INTERNAL

Digital Identity as Attribute Linking Opportunities And Vision

January 2019

HSBC

Opportunity

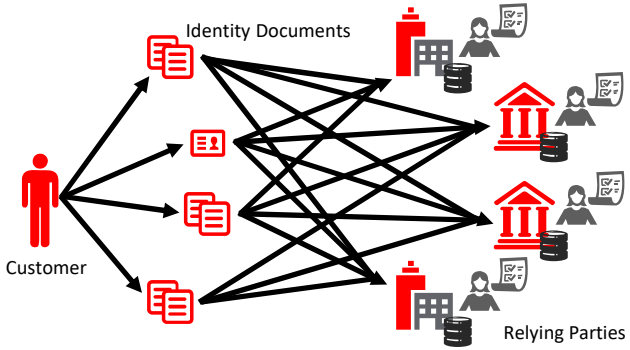
- Digital identity tackles a rapidly emerging unmet customer need – for customers to be able to frictionlessly and reliably assert their "identity" in ways that are a. easily (aka digitally) accessible in a broad range of use cases, but are also b. robustly assured and trustworthy in their underlying assertions
  - Tech titans (e.g., Facebook and Google) can provide simple digital accessibility to customers' attributes (through OAuth, OpenIDConnect etc) but without sufficient underlying trust assurance to be a basis for trusted identity assertion
  - Traditional trusted identity assertion providers (through passports, driving licences etc) can provide sound identity assurance but these analogue ID assurance approaches are cumbersome and time consuming to re-use

- "Digital identity" as a movement has the potential to transform society in 2 respects:
  - Firstly, providing consumers with a simple way to assert their identity, and relevant credentials, in the myriad different contexts where that's helpful for their daily lives
  - And secondly, and in reverse, using the power of these consumers' emerging digital footprints to transform how they build, maintain and assert those self-same "identities"

  i.e., …. as societies broaden and deepen their reliance of internet technologies to power everyday lives, we have not only a greater *need* for digital identities, but actually *new means* of asserting / verifying these self-same identities – particularly in areas such as: 1. "internet of things", 2. distributed ledger systems, 3. "augmented reality"

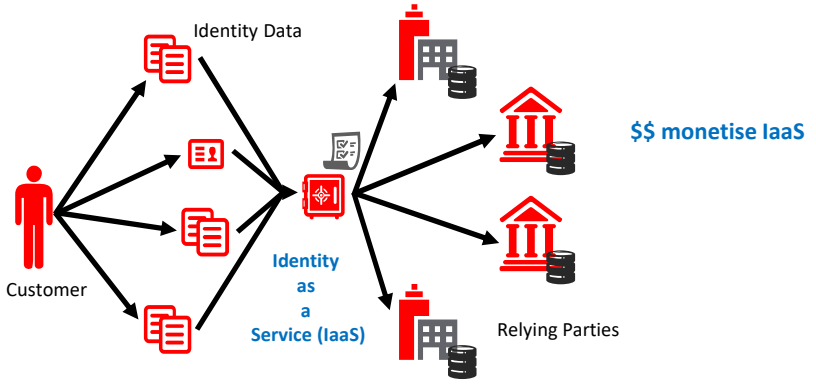
Current state

- Same proof-of-identity information requested from customers for different relying parties, often and then performs independent verification of this information; Customer data is persisted at each relying party and requires continual maintenance



Target state

- Customers' identity data and verification is managed as a service providing a **universally accepted, user-controlled Digital Identity**



Opportunity

There's a wide range of real world examples – where simple, instant digital customer data assurances could transform the experience – and even, in some cases, enable new experiences

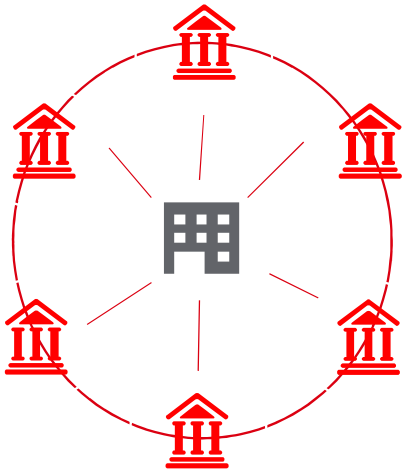
	Enabling instant digital "Customer Due Diligence" to enrol to new services	**Turning "digital payments" into "rich digital contract exchanges"**	**Enabling customers / citizens to make ad hoc ID proofs quickly and painlessly**
	Access to some services (e.g., banking) requires assured customer data and eligibility tests to be completed upfront – creating friction and re-work for both customer and service provider	*Some real world transactions require not just payments but assured personal data exchange at the same time; some service exchanges don't even exist today – as there is no simple mechanism to exchange these assurances*	*In a number of everyday situations, customers / citizens being able to prove their personal data easily and instantly can reduce friction and workload*
Some Examples	**Banking** • NTB account opening • ETB product / service opening • International on-boarding • Ongoing / remedial CDD	**Providing Personal Details + Payment** • Airline tickets + adv passenger info • Subscription sign up - phone, utilities, gym • LT and ST renting homes, house swaps	**Proof of Age** • Buying alcohol / gambling etc • Senior citizen access
	Government • Service entitlement (e.g., support services, health services etc) • Disbursement entitlement (e.g., pension, disability, payouts) • Background checks on employees etc • New ID issuance (e.g., passport, marriage cert, Tax ref etc.)	**Claiming disbursements** • G2C disbursements – e.g., pensions • Causal labour payroll • Lottery winnings • Insurance payouts	**Proof of Qualifications** • Job application • Regulated service provider (lawyer, doctor etc)
	Other • Health: patient records federation, provision entitlement • other	**Proving Eligibility at Point of Exchange** • Hiring car • Setting up insurances – home, car, other etc. • Sharing economy exchanges – e.g., nannies, house-sitters, carers etc.	**Proof of Anti-impersonation** • Restricted entry admissions • Claiming lost property etc.

