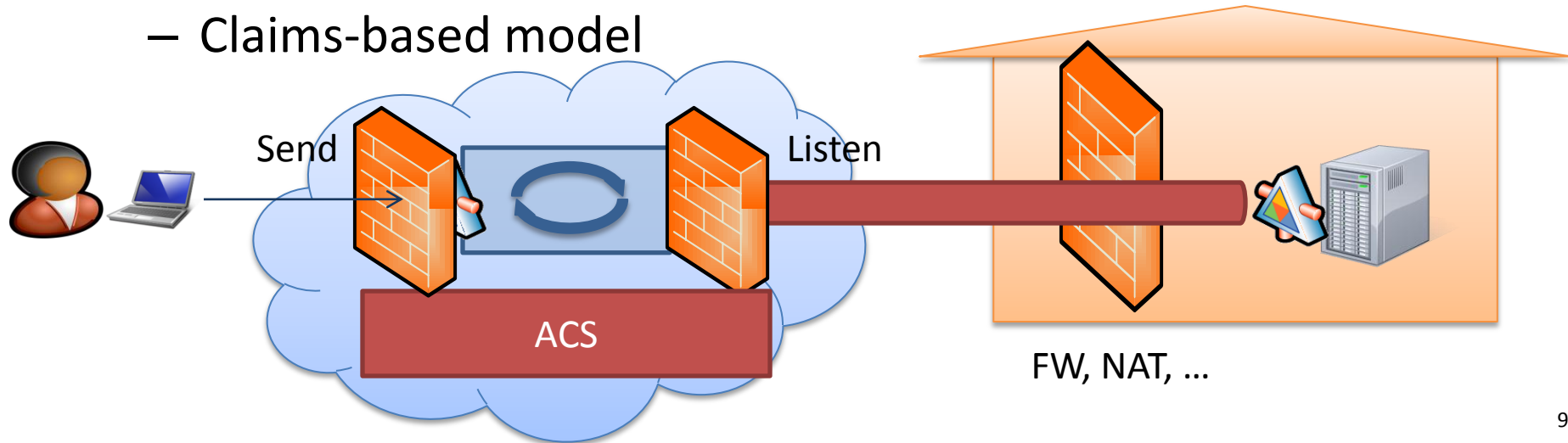
- Naming
 - Public namespace
 - **{scheme}://{solution}.servicebus.windows.net/{relpath}**
- Registry
 - Mapping between URIs and services
 - Readable via HTTP+ATOM
- Connectivity and eventing
 - Relaying between public (SB) and private endpoints

Demo

<http://felixdemos.servicebus.windows.net/remix09>

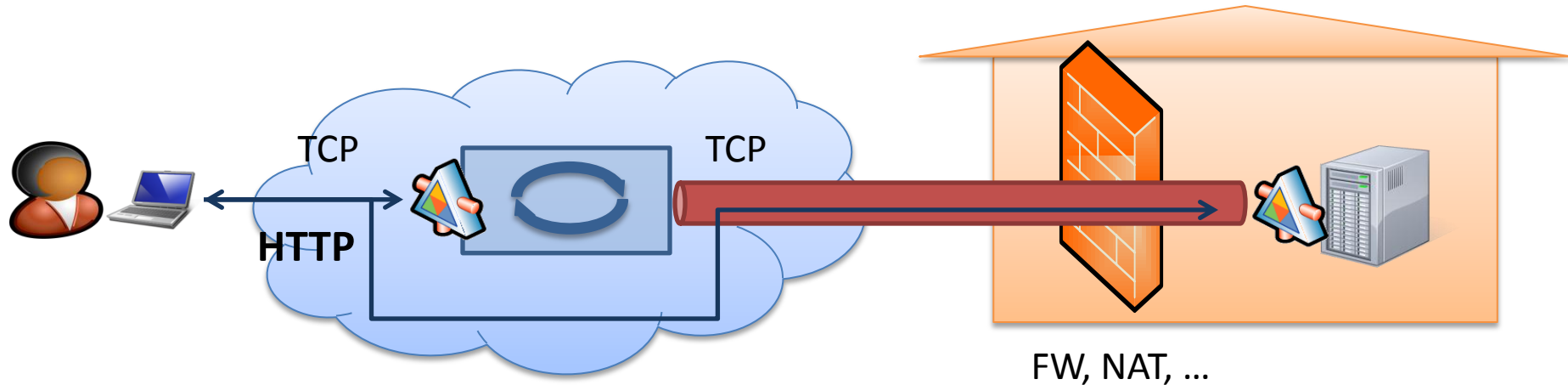
Service Bus Security

- DMZ externalization
 - Public endpoints hosted on the cloud
- Flexible Access Control with ACS
 - Claims-based model



