E-Commerce Anti-Fraud Measures: Balancing Security and Customer Friction

Karthik Kotha
Senior Software Engineering Manager
Kroger

About Me

- Lead Customer Identity, Fraud, & Privacy Teams at Kroger
- Full stack software dev experience with Vue.js, Angular, Java, and Node

UIC UNIVERSITY OF ILLINOIS CHICAGO

Northwestern | Kellogg

slalom

JPMORGAN CHASE & CO.

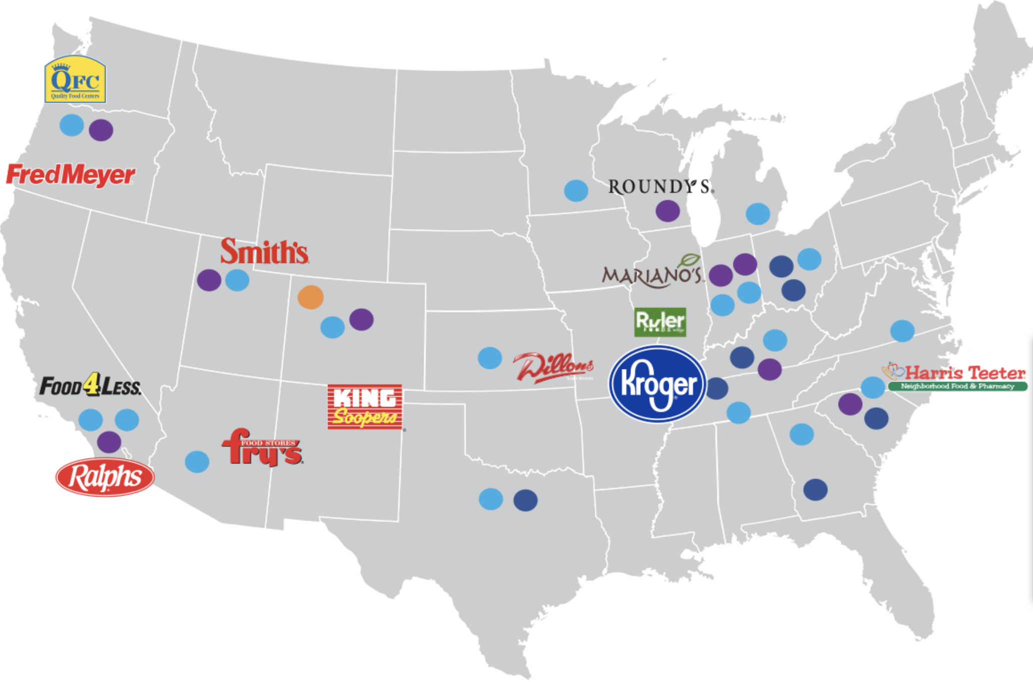
UPTAKE

ShipBob

Kroger

About Kroger

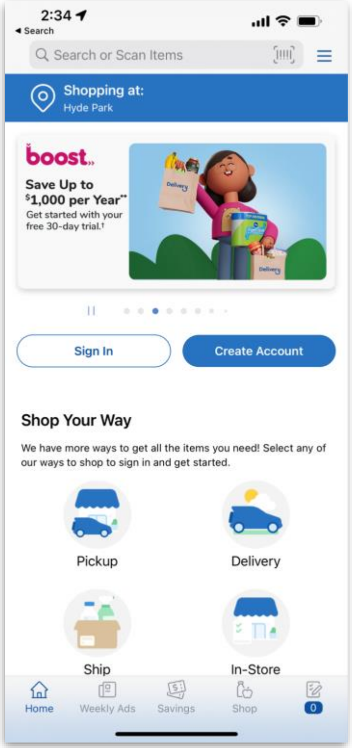
- $148.3 billion in revenue (2022)
- 2,750 grocery retail stores
- 11M Customers Daily
- Pickup & Delivery covers 98% of US Households
- ~70M+ Digital Accounts



84.51°
Baker's
fry's
Dillons
Copps
Food 4 Less
Smith's
Gerbes
Kroger
Kroger
Specialty Pharmacy
Kroger
Corporate Brands & Manufacturing
Kroger Personal Finance
Pay Less Super Markets
King Soopers
JayC Food Stores
Home Chef
QFC
Fred Meyer
City Market
Foods Co.
Pick 'n Save
Vitacost
Harris Teeter
Neighborhood Food & Pharmacy
Ruler Foods
metro market
Fred Meyer Jewelers
Owen's
Ralphs
The Little Clinic
Roundy's
Mariano's

