Minimum Viable Consent Receipt (MVCR) Specification v.05

Contents

Frontmatter

Status

First draft v0.04 for a complete outline for v.05 (note: first v.1 should be a functional spec by example)

Action Items

- [x] Markus Sabadello Insert walkthrough demo links).
- [x] John Wunderlich Edit the content and working, make less passive and more succinct, help make this the most simple bare bones but functional spec possible for first version.
- [x] Mark Lizar Open Notice Demo (in progress).
- [x] Mary Hodder Content editing, formatting review and updates ongoing.
- [ ] needs a flow chart
- [ ] finish consent receipt request extension and link to technical information

Version Tracking

Version	Status	Writer	Editor	Notes

v.01	Done	Mark Lizar	Mary Hodder	Summary of Intent
v.02	Done	Mark Lizar Mary Hodder	John Wunderlich	Stakeholder Analysis
v.03	Done	John Wunderlich, Mark Lizar	Mary Hodder	Summary of Compliance Contents
v.04	Done	Mark Lizar, Markus Sabadello	John Wunderlich Mary Hodder	Spec Outline & Demo (Mark), Technical Walkthrough (Markus)
v.05	In Progress			

Note to Collaborators

- Before you save please note what you changed in the field provided to the left of the save button
- For any structural changes to the tables or format please request these changes in the comment box, not by directly editing the spec itself

Links to Dependent Documents

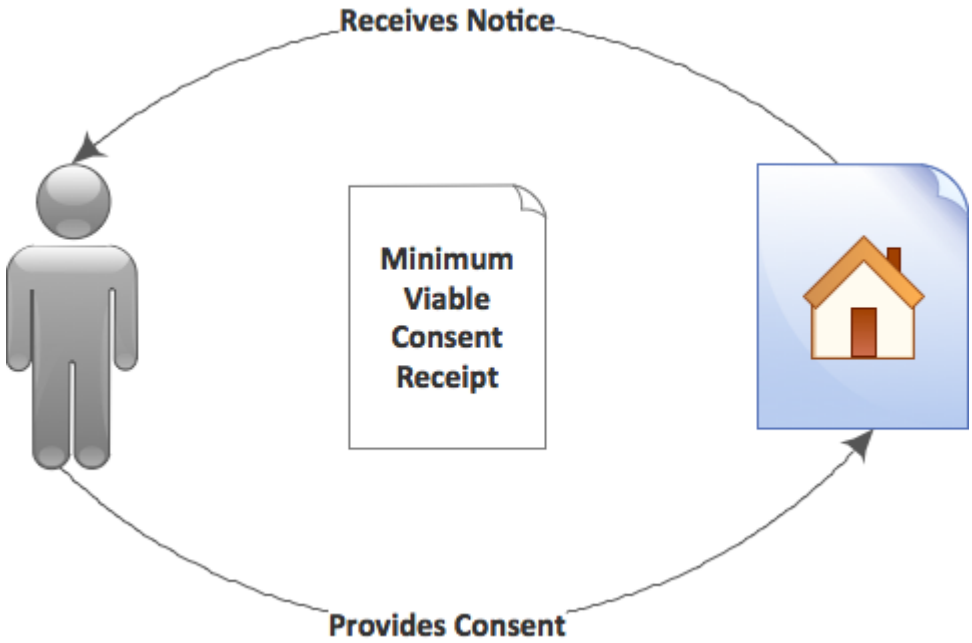
- Latest Consent Receipt Template
- Example 1: Open Notice Receipt Implementation
- Example 2: Respect Network PClound Implementation
- Ext Example: 3rd Party
- Compliance Audit
- MVCR Consent Notice Legislation Map
- Hackathon Video and Convergathon Hack Notes from July 12&13 2014 -->
- Scale of Compliance Use to measure the legal compliance of a consent receipt

Respect Network (RN) Technical Demonstration:

- Store a Consent Receipt in your RN personal cloud using XDI: http://amazon-respect-consent.herokuapp.com/
- List Consent Receipts in your RN personal cloud: http://open-notice.github.io/respect-network-receipts/

Introduction

A minimum viable consent receipt to document consent on the Internet is intended to serve the same purpose as a receipt for a cash transaction. It will provide a record of a transaction where notice of intent to process personal information is provided and consent for personal data processing is returned. Receiving a consent receipt immediately after a web, mobile or other internet based transaction provides an individual with an opportunity to confirm and, if needed, challenge collection of their personal information. Similarly, the consent receipt provides the data controller a clear signal as to what they can and cannot do with that person's information. The consent receipt provides protection for both sides against misunderstanding and can demonstrate compliance with regulations in the jurisdiction in which it was issued.



The MVCR will enable simple two party personal data transactions to be recorded by both sides (above). Extensions and developments of the consent receipt infrastructure will allow auditing and third party (including regulator) validation and confirmation of consent notices for compliance.

Background

The Open Notice Initiative is an effort that calls for open consent practices. This has resulted in the development of this specification for a Minimum Viable Consent Receipt (MVCR).

Overview

This specification creates a common format for provisioning consent receipts. The Minimum Viable Consent Receipt Specification will provide organisations with the ability to create and provision a record of consent. Proper construction of a consent receipt will require the record to be based on the minimum notice requirements for the jurisdiction in which the organization is operating (e.g. the jurisdiction of the data controller and internet location where the consent is located)

In addition to the specification for the MVCR, this document provides a simple audit and compliance scale to show by example how to assess the extent to which an issued consent receipt (CR) meets the standard of a minimum viable consent receipt.

