D.6 Consent API

About this Document

Introduction to iWelcome's Consent API

In CIAM solutions the profiles of end-users typically contain the user’s date-of-birth, name, gender, home address, etc. This will allow companies to address consumers in a more personalised way and to analyse the characteristics of their customer base and adjust their offerings and marketing efforts accordingly. Privacy aware consumers, however, may not be willing to provide companies with too much personal information. They don’t want their personal information to be used for data processing purposes they don’t even know about or they haven’t given their consent for. Consumers want to be in control of their personal information.

Further to this, the GDPR provides regulations to protect the privacy of consumers throughout the European Union. It prescribes rules for the processing of personal data; companies must be transparent about which personal information is somehow collected or processed. Processing of personal data can only take place based on certain legal bases. The most important ones are ‘contractually needed’ or ‘consent’.

What is consent? Consent is a mechanism of building trust between the user and an organisation. Consent is a tool allowing to process (collect, store, use, etc.) user data. For users, requirement of consent offers choice. Users have the ability to express their preference: allow the processing of their data, or not. GDPR defines consent as “*freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*“.
Users must be made aware of the consequences of their decision and how their data is or will be used. Consent also needs to be granular, meaning that different types of consent are possible for performing different tasks if data is used in a number of distinct ways.

iWelcome provides companies with a CIAM solution that allows companies to utilise extended consumer profiles and at the same time puts the consumer in control of their personal information and helps companies to be compliant with the GDPR. iWelcome’s CIAM solution includes the so-called ‘Privacy APIs’/'Consent-APIs' and ‘consent pages’.

The Consent-API focus is on consent as per GDPR regulations; consent given by a consumer to a data controller to do specific data processing on a type of personal data. This definition excludes consumer-to-consumer consents or mandates. iWelcome has based its consent definition on NISTIR 8112. The consent related attributes as defined by this document are partially reflected in the Processing Purpose API and the Attribute Consent API. Attributes that are generic for processing purpose are part of the Processing Purpose schema whereas attributes that are specific to an individual end-user are included in the Attribute Consent API.

On this Page

- About this Document
    - Introduction to iWelcome's Consent API
    - On this Page
    - Status
    - References
- API Description
    - Overview Diagram
    - Description of 'Resources' Managed by the Consent API
        - Processing Purposes
        - Attribute Consents
        - Consentable Documents
        - Document Consents
    - Multi-branding (segments)
    - Authentication and Authorisation
    - Events
- API Specification
    - Resources and Endpoints
    - Authentication
    - Schemas
    - API Usage Flow
    - Processing Purpose
        - Schema
        - Example: GET processing purposes (response)
    - Attribute Consents
        - Schema
        - Pagination
        - Examples
            - POST an attribute consent (request)
            - GET all attribute consents for a user (request)
            - GET all birthDate attribute consents for a user (request)
            - GET all attribute consents for a user (response)

        - DELETE all consents for attribute birthDate for a user
        - Delete all consents for a user
- Consentable Document
    - Schema
- Document Consent
    - Schema

Status

The status of this document is **FOR REVIEW** ; both the API and the API documentation are currently subject of QA process, so changes may be applied before general availability (GA).

Parts of the Consent-API are currently being finalised and are only briefly documented here: Consentable Documents endpoint and Document Consent endpoint. Both endpoints are related to the process of managing the users consent on - for example - Terms of service. These parts are marked in blue. Also the '/Me' authentication is not yet available in Release Candidate 1 for the forthcoming GA.

Readers of this document are encouraged to provide iWelcome with feedback on documentation or the APIs itself, to indicated areas of improvement.

