

# Open Banking and high assurance identity with IBM Security Verify

3.14.2023

---

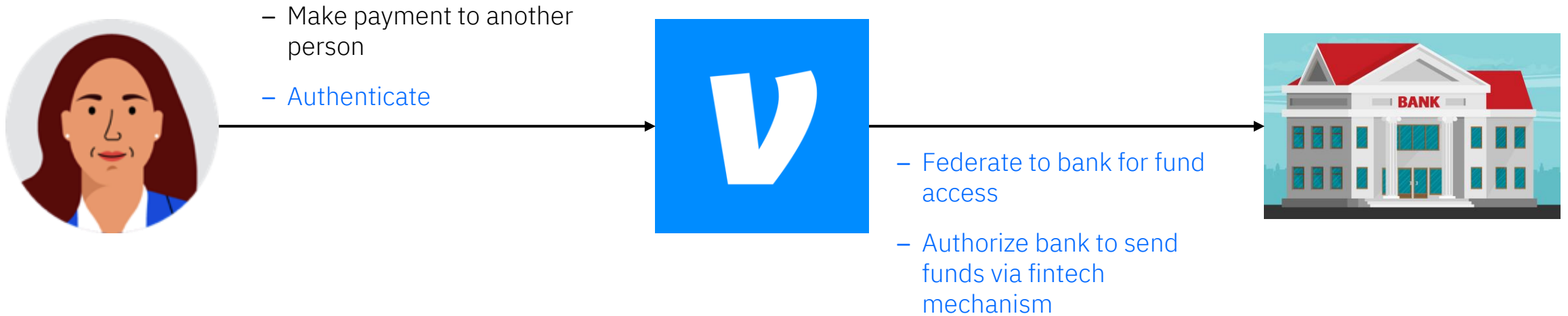
**Vivek Shankar**

Product