The MVCR will be extensible so that it can include items such as extended notice compliance details, operational context, and utlised as a channel trusted architecture, services and Privacy Enhancing Technology:

1. Consent notice details can be appended to the MVCR to accommodate different personal data sensitivity, data sharing and additional contextual compliance requirements.
2. A context field is a field in the MVCR indicating that there are contextual conditions and exceptions to consent that can be listed and applied by an organisation to the context of receiving consent (e.g. medical emergency overrides). In the MVCR the context is a flag with yes or no. If yes, the provider is stating that they implement a check list of contextual consent requirements. Additional contexts can also be added to a consent receipt.
3. Organisations can append trusted services links/icons to the receipt and further extend the assurance provided to capture multiple consent notice types e.g. cookie, terms of use.

> ***Specification by example*** *(SBE) is a collaborative approach to defining requirements and business-oriented functional tests for software products based on capturing and illustrating requirements using realistic examples instead of abstract statements. It is applied in the context of agile software development methods, in particular behavior-driven development. This approach is particularly successful for managing requirements and functional tests on large-scale projects of significant domain and organisational complexity.[1]* (https://en.wikipedia.org/wiki/Behavior-driven_development)

A key aspect of 'specification by example' is creating a single source of truth about required changes from all perspectives. This document is that source for the MVCR.

Objectives

The aim of this specification is to produce a receipt in a format that includes links to the policies asserted in the consent receipt. This will require an 'open notice' framework so that the policies can be verified and validated by third parties and regulators.

1. An organisation can use the MVCR to self assert that they are providing notice and getting implied consent in compliance with their policies and applicable regulations
2. A service user (individual) can save the MVCR to a personal data store and self assess if the receipt is compliant with the policies and practices of the organisation

Interoperability & Scalability

- Interoperable: a common format enables the consent provisioner (the individual) to mange consent globally, interoperability
- Open Notice is currently working on an open source *Open Consent Registry* (OCR) which will be a customisable registry that automates the functions required to provision, process, update and use consent receipts at scale.

Glossary

Consent Receipt (CR)	A single record of notice and consent created at the point where consent was provided or deemed to be provided (and the consent receipt should make clear which is the case).
Data Controller (DC)	An entity that processes personally identifiable information on behalf or and in accordance with the instructions of a data subject.
Data Subject (DS)	A natural person who is provides consent for the collection, use and disclosure of their personally identiable information.
Minimum	A Receipt will contain links to all policies that inform the consent.
Operational Context of Consent	The list of requirements for notice and consent in the jurisdiction and context in which the consent is given.
Personally Identifiable Information (PII)	Any information that (a) can be used to identify the Data Subject to whom such information relates, or (b) is or might be directly or indirectly linked to a Data Subject.
Trusted Services	A provider of Trust or Privacy icons, standard assurance, reputation services, trusted networks, trusted protocols, etc
Viable	Meets or exceeds regulatory minimum for notice in the jurisdiction where it is issued
Open Notice Framework	The collection and openning of organisational privacy policies and terms some projects that do this exist already; E.g. TOSSBACK

Minimum Viable Consent Requirements

The Minimum Viable Consent Receipt (MVCR) provides information contained in data fields that are used to link to the consent policy of the Data Controller in effect at the point consent is provided. (see Example1: Personal Cloud Storage of Receipt)

> ***Note:*** *For the consent receipt to be auditable and verifiable the consent policy must be accessible by any entity with the URI for the policy. Subsequent changes to the policy should not invalidate the URI for the policy in effect with the CR was issued.*

MVCR enables organizations to self-assert compliance with legislation and their own policies. The open notice (URI) provides this assurance in a transparent manner. To be compliant, a DC provides an auditable self-asserted MVCR which states that the DC will implement the contextual notice requirements listed in that MVCR. Most Data Controllers that identify the information that they collect, specify how it will be used, and that commit to not share personally identiable information with 3rd parties and to not collect sensitive personally identifiable information will be in compliance with most standards. If a DC does share personally identifiable information and/or collects sensitive personal information, an org can develop a custom extension, use an existing standard or register their consent receipt with trusted service providers. Trusted Service providers can provide assurances and audit frameworks that enable compliance with more stringent and complex obligations for sensitive information and/or 3rd party disclosure.

A MVCR that demonstrates compliance will assure a level of basic regulatory compliance and provide a communication channel for consent and notice. It is a digital record that both parties have. A human readable consent receipt should make sense at a glance, enable one click links or contacts with a data controller contact, and enable easy access to statements about purpose(s) and trust. (Note:Advanced applications would enable in context control of consent and use of data.) The receipt specifcation focuses on the minimum visual (human readable) format and a the specified machine readable record that can be aggregated, audited, and visualised. This open format can then be used by other projects to provide a record (visibility to trust services and PETS) In conjunction with other existing systems a consent record can be effective self-regulatory facilitator addressing many challenges with simple transparency of data control.

