Delivering on the MyData Principles

MyData 2018

Colin Wallis
Executive Director, Kantara Initiative
Kantara Initiative – A Snapshot


- Strong ethics & societal purpose. Low barriers to participation. Passionate about giving back control of identity & personal data

- Mission: the global consortium improving trustworthy use of identity and personal data through innovation, standardization and good practice

- Business model: Revenue from Membership, Sponsorship, R&D and Trust Framework Operations program management invested in specification development & publishing platform, and contributions to ISO, ITU-T, OECD ITAC and others

- Comprises global thought-leaders; Organizations & Individuals & Government agencies
Kantara’s International membership & x10 non-member participants

© Copyright 2018 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, ID Pro incubator.

- **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.
Session: Standards for delivering on the MyData Principles – all in 20 minutes!!

- “Take each of the MyData 6 Principles and gives examples of Kantara's work”
- “Offer your views on the current state of the standardization space”
Standards: What are the benefits? What are the principles?

- Cooperation
- Adherence to Principles
- Collective Empowerment
- Availability
- Voluntary Adoption
The treaty organisations are often the only recognised Standards bodies.
Adding jurisdictions that feed the Treaty orgs…
Adding industry consortia – both heavy and light standards development
And the resulting standards landscape?
(examples only)

<table>
<thead>
<tr>
<th>REGULATIONS</th>
<th>RULES - LAW</th>
<th>REQUIREMENTS</th>
<th>COMPLIANCE</th>
<th>STANDARDS</th>
<th>TRANSPARENCY</th>
<th>POLICIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 29134 Privacy Impact Assessment Guidelines</td>
<td>ISO 29151 Code of Practice for PII Protection</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISO 29184 Online Privacy Notices &amp; Consent (draft)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISO 27552 Enhancement to 27001&amp;2 for privacy management – requirements &amp; guidelines (draft)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISO TR 27550 Privacy Engineering (draft)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISO 27018 Code of Practice for PII processing on public clouds</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HIPPA 1996 Privacy Rule &amp; Security Rule</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>COPPA 1998</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Common Accord smart contract template</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kantara Consent Receipt Specification</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kantara User Submitted Terms – with Customer Commons (draft)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kantara User Managed Access Specification</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NIST 800-53 – Security &amp; Privacy Controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>W3C P3P Platform for Privacy Preferences Project</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>W3C DPVCG (Data Privacy Vocabularies and Controls Community Group) draft</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>W3C Tracking Preference Expression (DNT)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IEEE 7012 - Standard for Machine Readable Personal Privacy Terms (draft)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OASIS Classification of Everyday Living (COEL) TC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OASIS Privacy Management Reference Model (PMRM) TC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Why develop standards? (classic answer)
Why develop standards?
(be conscious of ‘standards weaponizing behaviour’)

❖ ‘A tick-box’ for an organisation to give the perception of sustainable ubiquity
❖ Lever to attract members, revenue and mind-share away from competitors
❖ Develop a walled garden for an exclusive ecosystem
❖ To give traction and credibility to a new regulation in a jurisdiction
❖ To create an ongoing revenue stream to support a market or product strategy
❖ To create standards outside of the classical model, and use the network effect from their adoption to drive them to be ‘de-jure’ (HT Drummond)
Kantara’s work that delivers on the 6 MyData Principles

...always using open standards and protocols
The MyData 6 Principles

- Human-Centric control of Personal Data
- Individual as the point of Integration
- Individual Empowerment
- Portability: Access and Reuse
- Transparency and Accountability
- Interoperability
Kantara’s work that delivers on the 6 MyData Principles

In collaboration with Customer Commons
UMA is designed to give an individual a unified control point for authorizing who and what can access a wide variety of digital assets, at their desired “grain”

Some use cases:

• For financial consumers
  • Discovering and aggregating UK pension accounts and sharing access to financial advisors

• In industrial and consumer IoT
  • For proactively or dynamically sharing smart device control or data with others

• Healthcare
  • Health Relationship Trust (HEART) WG: patient-controlled health data exchange
  • Part of the new OpenMedReady framework for trustworthy remote care

Attribution: Eve Maler, UMA WG Chair, VP of Innovation & Emerging Technology, ForgeRock
At the heart of the UMA 2.0 ecosystem are five foundational concepts that ensure the protection and privacy of data. These concepts are:

1. **Certified Device Identity**: Ensures that devices are authorized and trusted before any data exchange.
2. **Strongly Authenticated User Identity**: Guarantees that only authorized users are interacting within the ecosystem.
3. **User/device association**: Facilitates the connection between the user and the device securely.
4. **Consent for device data sharing with others**: Users have explicit control over who can access their data.
5. **Cryptographic auditability**: Ensures that transactions are traceable and tamper-proof.