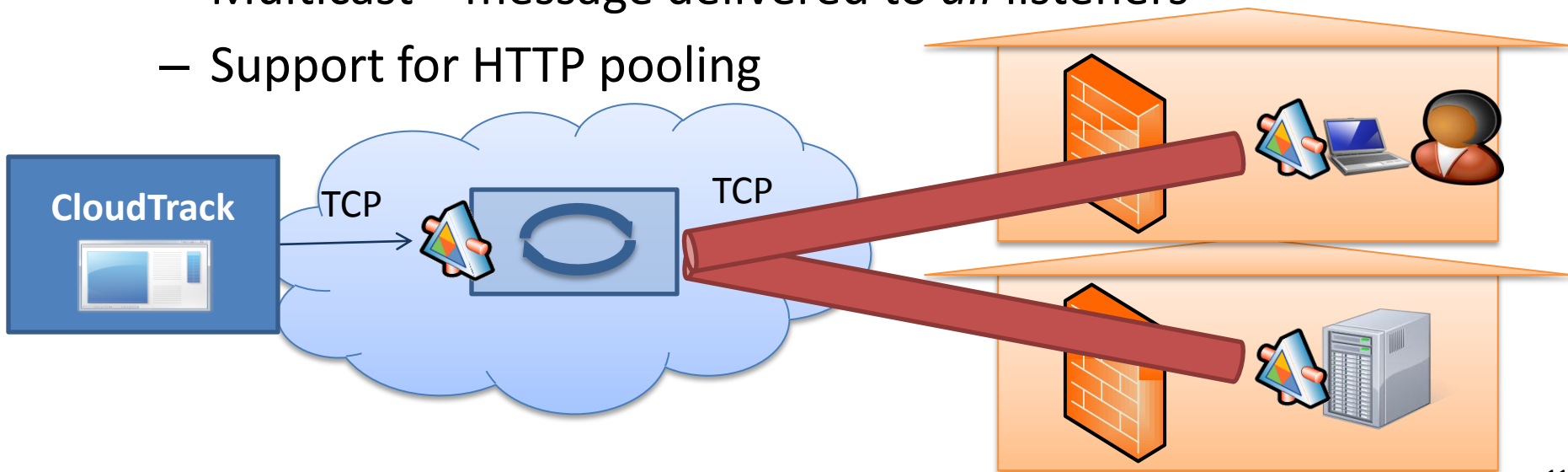
Connectivity

- WCF integration via *transport binding elements*
- Bidirectional (similar to **NetTcpBinding**)
- Request-reply (similar to ***HttpBinding**)



Datagram multicast (pub-sub)

- **NetEventRelayBinding** (oneway)
 - Multiple opened service hosts on the *same* URI
 - Multicast – message delivered to *all* listeners
 - Support for HTTP pooling