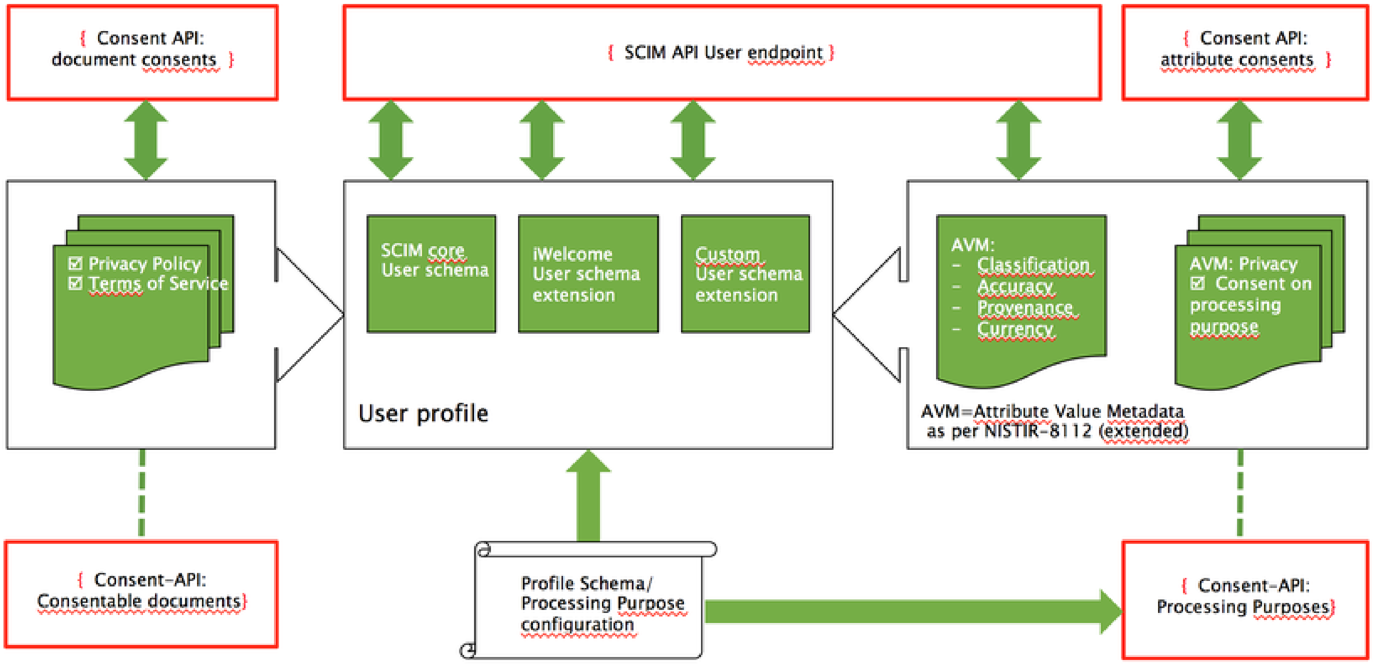
References

This page contains the following references:

- [NISTIR8112] - NIST Internal Report 8112 Attribute Metadata: A Proposed Schema for Evaluating Federated Attributes
- GDPR - EU General Data Protection Regulation
- [SCIM] - System for Cross-domain Identity Management, specification
- [iW-SCIM] - iWelcome product documentation for SCIM

API Description

Overview Diagram



{ Consent API: document consents }
{ SCIM API User endpoint }
{ Consent API: attribute consents }
☑ Privacy Policy
☑ Terms of Service
SCIM core User schema
iWelcome User schema extension
Custom User schema extension
User profile
AVM:
- Classification
- Accuracy
- Provenance
- Currency
AVM: Privacy
☑ Consent on processing purpose
AVM=Attribute Value Metadata as per NISTIR-8112 (extended)
{ Consent-API: Consentable documents}
Profile Schema/ Processing Purpose configuration
{ Consent-API: Processing Purposes}

Description of 'Resources' Managed by the Consent API

iWelcome's consent API provides access to the following resources:

- Processing Purposes
- Consentable Documents
- Attribute Consents
- Document Consents

Processing Purposes

The Processing Purposes can be used as follows:

- Every type of personal information can be associated with one or mulitiple processing purposes.
- Part of the set-up of these processing purposes is to record the legal basis for such processing. This legal basis is an attribute of each individual processing purpose.
- By querying the processing purposes that are administered in iWelcome, consumer facing portals and ‘MyPages’ can be transparant about processing purposes and their legal basis. Displaying this information to consumers contributes to building trust that their privacy is in good hands.
- Every Processing Purpose has a valiity status that reflects the lifecycle of that processing purpose.

