Orchestrating Digital Identity, Privacy and Assurance - the Kantara perspective

High Level Fireside Briefing

Chair: Colin Wallis, Executive Director, Kantara, EU
David Black, Consultant, ID Crowd, UK,
Mark Lizar, CEO, Open Consent Group, UK
Kantara on a Page

- ‘Commons’ ethics & societal purpose. No/Low barriers to participation. Passionate about giving back control of identity & personal data. Consent Receipt and User Managed Access specs
- **Scope:** The only industry consortium to have both identity and personal data scoped within its mission.
- **Mission:** the global consortium improving trustworthy use of identity and personal data through innovation, standardization and good practice
- **Tangible Deliverables & Business model:** Revenue from Membership, Sponsorship, R&D and Trust Framework Operations program management invested in specification development & publishing platform, and contributions to ISO, OECD Internet Technical Advisory Committee, UNCITRAL
- **Thought-leaders & trend-setters globally:** Organizations & Individuals & Government

Kantara translates to “wooden bridge” in Kiswahili, a hybrid language between Arabic and Bantu, depicted in Kantara’s ‘bridge’ logo.
Kantara’s International Membership
& x10 non-member

- US Postal Service
- MIT Trust: Data Consortium
- Government of Canada Treasury Board Secretariat
- +50 individuals
- One.Thing.Less

© Copyright 2019 Kantara Initiative, Inc
‘The Rhythm of Kantara’
‘Nurture, Develop, Operate – that’s what we do’

- **Nurture** emerging technical communities through our discussion & working groups and our incubators – present and past examples: Identity and Privacy R&D (KIPI) program, incubator for ID Pro.

- **Develop** and standardize community practices with specifications companies can understand, trust and implement.

- **Operate** conformity assessment programs to enable companies to meet their adherence goals to standardized practices needed to support their business.
Award-Winning, Trend-Setting, Compliance-Assisting Innovations

- **Kantara User Managed Access** - the world’s first open specification for delegated authorization, extending OAuth 2.0. Strong interest from GDPR, PSD2, Open Banking and other sectors. European Identity Conference award winner 2014. Currently awaiting IETF publication as an international standard.

- **Kantara Consent Receipt** - the world’s first digital receipt specification for personal data containing the conditions upon which the consent is given – giving agency over personal data to individuals. Annexed into International Standard ISO/IEC 29184 Online privacy notices and consent.

- **Kantara Trust Framework** - the world’s first to offer 3rd party accredited assessment, approval & grant of trust mark to product & solution service providers for NIST SP 800-63-3. IDESG’s IDEF self attesting scheme added Aug 2018.
<table>
<thead>
<tr>
<th>Inflection</th>
<th>athenahealth</th>
<th>experian</th>
<th>ID.me</th>
<th>SUNET</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZENTRY</td>
<td>USPS</td>
<td>NIXU</td>
<td>学認</td>
<td>KUMA</td>
</tr>
<tr>
<td>seadot</td>
<td>Zygma</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Example Deployments of Kantara’s Specifications

The UMA specification gives individuals a unified control point for authorising who & what can access their digital assets at their desired grain.

The Consent Receipt Specification define the requirements for a record of authority by a PII Principal to a PII Controller for processing of the Principal’s PII.

Customer Commons/Kantara Intent Casting UX and Human Readable terms

© Copyright 2019 Kantara Initiative, Inc
Kantara’s 10 Years Young this Year!
Important that the organisations relying on digital identities adopt a robust set of measures to determine whether an individual is who they say they are.
Validate evidence
Verify identity
Attestation of trust in biographic attributes
How robust was the issuance process?

Does the evidence contain any security features to make sure it is not a counterfeit?

Is there a source that can be checked to determine the evidence is valid and hasn’t been revoked?

Can the people checking the documents detect falsified or invalid documents?
A set of digital identity standards has been developed to assist those organisations undertaking the checks.

Evidence & methods graded to determine the strength of the resulting assured digital identity.
Adopt an outcome based standards approach to identity assurance
Creates a standards based ecosystem for buyers and sellers of digital identity.
Allows regulators to set their own compliance requirements in line with recognised standards.
Allows users to re-use their standards based digital identities
Allows interoperability across borders between national but equivalent standards
ID Crowd and Kantara widening the scope of assurance against standards into the private sector
Key Points

- Why the Consent Receipt (CR) is important!
- The Digital Transparency Problem: The work the CR is intended to solve.
- The journey to solve this problem continues at Kantara.
Ecosystem of Privacy Policy/TOS management
The road to solving the Biggest Lie problem

Active projects
- CommonTerms
- PrivacyChoice/PrivacyScore
- TOS;DR
- Docracy
- TOSSOS
- TOSSBack2
- EmanciTerm/VRM
- YouLuh
- Customer Commons
- OpenEula

2012-09-07. Schema by Solon Barocas, additions by Pär Lannerö (CommonTerms.net)
1. BATTLE SCARS FROM WRANGLING WITH PRIVACY
W3C:DNT Call for Collaboration (Standards)

Opening up the Online Notice Infrastructure An ‘Open Notice’ Call For Collaboration - https://www.w3.org/2012/dnt-ws/position-papers/23.pdf

Many Hackathons

Published Papers

ACM - Usable Consents

Ubicomp- Managing And Tracking the Use of Data With A Consent Receipt

The Rise of The Attribute Economy 2 - slidepiper.com

Engaged With Regulators

EU - GDPR – Consent As a Privacy Framework

US - NSTIC – National Strategy for Trusted Identities in Cyberspace

Canada – Meaningful Consent

...More on request

1. Privacy Laws would need to change
2. Privacy Standards were needed
3. Laws would need to be enforced
Consent Research Across Privacy Instruments

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Accountability</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Notice</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Consent</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Collection Limitation</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Use Limitation</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Disclosure</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Access and Correction</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Security Safeguards</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Data Quality</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Enforcement</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Openness</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
A Consent Receipt

A receipt is the oldest known writing in the world.
Sovereign Consent

MVCR: MINIMUM VAILABLE CONSENT RECEIPT

https://youtu.be/SOhnElkSSj0
Challenges
Not As Simple As We Thought

1. Needed an attribute level event based record for fine grained control
2. Needed a safe way to send and receive consent data (very sensitive)
3. Needed a common language for compliance and evidence

Solution Approach
Collaborate with Standards Organisations

ISO 29184  Consent Receipt  OASIS COEL  Privacy Control Vocabulary  Towards Privacy Based Agreements
2. EMERGING ECO-SYSTEM

Kantara


Open Notice Initiative

W3C Do Not Track

OASIS COEL

ISO 29184

CCPA

W3C Data Privacy Control Vocabulary

OPN

2023: ISO Consent Records & Receipts

© Copyright 2019 Kantara Initiative, Inc.
2019: Conditions for Digital Transparency and Personal Data Control

1. Laws would need to change
   • GDPR & CCPA

2. Standards were needed for consent
   • Consent Receipt Standard @Kantara

3. Laws would need to be enforced
   • €50 Million Fine to Google – Notice (not sufficient for consent)
Nurture. Develop. Operate. – that’s what we do!

davidblack@idcrowd.co.uk
Twitter: @identitygeeza
www.idcrowd.co.uk

mark@openconsent.com
Twitter: @OpenConsent @Smartopian
https://openconsent.com

colin@kantarainitiative.eu
Twitter: @KantaraColin
https://kantarainitiative.org