Agenda

- **Digital Identity as Attribute Linking – Making the Case**
- Proposed Approach in HSBC HK: Linking Digital Identity to Transactions

Standard / Default Model: Scheme-based Identity Models

However, the typical approach to digital identity is to try construct "schemes" – of ID providers, relying parties etc – to agree common definitions, standards, governance etc for sharing "digital identities" between the parties



Scheme members agree to

- Common, holistic and fixed definitions of "identity"
- Common standards for identity proofing
- Common technology, governance and liability models

Trust is embodied in the trustworthiness of the members and – typically - vested in the aggregated output of the due diligence (i.e. the "identity" itself) rather than in the underlying customer attributes, or events

Limitations of "Scheme-based" Identity Models

- Scheme-based trust frameworks are cumbersome to build and fragile to maintain, as they rely on all parties agreeing in exacting detail to:
  - A rigid template of attributes that define "identity"
  - A common set of due diligence standards for mutual assurance
  - A common set of technology standards
  - Multilateral commitments across liability, audit and governance
- The resulting "identities" are trusted, but highly aggregated in nature – and because they are holistic – they can neither be disaggregated nor augmented easily
- Because the scheme is borne of reliance on *who* is asserting the identity rather than *how* the identity is being asserted (i.e. the individual events that constitute the due diligence workflow), it reinforces – rather than challenges – the un-reconstructed approaches we have today to identity assertion
- Finally, they create market dynamics that create "winner takes all" network effects
  - Competitive schemes fight for local / global currency
  - In the meantime, individual players try to second guess which of these horses to back and which not to

Challenges with the "Scheme-based" Approach

These schemes have had some localised successes – but in terms of building a global, universal model for digital identity they face 5 critical issues

Enabling interoperability	• DI schemes are difficult to make inter-operable because
	  • They rely on specifying fixed definitions of "identity", standards of proof etc – that may not align across schemes
	  • They embody "trust" in the "ID providers" – but leave the underlying ID proofs themselves as a black box – which may make them unusable to relying parties outside of (and distant from) the scheme

Handling liability	• DI schemes are challenged to define who has "liability" for the identity assertions • i.e., if a relying party uses an identity assertion from an "ID provider" that turns out to be wrong who is liable – and how is that liability managed?
Linking "identity" to "eligibility"	• DI schemes that provide holistic "identities" will be challenged to fully solve many real world problems where the identity needs to be linked to additional attributes to pass "eligibility tests" (e.g., "has acceptable sources of wealth", "is not a PEP", "has purchased a valid ticket" etc.)
Unleashing vibrant, uncoordinated innovation	• DI schemes – by definition – rely on mutually agreed standards, approaches and acceptable players; this makes experimenting with and incorporating innovative new attribute sources or approaches difficult – as "everyone" needs to agree. This critically compromises the scheme's ability to create a rich environment of uncoordinated innovation-at-the-edge of the network
including richer corroboration sources	• DI schemes' trust model relies on the "trusted source" i.e., a provider of attributes who will attest to their veracity. But there's a large class of potentially valuable sources who are not "trusted sources but can generate "trust" through providing "corroborating events" (e.g., Amazon delivery / returns history or mobile phone location history as a "proof of address"). And innovation in our digital lives will make this class grow exponentially – schemes struggle to handle these sources that are NOT willing to assert themselves as "trusted sources" – but who actually have "hard to fake" event histories to offer

The outcome is "islands of digital identity" – a multiplicity localised schemes, struggling to cooperate, scale or innovate

An Alternative: Event-based Approach

- Digital identity is customer data that we trust
  - HSBC (and other similar players) remember customer data all the time; but currently have no mechanism for **remembering why we trust it**

- If we could remember why we trust customer data we could
  - remove costs (of duplicated due diligence processes)
  - enhance customer engagement (through progressive onboarding, IaaS etc)
  - add new product streams (like instant contracting and sharing economy contracting etc)

- We are looking to do this in a unique and revolutionary way
  - **through remembering the "events" that generated the customer data**
  - specifically, the events that created trustable linkages between customer data attributes

  in a machine readable way - and using these to manage / repair / reuse the veracity of the resulting "identity" that emerges

- This has the power to significantly de-scope digital identity use cases through
  - *reduce* use cases down to the specific attribute linkages required for that use case
  - *reimagine* all the possible events and ways those linkages could be made in a trustable way
  - *reuse* the attribute linkages made in use cases flexibly across all others

- If we could enable customers to **share their data and event histories** – i.e., the events that generated the customer data assurances – we have a much more flexible, transparent, de-centralised approach to "digital identity"

- As event-based approach, can enable a **vibrant, innovative digital identity ecosystem to grow organically** – enabling **digital identities to grow in reach and scope and to innovate and be reused – without the need for formalised tightly-controlled schemes**

