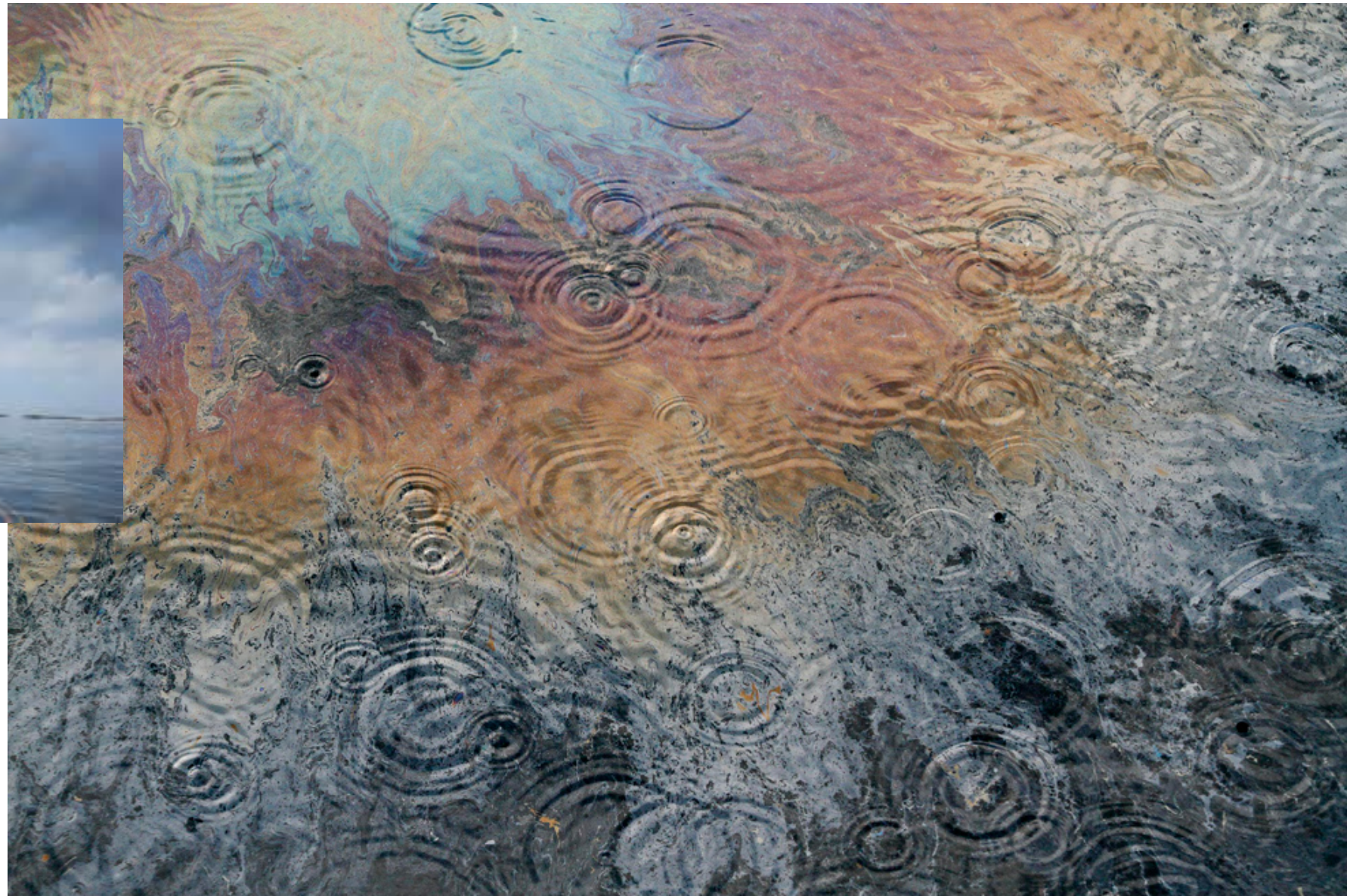
If customer accounts were cars…

If customer accounts were oil…



It’s time to clean up the environment

CIO Most read:

IMPERVA Manufacturer Swaps Out Guardium to Save 70% EXPAND

Home > Security

FEATURE

Is it time for Identity as a Service?

The concept of security these days goes well beyond insisting on complicated passwords. Are you sure your company is up to the task?

By Mary Branscombe | Follow
CIO | Nov 9, 2015 4:15 AM PT

RELATED TOPICS
Security
Data Protection

From Target to TalkTalk to whoever gets breached next week, the litany of companies that have lost customer data should be making businesses rethink not just how they protect customer

MORE LIKE THIS

How to get the most out of Windows 10 enterprise securi features

Connected vehicles as a technology platform: Don Bu Ford Motor Company

Windows 10 review: It's famil it's powerful, but the Edge browser falls...

on IDG Answers
If I buy a Chromebook and can't get to grips with OS can I convert to windows?

kim cameron @Kim_Cameron 31m
Yes. Right on time. Azure B2C *is* Account Management as a Service (AMAS): professionalized account management.
twitter.com/adamshostack/s…

> **adam shostack** @adamshostack
> @marypcbuk I know you probably don't write the headlines... It might be time for account management as a service. :)