Architect, IBM Security Verify

**Milan Patel**

Product Manager, IBM Security Verify

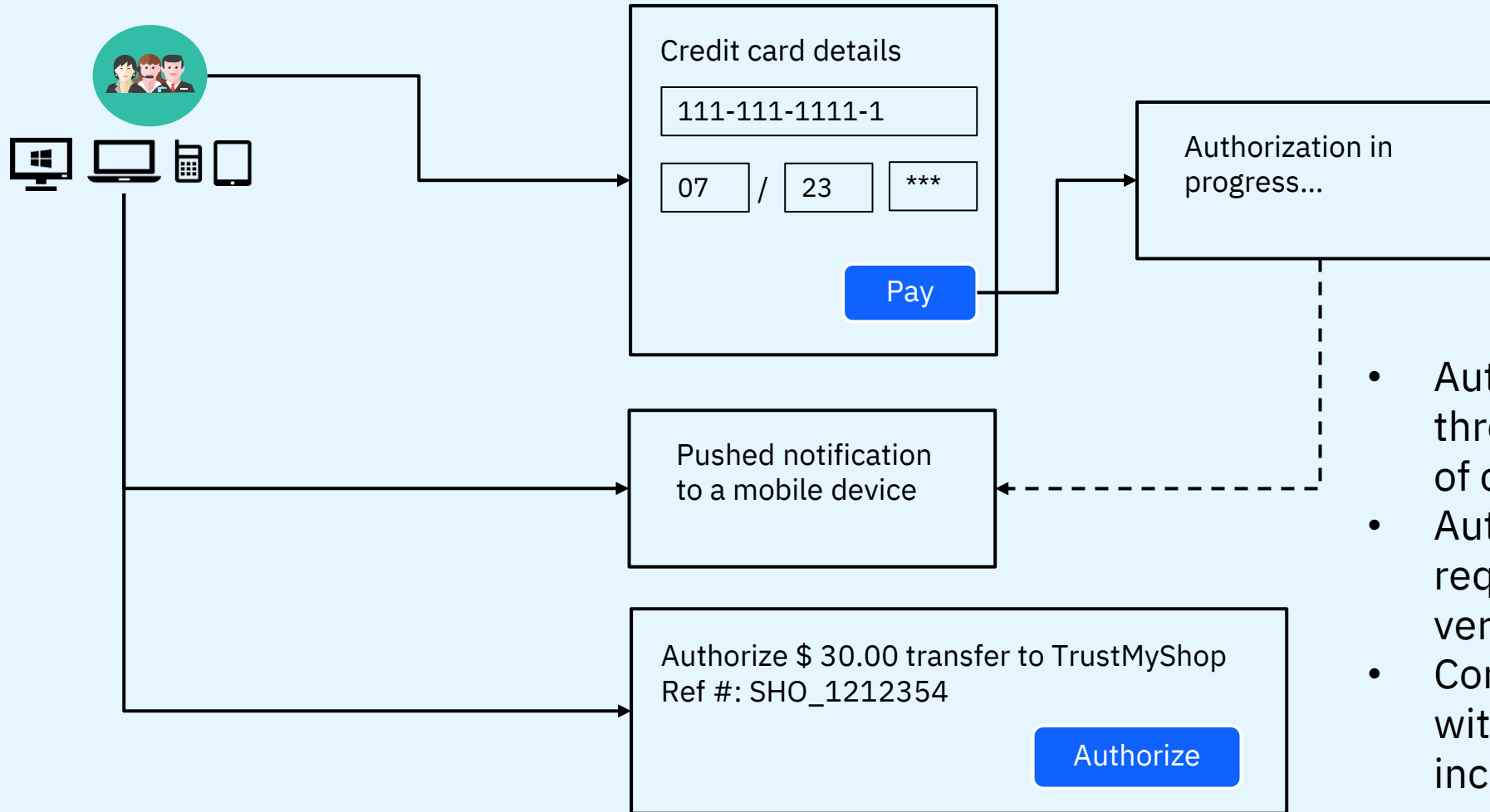
# What is an open banking scenario?