MVCR: Consent Notice Fields

Field Name	Field Description	Field Purpose / Explanation	Reason Field is Required	Cloud Receipt Capture & Sign: Format example in (XDI)

				Note: following lines all prepended with ([=]!:uuid:1111/ [+]!:uuid:9999)
Data Subject (DS)	Name or pseudonym of the Data Subject at minimum	Data Subject is primary party to consent	Data Subject is the consent contributor and primary party of the consent (which is why this is the first field of the MVCR) If not signed by Data Subject then its use post consent may be limited.	Data Subject: Alice [=]!:uuid:1111
Address (and jurisdiction) of Data Controller (DC)	Name of the entity issuing the receipt	Should be the entity / organization in receiving the personal data and is responsible for consent compliance.	Is the Data Controller and the primary party responsible for administration of the consent and consent receipt	Data Controller: Amazon [+]!:uuid:9999
Purpose	The purposes for which the personal information is being collected.	This is a single purpose at minimum linked to the short purpose notice, or policy of purpose.	A purpose notice is a basic and common legal requirement and functionally a requirement of consent.	[#receipt]!:uuid:1234[<#purpose>]<@0>&/&/"We need to process your payment." [#receipt]!:uuid:1234[<#purpose>]<@1>&/&/"We need your data to prevent fraud." [#receipt]!:uuid:1234[<#purpose>]<@2>&/&/"We will advertise to you."
Location of Consent	The location of the consent provision. from which the consent receipt originates.(For example the web page with the consent button.)	This indicates the 'point of consent' - hopefully a button where the user clicked "I agree" or "I consent" (i.e. the biggest lie) Can be a URI, URL, URN, This can also be a physical space where surveillance legal notice requirements exist (EU) - Global Positioning System (GPS)		[#receipt]!:uuid:1234<#location><$uri>&/&/"....."
Sensitive Personal Data Flag (Y/N)	Flag to categorise the information collected as sensitive or not (Y/N)	Each jurisdiction has classifications of sensitive personal information (privacy): The generally include health, financial, child protection (>14), youth protection(>19 or >22), educational, religious, Union categorisations	If Yes, then additional notice requirements are needed to confirm its compliance status. If No, then the consent is automatically compliant	[#receipt]!:uuid:1234<#sensitive>&/&/true
Third Party Sharing	Flag whether data is shared with third parties. (Y/N)	If true, then compliance is dependent upon additional notice requirements not present in a MVCR. This can be addressed with the "Third Party Sharing" extension.	If Yes, then additional notice requirements are needed to confirm its compliance status. If No, then the consent is automatically compliant	[#receipt]!:uuid:1234<#third><parties>&/&/true
Timestamp	When consent was obtained	To record when the user, either by implication or explicity, granted consent for the purposes described.		[#receipt]!:uuid:1234<$t>&/&/"2014-07-13T21:32:52"
Privacy Policy	The issuing entity's privacy policy (either inline copy, or reference to URI)	If not available, should provide a notice that it is missing	Is the minmum Policy (or short notice) Needed to create a consent receipt.	[#receipt]!:uuid:1234<#privacy><#policy>&/&/"copy of privacy policy here" or [#receipt]!:uuid:1234<#privacy><#policy><$uri>&/&/"https://..."
Operational Context Flag	Flag wether the Operational Requirements are present or not. (Y/N /Unknown)	For the presentation of consent there are contextual and prescriptive requirements in legislation, a check list of these elements is being crated in this draft below.	Consent has contextual compliance requirements for the notice to be sufficent. These depend on the location and format of the consent notices An organisation displays agreement (or not) to implement these OC requirements and this is reflected on the consent receipt.	

The MVCR Format Notice Requirements are currently in progress. The full reference table can be found here. The table below may not be current.

Notice Requirements A Receipt Must Meet	**Description**	**UK** **UK DPA 1998** **http://www.legislation.gov.uk/ukpga/1998/29**	**EU** **Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995**	**USA** **For Sharing Personal Sensitive Information with 3rd Parties**	**Canada**	**APEC**	**P3P**	**FTC FIPPS**	**OECD FIPPS**

			http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML						
Contact of Data Controller (DC)	Legally required to provide contact details of the DC	Schedule 1, Part II, 2.3 a)the identity of the data controller,	X						
Address of Data Controller (DC)	Legally required to provide contact details of the DC	(b)if he has nominated a representative for the purposes of this Act, the identity of that representative,	X						
Purpose(s)	Legally required to provide purpose for data control	(c)the purpose or purposes for which the data are intended to be processed, and	X						
Third Party Legal Requirements Transparency	This is a flag to see if additional notice extensions are requirements to assess compliance	(d)any further information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair.	X						
Sensitive Personal Information Collection Transparency	This is a flag to see if additional notice extensions are requirements to assess compliance	X	X						

Extensions for the MVCR

An extension can be appended to the MVCR to enable an organization to meet policy or other goals that are not regulatory requirements, but may be deemed to be best practices, or provide a better user experience for the data subject.

Extension Types

Core Extensions	Extend the MVCR
Operation Context	Core extension > *Note: For the MVCR First Draft there is only the online website format context, additional context can be added by extension*
Trusted Services	Trust Framework Extensions
Usability	Extensions that increase usability and adoption of the consent receipt

Core Extensions

In each jurisdiction, there are sensitive types of personal information found in privacy and data protection law. Each sensitive type corresponds to a jurisdiction, is defined by an industry, and has prescribed context requirements for the use of a notice. Core extensions can be added to the MVCR to meet more complex notice requirements and meet the requirements of multiple regulatory jurisdictions.