These elements are supported by various standards and alliances, including FIDO and Bluetooth, to enable secure, frictionless interactions. Attribution: Eve Maler, UMA WG Chair, VP of Innovation & Emerging Technology, ForgeRock
Legal relationships: Devices and artifacts
Making relationships and their changes auditable and machine-readable

1. Resource Rights Administrator
   - Resource owner
   - (Agency Contract)
   - Delegates-perm-authority-to
   - (Access Contract)
   - Delegates-mgmt-to
   - Legal devices: ToS, privacy notice (when an Individual)
   - Technical artifacts: Consent management record (outside UMA scope)

2. Authorization Server Operator
   - Authorization server
   - Licenses-perm-granting-to
   - Legal devices: OAuth client agreement (prior to resource owner context – licensing needs to be set up there)
   - Technical artifacts (type): Client credentials for UMA resource server (OAuth); PAT (UMA); all request/response messages between authorization server and resource server (UMA)

3. Resource Server Operator
   - Resource server
   - Legal devices: ToS, privacy notice (when an Individual)
   - Technical artifacts: Consent management record (outside UMA scope)
specification and the MyData 6 Principles

- Human-Centric control of Personal Data
- Individual as the point of Integration
- Individual Empowerment
- Portability: Access and Reuse
- Transparency and Accountability
- Interoperability
A privacy dashboard ecosystem requires standard data formats to be viable.
User Submitted Terms

“The User Submitted Terms effort has been working at Kantara in partnership with Customer Commons for three years on 3 layers of USTs: Human, Legal and Machine readable terms”. 
Intent Casting V.01
User Experience and Human Readable terms

JLINC is first case
.. and the MyData 6 Principles

- Human-Centric control of Personal Data
- Individual as the point of Integration
- Individual Empowerment
- Portability: Access and Reuse
- Transparency and Accountability
- Interoperability
Standardized Consent Receipts
issued to a data subject
whenever they consent
to personal data processing
will help enable a product ecosystem
that assists the data subject
to exercise their data rights...
Consent Receipt Specification

Version: 1.1.0

Document Date: 2018-02-20

Editors: Mark Lizar, David Turner

Contributors: Richard Beaumont, Chris Cooper, Sal D'Agostino,
Rupert Graves, Iain Henderson, Mary Hodder,
Harri Honko, Andrew Hughes, Tom Jones,
Robert Lapes, Oliver Maerz, Eva Miler, Jim Pasquale,
Samuel Tuominen, John Wunderlich

Produced by: Consent & Information Sharing Work Group

Status:

This document is a Kantara Initiative Technical Specification Recommendation produced by
the Consent & Information Sharing Work Group, and has been approved by the Group. The
Public Comment and Intellectual Property Rights Review has been completed. It has been
approved by the Membership of the Kantara Initiative. See the Kantara Initiative Operating
Procedures for more information.

Abstract:

A Consent Receipt is a record of authority granted by a Personally Identifiable Information
(PII) Principal to a PII Controller for processing of the Principal’s PII. The record of consent
is human-readable and can be represented as standard JSON. This specification defines the
**A Consent Receipt that is human readable**

### Consent Receipt

<table>
<thead>
<tr>
<th>Version</th>
<th>KI-CR-v1.1.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jurisdiction</td>
<td>Discworld</td>
</tr>
<tr>
<td>Consent Timestamp</td>
<td>11/15/2017, 12:00:00 PM EST</td>
</tr>
</tbody>
</table>

