If customer accounts were cars...
If customer accounts were oil...
It’s time to clean up the environment

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 | Nov 2, 2016 at 15:00 GMT

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 information and assets but whether they want to lose customer and consumer trust.

By Mary Branscombe | Nov 2, 2016 at 15:00 GMT

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.

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)

<table>
<thead>
<tr>
<th><strong>86%</strong></th>
<th>Azure AD manages identity data for &gt;5 M organizations</th>
</tr>
</thead>
<tbody>
<tr>
<td>of Fortune 500 companies on Microsoft Cloud (Azure, O365, CRM Online and PowerBI)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>1 Trillion</strong></th>
<th><strong>50 M</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Azure AD authentications since the release</td>
<td>Office 365 users active every month</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>More than <strong>500 M</strong> objects hosted on Azure Active Directory</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>&gt;1 Billion</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>authentications every day on Azure AD</td>
</tr>
</tbody>
</table>

Trillion Azure AD authentications since the release of the service

Office 365 users active every month
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 policy:

- **Base Policy**
  - Policy from which this one inherits

- **Building Blocks**
  - Claims Schema
  - Claims Transformations
  - Content Definitions

- **Claims Providers**
  - Federation Metadata

- **User Journeys**
  - Sequence of workflow steps
  - Sequence and redirection of claims providers

- **Relying Party**
  - Requested Output Claims

- Your customer. Your Experience!

- Mashable flows!
  - Bring your own Identity
  - CSPs, Idps, Attribute providers and verifiers
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

Trust Framework Operator
Runs the Trust Framework as a business, legal and social entity

Identity Experience Engine Operator
Compute and operational services delivering the policies
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
Customer Admin Portal

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

User data schema with default and custom parameters
2015 Launch of iOS, Android, WP apps
Real Madrid F.C. has 450 mn fans worldwide
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:

Sean Deuby and 6 others follow

ScaryMary Branscombe @marycbuk · Nov 2
So @alex_a_simons got @kim_cameron to blog again; I’m feeling quite nostalgic ;)

Love it!
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

AAD B2C – Identity Experience Engine

Relying Party Application

C

R

p=policy

R

Request Token

C

Consume Tokens

Microsoft Functionality

Policies

R

C

User Input

User Directory

Workflow

Token Issuer

GovUK Verify

User Input

MFA

Email Validation

Verify Phone
SMS or Call

Verify Email
Address

Fully Graph API accessible
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](https://azure.com/pricing).
# How much will it cost?

<table>
<thead>
<tr>
<th>STORED USER/MONTH</th>
<th>PRICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>First 50,000</td>
<td>Free</td>
</tr>
<tr>
<td>Next 950,000</td>
<td>$0.0011</td>
</tr>
<tr>
<td>Next 9,000,000</td>
<td>$0.0009</td>
</tr>
<tr>
<td>Greater than 10,000,000</td>
<td>$0.0008</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AUTHENTICATIONS/MONTH</th>
<th>PRICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>First 50,000</td>
<td>Free</td>
</tr>
<tr>
<td>Next 950,000</td>
<td>$0.0028</td>
</tr>
<tr>
<td>Next 9,000,000</td>
<td>$0.0021</td>
</tr>
<tr>
<td>Greater than 10,000,000</td>
<td>$0.0014</td>
</tr>
</tbody>
</table>