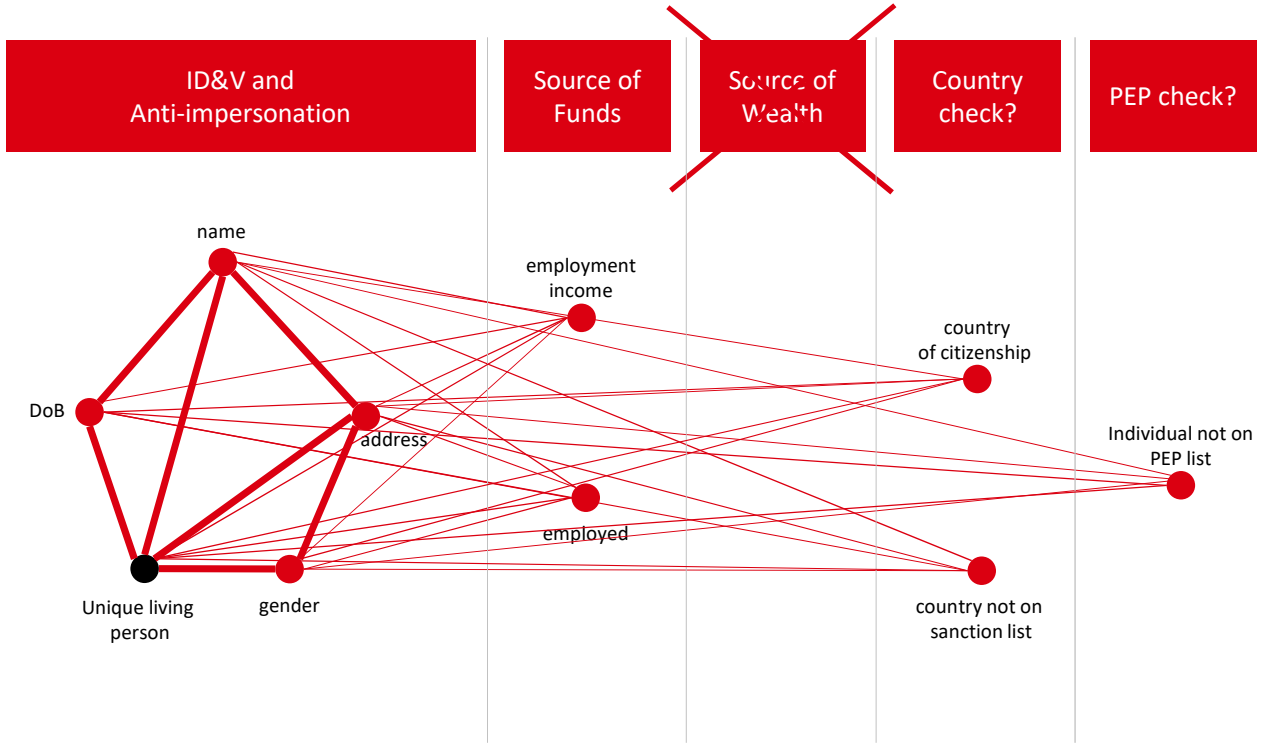
- Underpinning this approach is each player operate some form of orchestrator + event log:
  - a data model – with common semantics and syntax to remember events (and attribute linkages)
  - a rules engine – with the capability to analyse, graph attribute linkages, and veracity, from events; maintain / repair / reuse both customer attributes and integrated "identities"

An Event-based Approach – Use cases as attribute linkages required

Scenario

- Non-HSBC customer currently lives in UK, but is moving with work to UAE
- Wishes to join HSBC and open bank accounts in UK, UAE and US
- HSBC wishes to “remember events” in UK-centric KYC process, and re-use them to open bank accounts in UAE and US as a seamless customer experience
- Additional events to satisfy UAE/US business rules are also “remembered”, to be re-used in other use cases
- Note: (not included here) Account Set up process then bonds new HSBC identifiers (account #, channel p/words etc) to the person

Required Attribute Linkages (Account Opening Process)

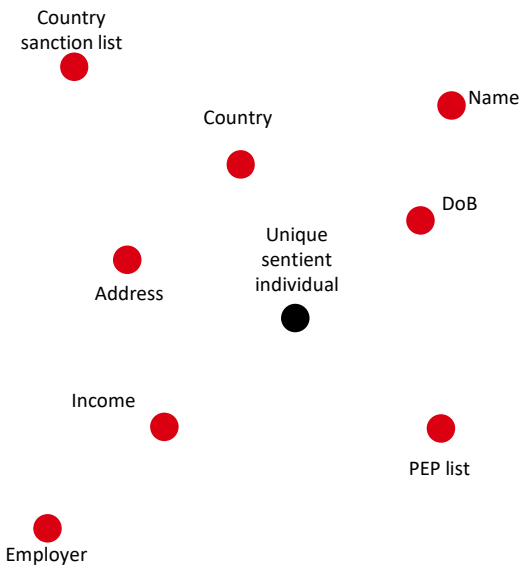


illustrative

An Event-based Approach – Events as sources of attribute linkage assurances

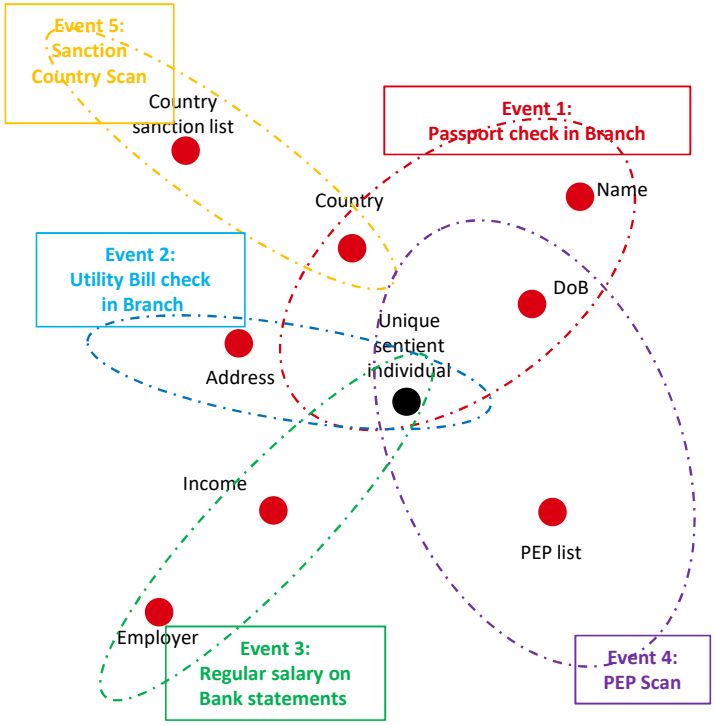
Nodes

Individual attributes (i.e. “raw” data), reference lists and entities are registered as nodes, and associated with key properties such their storage location



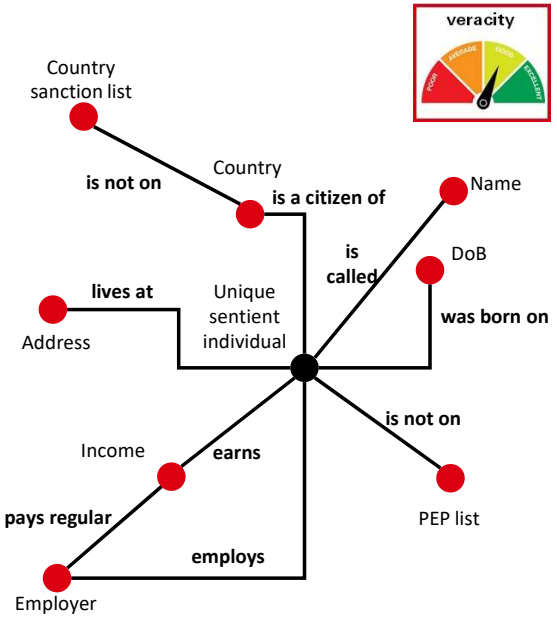
Events

Treated as a primary data object, authored by the use case workflow that undertook them, and recorded and stored separately by AREIO