Details

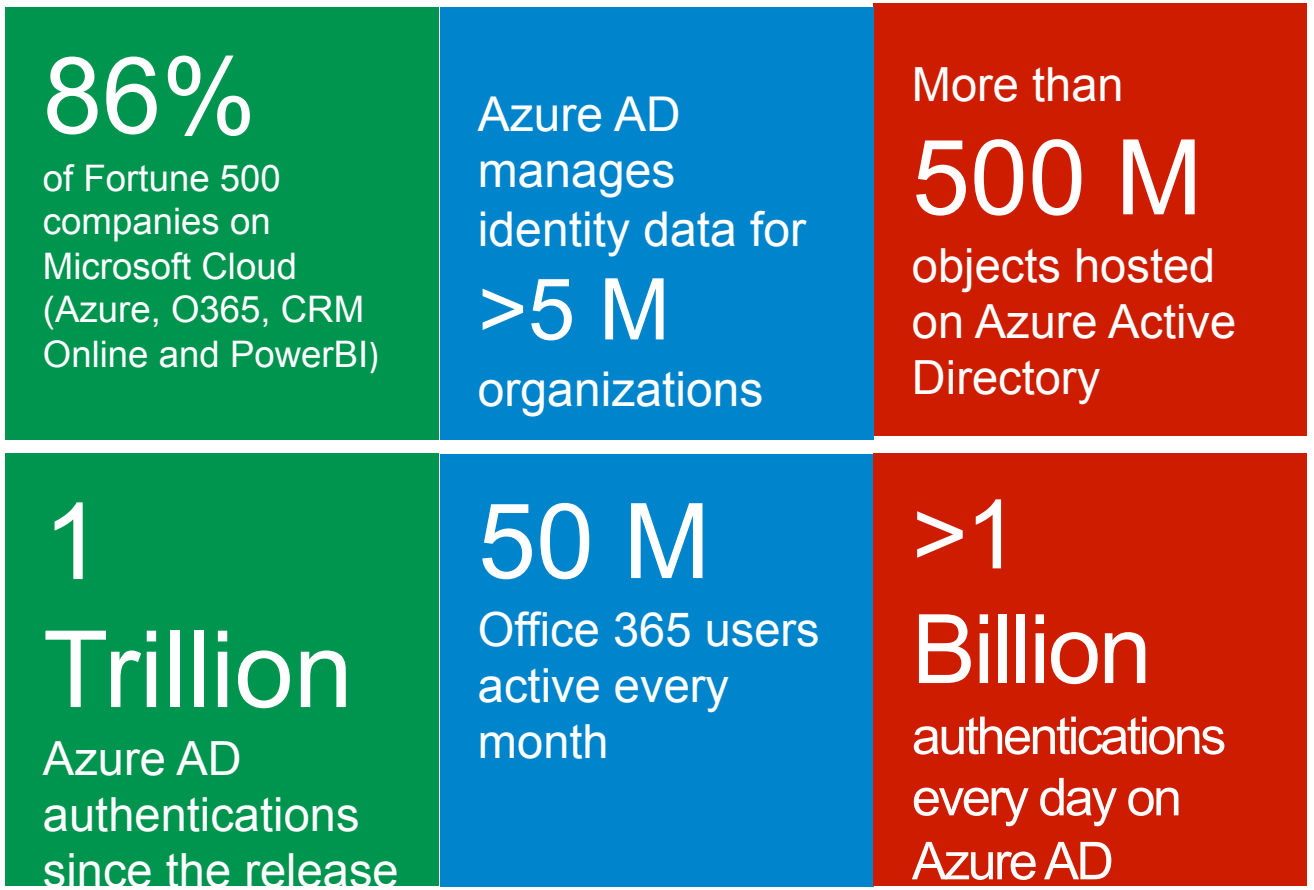
Mary Branscombe retweeted
kim cameron @Kim_Cameron
Exactly. Azure B2C is uses an Identity Experience Engine to go beyond "accounts" to customer relationships.

> **Mary Branscombe** @marypcbuk
> @adamshostack I think B2C is a bit broader than just account management; @Kim_Cameron had a post on more of the policy t'other day

Details

Professionalizing Identity: IdM Services

- *IdM services for enterprises are totally unlike consumer identity systems*
- Example: Azure AD - Microsoft's Identity Management as a Service for organizations
- Millions of **independent** identity systems **controlled** by enterprise and government "tenants"
- Information is **owned and usable by the controlling organization** - not by Microsoft
- Born as an on-premise identity system for employees, has now extended into the cloud
- Has now evolved to manage an organization's relationships with its customers/citizens and partners (B2C and B2B)



Newest Trend: Professionalization of B2C

So organizations of any size can:

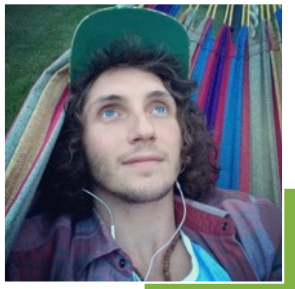
- dramatically reduce **risk**, cost, and complexity
- handle all their different customer relationships within a consistent framework
- grow without limitation
- safely accept all kinds of devices
- gain exceptional control of user experience

What is different about B2C?

- “What are the differences between the way businesses interact digitally with their customers and the way they interact with their employees?”

Employee

- “Known”
- IT Managed
- Single context
- Not context aware



Customer

- Moves from unknown to known
- Marketing & Sales
- Lowest possible friction
- Fully context aware
- Pay as you go