Core extensions can be used by policy makers to localise the use of consent notices to operational contexts and more granular applications of enforcement.

Operational Context (OC): Legal Requirement for the MVCR Context (in progress)

This is essentially a check list of provisions for the implementation of a consent notice. It will be used to provide assurance that the consent is fair and reasonable. There are specific and existing policies that are used to create this checklist. Many jurisdictions have prescriptions for the text required to accompany specific types of consent as terms defining those requirements. This is also the case with notice requirements.

As a part of creating a receipt for a data subject an organisation displays that they have agreed to implement (or not), the OC requires a checklist accompany the receipt. This functions as a flag: yes or no, If yes, then there is a self assertion that the notice will be provided in a fair manner with all of the required considerations as prescribed in law in that jurisdiction. This is then reflected on the consent receipt.

> ***Instructions:*** *This is a self asserted option, the Operational Context is a yes or no flag that the receipt provisioner turns on or off. Operational context is dependent on the location of consent, the use of personal data, the origin of the data, and type of data provided. As Context of a consent can vary significantly operational requirements will also vary.*

Fair & Reasonable Consent Conditions

This table documents the checklist of elements for Operational Context.

Context: Location Specific	**Description**	**UK** **Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995** **http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML**	**EU**	**USA**	**Canada**
Website consent form	Provides notice at point of consent for the consequences of not provisioning consent	X (put in legal ref)	X		
Website consent form	Indicates what is required, and optional information, to provide for consent	X	X		
Mobile application					
Entering Physical Space	Sign posted upon entry to physical space				

Trusted Services

3rd party trusted services can also be used to extend the compliance or trust inherent to corporate process and these can be added in the form of linked Icons to a MVCR.

MVCR Proposed Extensions Table (in progress)

These are the extensions tables. This is an active list of extensions being planned and/or developed need to include the name of the filed, have a description, context, benefit, and examples.

The various table currently include.

Re-Usability

Re-Usability of a consent may come from adding a protocol, or a compliance level, or a receipt capture option. In the table below, a 'Consent Receipt Request' extension is listed-- this was developed at the Data privacy Legal Hackathon, Feb 2014.

Extension Road Map

List of current or planned extensions

Priority	**Extension Type**	**Field Name**	**Description**	**Instructions**	**Legal Requirement Jurisdiction (this item must be listed on LR table)**	**Context** **(this item must be listed in the Operational Requirements table)**	**(Re-Usability / Interoperability Benefit)**	**XDI Example**
1	Core Extension	Jurisdiction	The jurisdictions of the parties: the data protection authority is mandatory.	• this is taken from the data controller address and the location of the consent. • optional the jurisdiction of for the data subject can be added with the consent of the data subject and if the receipt is stored directly in a personal data store.	All		Re-Usability: enables receipt to be used as evidence or for the purpose of legal data controls out of context of the consent event.	[#receipt]!:uuid:1234<#jurisdiction> /$ref/[=]!:uuid:1111<#jurisdiction> [=]!:uuid:1111<#jurisd

								iction>&/&/"US" [+]!:uuid:9999<#jurisdiction>&/&/"DE"
2	Core Extension	Collect Sensitive Personal Data		1. Sensitive personal data categories need to be listed by jurisdiction 2. legal and industry notice requirements need to be listed, 3. the OC table needs to be updated with the physical requirements				
3	Core Extension	3rd Party Trusted Services Extension (this is the functionality for Registry)	ability to add trusted services to the minimum viable consent receipt	This incorporates 3rd party sharing and purpose listing format				
4	Request Extension	Consent Receipt Request Extension	This is a button a user can press to request a consent receipt from a business	• scrape consent session and send request to MVCR DC Contact field for a reciept (byproviding a form)	• hypothetical: if an org responds with all of the information, they automatically receive an above-compliant rating	This is for all contexts of the MVCR	Re-Usability	
5	Operational Context Extension - Cookie	Policy Extension for Consent Cookie Policy Link	The issuing entity's cookie policy Link (either inline copy, or reference to URI)	If not available, should provide a notice that it is missing or self assert an icon	Legally in the EU a cookie requires explicit assent			[#receipt]!:uuid:1234<#cookie><#policy>&/&/"copy of cookie policy here" or [#receipt]!:uuid:1234<#cookie><#policy><$uri>&/&/"https://..."
6	Operational Context Extension - TOS / TOU	Policy Extension for Terms of Service Link	The issuing entity's terms of service (either inline copy, or reference to URI)	If not available, should provide a notice that it is missing	Legally Terms need to be open and accessible in order to be fair and reasonable.			[#receipt]!:uuid:1234<#tos>&/&/"copy of tos here ..." or [#receipt]!:uuid:1234<#tos><$uri>&/&/"https://..."
7	Operational Context Extension - Privacy / Data Policy	Policy Extension for Privacy Policy / Data Policy Link	The issuing entity's privacy or data policy (either inline copy, or reference to URI)	If not available, should provide a notice that it is missing	Legally Privacy Policies are required in the US, and should be open and accessible in order to be fair and reasonable.			[#receipt]!:uuid:1234<#pp>&/&/"copy of privacy policy here ..." or [#receipt]!:uuid:1234<#pp><$uri>&/&/"https://..."
8	Retain copy of all notices with receipt	Store all notice data option as a part of signed receipt						