## Identity is the core to open banking flows

- Authorizing sharing of PII (ex: bank account, address, name, etc)
- Requiring consent of use of PII for very specific reasons
- Fully transparency and user awareness of what is shared and why

# Typical end user flow



- Authentication performed through an identity provider of choice – Social or native
- Authorization policy requires possible biometric verification
- Consent statement recorded with reference number included

# Mission: Help securely connect any identity to any resource

## IBM Security™ Verify

### Continuous Access and Governance



Directory, SSO, & MFA



Governance & Lifecycle



Adaptive access w/AI



Privileged access



Passwordless & FIDO2



Privacy and consent management

### Workforce Identity

Drive cloud modernization, technical agility and user productivity

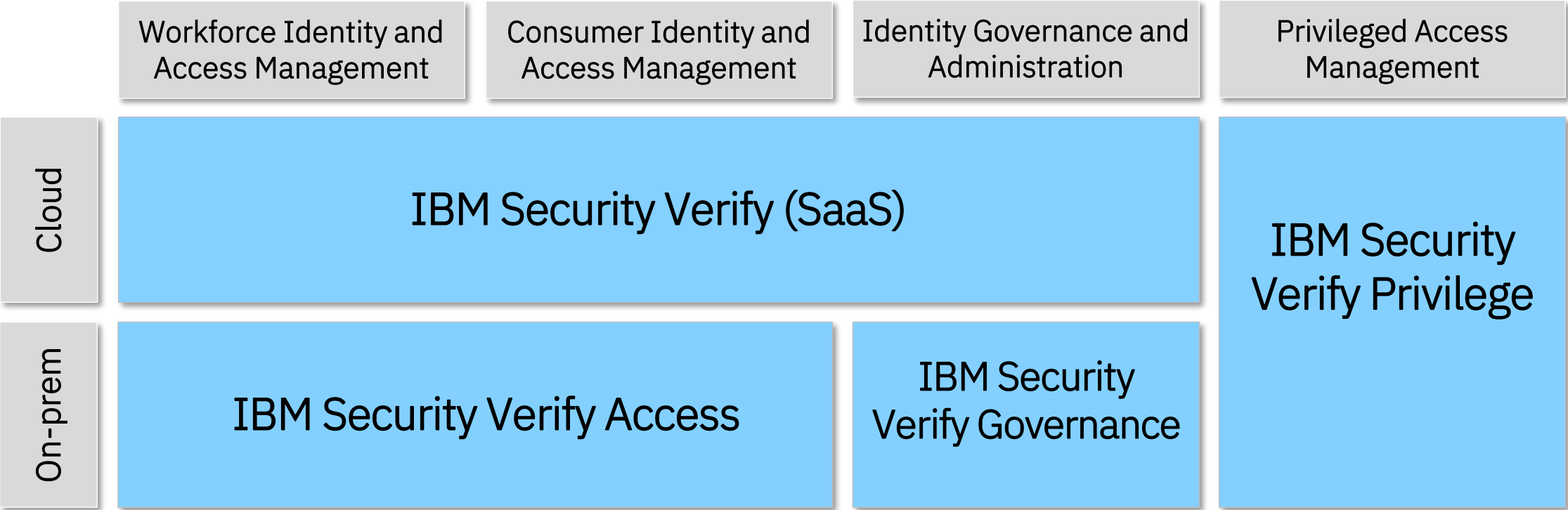
### Consumer Identity

Deliver on-demand, personalized, and trusted experiences

### Hybrid Cloud Resources

Cloud Apps | On-Prem Apps | Mobile Apps | Data  
VPNs | Servers | Databases | Mainframes

# IBM Security Verify Portfolio



# IBM Security Verify Deployment locations and certifications

## Deployment locations

● United States

● Europe

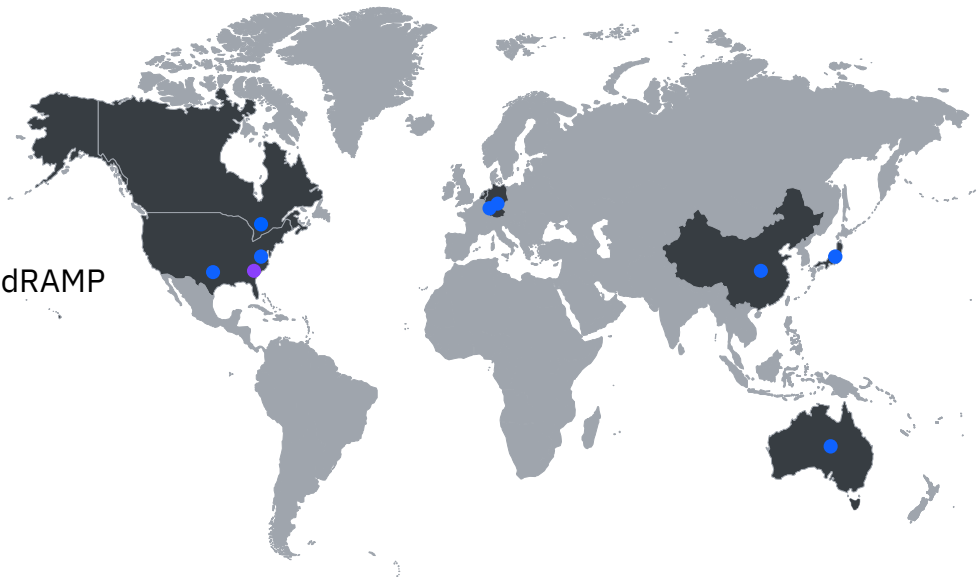
● China

● Government (FedRAMP Ready)

● Japan

● Canada

● Australia



Open Banking profile *certification*:

- mTLS
- Private Key
- PAR
- AU geo certification
- UK geo certification
- JARM
- CIBA – 1H23\*