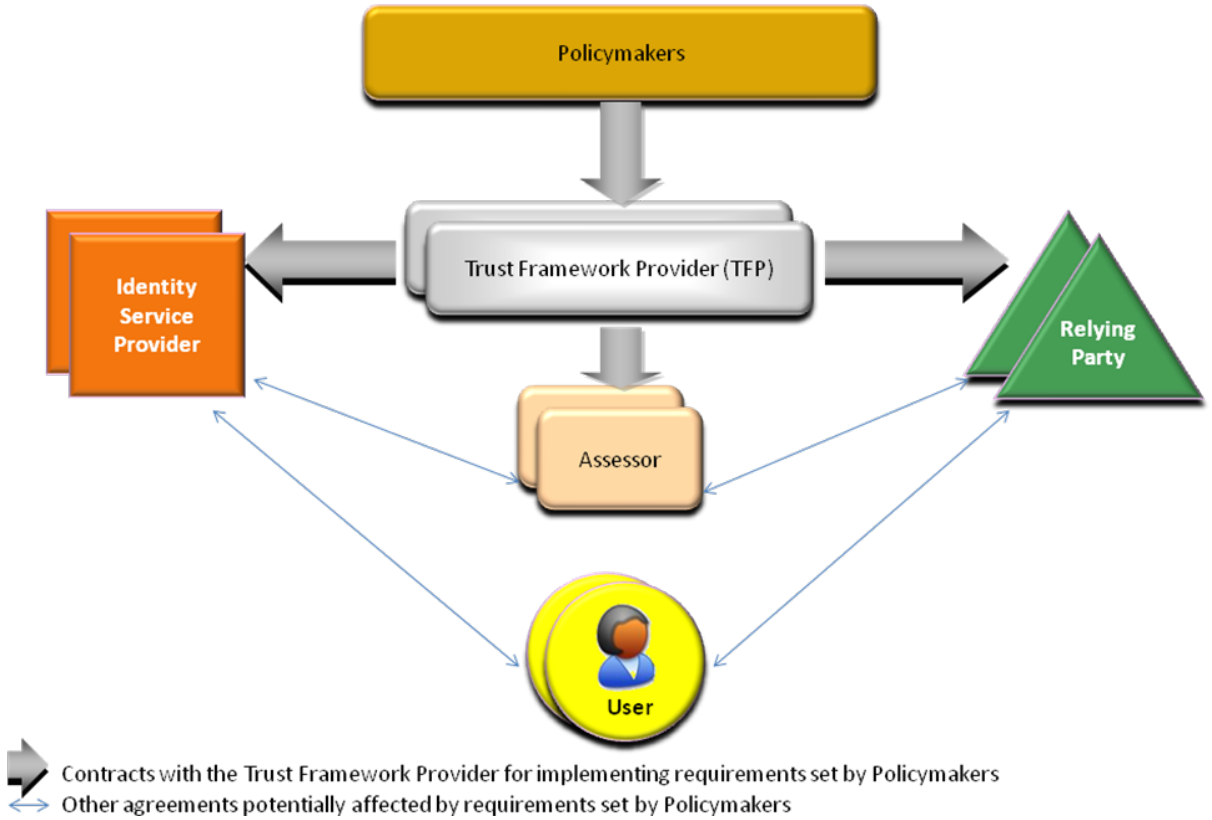
What is different about B2C?

- B2C scenarios demand, above all else, the ability to customize the customer's identity experience to what is right for whatever they are doing.

