Consent Receipt API

This server provides a consent receipt generation API. The API consists of a single endpoint:

http://www.consentreceipt.org/mvcr/api

This endpoint accepts HTTP POST requests with input in the form of JSON (application/json) documents and output in the form of a signed JSON Web Token (application/jwt).

How It Works

The API takes in a JSON document describing the consent transaction for which the receipt is to be generated. This object includes artifacts such as the presiding jurisdiction for the consent action, an identifier for the party consenting. The output of the API is a signed JSON Web Token (JWT) whose payload consists of all of the input data as well as several additional fields. This JWT is digitally signed by the server.

Top-level fields in the input JSON object

Field Name	Data Type	Description	Example Input	Required
jursidiction	string. ISO two-letter country code if applicable, otherwise free text	this is the location of processing	US	✓
sub	string.	Subject provided identifier, usually email addressClaim, defined/namespaced by the issuer	example@example.com	✓
SVC	array of strings.	this is global context for consent	["Company Name" , "Service Name"]	✓
notice	string. HTTP URL	Link to the short notice enables usability and layered policy. to provide enhanced transparency about data collection and information sharing practices	http://example.com/notice	✓
policy_uri	string. HTTP URL	the internet and immediately accessible privacy policy of the service referred to by the receipt	http://example.com/privacy	✓
data_controller	object	The identity and company of the data controller and any party nominated to be data controller on behalf of org	{"on_behalf": true, "contact": "Dave Controller", "company": "Data	✓

The object contains information of the data controller in the following fields: Data Field Name Type **Description** Example Input Required on_behalf boolean. acting on true behalf of an organization? Jon Doe contact string. person to contact Data Controller Inc. company string. company name address string. physical 123 Main St., Anywhere address email string. contact email jon@datacontroller.com Email address address contact 00-000-000-0000 phone string. Phone phone number number

{"on_behalf": true, "contact": "Dave ✓
Controller", "company": "Data
Controller Inc.", "address": "123
St., Place", "email":
"dave@datacontroller.com", "phone":
"00-123-341-2351"}

consent_payload	object. Keys are the name of the consent, values are whether or not the user has agreed.	Examples include: Device Identifier, UID, IP Address, Browser Fingerprint, DNT signal client header, .Mobile device id	{"privacy policy" : "agree","ToS" : "agree"}	✓
purpose	array of strings.	this is a short description of the purpose list of normative values in a global registry (services need to map specific actions to things in the registry should we require services to document these mappings?)	["marketing", "research"]	✓
pii_collected	object. Keys are the name of the field, value is the information collected.	Personal information collected in relation to, or adjacent of purposes specified	<pre>{"name" : "Example Example", "email" : "example@example.com"}</pre>	✓
sensitive	array of strings.	What is determined to be personal information can be from a big list of all defined personal information categories from all jurisdictions. (this indicates that it is possible	<pre>["http://example.com/medical", "http://example.com/financial"]</pre>	√

http://api.consentreceipt.org/doc/

depending on where parties are that this is sensitive)

		depending on where parties are that this is sensitive,		
sharing	array of strings.	This refers to the sharing of personal information collected about the individual, with another external party by the service provider, bound under the privacy policy and terms.	["contact information", "demographic information"]	✓
context	array of strings.	Operational Context refers to the conditions that ensure the consent is fair, reasonable and proportional., e.g. if it is on a website, then there are requirements like; are mandatory fields indicated, is there a separate consent for privacy policy and terms of service? set of registry values?	<pre>["active privacy policy consent", "passive terms of service consent"]</pre>	✓
aud	string. HTTP URL	Audience URI that identifies the target service of this consent	http://engageidentity.com/protected	
scopes	string. space separated string values	What you're allowed to do on the service (these can be tied to legal / business / technical layers)	read update	

Additional output fields of the signed JWT

Field Name	Data Type	Description	Example Output
iss	string. HTTPS URL	this is the location of processing	http://www.consentreceipt.org/
jti	string.	Unique identifier for this c onsent receipt	9ef6b81a414b2432ec6e3d384c5a36cea8aa0c30d3dd2b67364126ed80856f9c20654f032eef87ad981187da8c23c1186eefe1503714835c2e952bbb3f22729c
iat	number. Integer number of seconds since 1970- 01-01 00:00:00 GMT	Timestamp of when the token was issued	1435367226

Digital signature information

The output JWT is signed using the RS256 algorithm defined in JSON Web Signatures. The server's public key is published in JSON Web Key format at:

http://www.consentreceipt.org/api/jwk (http://www.consentreceipt.org/api/jwk)

Example

An example input to the API is the following JSON object:

```
{
        "jurisdiction" : "US",
        "sub" : "sarah@example.com" ,
        "svc" : ["amazon", "amazon express"] ,
        "notice" : "http://example.com/notice" ,
        "policy_uri" : "http://example.com/policy" ,
        "data_controller" : {"on_behalf": true, "contact": "Dave Controller", "company": "Data Controller Inc.", "address": "123 St., Place", "
email": "dave@datacontroller.com", "phone": "00-123-341-2351"},
        "consent_payload" : {"privacy policy" : "agree","ToS" : "agree"} ,
        "purpose" : ["marketing", "research"] ,
        "pii_collected" : {"name" : "Sarah Squire", "email" : "sarah@engageidentity.com"} ,
        "sensitive" : ["http://example.com/medical","http://example.com/financial"] ,
        "sharing" : ["contact information", "demographic information"] ,
        "context" : ["active privacy policy consent","passive terms of service consent"] ,
"aud" : "http://engageidentity.com/protected" ,
         "scopes" : "read update"
}
```

