Intro to the Identity Experience Engine

Kim Cameron, Microsoft Architect of Identity
ISSE Paris November 2016
Intro to the Identity Experience Engine (IEE)

• Withering away of the enterprise domain boundary means identity tech must evolve
  • From: the app-to-domain federation model
  • To: app-to-world federation model

• Different app users will “bring their own identities” of differing believability
  • Loss of domain-era single truth mean apps need an engine that can orchestrate user experiences to
    • Take advantage of identity providers
    • Augment claims by picking them up from specialized “claims providers”
    • Assemble, mash and arbitrate claims to deliver a claimset the app can “act on”
    • Apply authorization policies based on the claims
    • Invoke additional processes and workflows to strengthen confidence and relationships
Identity Experience Engine (IEE)

- Architecturally, the IEE is a new piece that operates on behalf of the app
  - IEE does not replace IdPs but rather allows apps to live in a multi-IdP world

IEE exposes the underlying technology used in the Azure B2C product now in GA – we have been collaborating for 4 years with select customers to define the general purpose engine which we previously referred to using the codename “CPIM”
Handling the big shift towards B2B and B2C

• "IDaaS for Customers and Citizens"
  • It’s about providing all IAM functions an application needs to handle a customer/citizen audience

• "IDaaS for Partners & Supply Chain"
  • It’s about providing all IAM functions an application needs to handle their partners and supply chain

• Combining the two capabilities allows to adequately sustain multisided platforms (MSPs) initiatives
IEE adds a “User-Driven” Identity Lifecycle Model

- **Administrator Managed**
  - Identities are created, updated and deleted by administrators through the identity management portal.
  - Administrative actions are constrained by OIM governance policies

- **Federation Managed**
  - Identities are created and deleted in one or more external systems such as on-premises AD or HR systems. The identities are then synchronized into the cloud using AAD Connect or Microsoft Identity Manager – and thereafter remain in sync.

- **User Driven**
  - People create and manage aspects of their identities – and request entitlements – through User Journeys based on policy
  - Users in approval roles approve new identities, attribute changes and entitlements through portals or IES User Journeys implementing policy

- **Externally Provisioned**
  - Systems create and manage OIM identities using the Microsoft Graph or the SCIM protocol
    - Provides integration with 3rd party governance systems like Sailpoint
    - OIM can also provision into external systems based on its provisioning policies
How we are factoring IEE in AAD
Dimensions of IEE User Journeys

- Trust Framework Policy
- Interactive Experiences
- Claims-driven Logic
- Claims Exchanges
- Persistence
- Reliability
- Security
- Communities of Interest (reuse)
- Inheritance and refinement
IEE Journeys help companies create and enhance relationships with customers, partners and employees. And in government, IEE Journeys can empower citizen identity.

By way of example, here are some IEE Journeys created by a national government - as experienced by the citizen (i.e. the interactive dimension)
Please read the privacy statement
Please take a moment to review our new Privacy Statement.

GovID Privacy Statement and Cookies

Any personal data you volunteer will be used for the purpose for which you supply it and will be treated with the highest standards of security and confidentiality, strictly in accordance with the Data Protection Acts 1988-2003, the Social Welfare Consolidation Act 2005 (as amended) and applicable PII directives. It will only be shared, if necessary, with other Government Departments/Agencies, the Department’s servants and agents in accordance with law.

This statement relates to our privacy practices in connection with this website. Some technical terms used in this statement are explained at the end of this page.

Data Protection Acts

By clicking ‘I Agree’ you state that you agree to the terms of the privacy statement.
Register

A verification code has been sent to your specified email address. When you have received the email containing the verification code please copy it into the 'Verification Code' field below and click 'Verify Code'.

EMAIL ADDRESS

Once you have entered your email address you will need to request a verification code by clicking the 'Send Verification Code' button.

![Verification Code Input Field]

[Verification Code] [VERIFY CODE] [RESEND CODE]

[PROCEED] [QUIT]
Register

1. PRIVACY STATEMENT  2. VERIFY EMAIL  3. ACCOUNT DETAILS  4. VERIFY PHONE  5. COMPLETE

Please note that all fields are mandatory

FIRST NAME

LAST NAME

PASSWORD

Your password must have a minimum of 8 characters, maximum of 16 characters and contain at least 3 of the following: lowercase characters, uppercase characters, numbers (0-9), and one or more of the following symbols @ # $ % ^ & * ( ) [ ] { } | ; : . , _ - = `[ ]` { } ": ; , ", ", , ", , 

CONFIRM PASSWORD

ALTERNATE EMAIL ADDRESS

We require an alternate email address so that you can recover your account if you forget your password. If you don’t have an alternate email address, please create one with an email provider.

PROCEED  QUIT
Register

Self Asserted With Phone Verification

In order to complete your registration, you will need to provide a mobile phone number to which we can send a verification code. We will use your phone number for Two Factor Authentication (2FA) to secure functionality within your account. Please provide your country code and mobile phone number below and click the 'Send Verification Code' button to receive a text message with a verification code.

Somewhere (+55)

A verification code has been sent to your specified mobile phone number. Please copy it into the 'Verification Code' field below and click the 'Verify Code' button, or send a new code.
Digital Id created and returned

GovID

Register

GovID Basic registration complete

You are now registered with a GovID Basic account.

To access advanced services you will need to upgrade to a GovID Verified account.