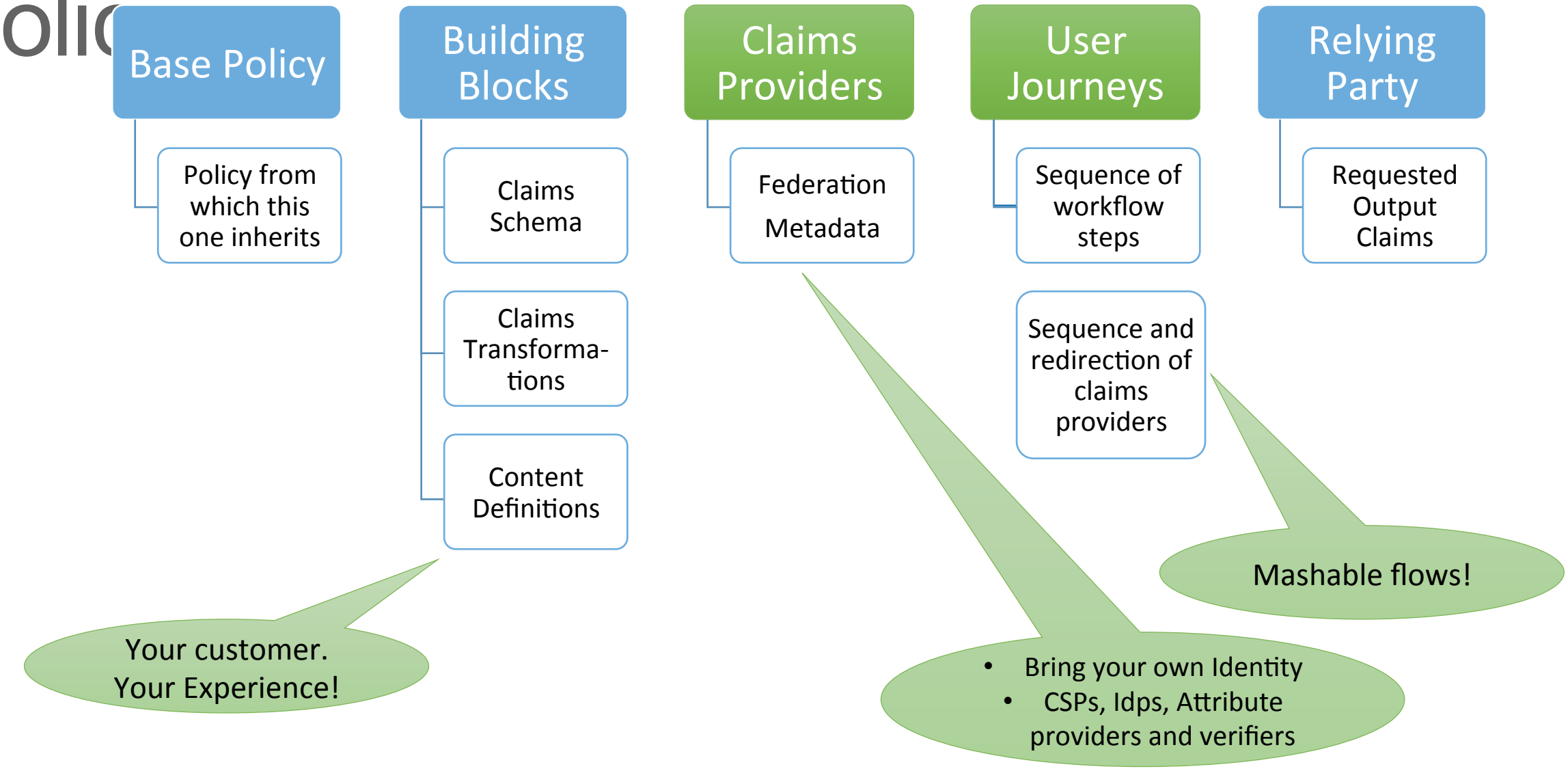
Azure AD B2C

- Fully customizable “user journeys” and visuals
- based on an *Identity Experience Engine* **driven by** *Trust Framework Policies*
- Trust Framework Authors create the policies
- Application developers call the engine and it does **all the heavy lifting**, applying the policy and controlling security

Trust Framework Policies concretize the tech concepts of Trust Frameworks (OIX)



Components of a Trust Framework polic

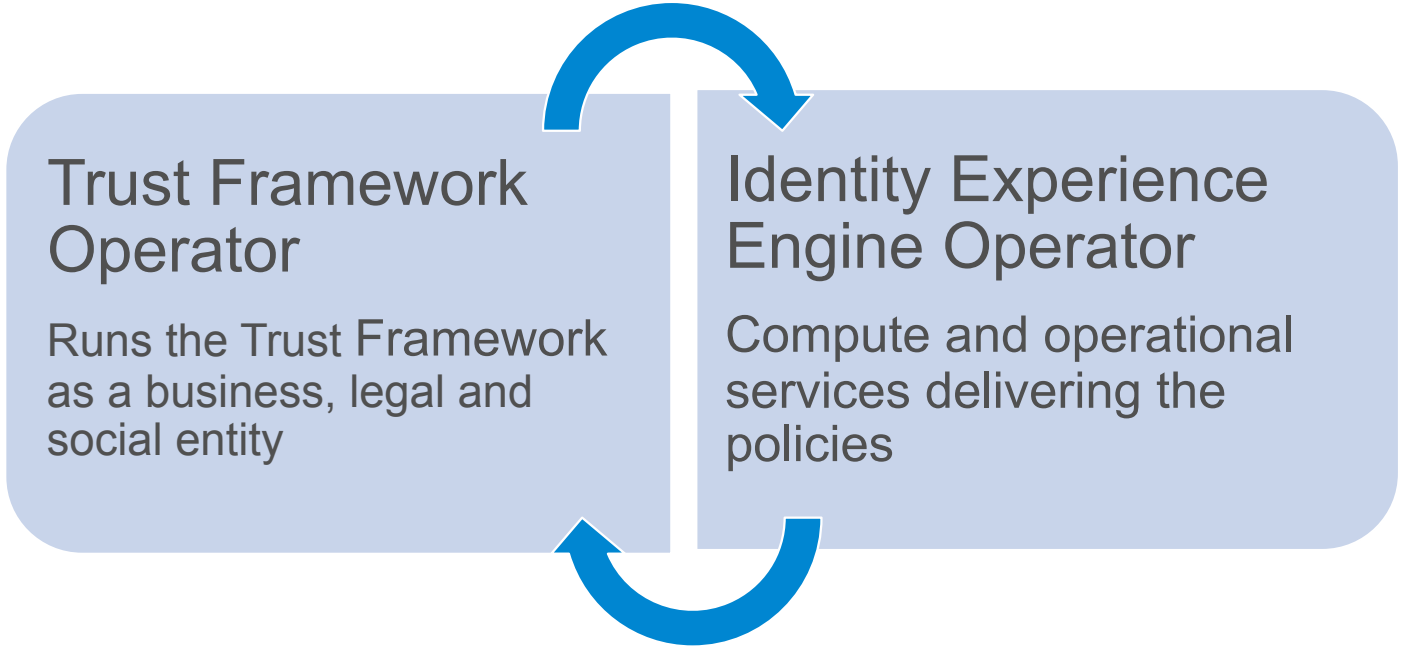


Trust Frameworks are Useful at Different Levels

- Single application
- Single Organization
- Complex Organization with many divisions
- Horizontal Sets of Organizations
- Vertical Sets of Organizations