Attribute Consents

For data processing that requires the user’s consent, iWelcome provides the attribute consent endpoint. Attribute consents serve the following use cases:

- When a user has given his consent to use one of his personal data (attributes) for a certain processing purpose, this consent can be stored with the user’s digital identity.
- In a similar way, when users revoke such a consent, the consent can be deleted from the user’s identity.
- Applications that do the actual data processing can find out for an individual user whether a consent was given. If not, the application should not process the data.
- Consumer facing applications such as ‘MyPages’ can display to the user for what processing purposes their personal data is used including the ones with consent.

Consentable Documents

The Consentable Documents endpoint will allow customers to:

- Manage legal documents like Terms of Service or Privacy Policy.
  - Multiple versions of a document can be stored and accessed.
  - Documents can be stored in multiple languages (locales).
- Every Consentable Document has a valiity status that reflects the lifecycle of that document.

Document Consents

iWelcome will provide the document consent endpoint to allow customers to store and retrieve consents given by the user on any of the documents exposed by the Consentable Documents API.

Multi-branding (segments)

iWelcome's IDaaS can support multiple consumer 'brands' to be serviced from a single tenant. This includes a segmentation of the consumer database where a single consumer can have a digital identity in each of the segments without conflicting identifiers; the consumer will experience having two accounts for two different 'brands' without being aware that they are hosted by a single iWelcome environment.

Not only will every brand have its own segment of digital identities, also every barnd will have its own processing purposes and consentable documents.

Authentication and Authorisation

The consent-API is protected to prevent misuse; authentication is required to access the various endpoints.

Aiming at the use cases indicated above, iWelcome distinguishes between server-to-server usage and self-service usage, a.k.a. '/Me':

- **Server to server (S2S).** Applications in the IT-landscape that are involved with consents can be set-up with credentials to access the protected consent-API based on basic authentication. Once authenticated, such applications are authorised to perform full CRUD on the consents of any of the users.
- **'/Me'.** Consumer-facing web applications such as 'MyPage' can invoke the /Me endpoint of the consent-API from a browser. In this case the API is protected by requiring the user to be logged in. An autheticated user can access the consent-API and perform full CRUD on his own consents; the scope of consents that can be accessed or created is limited to only the consents of the authenticated user.

Events

Usage of the Consent-API is reflected by the following events:

- Consent given (posted) on processing purpose
- Consent revoked (deleted) on processing purpose
- Consent given on a document such as Terms of Service and Processing Purpose

API Specification

iWelcome's consent-APIs are a set of RESTful webservices to access and manipulate:

- 'resources' applicable to all users:
    - data processing purposes
    - consentable documents
- 'resources' that are specfic to individual users:
    - attribute consents
    - document consents

Resources and Endpoints

iWelcome's API versioning allows clients to access the latest version of an API by ommitting the version from the URL. For example, instead of using endpoint `'/consents/v1/processing-purposes'` clients may choose to invoke `/consents/processing-purposes`.

Methods	API Version	Authentication	URL
Processing Purposes			
PUT	❌		The PUT method for Processing Purposes is currently not supported. These can be configured by iWelcome professional services.
GET	v1	S2S, /Me	/consent/v1/processing-purposes
Consentable Documents			
PUT	❌		The PUT method for consetable documents is currently not supported. These can be configured by iWelcome professional services.
GET	v1	S2S, /Me	
Attribute Consents			
POST	v1	S2S	/consent/v1/attribute-consents

GET	v1	S2S	/consent/v1/attribute-consents
			/consent/v1/attribute-consents/{consentId}
			/consent/v1/attribute-consents/users/{userid}

DELETE	v1	S2S	/consent/v1/attribute-consents/{consentId}
POST	v1	/Me	/consent/v1/attribute-consents
GET	v1	/Me	/consent/v1/attribute-consents /consent/v1/attribute-consents/{consentId}
DELETE			/consent/v1/attribute-consents/{consentId}
Document Consents			

POST	v1	S2S	
GET, DELETE	v1	S2S	
GET DELETE	v1	S2S	
POST	v1	/Me	
GET, DELETE	v1	/Me	
GET, DELETE	v1	/Me	

Authentication

Access to the consent-API always require authentication, either server-to-server (S2S) or when invoked from a browser the end-user must be authenticated ("/Me").