## Compliance and certifications



PCI DSS Certified  
Since 2020



SOC2 Type 2 & 3 Certified  
Since 2020



ISO 27001 Certified  
Since 2017



HIPAA Ready as of  
August 2022

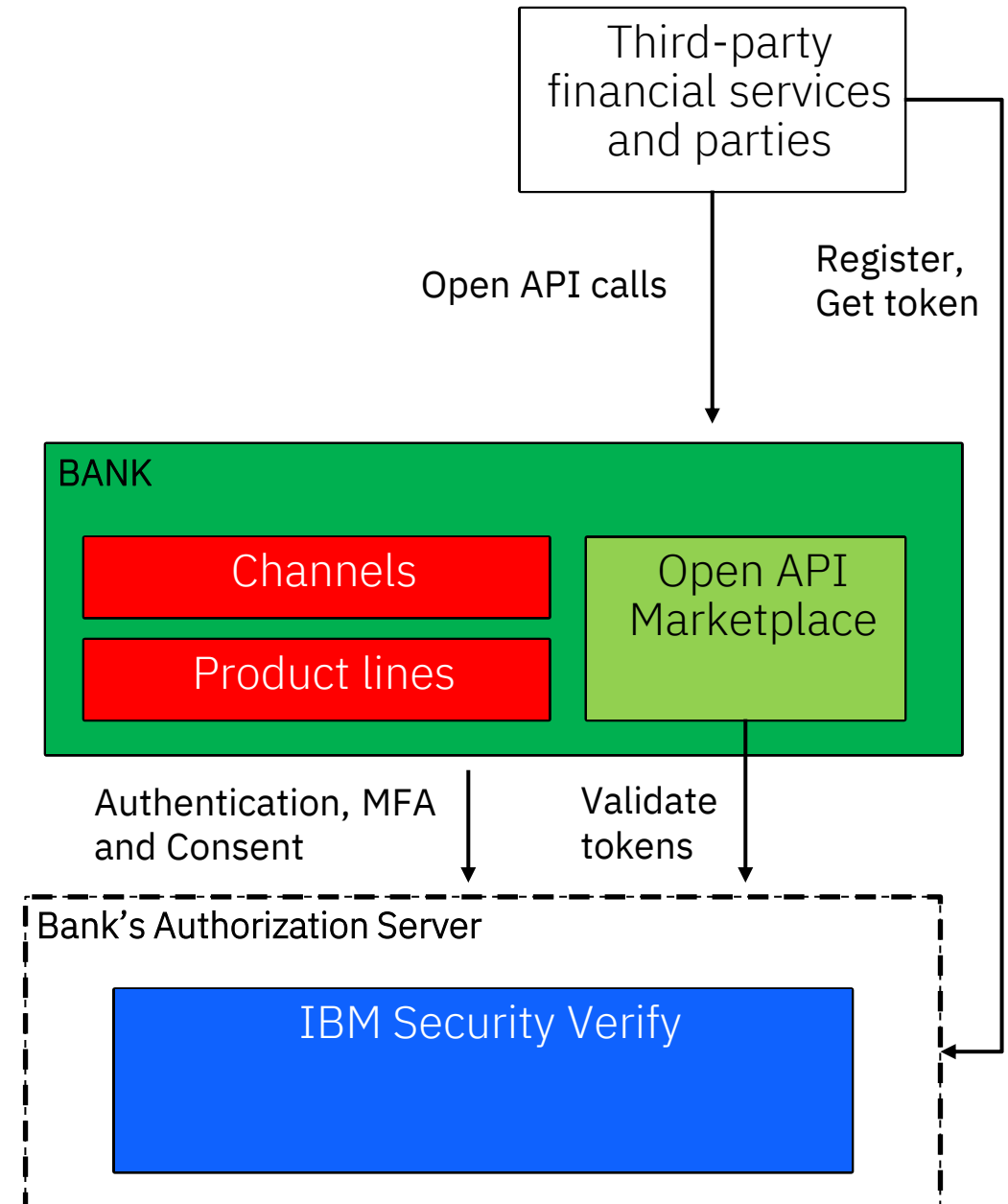


**FedRAMP**

ATO in Progress

# Open Banking needs and drivers

- Focus on how consumer data is shared and used for financial transactions – FinTech with traditional banking.
- Open APIs to facilitate the exchange of data, processes and apps to an ecosystem of developers, vendors and partners.
- Create an irrevocable link between a customer's profile and evidence of consent.
- Open Banking by region
  - EU General Data Protection Regulation (GDPR)
  - European Payment Services Directive (PSD2)
  - UK Open Banking Initiative (OBIE)
  - Australia Consumer Data Rights (CDR)
  - Brazil Security Working Group