- Define and document security and privacy behaviors and compliance

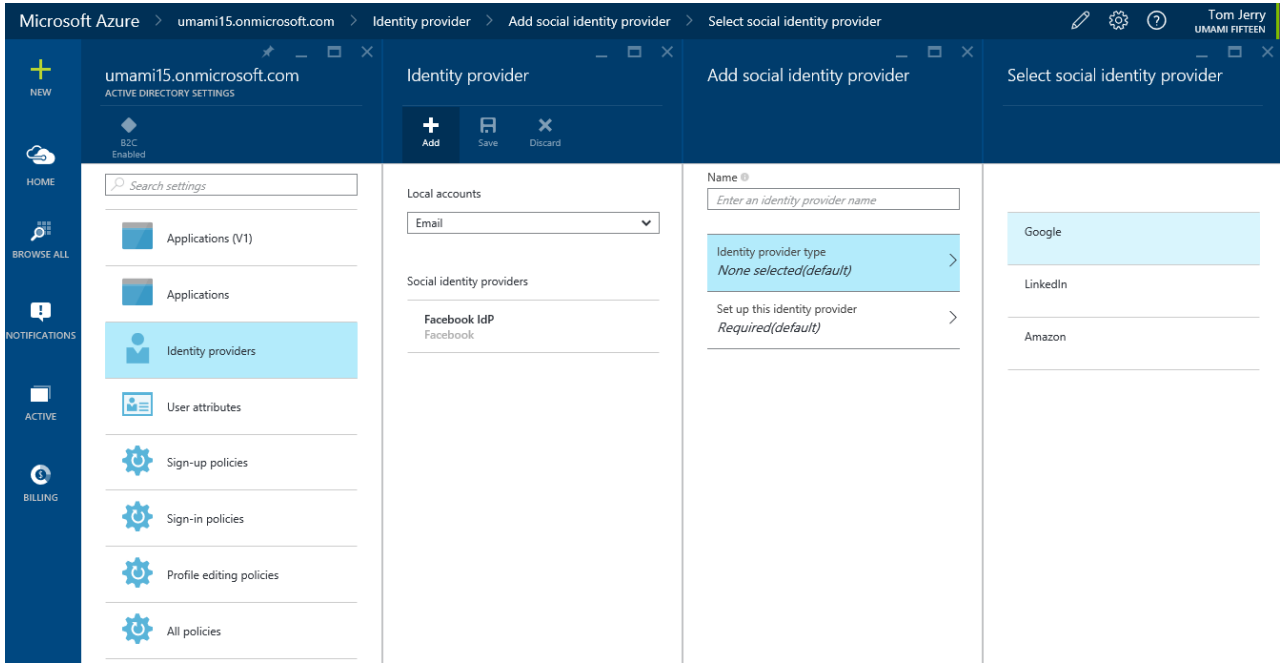
Cloud era operational model



B2C Basic – packaged identity experiences

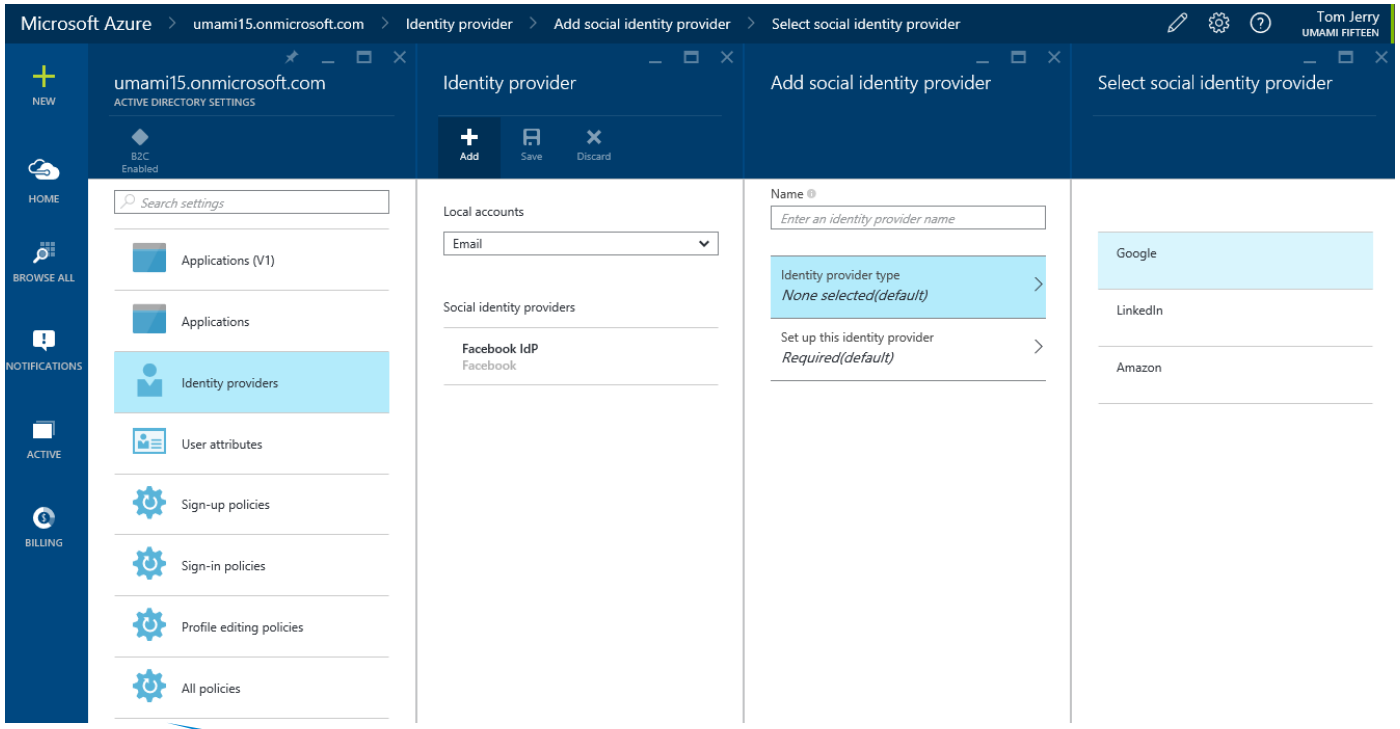
- Meet IDaaS needs of typical apps and enterprises
- ID Providers:
  - top social networks
  - app-specific local accounts
  - phone/email verification
- Simple portal configuration customizes the TF policies for each application
- Enterprise controls “look, feel and content” of user experience
- Engine guarantees the security and privacy of the system
- Upgradable to “advanced” at any time