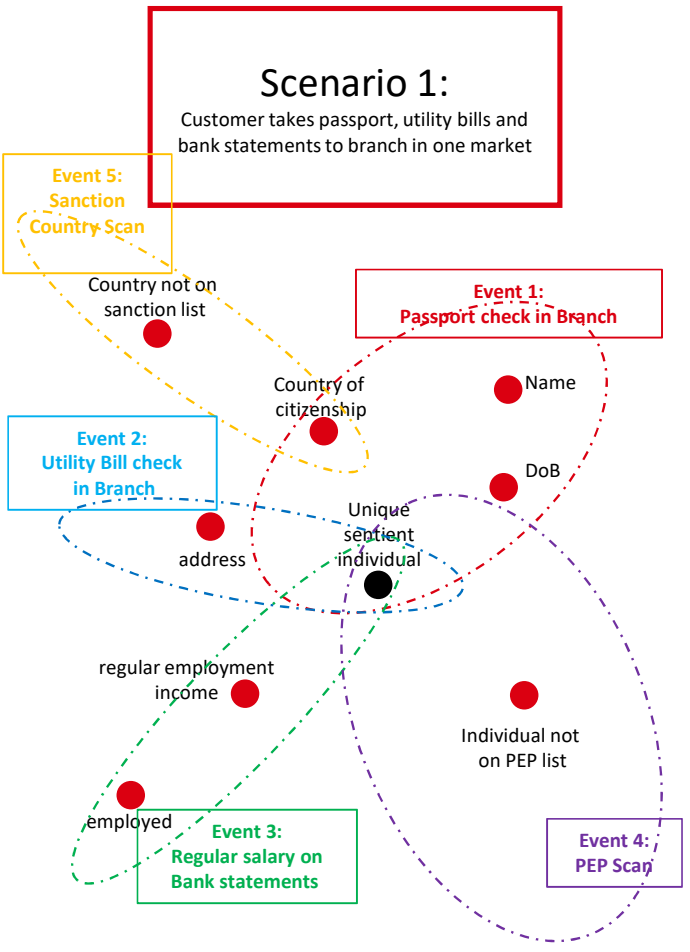


Linkages

Inferred to a given level of assurance by the AREIO workflow, based on the record of events, and can be aggregated by AREIO or use case workflows into “identities”



An Event-based Approach – Record event history, convert workflow into "if … then" event rules



INTERNAL

"Today"

A **"event rules" ensure veracity at the event level**

Event 1: Passport check in Branch

- Passport valid
- Claimant present
- Photo match
- Employee / date / time
- Copy taken
- S/visor QA

Event 2: Utility Bill check in Branch

- U / Bill valid
- U/Bill >3 m's
- Name matches PP
- Employee / date / time
- Copy taken
- S/visor QA

• • •

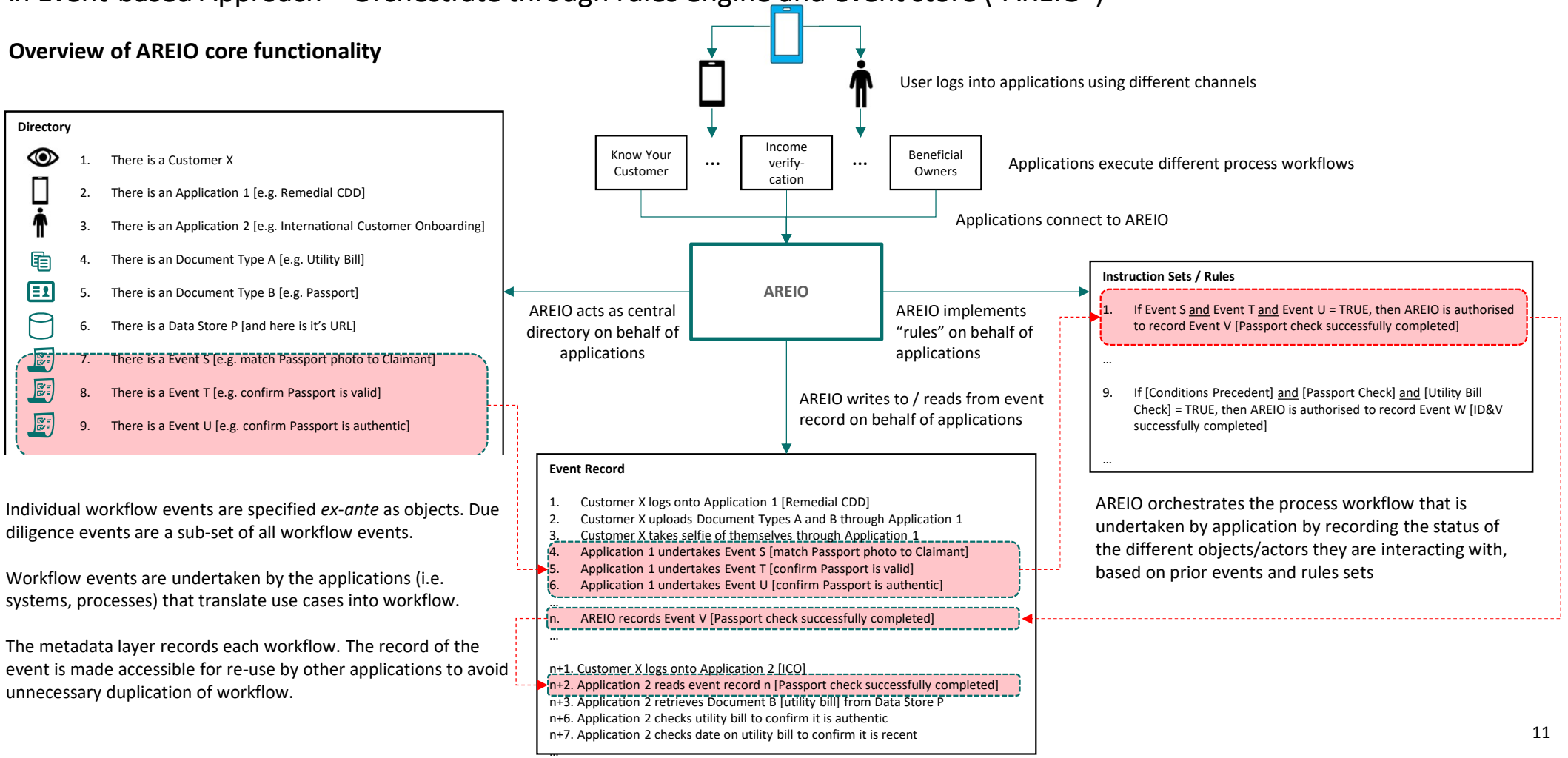
B **"A/O eligibility rules" ensure required veracity and eligibility at the use case level**