Specification Examples

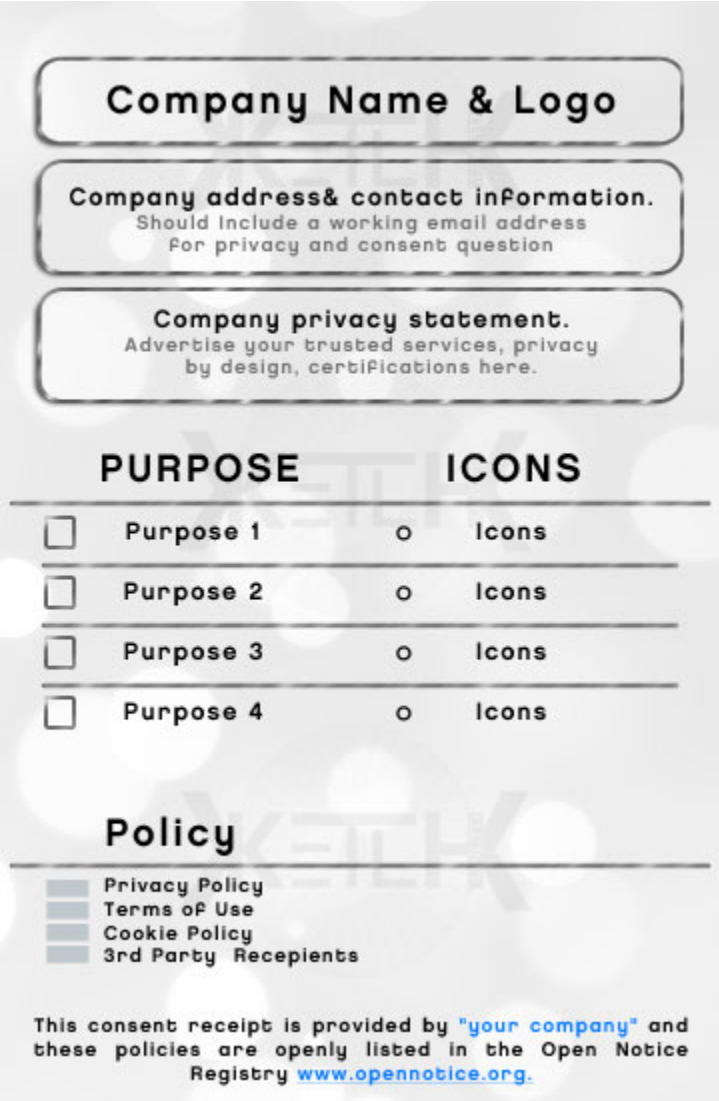
Open Notice Web Site

Consent Receipt Technical Demonstration

- Provides a simple consent receipt to show compliant policy (in progress) http://on.smartspecies.com/receipt-example/
- Show Directory of Supporters with consent to appear directory managed by supporters personal data store (in progress)

MVCR Consent Receipt Template

The MVCR has a base template v.1 that we have using to wireframe consent receipts: V.1



Latest Template Version

We provide a template to guide design and development of the MVCR. A GUI design is out of scope of this specification version. What is provided by default is the Consent Receipt Template we are using for technical design.