Microsoft Azure Active Directory B2C Portal

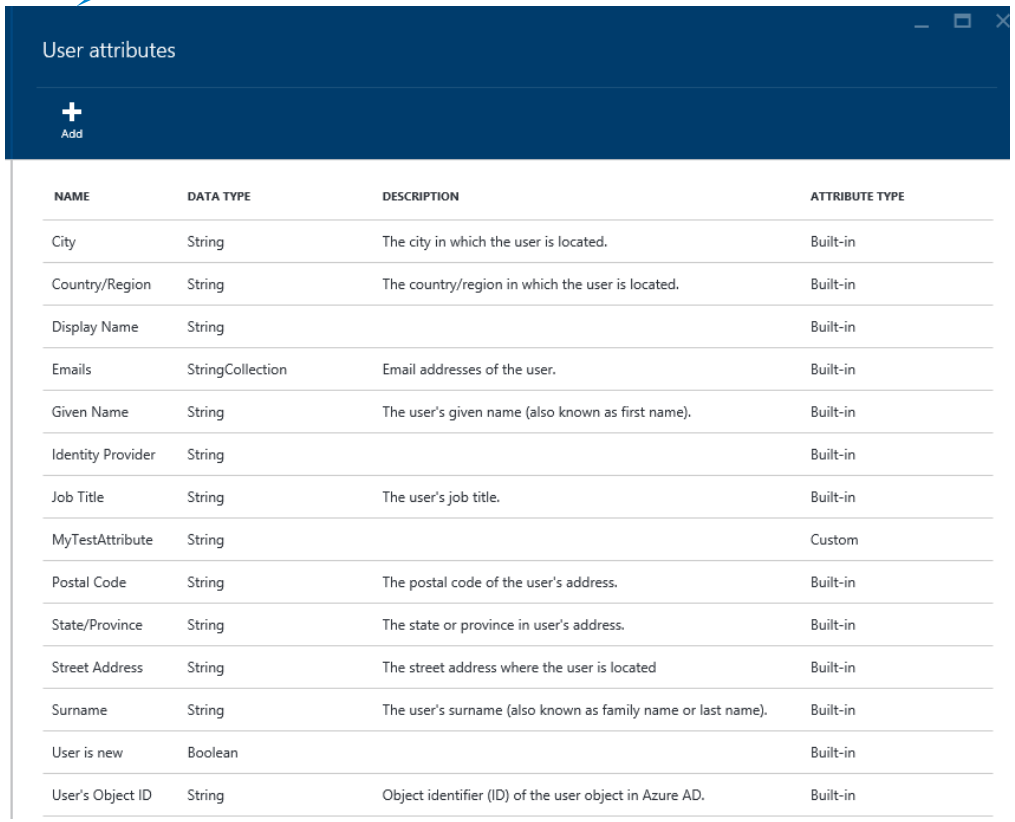


The portal configures the “Microsoft **Basic** Trust Framework”

Customer Admin Portal



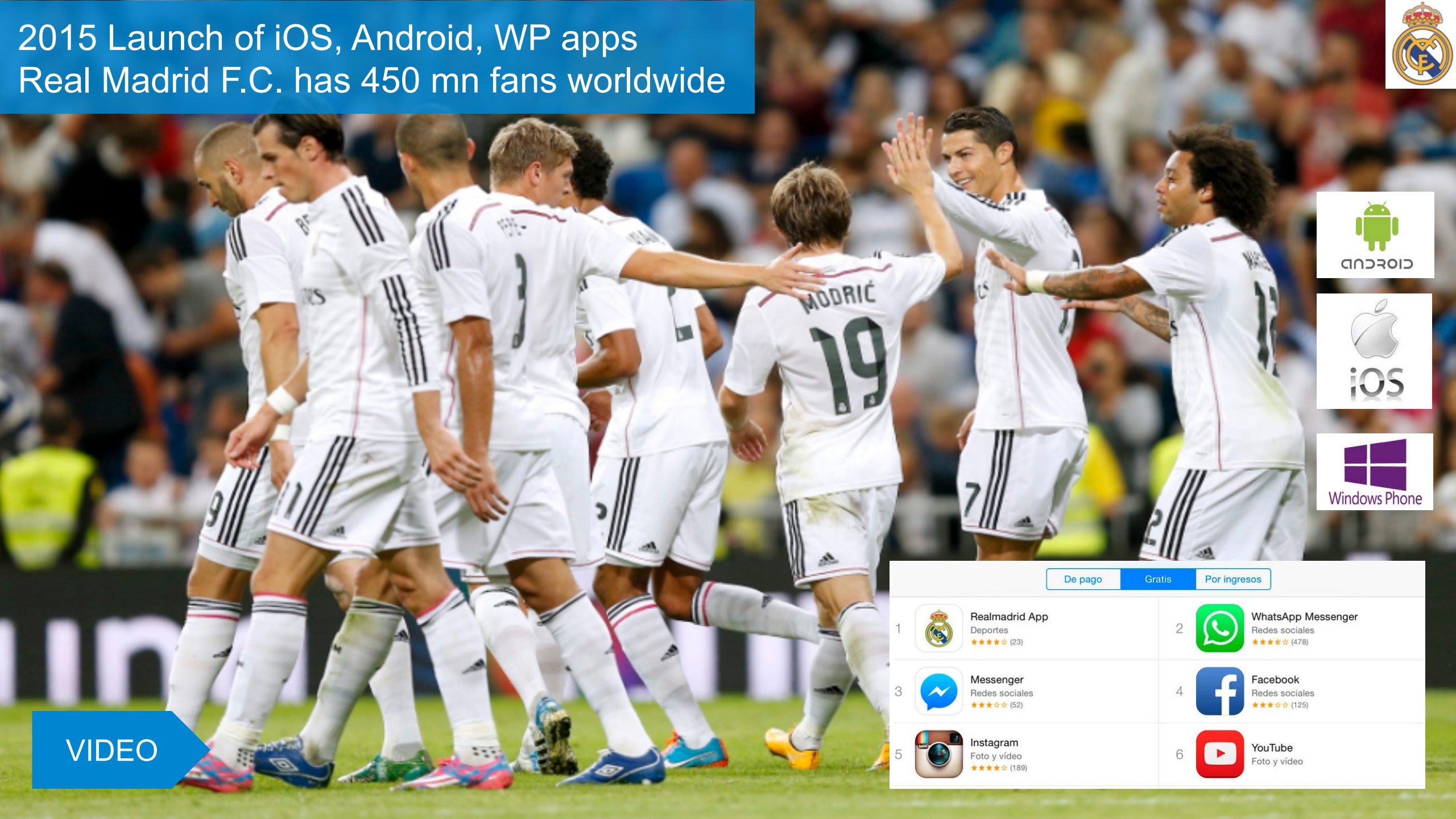
User data schema with default and custom parameters