# Benefits

## For financial providers and services



Access to  
customer data



Better  
collaboration

## For consumers



Centralized  
authorization



Innovative  
solutions



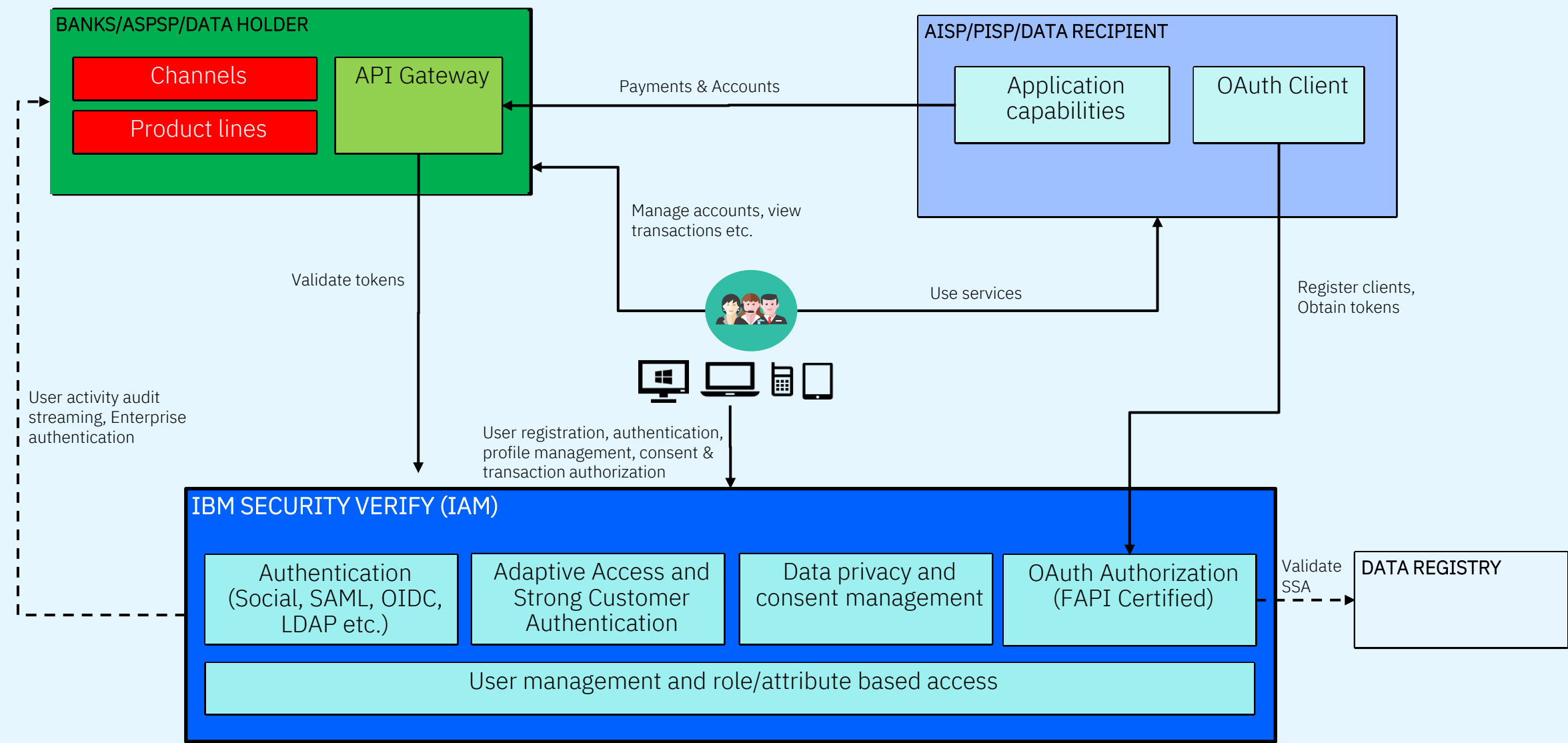
Customer  
delight

Verify helps here

- Standardizes how IdP (Banks) and RPs (FinTech) can securely exchange consumer data (ex: claims and transactions)
- Provides native consumer flows and frictionless authentication experience
- Issues security tokens to enable fine grained access to customer data
- Enforces strong customer authentication and advanced data privacy policies to drive authorization and consent
- Financial fraud detection and ML-driven threat analysis