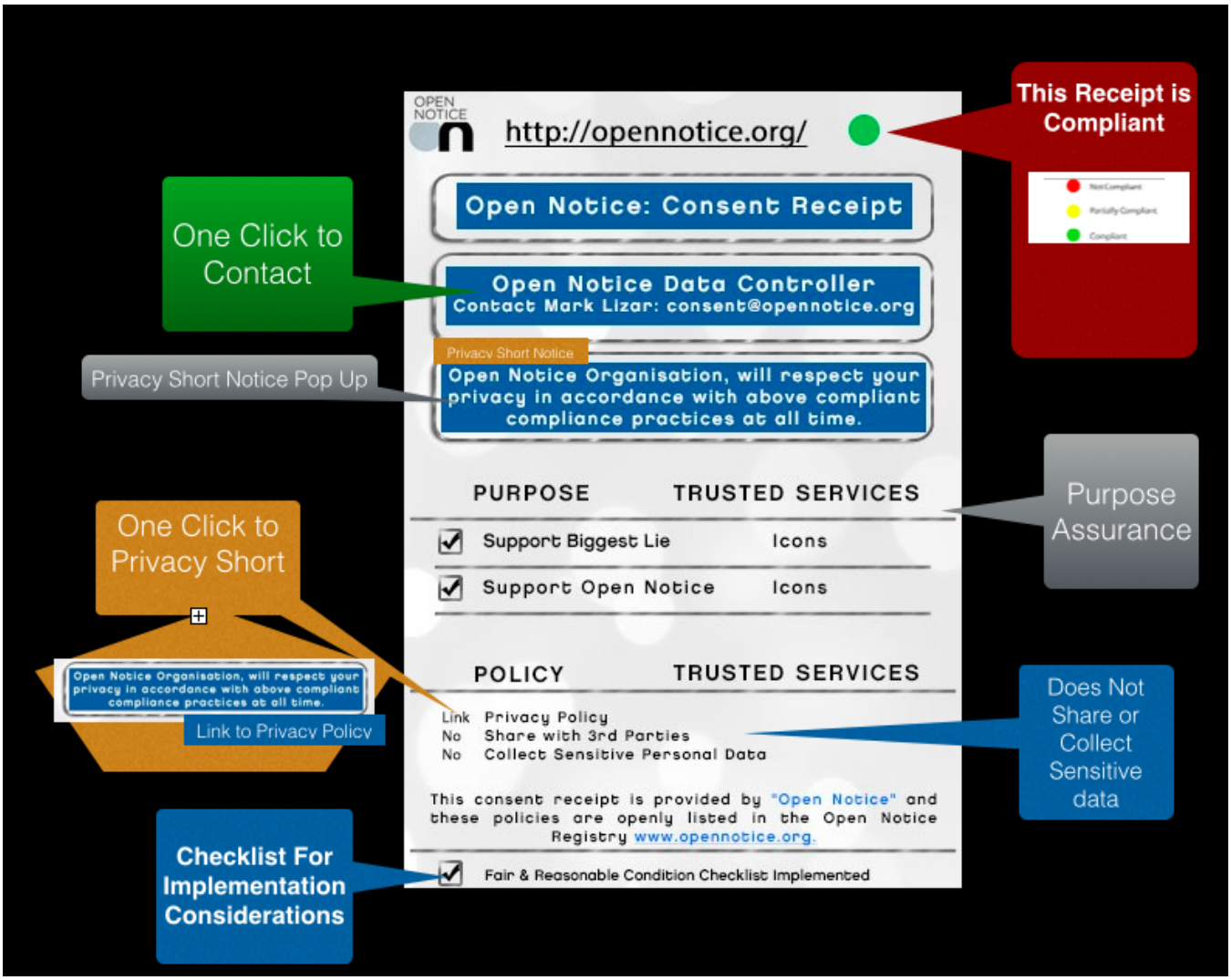
Example 1: Open Notice Minimum Viable Consent Receipt

Open Notice Website - Consent Receipt - Technical Demo

- Provides a simple consent receipt to show compliant policy (in dev progress) http://on.smartspecies.com/receipt-example/

(Example (in progress) can be found at http://on.smartspecies.com/support-open-notice/

Image:ON-CR: Example



Example 2: Storing Receipt in Personal Data Store: Technical Walkthrough Example with Respect Network

Respect Network (RN) Technical Demo:

- Store a Consent Receipt in your RN personal cloud using XDI: http://amazon-respect-consent.herokuapp.com/
- List Consent Receipts in your RN personal cloud: http://open-notice.github.io/respect-network-receipts/

Amazon Respect Use Case: With the Respect Network and Open Notice
(Note: Amazon Respect is a Fictitious organisation used here only as an example)

(http://open-notice.github.io/consent-receipt/amazon-mock/signup.html)

Implementation of consent receipt which is signed & created by a DC and stored in a personal cloud.

To make consent receipt use scalable, CRs needs to be signed and put in a personal data store as part of the Respect Network.

This specification and demo is created to demonstrate a MVCR being implemented without the need for an Open Notice Registry with the Respect Network (Trusted Network) Trust Framework which natively has the ability to provision receipts to the highest level of compliance. This walk-through demo is intended to demonstrate how a consent receipt can be stored in a personal cloud from this spec document and demonstrate 'Fast Track' usability.

