

Understanding Cardpace in an enterprise setting: PART 2

Kim Cameron,
Chief Architect of Identity
Microsoft

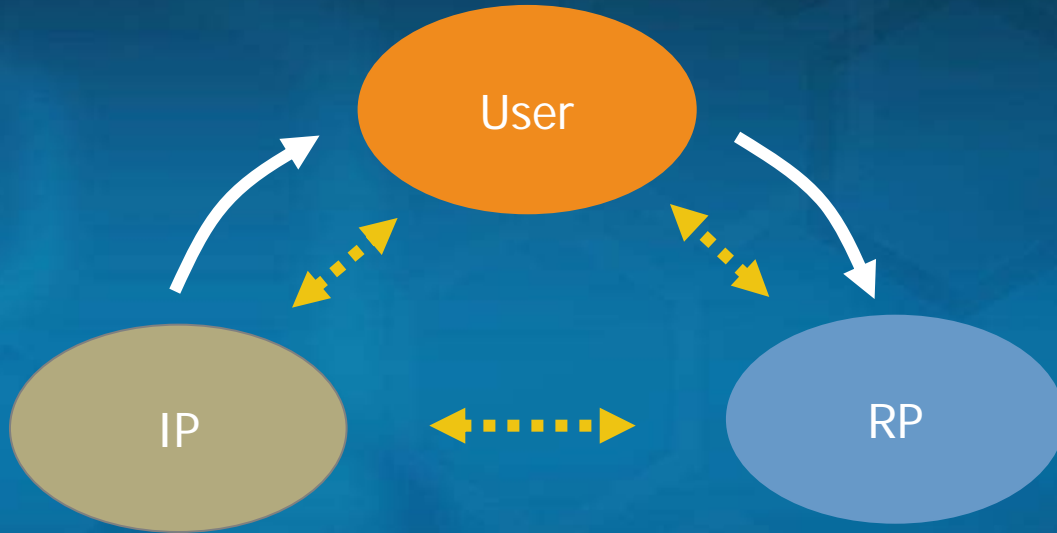
Enterprises are consumer facing

- Many enterprises have relationships with individuals and small businesses
- These are often not central to consumers' lives, but are still **important when important**
- Information Card strengths:
 - Fast acquisition
 - Intermittent relationships
 - Risk reduction: anti-phishing and information minimalization
- Ubiquitous availability of COTS software

Dual architectures?

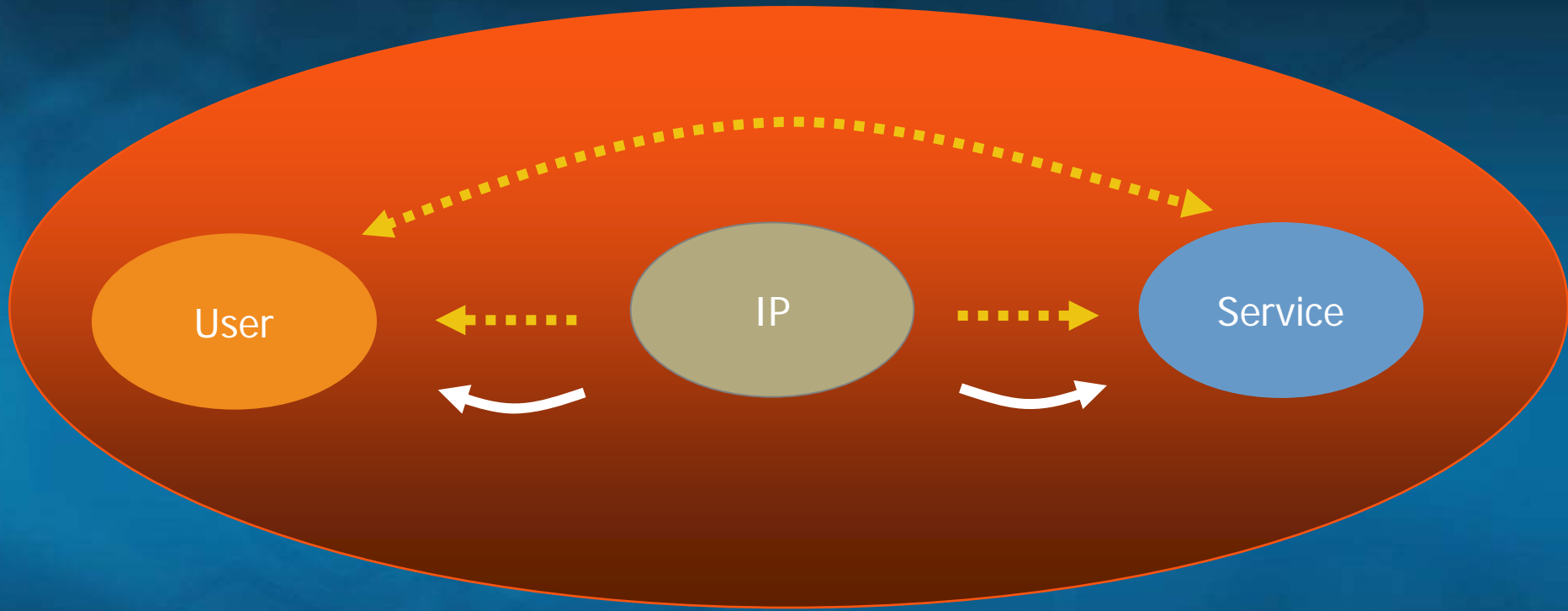
- Assume for a moment that Information Cards become progressively more ubiquitous
 - For example, if large internet sites enable billions of users
- Increasing pressure to adopt Information Card for external relationships
- Is it desirable to have a dual architecture – one for outside and one for inside – in the age of “de-perimeterization”?