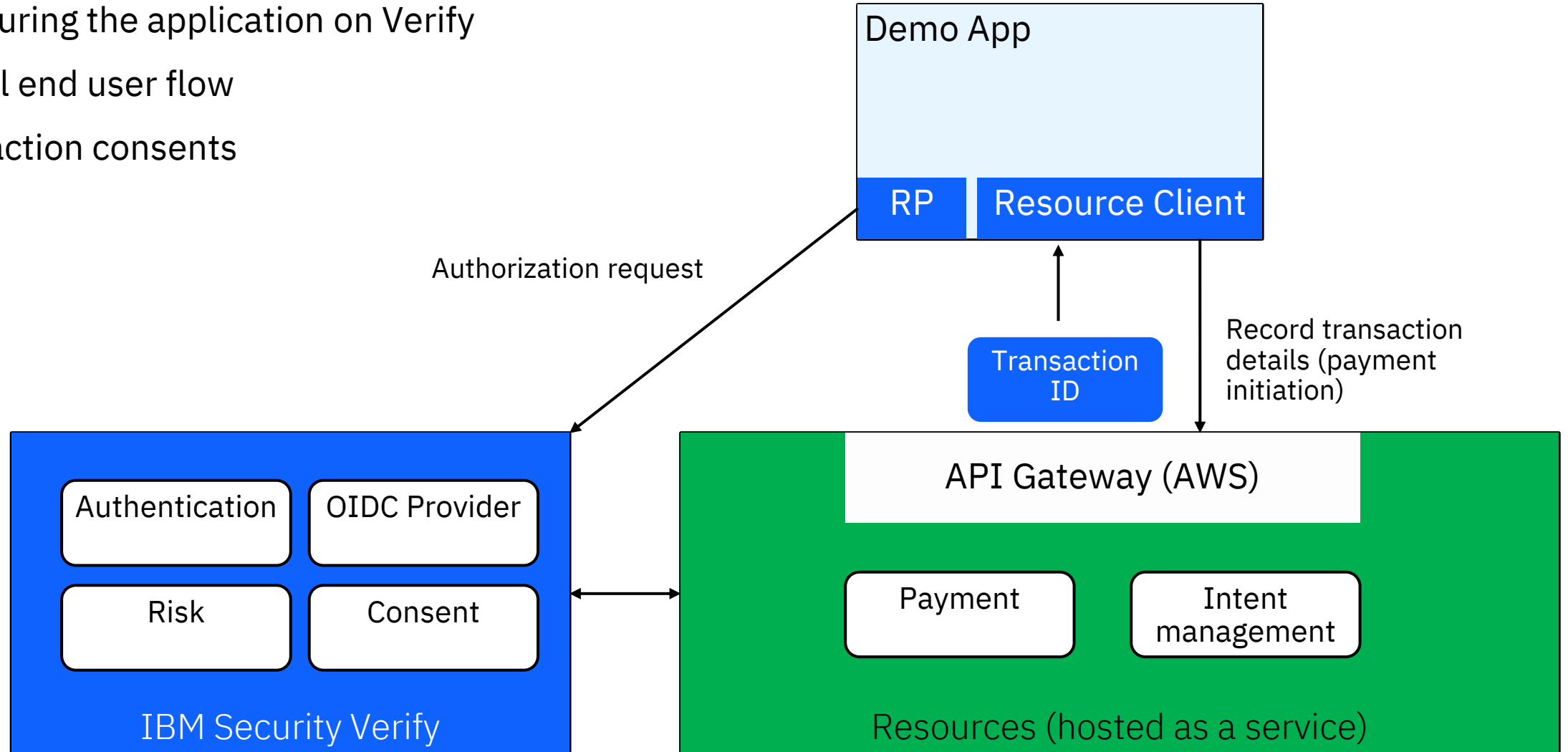


# Example Financial Grade API (FAPI) Blueprint



# Demo with Verify

- Configuring the application on Verify
- Typical end user flow
- Transaction consents



# IBM Security Verify is primed...

- ✓ Out of the box connector to align to the necessary Open Banking profiles
- ✓ Third-party regulation and provisioning
- ✓ Secure token management and issuance
- ✓ User consent
- ✓ Secure customer authentication
- ✓ Financial fraud prevention
- ✓ Threat detection and response

The screenshot displays the IBM Security Verify web interface. On the left is a navigation sidebar with options like Home, Applications, Directory, and Authentication. The main area is titled 'Add application' and shows configuration for 'OpenID Connect for Open Banking'. It includes tabs for General, Sign-on, and API access. A modal overlay in the foreground shows a transaction confirmation from 'Big Blue Bank' for \$1,500, with a 'Verify with Touch ID' prompt and a FIDO logo. To the right, a 'Consent details' panel lists application information, user details, and consent metadata.