Access the following services:

- MYWELFARE
- JOBS
Registration is one journey amongst several through which citizens manage their own identities and interact with government departments.

The Government Trust Framework is implemented through a set of User Journeys shared by Government applications:

- Register
- Login
- Login SMS
- Manage
- Verify
The Claims Exchange Backend Dimension

Claims Exchanges

Consent Recording
User provides name etc
Search for User with the same email
Azure AD Store
The Claims Exchange Backend Dimension
User Provides Email
User provides name etc
Phone Factor validation Module
User Provides Phone
Create the citizen record
Azure AD Store
If new email
Self Asserted Provider
Return claims
Self Asserted Provider
Return objectid and claims if match found
Self Asserted Provider
Return claims
Self Asserted Provider
Return claims
Self Asserted Provider
Return objectid and claims if match found
Search for User with the same email
Email validation Module
Create the citizen record
The Developer Dimension: Simplicity, Safety

One line OAuth2 or SAML redirect

https://login.microsoftonline.com/tenant.onmicrosoft.com/oauth2/v2.0/authorize?p=B2C_1A_Registration
&client_id=6b5474c4-0f28-4b10-b7ad-69dee3ab0380
&nonce=defaultNonce&
&redirect_uri=http%3A%2F%2Flocalhost%2F
&scope=openid
&response_type=id_token
&prompt=login

Response: json dictionary containing the user’s claims
Security and Reliability

• The Application does one “redirect” to AAD and everything else materializes through the service

• Professionalizes security and privacy protection
  • Applications control visuals, IEE provides security and privacy
  • Example: badly written applications cannot create CORS or javascript attack vectors that endanger the authorization/authentication system as is normally possible

• Provides 24/7 operational guarantees with multi-site redundancy and JIT scaleout
Other User Journeys in the Government Trust Framework
Search for your next job

Search for a job:

- All Categories
- Location
- Keywords e.g. Nurse, Supervisor

5189 LIVE JOBS TODAY

- Indian Executive Curry Chef
  - COMPANY DETAILS CONFIDENTIAL

- Tattoo Artist
  - WILDCAT INK

- Property Accounts Administrator
  - COMPANY DETAILS CONFIDENTIAL

- Senior Sales Consultant

- Coffee Shop Assistant/ Cleaner

- Caretaker/ Maintenance Person

[VIEW ALL LIVE JOBS]
In order to log into your GovID Verified account, you need to provide a code which will be sent via text to the following phone number we have on record for you (some digits masked for security).

**** **** 575 - Mobile Phone

[SEND VERIFICATION CODE] [QUIT]
Manage Account

Verify Basic Account
Verify your account by requesting a GovID Verification Code to either your Address or to a phone number that was verified in a Local Office.

Update Phone Number
Update your phone number which is used for account recovery and Two Factor Authentication on GovID Verified accounts.

Change Password
Change your password to increase the security on your account.

And more User Journeys
Based on Trust Frameworks

• Benefits of Trust Framework
• Show how Trust Frameworks support communities of interest like a government
• Claims driven logic
• Inheritance and refinement, like the journeys shown here
Do you need a GovID Verification Code?

In order to access more services you will need to verify your GovID Basic account by providing a GovID Verification Code that we will send to you either by verified phone or post. A verified phone number is a mobile phone number that has been paired with you in person in a Local Office.

Getting a GovID Verification Code

Please select how you wish to receive your GovID Verification Code

Send to:

- Postal Address
- Verified Mobile Phone

OR

I HAVE RECEIVED A CODE BY POST
Linking to Govt Claims Provider
Send a GovID Verification Code to your Verified Mobile Phone

As a security measure we will text a verification code to the mobile phone number we have on record for you. Click the 'Send Verification Code' button to receive a code to the phone number listed below (some digits masked for security).

**** ***75 - Mobile Phone

SEND VERIFICATION CODE  QUIT
In-Person linked to digital Id

Verify Basic Account

Account Verified

Your GovID account is now verified.

To further protect your GovID account, we have added a second level of authentication known as Two Factor Authentication (2FA). Going forward you will be required to provide a code at login that will be sent to your phone. This is mandatory for all verified GovID accounts.

We have the following number on record for your GovID account:

**0951463575 - Mobile Phone**

If this is not the phone number you want to use when logging in, please update your phone number under Manage Account.

Access the following services:

**MyVI**

**Jobs**
Enter card id from in-person meeting

Retrieve custom claims using with the object Id

Azure AD Store

Username / Password

AAD Local IdP

Mark citizen record as verified

Link Digital Id to Gov Id

Azure AD Store

Return claims to the application
Flexibility in Persistence and Claims Sourcing

• Persistence
  • Reads from and writes to any store that supports REST or identity protocols
  • Different attribute sets can live on different stores and be combined
  • Satisfies compliance requirements

• Example:
  • Roles in an existing roles store
  • Different stores in different GEOs
  • PII or Secret claims
Works using Standard Protocols

• Domain-era federation

• Cloud-era federation

(Same protocols with the addition of a “policy” parameter)
Endless examples of uses

Within Microsoft
- MSA
- Azure AD
- Linked In

Federal Apps
- City A Police
- City B Police
- ... 70 other forces
- National Intelligence
- Federal Department

Multi-National Company
- European Employees
- US Employees
- National ID Systems
- Social Networks
- Home Office

Social Networks

National ID Systems
- Aadhar
- Other Verified IDs