Agenda

- North Star Metrics
- Roadmap
- Email Verification
- Migration to Azure AD B2C
- Conditional Access
- Lessons Learned



Save Up to $1,000 per Year**
Get started with your free 30-day trial.†

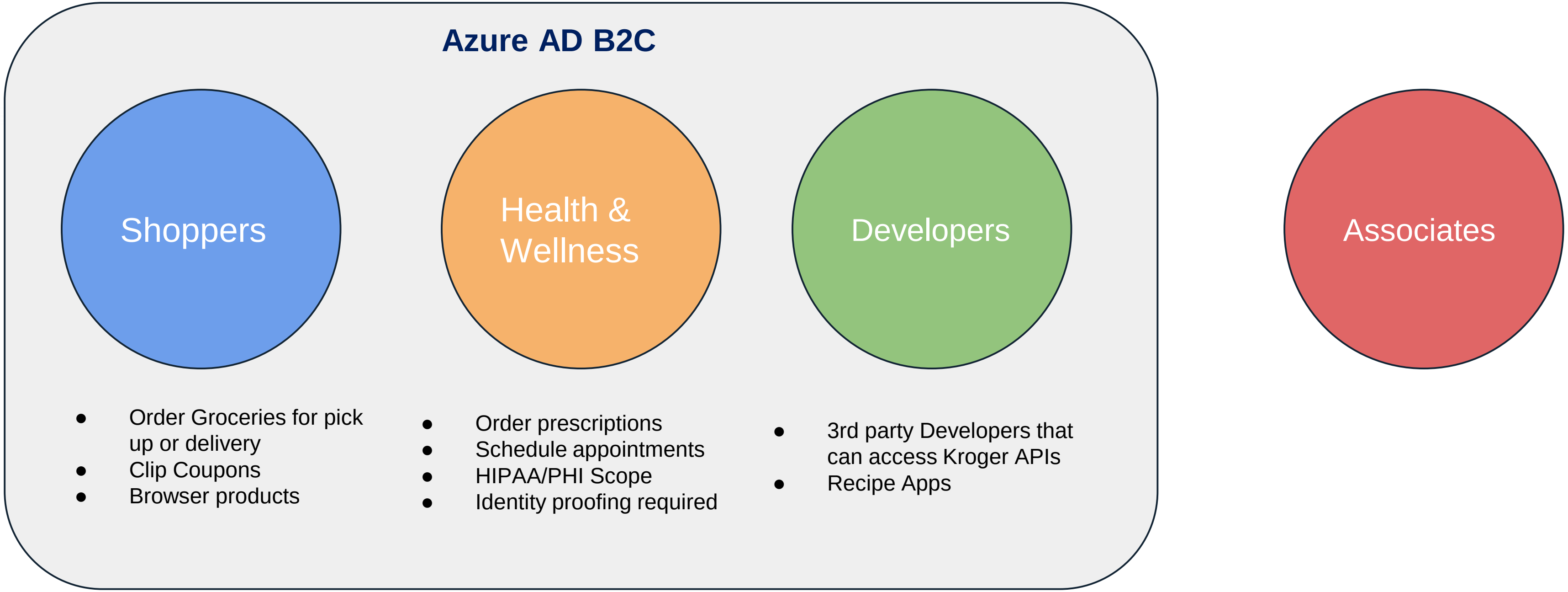
Shop Your Way

We have more ways to get all the items you need! Select any of our ways to shop to sign in and get started.

North Star Metrics

- No mass password resets
- No revenue impact | Zero down time
- Cannot significantly increase call center volume
- 100% of active users should be Email verified
- Enable Email/Phone factor MFA capability
- Reduce Credential Stuffing attacks
- Reduce Chargebacks, ATOs, and Multi-Accounting
- Privacy and HIPAA compliant

CIAM Profiles



Azure AD B2C

Shoppers

- Order Groceries for pick up or delivery
- Clip Coupons
- Browser products

Health & Wellness

- Order prescriptions
- Schedule appointments
- HIPAA/PHI Scope
- Identity proofing required