NAME	DATA TYPE	DESCRIPTION	ATTRIBUTE TYPE
City	String	The city in which the user is located.	Built-in
Country/Region	String	The country/region in which the user is located.	Built-in
Display Name	String		Built-in
Emails	StringCollection	Email addresses of the user.	Built-in
Given Name	String	The user's given name (also known as first name).	Built-in
Identity Provider	String		Built-in
Job Title	String	The user's job title.	Built-in
MyTestAttribute	String		Custom
Postal Code	String	The postal code of the user's address.	Built-in
State/Province	String	The state or province in user's address.	Built-in
Street Address	String	The street address where the user is located	Built-in
Surname	String	The user's surname (also known as family name or last name).	Built-in
User is new	Boolean		Built-in
User's Object ID	String	Object identifier (ID) of the user object in Azure AD.	Built-in

ID Providers (and claims providers) welcome and their respective scopes

2015 Launch of iOS, Android, WP apps
Real Madrid F.C. has 450 mn fans worldwide



ANDROID

iOS

Windows Phone

De pago	Gratis	Por ingresos

1	Realmadrid App Deportes ★★★★☆ (23)	2	WhatsApp Messenger Redes sociales ★★★★☆ (478)
3	Messenger Redes sociales ★★★☆☆ (52)	4	Facebook Redes sociales ★★★☆☆ (125)
5	Instagram Foto y vídeo ★★★★☆ (189)	6	YouTube Foto y vídeo

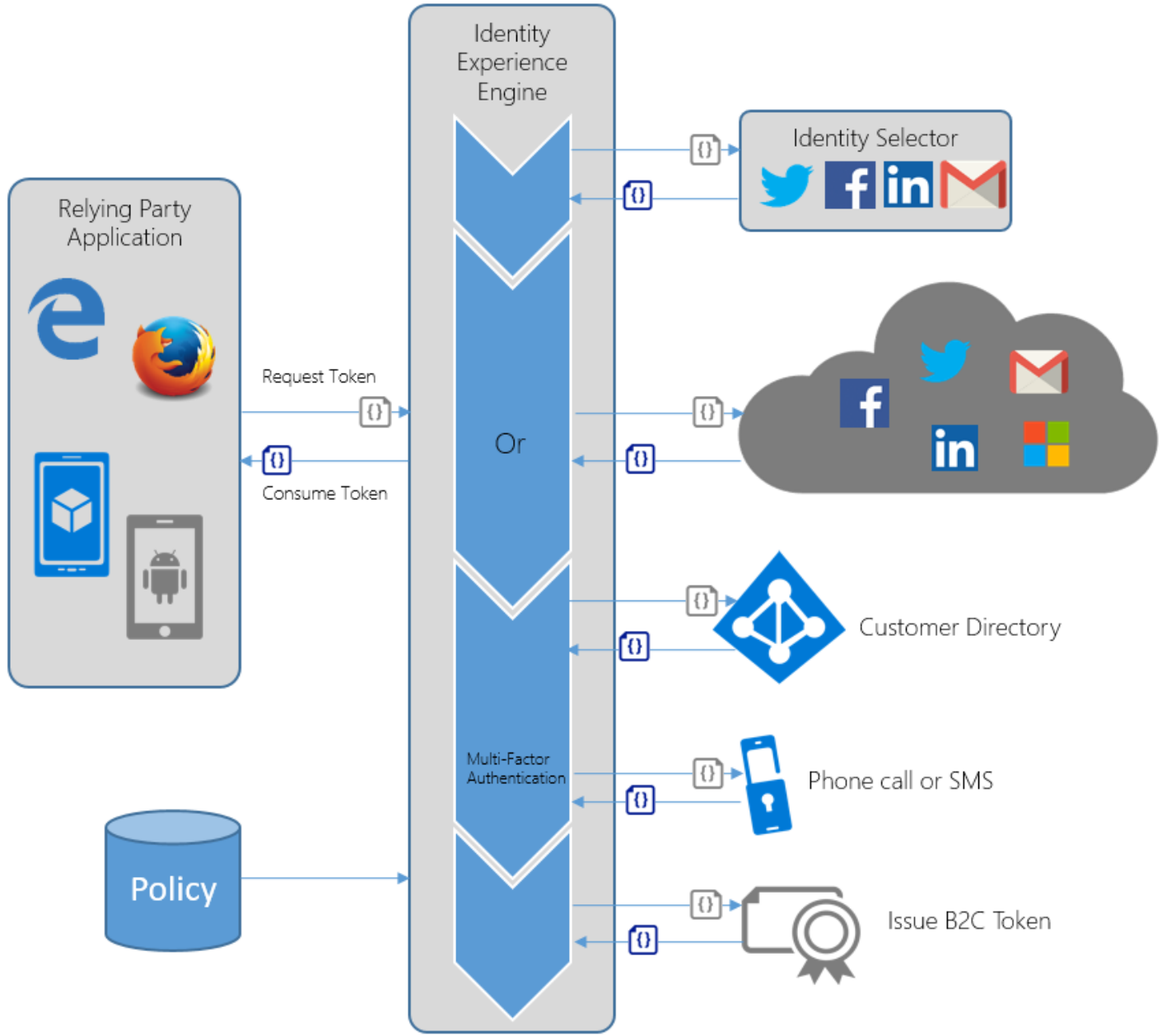
VIDEO

Flog my blog

Identityblog.com

Lost in translation

It was pretty exciting to start posting again and once more feel like part of the *twitoblogosphere*, or digital reality, or whatever we're calling it. I have to admit to not a small amount of regret for having neglected my blog for so long – in spite of my long list of "excellent reasons" for having done so. I was therefore prepared for a nudge or two from my friends, like Mary Branscombe's:


Identity Experience Engine
Relying Party Application
Request Token
Consume Token
Or
Identity Selector
Customer Directory
Multi-Factor Authentication
Phone call or SMS
Policy
Issue B2C Token

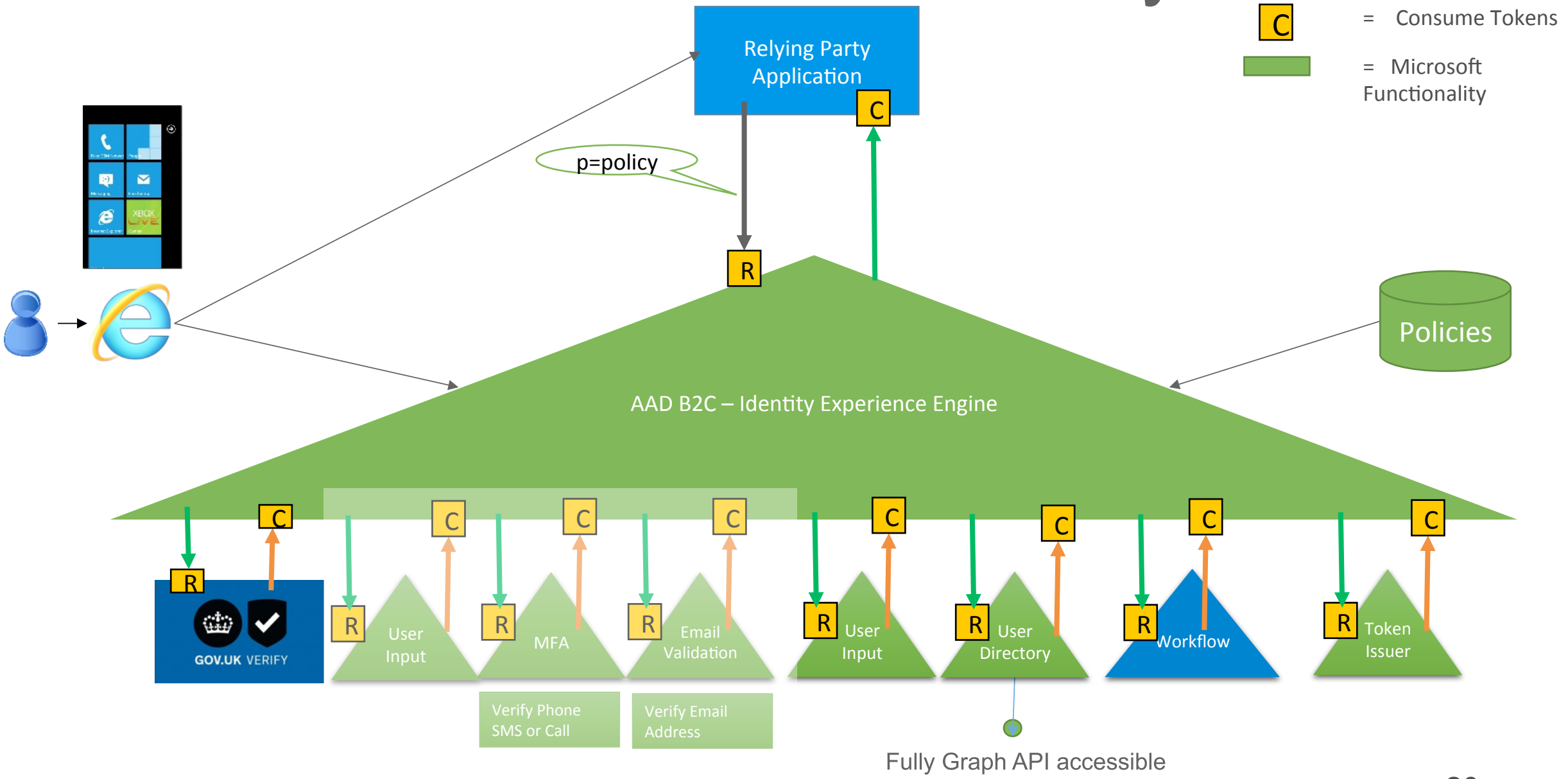
B2C Premium – create your own trust framework

- All the requirements of an Identity “Hub”
- Ability to manage data on behalf of trust framework members (optional)
- Create your own trust framework through declarative policies

Full flexibility to define and configure:

- User Journeys
- Identity Providers
- Relying Parties
- Authentication Requirements
- Multifactor orchestration
- Integration with Claims Verifiers
- Shared Schema and mappings to participants
- Claims Transformations and Data Minimization
- Blinding and encryption
- Claims Storage
- Protocol Conversion (SAML, Oauth2, and OpenIdConnect)

PremiumTrust Framework Policy



How much will it cost?

- B2C will be charged on a consumption basis. You pay only for the resources you use.
- There will be three meters, billed monthly:
  - Number of user accounts in the directory
  - Number of authentications
  - Number of multi-factor authentications
  - More: Azure.com pricing page.

How much will it cost?

STORED USER/MONTH	PRICE
First 50,000	Free
Next 950,000	$0.0011
Next 9,000,000	$0.0009
Greater than 10,000,000	$0.0008

AUTHENTICATIONS/MONTH	PRICE
First 50,000	Free
Next 950,000	$0.0028
Next 9,000,000	$0.0021
Greater than 10,000,000	$0.0014