Server-to-server authentication is supported by the following mechanisms:

- Basic authentication
- Optionally static IP-filtering can be applied as well.

"/Me" authentication makes use of cookies in the end-users' browsers, after the user has logged in to iWelcome.

Schemas

This section provides an overview of the data that is relevant for the various 'resources'.

The data schema's for the various APIs will most likely evolve when new versions of the consent APIs are made avaliable. For reasons of forward compatibility, client applications are strongly recommended to ignore any data elements that are not part of the current schema. Also, clients should not make assumptions about the order in which data elements appear in the json objects.

API Usage Flow

In support of a registration process, a typical sequence of calls from a registration process to the API would be:

1. Obtain a list of consentable documents by doing a GET on consentable documents, such as Terms-Of-Service and Privacy Policy.
2. Obtain a list of processing purposes by doing a GET on processing purpose.
3. Create a user through iWelcome's SCIM endpoint.
4. Store the end-user's consents on consentable documents by doing a POST on document consent endpoint.
5. Optionally store end-user's consent on processing purposes by doing a POST on attribute consent endpoint.

In support of a self-service page , a.k.a. 'MyPage', the following sequence could be used:

1. Obtain a list of all processing purposes (for a given attribute).
2. Obtain applicable consents that were given by the user.
3. Display processing purposes on MyPage:
    a. contractual purposes are displayed for information and transparancy.
    b. consented processing purposes are displayed with a checkbox 'enabled'.
    c. processing purposes without consent can be displayed with a 'disabled' checkbox.

Processing Purpose

Schema

Field	Description	Mandatory/ Optional on GET	Possible Values
processingPurposeCode	Opaque identifier for the processing purpose.	M	
LegalBasis	Legal basis for processing of the personal data, as indicated by GDPR (Article 6)	M	"consent" "contract" "legal obligation" "vital interest of data subject" "public interest" "legitimate interest persued by data controller"
attributeName	Name of attribute. The name of the attribute must be equal to the name of the attribute in the SCIM interface, but excluding the SCIM-schema extension.	M	See SCIM documentation D.2 Interface Description: SCIM (Tulip 1.3)
data controller	The name of the Date Controller, as indicated by GDPR	M	Configured value per consumer segment. For all clarity, this is NOT iWelcome. IWelcome is data processor; consumers have no relation with iWelcome as a data processor.
default_cache_time_to_live	The length of time for which an attribute value may be cached in the context of the processing purpose.	O	Format of a 'duration' as specified by ISO-8601; for example "P1Y2M10DT2H30M".
data_retention_period	Amount of time prescribed by customer's Data Retention Policy for which the attribute value must be kept in the context of the processing purpose.	O	Format of a 'duration' as specified by ISO-8601, for example "P1Y2M10DT2H30M". Note that current version iWelcome does not automatically purge data 'by default' at the end of a retention period. Instead iWelcome features configurable data management capabilities; hence aiming at purging of data that is consistent with the customer's Date Retention Policy.
tags	Tags can be used by the client to filter processing purposes; the client may choose to display processing purposes and/or modify attribute consents only for certain tags.	O	This is a multi-valued field and its values are configurable strings. Clients are strongly recommended to ignore any tags not relevant for the client. iWelcome may return tags not requested by the customer.
processing purpose description		M	list of pairs of (locale, string)
status	Status of the processing purpose that indicates the current validity of the processing purpose.	M	**"active"**- the attributes are currently being used for the indicated processing purpose; new consents can be POSTED. **"sunset"**- consents for a processingPurpose with this status can be displayed, but no new consents may be posted for this processingPurpose. **"inactive"**- the attributes are no longer processed in the way indicated here. Any consent given in the past should not be displayed.