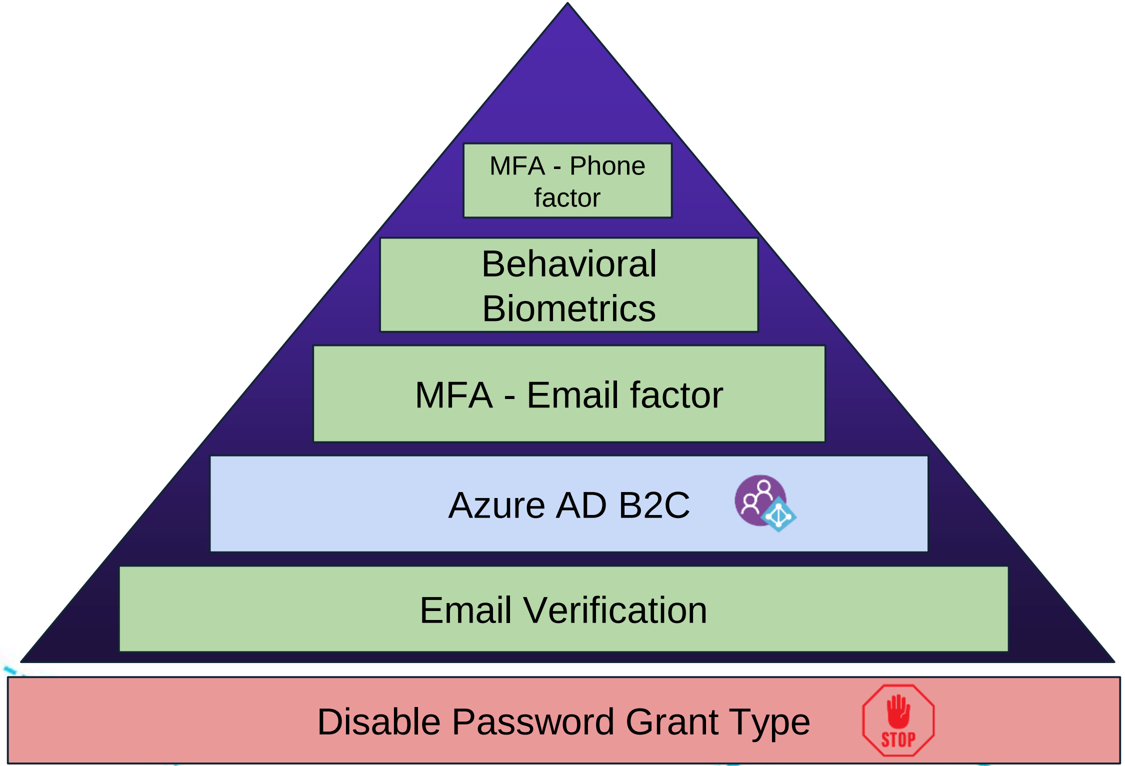
Developers

- 3rd party Developers that can access Kroger APIs
- Recipe Apps

Associates

Our Journey

Accounts Anti-Fraud Foundation



MFA - Phone factor

Behavioral Biometrics

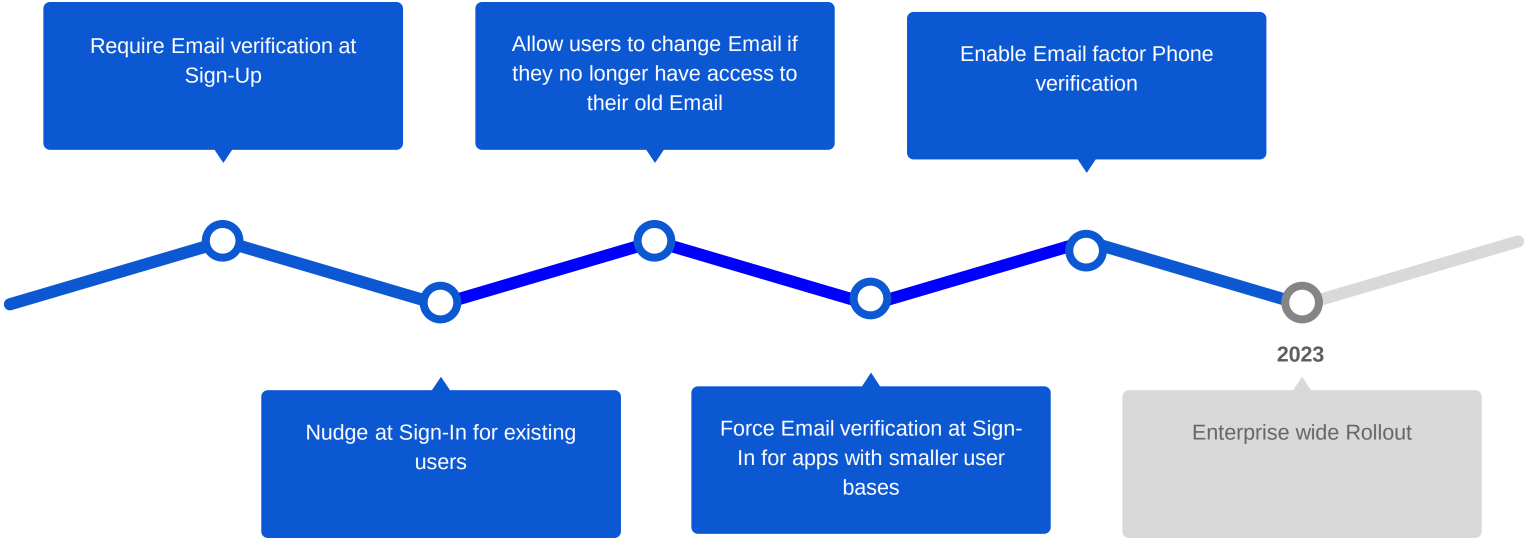
MFA - Email factor

Azure AD B2C

Email Verification

Disable Password Grant Type

Email Verification



Require Email verification at Sign-Up

Nudge at Sign-In for existing users

Allow users to change Email if they no longer have access to their old Email

Force Email verification at Sign-In for apps with smaller user bases

Enable Email factor Phone verification

2023

Enterprise wide Rollout

Azure AD B2C