- Successful ID&V and AI test
- Individual >18, with legitimate income source
- Not sanctioned individual or CoC
- All events performed in last 3 m's

AREIO use case rules engine(s)	AREIO central rules engine(s)	AREIO (meta-) data store
• Use case writes event details to AREIO (meta-)data store		• Business EVENTS recorded as discrete new events
	• If … then rules define change of attribute relationship STATUS	• Changes of STATUS recorded as discrete new events
	• If … then rules define new PROOFS completed	• New PROOFS recorded as discrete events
• AREIO business rules engine encodes "KYC eligibility rules"	• If … then rules define new ELIGIBILITY TESTS performed	• New ELIGIBILITY TESTS outcomes recorded as discrete
	• AREIO makes event history discoverable	
	• AREIO If … then rules orchestrate events to repair STATUS	

An Event-based Approach – Orchestrate through rules engine and event store ("AREIO")

Overview of AREIO core functionality



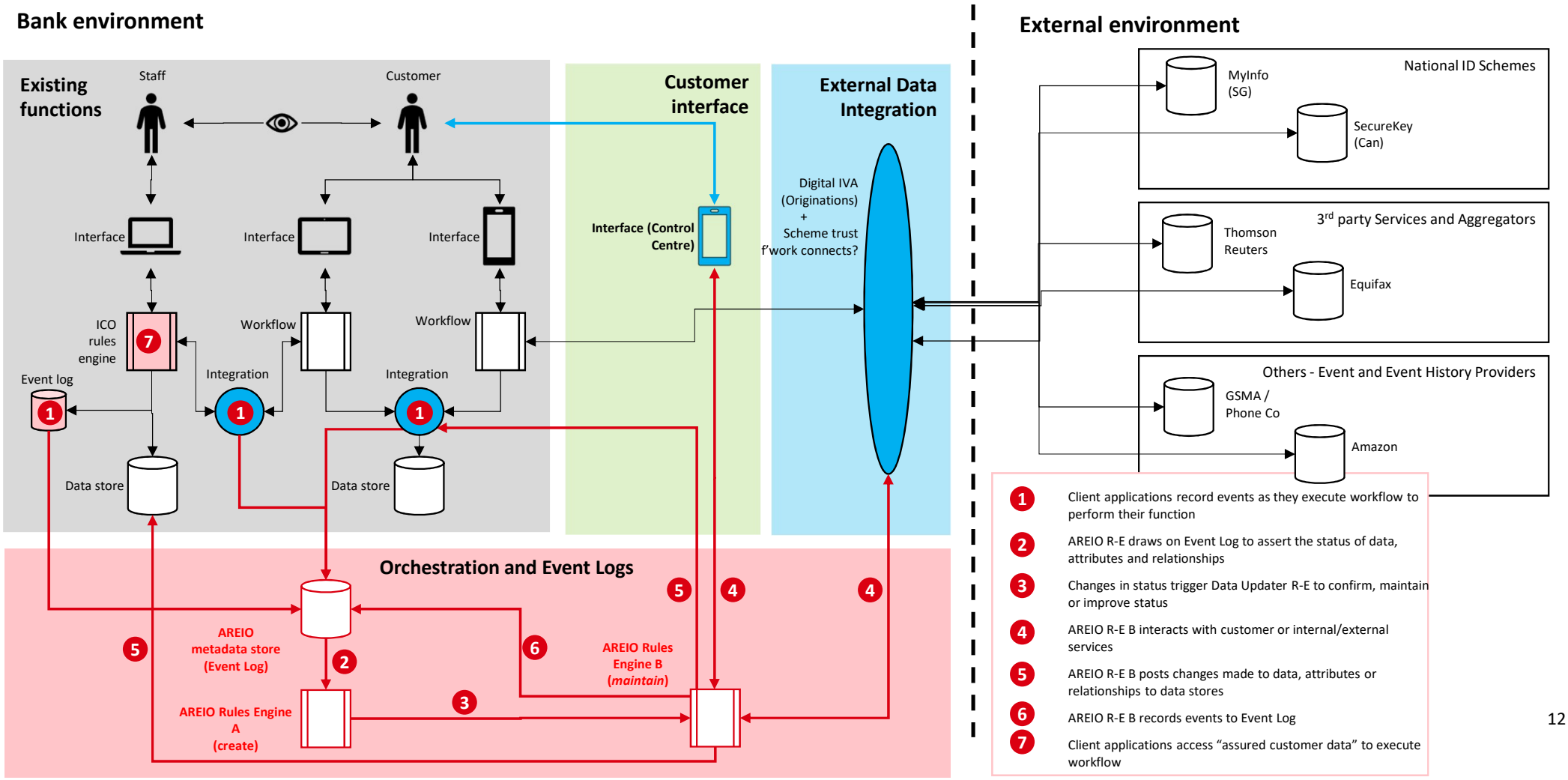
Individual workflow events are specified *ex-ante* as objects. Due diligence events are a sub-set of all workflow events.