Identity Metasystem Model



Trust 

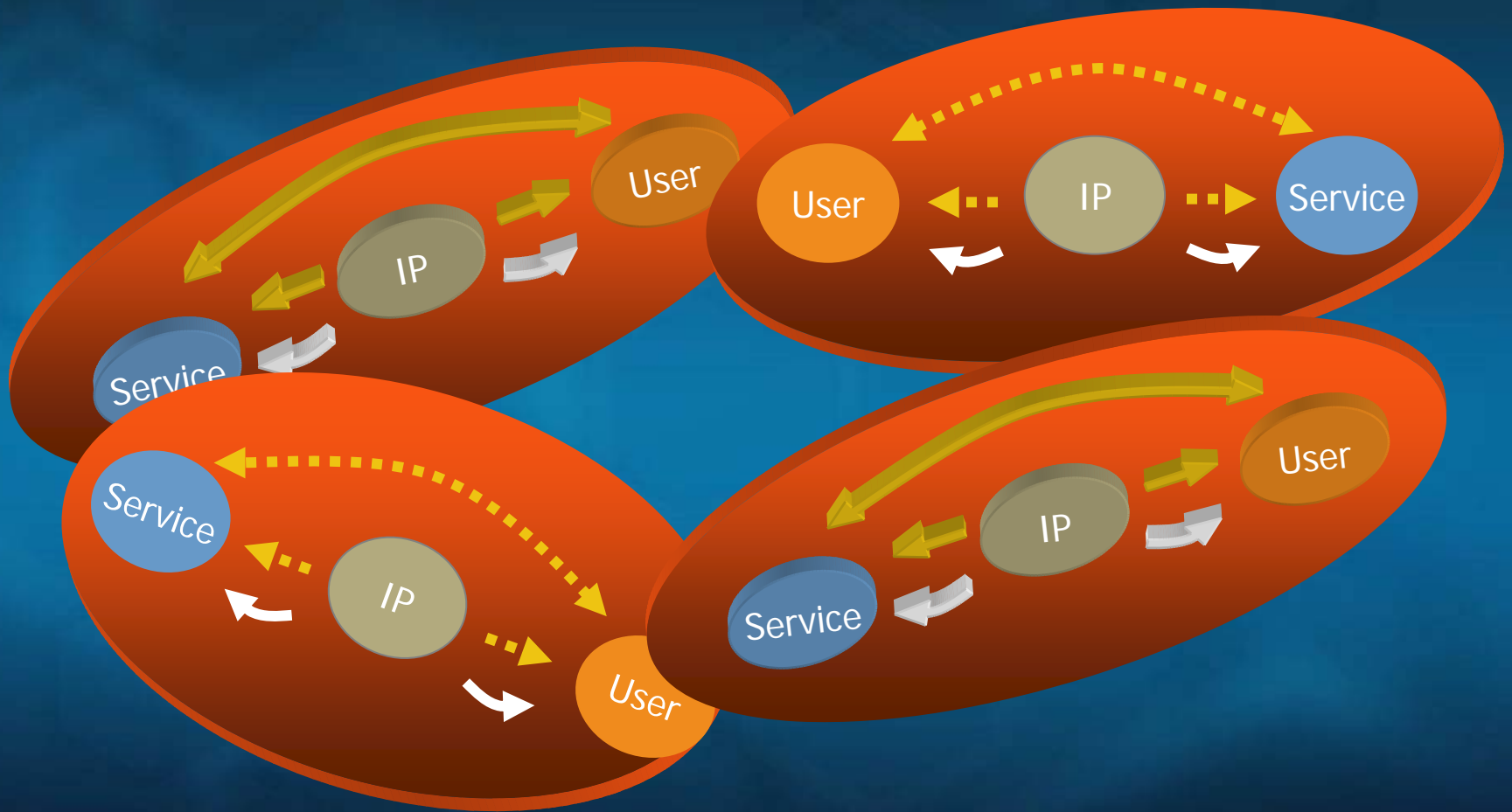
Domain Based Model



In the beginning, the Identity Provider created principals:
users and services

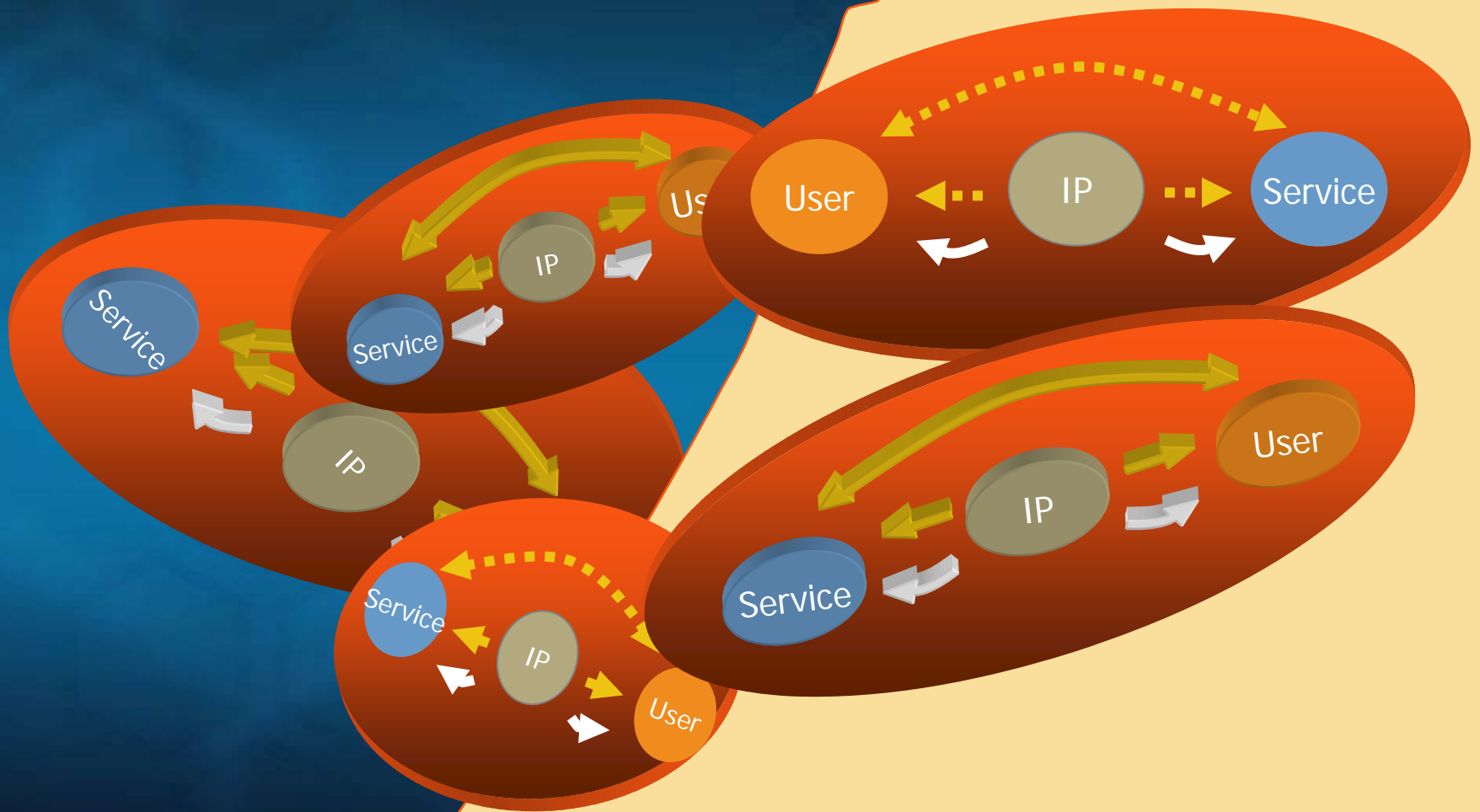
Trust 

Multiple Domain Model



Oh oh – there is not one, but *several* domains

Meshed Enterprise Model



Make that – not just several – but *large* numbers of domains

Empowering users

- Achieving access control while granting access has been really really hard.
 - Inefficient, unreliable, unsafe
 - Hand crafted by professionals
- Conclusion was to disappear the user from any involvement – including the business units
- General solutions require increasingly complex policies
- Alternate approach – make it easy enough that users can do it – albeit under adult supervision

Trust is local

- It's the relying party that decides who and what can access its resource
 - Can be delegated to “authorization STS”
- In the enterprise this should be a business decision, made by the business unit, not the IT department
 - Has been impossible, because it's just too hard
- Organization-wide relationships may not be germane to a specific context
 - Need to accommodate both enterprise-wide policy and relative autonomy of business units
- Main role of Information Cards in the enterprise: devolve access control to the business users who own resources

Conclusions

- Using Information Card architecture provides benefits throughout the new enterprise mesh
- Simplification and visualization allow us to devolve control to the owners of resources
- Extension of visual metaphors required so setting access control policy on relying parties is as easy as selecting an Information Card
- Ultimately, the benefits of a single user experience at home and in the enterprise