**Consent details**

<b>User</b>	
User name	[REDACTED]
Realm	[REDACTED]
<b>Consent details</b>	
Application	Open Banking TPP Demo
Purpose/EULA	Open Banking payment
Attribute/Resource	ibm:openbanking_intent_id
Attribute/Resource value	55fe4385-cc22-411e-8550-93c65810b274
Access type	default
User response	Allow
<b>Additional info</b>	
Client IP	103.252.202.186
Consented on	Oct 6, 2022   11:00 PM SGT
Last modified	Oct 6, 2022   11:00 PM SGT
Consent begins	Oct 6, 2022   11:00 PM SGT
Consent expires	Oct 8, 2022   11:00 PM SGT

# Generic Certifications

FAPI 1 Advanced Final (Generic)									
Organization	Implementation	FAPI Adv. OP w/ MTLS	FAPI Adv. OP w/ MTLS, PAR	FAPI Adv. OP w/ Private Key	FAPI Adv. OP w/ Private Key, PAR	FAPI Adv. OP w/ MTLS, JARM	FAPI Adv. OP w/ Private Key, JARM	FAPI Adv. OP w/ MTLS, PAR, JARM	FAPI Adv. OP w/ Private Key, PAR, JARM
IBM	IBM Security Verify (as of May 2022)	<a href="#">11-Jul-2022</a> <a href="#">view</a>	<a href="#">11-Jul-2022</a> <a href="#">view</a>	<a href="#">11-Jul-2022</a> <a href="#">view</a>	<a href="#">11-Jul-2022</a> <a href="#">view</a>	<a href="#">13-Dec-2022</a> <a href="#">view</a>	<a href="#">13-Dec-2022</a> <a href="#">view</a>	<a href="#">13-Dec-2022</a> <a href="#">view</a>	<a href="#">12-Dec-2022</a> <a href="#">view</a>
IBM	IBM Security Verify Access 10.0	<a href="#">05-Aug-2022</a> <a href="#">view</a>	<a href="#">05-Aug-2022</a> <a href="#">view</a>	<a href="#">05-Aug-2022</a> <a href="#">view</a>	<a href="#">05-Aug-2022</a> <a href="#">view</a>	<a href="#">17-Nov-2022</a> <a href="#">view</a>	<a href="#">21-Nov-2022</a> <a href="#">view</a>	<a href="#">17-Nov-2022</a> <a href="#">view</a>	<a href="#">12-Oct-2022</a> <a href="#">view</a>

Financial-grade API (FAPI) 1.0 Second Implementer's Draft									
These deployments have achieved certifications for the Financial-grade API (FAPI) 1.0 Second Implementer's Draft, as published October 2018, conformance profiles:									
Note: Between FAPI 1.0 Second Implementer's Draft and the publication of the 'Final' revision, the Read/Write profile name was changed from 'R/W' to 'Advanced'.									
Organization	Implementation	FAPI R/W OP w/ MTLS	FAPI R/W OP w/ MTLS, PAR	FAPI R/W OP w/ Private Key	FAPI R/W OP w/ Private Key, PAR	UK-OB R/W OP w/ MTLS	UK-OB R/W OP w/ Private Key	AU-CDR R/W OP w/ Private Key	AU-CDR R/W OP w/ Private Key, PAR
IBM	IBM Security Verify Access 10.0	<a href="#">26-May-2020</a> <a href="#">view</a>		<a href="#">26-May-2020</a> <a href="#">view</a>					

Certified Financial-grade API Client Initiated Backchannel Authentication Profile (FAPI-CIBA) OpenID Providers					
These deployments have achieved certifications for these Financial-grade API Client Initiated Backchannel Authentication Profile (FAPI-CIBA) conformance profiles:					
Organization	Implementation	FAPI-CIBA OP poll w/ MTLS	FAPI-CIBA OP poll w/ Private Key	FAPI-CIBA OP Ping w/ MTLS	FAPI-CIBA OP Ping w/ Private Key
IBM	IBM Security Verify Access 10.0	<a href="#">11-May-2022</a> <a href="#">view</a>	<a href="#">11-May-2022</a> <a href="#">view</a>	<a href="#">11-May-2022</a> <a href="#">view</a>	<a href="#">11-May-2022</a> <a href="#">view</a>

Source: [https://openid.net/certification/#FAPI\\_OPs](https://openid.net/certification/#FAPI_OPs)