#### Collection Method

- Web Subscription Form with opt-in for marketing

#### Consent Receipt ID

c1b6fd5e-b7e5-4e65-8688-e9a656a021

#### Public Key

```
0a.5:1d.40.53.50.4b.5f.11b.2a.83.a9.d1:40.02.cc.31.b6.4e.77.bf.5e.a0.db.4f.00.22.0c.6c.23.54.67.83.12.3d.3e.b6.e7.09.71.60.54.01:4b.6b.4d.1e.3b.42.53.35.7b.6b.9f.7d.5e.b2:cb.0b.0e.a1.bf
```

#### Language

- English

### Consent Parties

#### Information Subject

- Bowden Jeffries

#### Information Controller

- **PII Principle ID**: Ankh-Morpork Times
- **PII Controller Name**: William de Word, Chief Editor & Data Protection Officer
- **PII Controller Address**: Ankh-Morpork Times, Gleam Street, Ankh-Morpork, Discworld
- **PII Controller Email**: william@times.ankh-morpork.xyz
- **PII Controller Phone**: (555) 555-5555 (3429)
- **PII Controller URL**: https://www.times.ankh-morpork.xyz/contact

#### Privacy Policy

https://times.ankh-morpork.xyz/privacy_2017

### Data, collection and use

<table>
<thead>
<tr>
<th>Service</th>
<th>Digital Subscription and News Alerts</th>
</tr>
</thead>
</table>

#### Purposes for collection and use

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Purpose Category</th>
<th>Consent Type</th>
<th>PII Categories</th>
</tr>
</thead>
</table>
| Fulfil Digital Subscription | Provision of services | EXPLICIT | • Technical  
  • Demographics  
  • Financial  
  • Contact |
| Marketing | Marketing | EXPLICIT | • Demographics  
  • Financial  
  • Contact |
| Financial Record Keeping | Fiduciary obligation | N/A | • Financial |
| Law Enforcement | Legal obligation | N/A | • All |

#### Termination

https://times.ankh-morpork.xyz/privacy_2017#termination

#### Third Party Disclosure

- True

#### Third Party Names

- Outsourced printer
- Outsourced fulfillment vendor
- Bank
- Law enforcement with subpoena
- Digital Advertising Agency

#### Sensitive PII

- Yes

#### Sensitive PII Category

- Financial Information

© Copyright 2018 Kantara Initiative, Inc.
..and Machine readable

- Signed JWT
Receipt Viewer

Please Note: This page and functionality is still under development, please make note of any issues or bugs

Receipt Content

Decoded Receipt

Raw Content   Kantara v1.1   GOPR

CR V1.1 fields mapped to GDPR lexicon
Version: Ki-CR-v1.1.0
Jurisdiction: Finland
Consent Timestamp: 1535290280
Collection Method: Consent page during login
Consent Receipt ID: fc12f55c3178520ee7613ab942351908278c78d92d
Language: en

Parties Fields
Data Subject ID: andrew@interopdemo.com
Data Controllers:
- Data Controller: Ubisecure Bookshop
- Data Controller Name: John Moore
- Data Controller Address: moore@ubisecurebookshop.cc
- Data Controller Email: +358-29-1700-851
- Data Controller Phone: https://www.ubisecurebookshop.com/privacy

Privacy Policy

Data, Collection, and Use Fields
Services:
- Service: Digital subscription and news a
- Purpose: FULL
- Purpose Category: EXPLICIT

© Copyright 2018 Kantara Initiative, Inc.
specification and the MyData 6 Principles

- Human-Centric control of Personal Data
- Individual as the point of Integration
- Individual Empowerment
- Portability: Access and Reuse
- Transparency and Accountability
- Interoperability
Future Work

- Update Consent Receipt specification
- CR Templates for multi-jurisdiction, and Privacy Notice template
- Make it a ‘data receipt/certificate/contract’
- Co-ordinate Kantara’s CR, UMA and UST with Consent Practices WG
- Encourage inclusion in codes of practice
- Conformity assessment scheme
- Issue trust marks
Conformity Assessment for Personal Data standards & specifications coming..
Nurture. Develop. Operate. – that’s what we do

colin@kantarainitiative.org
Twitter: @KantaraColin @KantaraNews
Join us at https://kantarainitiative.org/membership/