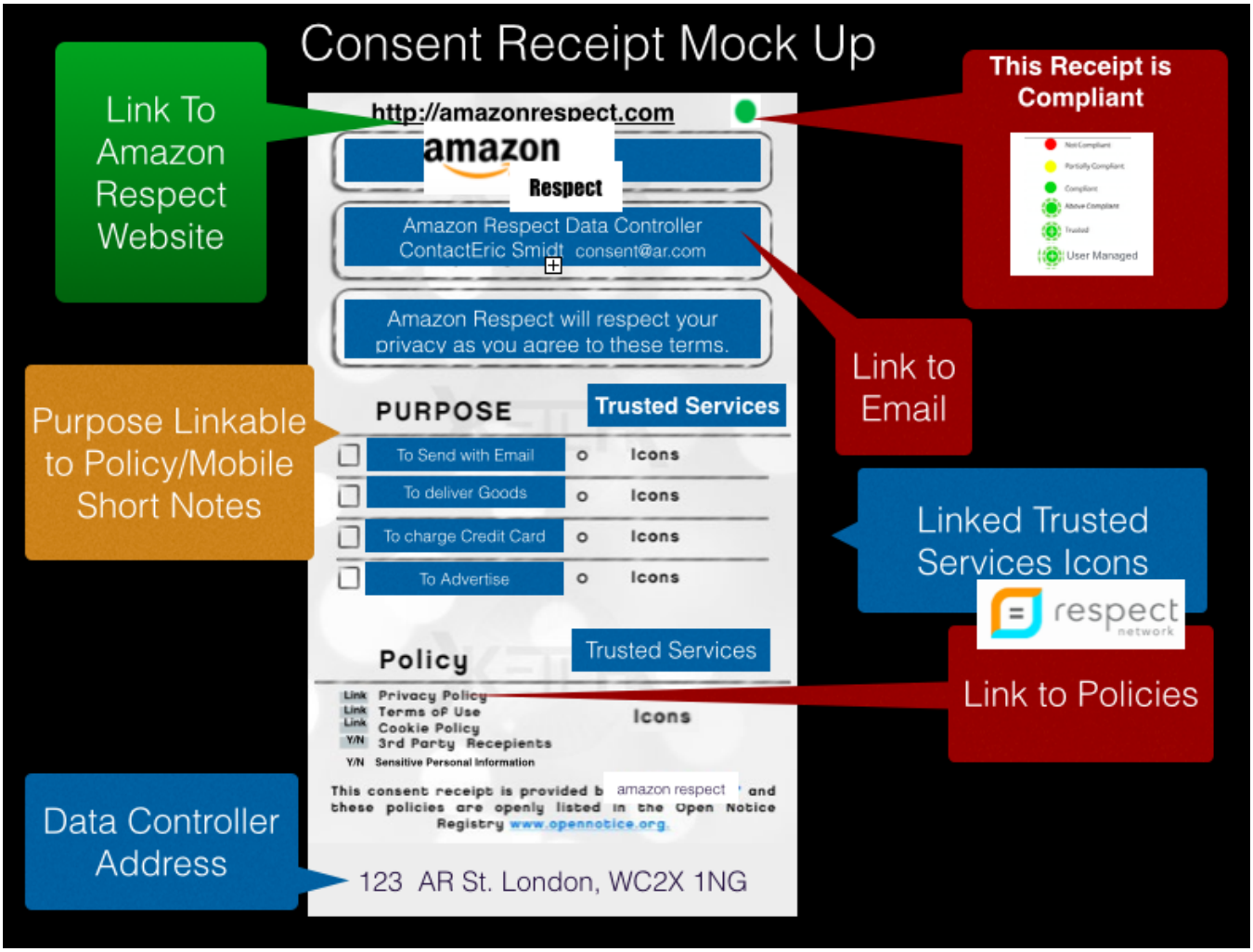
1. DS goes to amazonrespect.com website
2. Website presents form and asks for consent:
    a. either to sign up initially, or
    b. for additional consent and profile management when already logged in

3. DS agrees (clicks on “i agree” button)
4. DC website initiates creating a receipt for the consent just given.
5. DC checks for reciept data collection and notice extensions and finishes creating the receipt.
6. The receipt is signed by DC.
7. DC website sends an XDI message to DC’s RN cloud to store the signed receipt.
8. DC shows popup window with options (what to do with the receipt). The signed receipt is embedded in the popup window.
    a. email to DS using email address in amazon profile
    b. store in users personal cloud
    c. capture in browser
    d. download receipt as pdf
    e. opt out of a receipt.
9. DS clicks on “store receipt in my RN cloud”. (default option)
10. Popup window asks DS: what is your cloud name?
11. DS types cloud name =alice
12. Popup window runs XDI discovery to find DS’ RN cloud
13. Popup window sends an XDI message to DS’ RN cloud to store the signed receipt

The Re-usability of a MVCR can then be made scalable for re-use in aggregate. This is beyond the point of consent for the data subject, with a process in whch the receipt is digitally signed by both parties.

This process also identifies the jurisdiction of the Data Controller and of the Data Subject. This example includes signing of the receipt by the DC. (Note: The digital signing of the DS (data subject) is currently out of scope of the first draft1.)

MVCR Mock Up for Amazon Respect Use Case



MVCR Compliance

Audit

****

Each field on a Minimum Viable Consent Receipt is included in response to legal notice requirements. If legal requirements are present, a "yes" or "no" flag is added to the consent receipt.

The MVCR has a maximum rating of "compliant." Additional Ratings e.g. "above compliant", "trusted", and "user managed" will be provide with extensions.

A compliant rating can be self asserted within the provision of this consent receipt. A scale of compliance is used for each of these notice information elements. If one or more elements do not work, or are not verifiable, then a status of "partially compliant" is provided. Further infrastructure is needed to record disputes to self asserted claims.

If all elements are not verifiable, then the consent is no longer compliant or verifiable for basic compliance level rating.