This produces output like the following signed JWT:

eyJhbGci0iJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJqdXJpc2RpY3Rpb24i0iJVUyIsInN1YiI6InNhcmFoQGV4YW1wbGUuY29tIiwic3ZjIjpbImFtYXpvbiIsImFtYXpvbiBleHByZXNzIl0sIm5vd GljZSI6Imh0dHA6Ly9leGFtcGxlLmNvbS9ub3RpY2UiLCJwb2xpY3lfdXJpIjoiaHR0cDovL2V4YW1wbGUuY29tL3BvbGljeSIsImRhdGFfY29udHJvbGxlciI6eyJvbl9iZWhhbGYiOnRydWUsImN vbnRhY3Qi0iJEYXZlIENvbnRyb2xsZXIiLCJjb21wYW55IjoiRGF0YSBDb250cm9sbGVyIEluYy4iLCJhZGRyZXNzIjoiMTIzIFN0LiwgUGxhY2UiLCJlbWFpbCI6ImRhdmVAZGF0YWNvbnRyb2xsZ XIuY29tIiwicGhvbmUi0iIwMC0xMjMtMzQxLTIzNTEif5wiY29uc2VudF9wYXlsb2FkIjp7InByaXZhY3kgcG9saWN5IjoiYWdyZWUiLCJUb1Mi0iJhZ3JlZSJ9LCJwdXJwb3NlIjpbIm1hcmtldGl uZyIsInJlc2VhcmNoIl0sInBpaV9jb2xsZWN0ZWQiOnsibmFtZSI6IlNhcmFoIFNxdWlyZSIsImVtYWlsIjoic2FyYWhAZW5nYWdlaWRlbnRpdHkuY29tIn0sInNlbnNpdGl2ZSI6WyJodHRw0i8vZ XhhbXBsZS5jb20vbWVkaWNhbCIsImh0dHA6Ly9leGFtcGxlLmNvbS9maW5hbmNpYWwiXSwic2hhcmluZyI6WyJjb250YWN0IGluZm9ybWF0aW9uIiwiZGVtb2dyYXBoaWMgaW5mb3JtYXRpb24iXSw iY29udGV4dCI6WyJhY3RpdmUgcHJpdmFjeSBwb2xpY3kgY29uc2VudCIsInBhc3NpdmUgdGVybXMgb2Ygc2VydmljZSBjb25zZW50Il0sImF1ZCI6Imh0dHA6Ly9lbmdhZ2VpZGVudGl0eS5jb20vc HJvdGVjdGVkIiwic2NvcGVzIjoicmVhZCB1cGRhdGUiLCJqdGki0iI50GI1Yzg50TVkMzExNjI0ZGI0M2U0Zjk20GJkYmYyZWMzYTIxNDFhNDU4NTM00DJiMGNiMTFj0GRmMWZjNzkzMDkyYjEx0TJ jYzRlZmE4ZmRlZjFkMGNlZTA4ZGFhMDkwMTlkMTkxYjlmyzY2NGFi0Tg30WQwYWE40GVVNGNmNCIsImlhdCl6MTQzNTg1NTI0MzQ3MSwiaXNzIjoiaHR0cDovL3d3dy5jb25zZW50cmVjZWlwdC5vc mcifQ.MFXoyWoFD-UQRhErGBteXRLHgdB2Rp-EABXIb3gLGU0lv_U-B87ks4GaJd4jLmsMpTvLRKaPlE81xDVirtw9DTFQ79UMKZKyKMMpJSltLXVgWzoEmt_7cxeQPV0IS01djemYmkEN03tN-zhJbYlWeHl3iamFAsXXZZ4rkfRX9i2LTYpIGA5ecdQpqLQ7YimaRta7hTnCNXZs_x57s7uYCLwu--Q1EQKhAgpft4GYI9ziAiTn5KYJdyC6Rdcba5N2NnQzffl0_RhAiCuo9pvcInL3IK6Xf3c-R9XLW QdZj05LBk0 Gn2S6t6BAKhAYWJL687KZ ESXziPXi7TIf nA

The header portion of the JWT contains:

```
{
    "alg": "RS256",
    "typ": "JWT"
}
```

The payload portion of the JWT contains:

http://api.consentreceipt.org/doc/

```
"jurisdiction": "US",
 "sub": "sarah@example.com",
  "svc": [
   "amazon",
   "amazon express"
 ],
 "notice": "http://example.com/notice",
  "policy_uri": "http://example.com/policy",
  "data_controller": {
    "on_behalf": true,
    "contact": "Dave Controller",
    "company": "Data Controller Inc.",
    "address": "123 St., Place",
    "email": "dave@datacontroller.com",
    "phone": "00-123-341-2351"
 },
 "consent_payload": {
    "privacy policy": "agree",
    "ToS": "agree"
  "purpose": [
    "marketing",
    "research"
  "pii_collected": {
   "name": "Sarah Squire",
    "email": "sarah@engageidentity.com"
 "sensitive": [
   "http://example.com/medical",
    "http://example.com/financial"
  "sharing": [
   "contact information",
    "demographic information"
  "context": [
   "active privacy policy consent",
    "passive terms of service consent"
 "aud": "http://engageidentity.com/protected",
 "scopes": "read update",
 "jti": "98b5c8995d311624db43e4f968bdbf2ec3a2141a45853482b0cb11c8df1fc793092b1192cc4efa8fdef1d0cee08daa09019d191b9fc664ab9879d0aa88ee4cf4",
 "iat": 1435855243471,
 "iss": "http://www.consentreceipt.org"
}
```

(https://kantarainitiative.org/confluence/display/infosharing/Home)

The Example Consent Receipt Generator is brought to you through the expertise of the Kantara Initiative Consent and Information Sharing Work Group and through funding provided by the Kantara Initiative (http://kantarainitiative.org/).





(http://kantarainitiative.org/)

http://api.consentreceipt.org/doc/