Workflow events are undertaken by the applications (i.e. systems, processes) that translate use cases into workflow.

The metadata layer records each workflow. The record of the event is made accessible for re-use by other applications to avoid unnecessary duplication of workflow.

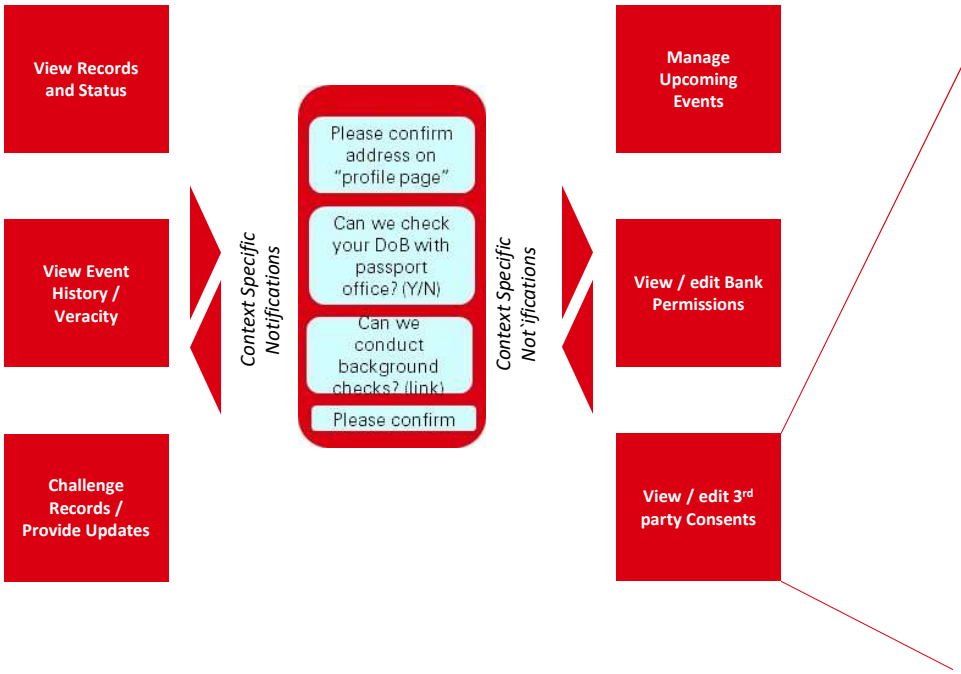
AREIO orchestrates the process workflow that is undertaken by application by recording the status of the different objects/actors they are interacting with, based on prior events and rules sets

An Event-based Approach: Expand scope across *internal* touch-points, data services and use cases



An Event-based Approach – Enable customers to share their event histories as “open IaaS”

IaaS providers create customer apps for customers to manage their records *and* their events (histories and upcoming)



Typical customer IaaS app

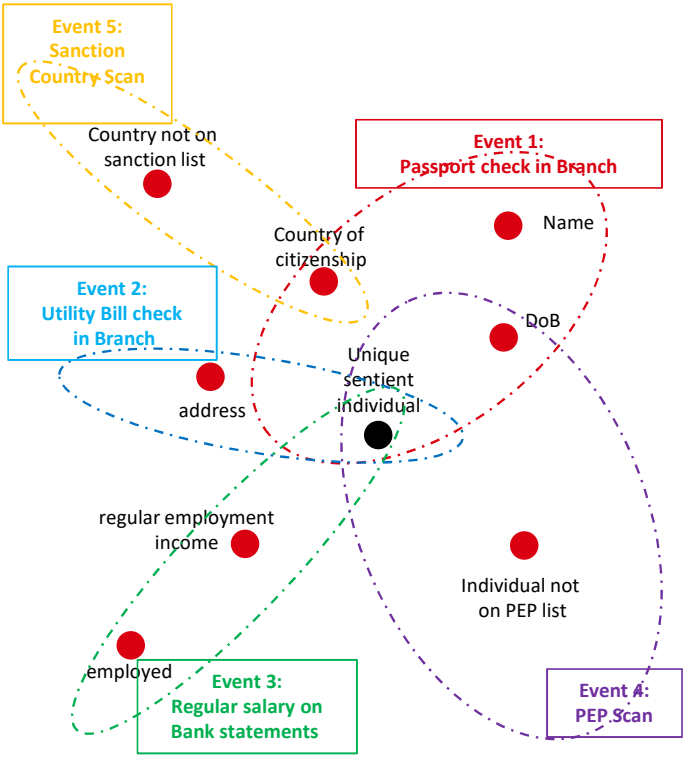
IaaS consumers use customers’ event histories either as 1. holistic assurances or as 2. assurances that contribute to use cases

- IaaS consumers (aka “relying parties”) can receive event histories from customers – as underlying sources of trust
- IaaS consumers may take these are sufficient for their use case but may not e.g.,
  - The IaaS consumer *decides* if they trust the event history as having sufficient veracity for their use case
  - The IaaS consumer *adds* other events (either self generated or from other parties) to augment trust or to bind in additional eligibility tests relevant for the use case (proof of wealth, has valid ticket, is alive today, is blind etc etc)

An Event-based Approach – Enable event providers to innovate data assurance events overtime

Scenario 1:

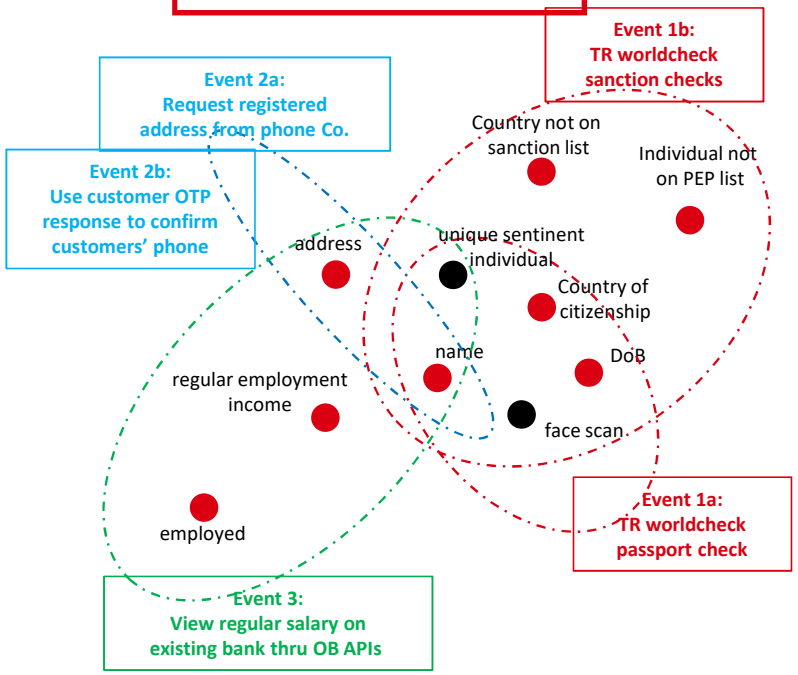
Customer takes passport, utility bills and bank statements to branch in one market



"Today"

Scenario 2:

Customer scans face, passport and bank card on mobile phone + gives consents
Bank uses OB APIs, phone Co's + SMS OTP, TR Worldcheck to complete checks

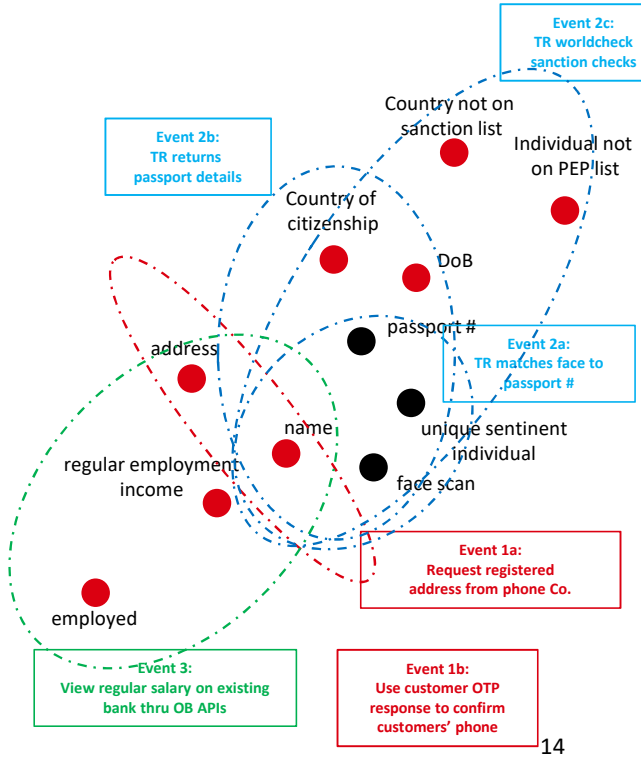


"Tomorrow"

Scenario 3:

Customer takes selfie + gives consents

bank uses phone Co's + SMS OTP to autofill, then checks with TR Worldcheck, OB APIs



"Someday"

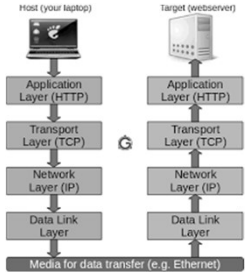
An Event-based Approach: Innovation through “common semantics” rather than “membership schemes”

In other fields, promoting a vibrant, innovative ecosystem has been more successful where it has focused more on sharing a thin layer of “common semantics” between players than trying to build cumbersome “membership schemes”

Barcodes

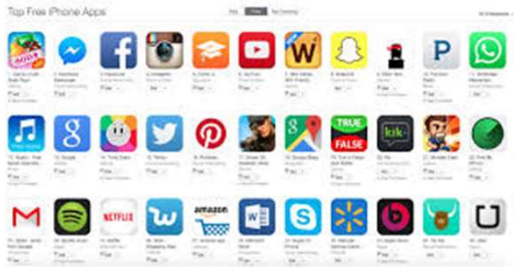
- Barcodes enabled significant innovation in retailing
- Related innovation: till systems, stock control systems, product management approaches, promotions capabilities etc.

TCP/IP



- TCP/IP enabled transformational innovation of the internet
- Related innovation: websites, email, e-commerce, social media etc.

Apps



- Apps enabled creation of a vibrant mobile internet
- Related innovation: native apps, hybrid apps, app stores, app developer systems and ecosystems etc.

An Event-based Approach – How It Transforms Our Ability to Build An Organic, Vibrant DI Ecosystem – Capable of Innovating and Evolving through De-centralised Actions of Individual Participants

	Source-based Trust Federated through Schemes	Event-based Trust Federated through a Marketplace
Enabling interoperability	• Negotiated inter-operability between schemes  • Schemes need to agree common definitions, standards, governance models etc – and accept each others' "black box" trust assurances	• Promiscuity by individual players  • IaaS consumer/providers seek data and/or event histories from other providers – but use own rules engine to match to use case requirements
Handling liability	• Needs formalised liability model  • ID providers assert "assured identities; relying parties in rely on these in their work processes need to clarify who is liable when they rely on an bad assertion	• No (or, at least, limited) liability transfer involved  • IaaS consumer/providers consume event histories from other providers – they decide, for themselves, whether the collection of events represents sufficient assurance
Linking "identity" to "eligibility"	• Attributes included defined by scheme (and fixed)  • Schemes define ID to include a standard, limited, set of attributes; eligibility tests (source of wealth, not a PEP, has valid ticket, is blind, etc etc) all require an additional (non-persistent?) validations outside the scheme	• Attributes linked can be completely use case specific  • IaaS consumer/providers seek data and/or event histories from other providers – but can combine exactly as required to meet their specific use cases
Unleashing vibrant, uncoordinated innovation	• Scheme trust sources need to be agreed by all users  • Schemes need to ensure all relying parties accept trust-worthiness of ID assertions – meaning innovating / adding to the system requires perpetual, cumbersome scheme-wide agreement (and thus central coordination?)	• New event types can be added by anyone, anytime  • IaaS consumer/providers can add new data sources, matching techniques, corroborating events etc anytime – that then anyone can consume
including richer corroboration sources	• "Trust" limited to "trusted sources"  • IaaS providers assert *they* are the source of trust in the digital identity assurances	• "Trust" expanded to "hard to fake" event histories  • IaaS consumer/providers can include "hard to fake" event histories (returns to Amazon for proof of address, mobile location data etc) – even when "source" doesn't make any trust claim