Why migrate to B2C?

Existing AuthN/AuthZ:

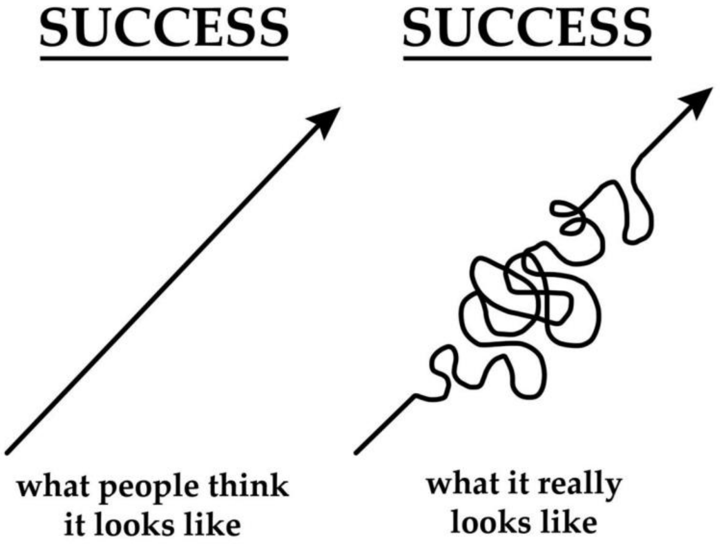
- Hodge-podge of custom built Token & Session Cookie based Auth
- Very hard to work with, devs scared to touch anything related to Auth
- Difficult to find the boundaries of AuthN and AuthZ
- Insecure

Auth w/ Azure AD B2C

“Friends don’t let friends build their own Auth” - An Okta T-Shirt

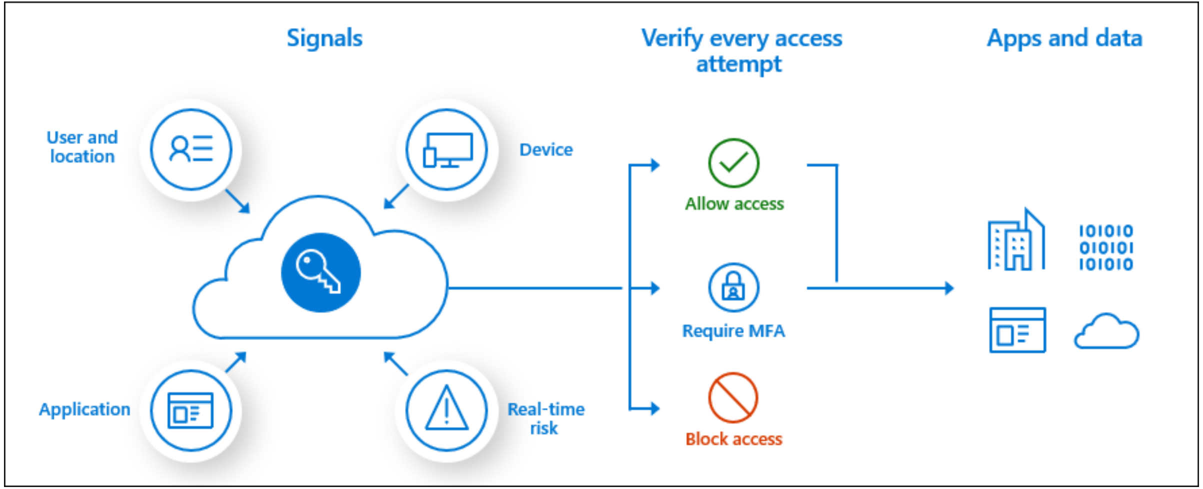
- Universal Login capability with SSO
- Built-in MFA capabilities
- Microsoft Auth Libraries (MSAL) makes auth approachable for devs with no identity experience
- Allows integration with other vendors for identity proofing, fraud, and etc
- Built-in Social Sign-in capabilities