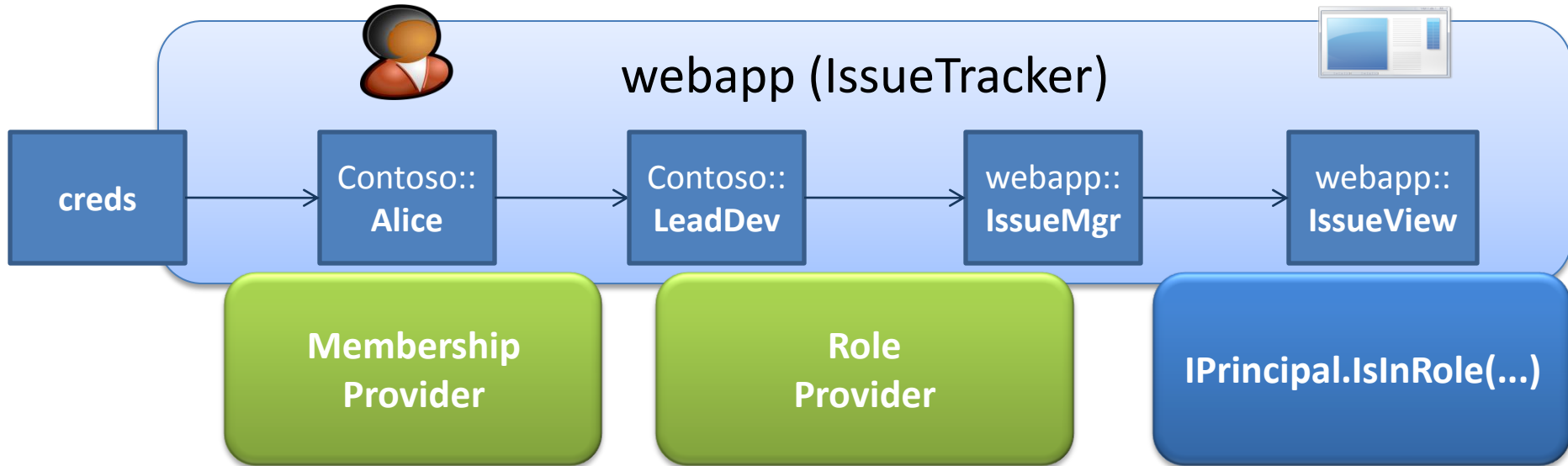
Access Control Service

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

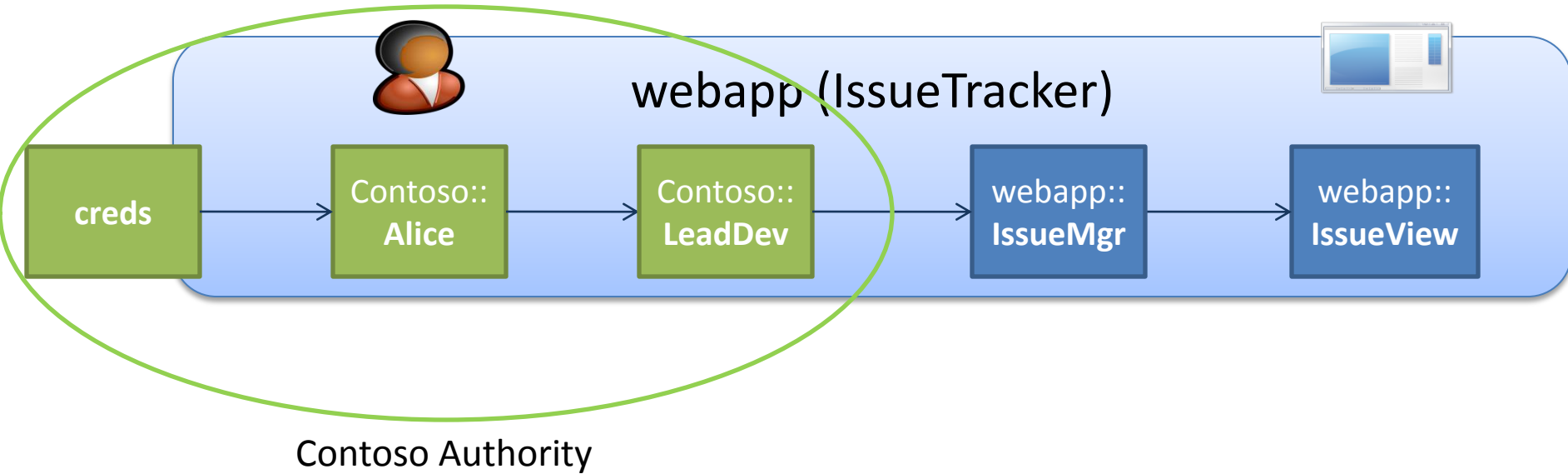