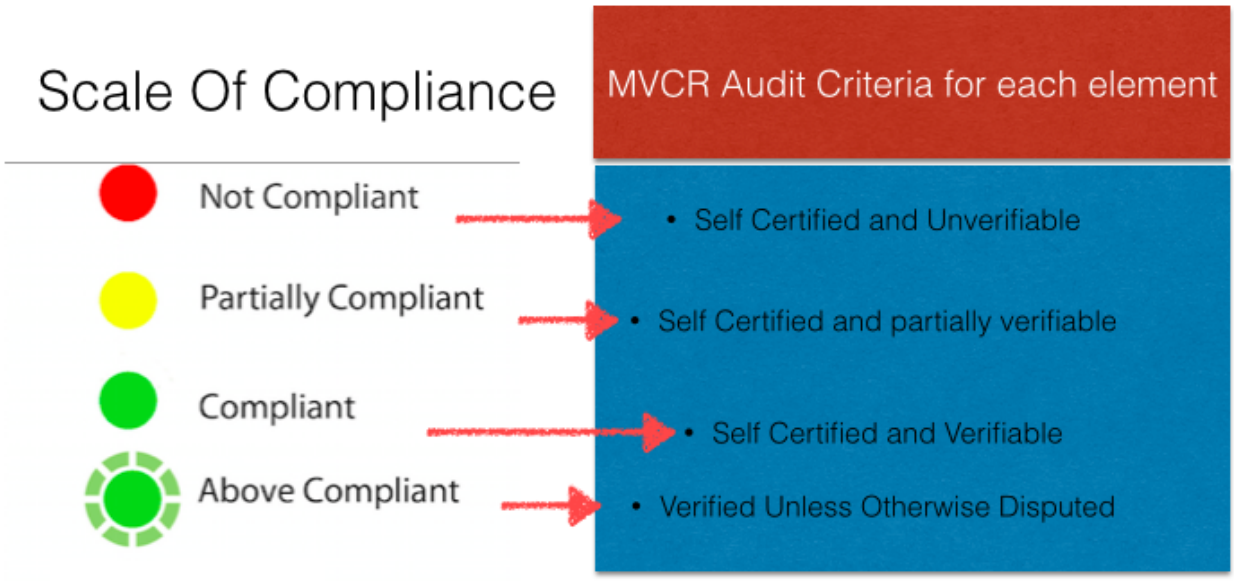
Notice Compliance Checklist	Non Compliant	Partially Compliant	Compliant	Above Compliant	Trusted	User Managed
Contact of DC			X			
Address of DC			X			
Purpose(s)			X			
Sensitive Data (If NO)			X			
Share with 3rd Party (If No)			X			
Agree to implement context checklist? (Y/N)			Yes			
Any items above self asserted? Disputed or un-verifiable (Y/N Flag) (If No) (if Yes and unresolved = Non-Compliant)	Y		N			

(NOTE: Additional architecture is needed to mediate compliance level ratings.)

MVCR Compliance Assurance Audit & Compliance Scale

Each item in the MVCR will be rated with this scale presented below

- The compliance scale below is based on the ICO table of compliance located here from the UK Information Commissioner's Office: http://ico.org.uk/for_organisations/data_protection/working_with_the_ico/~/media/documents/library/Data_Protection/Detailed_specialist_guides/auditing_data_protection.pd



Trusted Services Appendix

Trusted services, networks and frameworks can be used to meet or exceed notice (and therefore consent) legal requirements. They may also address the need for assurance and trust for people, in order that consent and its management can be automated and more usable. It is for seen that a notice registry is the natural place for trust services to register their services.

A process for auditing and verifying all trust services needs to be in place for trust services to be trustable. Then when an organisation enrols into the registry they can also add (or manage) trust services that has been added to the receipt.

This table maps the list and categories of assurance framework with examples and notes on interoperability to a category of service.

Type of Trust Framework	• Consent Policy Format	**Personal Policy Preference**	**Consent Extension Location**	**Trusted Service Provider Examples**		
Tracker: Analytics etc.	Cookie	Do Not Track	browser header	cookiepedia, privacy clearing warehouse, Ghostery		
Terms of Use Policy	Agree to terms			TOS;DR, Citizen Me		
Policy Tracking Services	Policy Comparison	Has terms materially changed (is consent still compliant?)		TOSBack		
	Consent Type	What kind of consent has been received	To record the type of consent or whether there is an exception to the requirement for consent.			
Reputation	Trust Framework			(all trust services provide reputation)		
Privacy Icons	Pictorial Short Notices			Disconnect Me		
Third Party Ratings	Effect ratings from third parties			Disconnect Me		
Capture of Personal Preference at Time of Consent	Does the issuing entity acknowledge DNT	If not available, should provide a notice that it is missing		[#receipt]!:uuid:1234<#dnt>&/&/true		
Data Control Protocol				User Managed Access		
Trusted Network Service				Respect Network		
Standards						
Certificates				TrustE		
Levels of Assurance				KI: Identity Assurance Framework		

Design Appendix:

Summary Design Goals to Assess: MVCR

1. Transparency: The MVCR receipt is a common format for the legally required policies which provide notice. Links to all notices demonstrate a much higher level of minimum viable notice (for consent) legal compliance. This standard is intended to augment the existing legal notice and consent infrastructures that is already in place and reward greater transparency of consent with higher default usability. .
2. Extensible: The MVCR Spec is intended to be easily extensible and auditable, with a jurisdicitional legal compliance audit built in for making transparent legal context and controls of a consent transaction. Meaning that consent legal notice requirements are different by jurisdictions, industry, for various sensitive data types, for sharing to 3rd parties, tracking (cookie consents), in additional to personal and contextual consent preferences of the individual. Extensions are notice requirements layered onto this MVCR format to meet and match legal requirements and trust frameworks to address cross jurisdictional management of consent.
3. Trusted Services Vehicle: A receipt passed to the service user at time of consent provides a legal trust framework to build upon. As a result it is the MVCR is intended as a vehicle for delivering trusted services to the individual. A stakeholder can utilise trust services, which are then linked to the receipt, which further extend the compliance and "fast track" usability of consent and identity management by using a spec compliant receipt. Eg.privacy icons, TOS reputation, certifications, trusted networks, and protocols
4. MVC is intended to be an all purpose consent process enhancement.
5. This MVCR specification is intended to be used so any organisation can implement the spec and provide a MVCR.