An Event-based Approach – How Do We Build A Shared Ecosystem

1 Change What We Talk Together About

- STOP trying to agree:
  - Common identity definitions
  - Common assurance level definitions
  - Shared governance models
  - Shared liability models
- START trying to agree
  - Common semantic language
  - Common message content (i.e., attributes, plus event history data)

2 Build Our Own Event Stores and Rules Engines

- Attribute Providers
  - Consider recording event history as well as attributes
  - Consider sharing event history – rather than just unassured attributes
- Trust Providers
  - Consider how you can expose your underlying event history – not just "black box" outcomes
- ID Consuming Parties
  - Build your own rules engines
  - Convert your use cases into "required attribute linkages"
  - Expand attribute sources and event histories to address use cases

3 Keep Building Our Apps and Our Attribute Exchange Platforms

More than ever, this ecosystem needs:

- A plethora of attribute providers providing
  - Untrusted attributes, to feed into corroboration events
  - Event histories to provide data assurances
- A plethora of customer-facing apps for customers to own, manage, federate, repair their "event histories" – and thus their digital identities
- A plethora of consuming parties – either
  - Consuming events in their rules engines
  - Consuming the outputs of others' rules engines

Agenda

- Digital Identity as Attribute Linking – Making the Case

- **Proposed Approach in HSBC HK: Linking Digital Identity to Transactions**

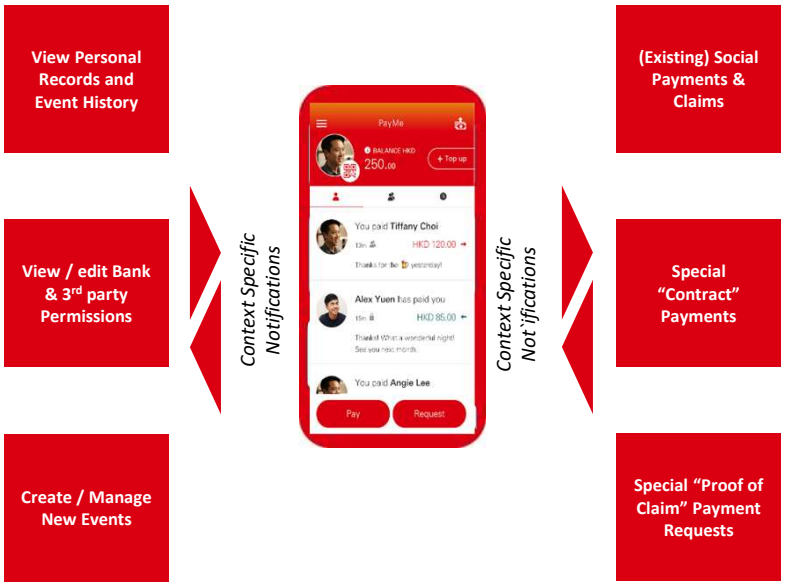
Proposed Approach in HSBC HK

Ongoing / remedial CDD provides use case to activate customers' control centres (including personal data and event histories). HSBC HK's position in HK domestic payments (e.g., with payme) should then enable us to fast start enabling customers to combine personal data assurances with payments – to create some"rich digital contract exchanges"

	Enabling instant digital "Customer Due Diligence" to enrol to new services	**Turning "digital payments" into "rich digital contract exchanges"**	**Enabling customers / citizens to make ad hoc ID proofs quickly and painlessly**
	Access to some services (e.g., banking) requires assured customer data and eligibility tests to be completed upfront – creating friction and re-work for both customer and service provider	*Some real world transactions require not just payments but assured personal data exchange at the same time; some service exchanges don't even exist today – as there is no simple mechanism to exchange these assurances*	*In a number of everyday situations, customers / citizens being able to prove their personal data easily and instantly can reduce friction and workload*
Some Examples	**Banking** • NTB account opening • ETB product / service opening • International on-boarding 1 • Ongoing / remedial CDD	2 **Providing Personal Details + Payment** • Airline tickets + adv passenger info • Subscription sign up - phone, utilities, gym • LT and ST renting homes, house swaps	**Proof of Age** • Buying alcohol / gambling etc • Senior citizen access
	Government • Service entitlement (e.g., support services, health services etc) • Disbursement entitlement (e.g., pension, disability, payouts) • Background checks on employees etc • New ID issuance (e.g., passport, marriage cert, Tax ref etc.)	**Claiming disbursements** • G2C disbursements – e.g., pensions • Causal labour payroll • Lottery winnings • Insurance payouts	**Proof of Qualifications** • Job application • Regulated service provider (lawyer, doctor etc)
	Other • Health: patient records federation, provision entitlement • other	**Proving Eligibility at Point of Exchange** • Hiring car • Setting up insurances – home, car, other etc. • Sharing economy exchanges – e.g., nannies, house-sitters, carers etc.	**Proof of Anti-impersonation** • Restricted entry admissions • Claiming lost property etc.

Proposed Approach in HK

Combined Customer Control Centre and Payments App(s)



Customers Control Access to Their Assured Data; by Combining into Payments HSBC HK Enables New Classes of Transactions / Exchange

- HSBC's ongoing CDD requirement means we will benefit from building data assurance rules engine and event history – and providing customers with consent and permissioning control over it
- By then providing customers with ability to combine these data assurances with payments HSBC HK can start offering a wide range of better exchange experiences:
  - Streamlined air ticket, car hire etc purchasing
  - Instant sign up for utilities, services, insurance contracts
  - Sharing economy assured exchanges etc
  - Simple G2C disbursement claims
  - Instant, simple insurance claims
  - Lottery winning claims etc