Identity and Authorization



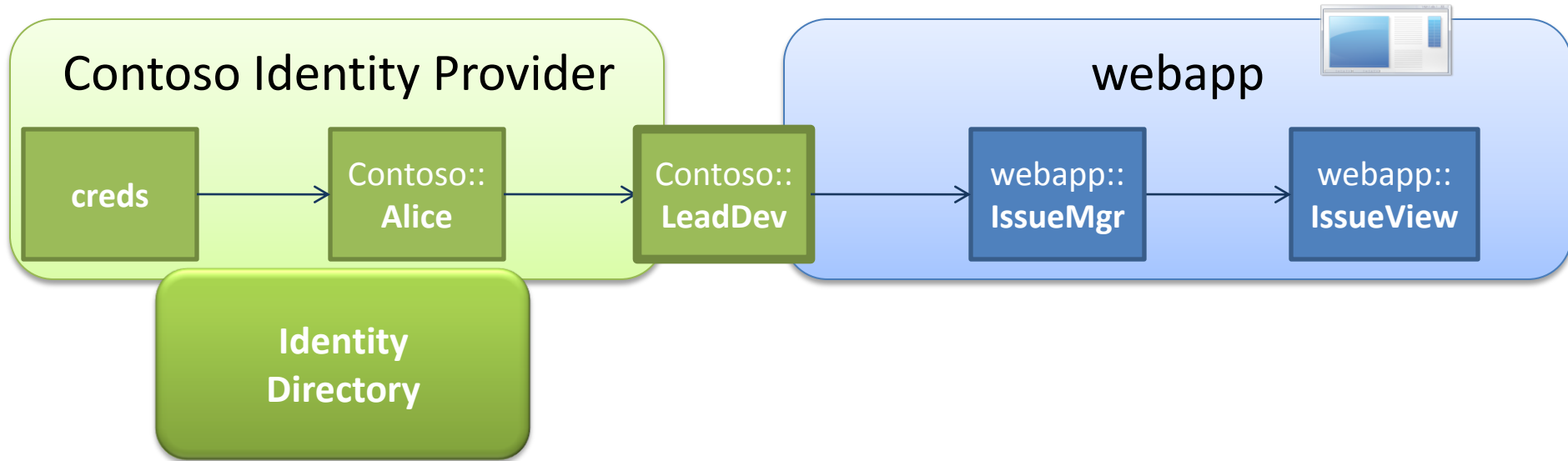
Centralized Solution



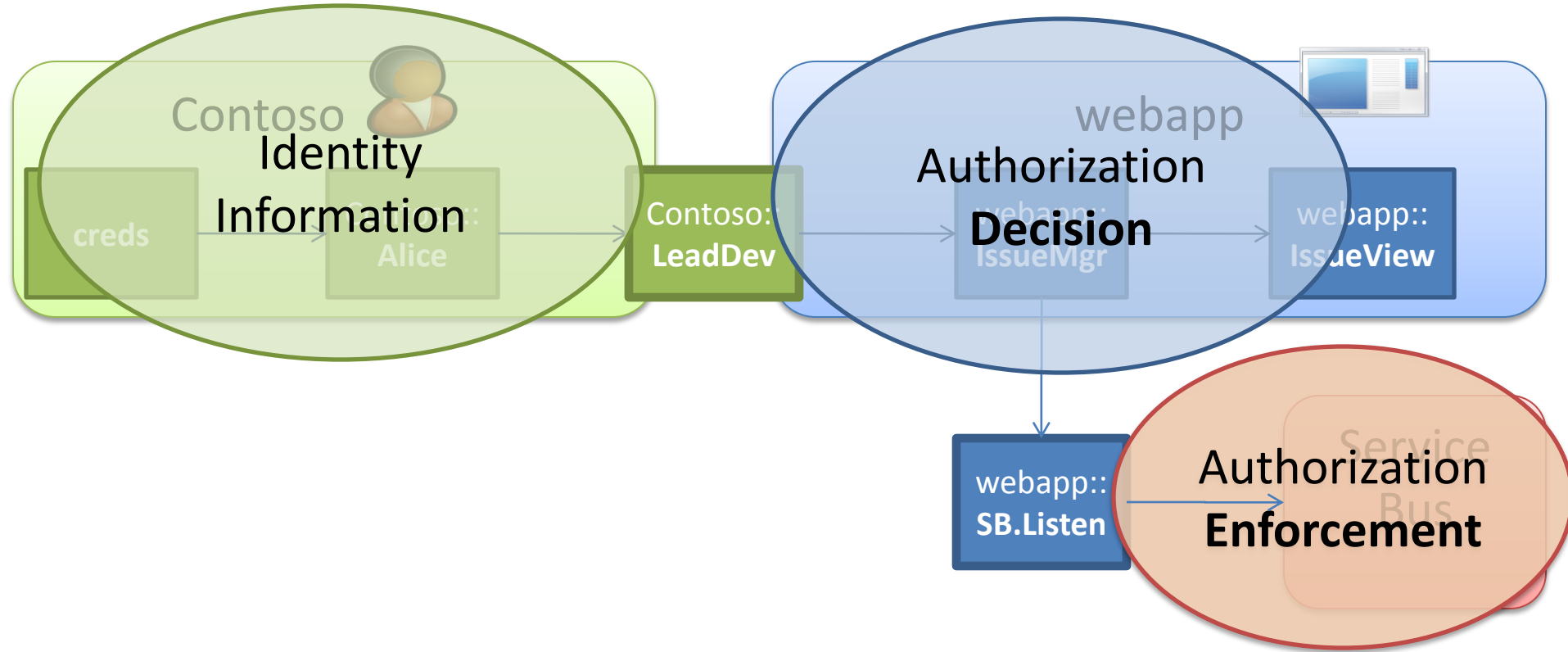