How to get all apps onto B2C?



- Build Just-In-Time (JIT) migration
  - Migrate without users even noticing!
- Dual password writes
  - Allows us to stagger the launch and avoid a big bang release

Adding targeted friction



- Use a vendor for your fraud engine. Vendors can see user behavior across companies, which is very valuable.
- Downsides:
  - Some vendors' code to enable this can be very big and may slow down your entire app
  - Be thoughtful when and where to add friction

MFA

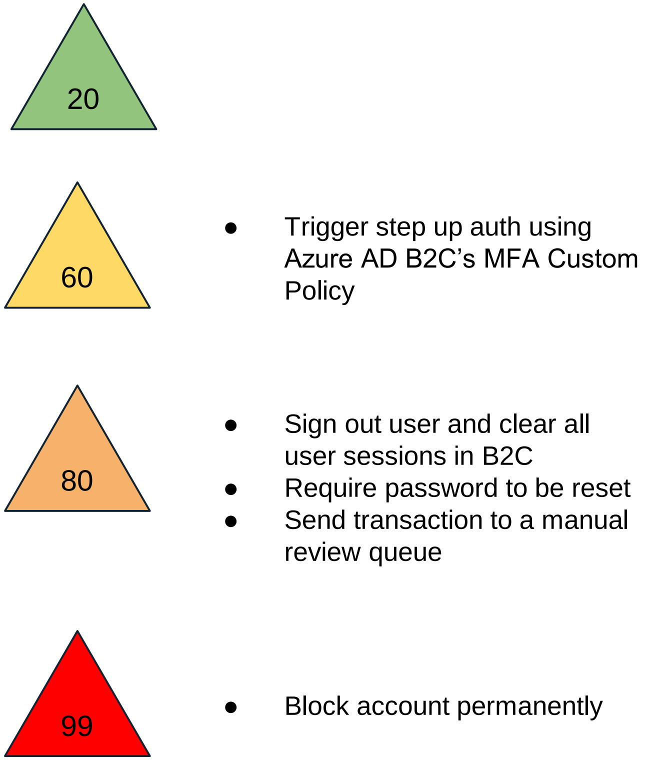
PASSWORD
******
MULTIFACTOR AUTHENTICATION
LOGGED IN
NIST National Institute of Standards and Technology U.S. Department of Commerce
www.nist.gov

- Ad-Hoc: clients decide when to send user through an Azure AD B2C MFA flow for step up Auth
  - B2C makes this easy by providing a MFA only policy
- Trusted Device: Require at Sign-In on a new device

Conditional Access

Signals

- Sign-In on new device/location
- UBA
- Type of items in cart
- Modifying credit cards
- Modifying delivery address and other profile data
- Account create date
- EMail enumeration