# Regional Certifications

## UK Open Banking (Based on FAPI 1 Advanced Final)

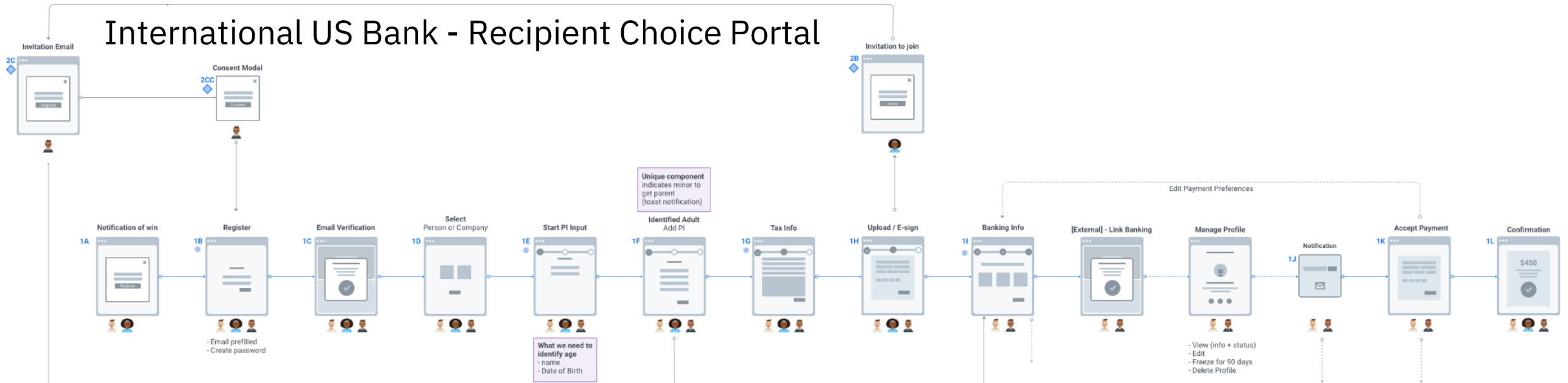
Organization	Implementation	UK-OB Adv. OP w/ MTLS	UK-OB Adv. OP w/ Private Key
IBM	IBM Security Verify (as of May 2022)	<a href="#">12-Nov-2022</a> <a href="#">view</a>	<a href="#">12-Nov-2022</a> <a href="#">view</a>
IBM	IBM Security Verify Access 10.0	<a href="#">27-Oct-2022</a> <a href="#">view</a>	<a href="#">27-Oct-2022</a> <a href="#">view</a>

## Australia CDR (Based on FAPI 1 Advanced Final)

Organization	Implementation	AU-CDR Adv. OP w/ Private Key	AU-CDR Adv. OP w/ Private Key, PAR	AU-CDR Adv. OP w/ Private Key, PAR, JARM
IBM	IBM Security Verify (as of May 2022)	<a href="#">18-Jul-2022</a> <a href="#">view</a>	<a href="#">18-Jul-2022</a> <a href="#">view</a>	
IBM	IBM Security Verify Access 10.0	<a href="#">29-Oct-2022</a> <a href="#">view</a>	<a href="#">28-Oct-2022</a> <a href="#">view</a>	

Source: [https://openid.net/certification/#FAPI\\_OPs](https://openid.net/certification/#FAPI_OPs)

# International US Bank - Recipient Choice Portal



## Background

A US based bank has tasked by a Gaming company to provide capabilities to capture and manage recipient data, and facilitate client payments.

As these recipients may not be bank account holders, they needed a new approach on how to handle consumer identities and collect preferences in regard to their payout routing

## The solution needed to

Capture and authenticate recipient data and payment preference details with a global reach.

Perform risk management and due diligence capabilities such as KYC, Sanction screening and tax implications.

Provide a solution which allows us pay client recipients who are minors and need parental consent

## IBM's value proposition

Accelerate your speed-to-market with proven assets and intellectual property around Identity and Payments solutions

Reduce delivery risk by providing global experience system integrators with financial services and payment experience

Support key executive, design and implementation decisions with relevant technology, payment, risk and compliance expertise

## Our Solution

A collaborative team of GBS Risk and Compliance, GBS iX and IBM Security worked together to deliver:

Comprehensive UI/UX Design with Persona Mapping

CIAM Architectural Design Based on IBM Security Verify SaaS,

Payment Routing and Linking capabilities with payment options like PayPal and Zelle

# Thank you

Follow us on:

[ibm.com/security](https://ibm.com/security)

[securityintelligence.com](https://securityintelligence.com)

[ibm.com/security/community](https://ibm.com/security/community)

[xforce.ibmcloud.com](https://xforce.ibmcloud.com)

[@ibmsecurity](https://@ibmsecurity)

[youtube.com/ibmsecurity](https://youtube.com/ibmsecurity)

© Copyright IBM Corporation 2022. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