Decentralized Authority



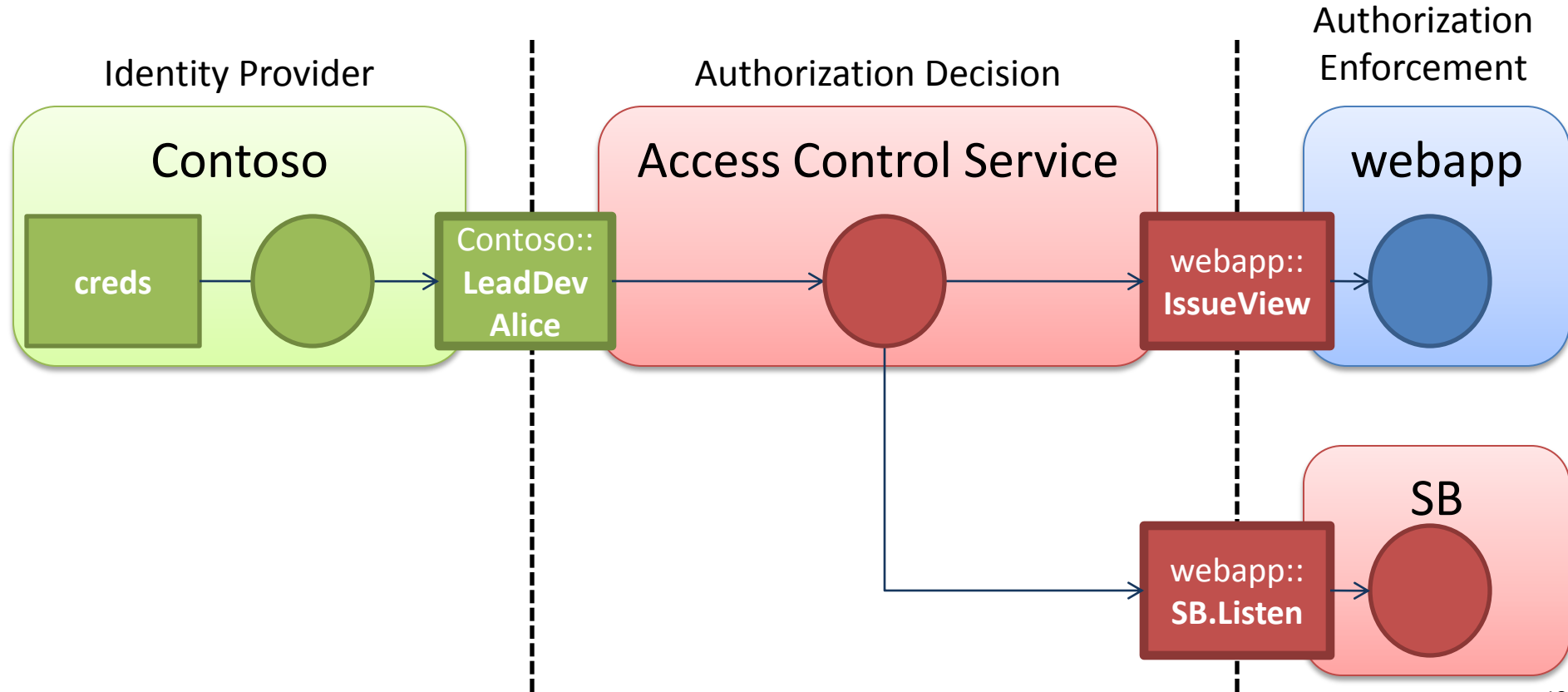
Decentralized Authority



Decision \neq 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