20

60

- Trigger step up auth using Azure AD B2C’s MFA Custom Policy

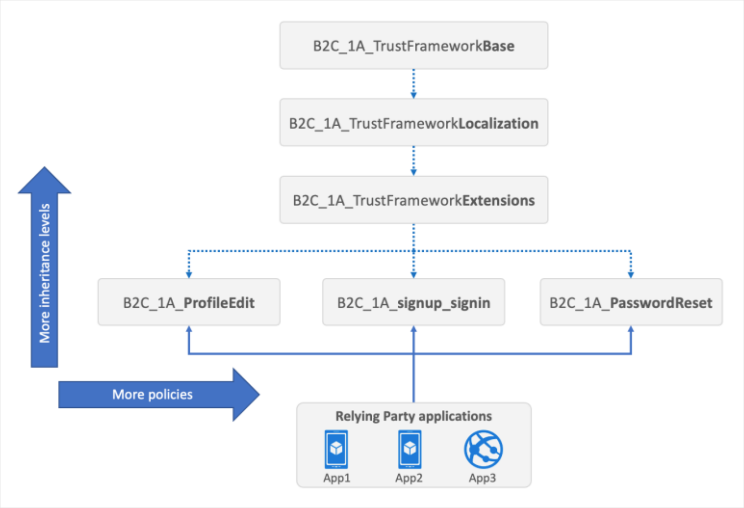
80

- Sign out user and clear all user sessions in B2C
- Require password to be reset
- Send transaction to a manual review queue

99

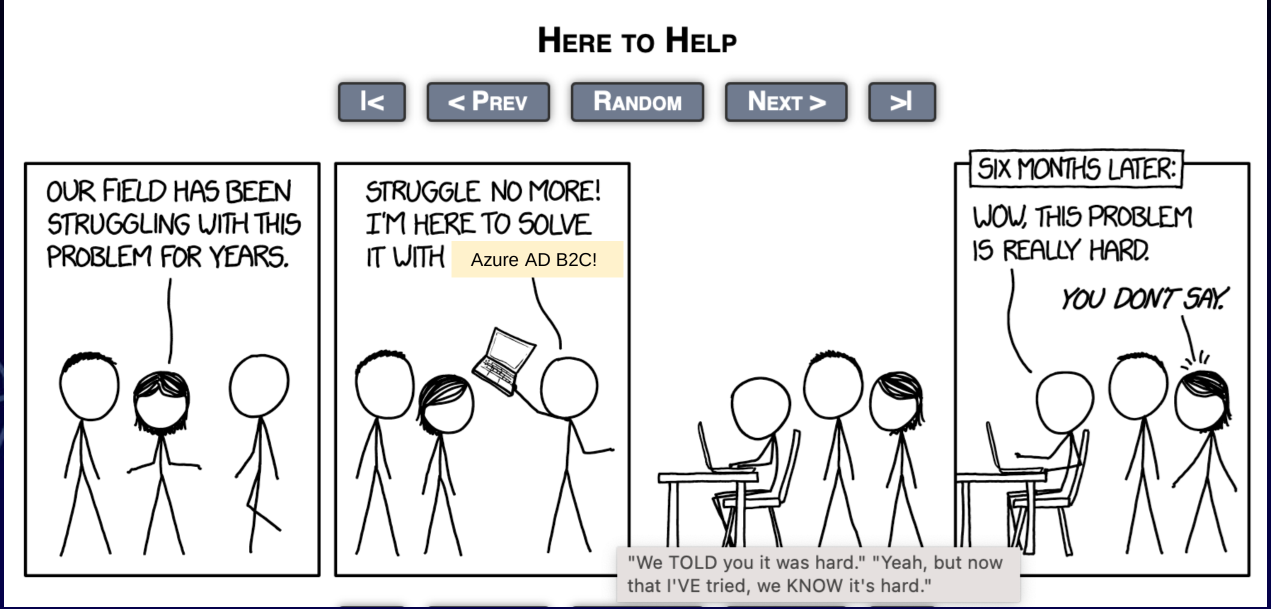
- Block account permanently

Lessons Learned with Azure AD B2C


B2C_1A_TrustFrameworkBase
B2C_1A_TrustFrameworkLocalization
B2C_1A_TrustFrameworkExtensions
More inheritance levels
B2C_1A_ProfileEdit
B2C_1A_signup_signin
B2C_1A_PasswordReset
More policies
Relying Party applications
App1
App2
App3

- XML based custom policies are hard to work with and maintain
  - Not very approachable for developers
  - No UI editor like Auth0
- No passkeys support
- Single Sign-On is a powerful feature
- We don’t have to build our own IdP
- Able to integrate with existing and new vendors

Thank You!



Here to Help

|<
< Prev
Random
Next >
>|
OUR FIELD HAS BEEN STRUGGLING WITH THIS PROBLEM FOR YEARS.
STRUGGLE NO MORE! I'M HERE TO SOLVE IT WITH Azure AD B2C!
SIX MONTHS LATER:
WOW, THIS PROBLEM IS REALLY HARD.
YOU DON'T SAY.

"We TOLD you it was hard." "Yeah, but now that I'VE tried, we KNOW it's hard."

Karthik Kotha

Senior Manager - CIAM
Kroger