Example: GET processing purposes (response)

```
[
    {
        "id": "1",
        "descriptions": [
            {
                "locale": "en_GB",
                "description": "to manage your account"
            },
            {
                "locale": "nl_NL",
                "description": "om je account te beheren"
            }
        ],
        "legalBasis": "contract",
        "attributeName": "emails",
        "dataController": "iWelcome B.V.",
        "default_cache_time_to_live": null,
        "data_retention_period": null,
        "tags": [
            "step1",
            "step2"
        ],
        "status": "active"
    },
    {
        "id": "2",
        "descriptions": [
            {
                "locale": "en_GB",
                "description": "to address you personally in our
communications"
            },
            {
                "locale": "nl_NL",
                "description": "om je persoonlijk te kunnen aanspreken
in onze communicatie"
            }
        ],
        "legalBasis": "consent",
        "attributeName": "name",
        "dataController": "iWelcome B.V.",
        "default_cache_time_to_live": null,
        "data_retention_period": null,
        "tags": [
            "step1",
            "step2"
        ],
        "status": "active"
    },
    {
        "id": "3",
        "descriptions": [
            {
                "locale": "en_GB",
                "description": "to confirm you have the minimum age of
18"
            },
            {
                "locale": "nl_NL",
                "description": "om te bevestigen dat je 18 jaar of ouder
bent"
```

```
            }
        ],
        "legalBasis": "contract",
        "attributeName": "birthDate",
        "dataController": "iWelcome B.V.",
        "default_cache_time_to_live": null,
        "data_retention_period": null,
        "tags": [
            "step1",
            "step2"
        ],
        "status": "active"
    },
    {
        "id": "4",
        "descriptions": [
            {
                "locale": "en_GB",
                "description": "use for statistical analysis of our user
population"
            },
            {
                "locale": "nl_NL",
                "description": "gebruik voor statistische analyse van
ons klanten bestand"
            }
        ],
        "legalBasis": "consent",
        "attributeName": "birthDate",
        "dataController": "iWelcome B.V.",
        "default_cache_time_to_live": null,
        "data_retention_period": null,
        "tags": [
            "step1",
            "step2"
        ],
        "status": "active"
    },
    {
        "id": "5",
        "descriptions": [
            {
                "locale": "en_GB",
                "description": "to better customise our offers to you"
            },
            {
                "locale": "nl_NL",
                "description": "om onze aanbiedingen beter op uw wensen
af te stemmen"
            }
            ],
            "legalBasis": "consent",
            "attributeName": "gender",
            "dataController": "iWelcome B.V.",
            "default_cache_time_to_live": null,
            "data_retention_period": null,
            "tags": [
                "step1",
                "step2"
            ],
            "status": "active"
        }
    ]
```

Attribute Consents

Schema

Field	Description for Attribute Value Metadata Element (either NIST-specified or iWelcome specified)	Mandatory in a POST	Possible Values
id	Opaque identifier for the attribute consent record	M	
userId	Opaque identifier for the end-user as returned by iWelcome's SCIM interface	M	
processingPurposeId	Opaque identifier for the processing purpose as returned by a GET on the processing purpose endpoint	M	Only references to Processing Purposes having ‘consent’ as LegalBasis are accepted, since other processing purposes don’t require the consumer’s consent.
attribute - name	Name of the attribute as applicable for the processing purpose	O	Attribute names are defined by SCIM Core Schema or are configured in a custom SCIM schema extension.
consent - date	The date on which express consent for the processing purpose of the attribute value was acquired	O	No restrictions on the date, formatted as specified in section 3.2.7 of the XML Schema Datatypes Specification (e.g. 2008-01-23T04:56:22Z)
consent - locale	The locale that was used to communicate the processing purpose to the end-user	M	Possible values are configurable, for example locale": "en_GB" or "nl_NL".

Pagination

Pagination in response payload is applied whenever a GET returns multiple consents.

URL parameter	default value	acceptable values	
page	1	any	The number of the (next) set of consents in the response message
size	20	1..100	The number of consents in the response message

Examples

POST an attribute consent (request)

```
{
  "userId": "945a788f91874e9a94f0eca51a8ce03c",
  "processingPurposeId": "4",
  "attribute": {
    "name": "birthDate"
  },
  "consent": {
    "locale": "en_GB"
  }
}
```

GET all attribute consents for a user (request)

```
GET
http://www.ongo.com/api/consents/v1/users/945a788f91874e9a94f0eca51a8ce0
3c/attribute_consents/attributes
```

GET all birthDate attribute consents for a user (request)

GET http://www.ongo.com/api/consents/v1/users/945a788f91874e9a94f0eca51a8ce03c/attribute_consents/attributes/birthDate

GET all attribute consents for a user (response)

```
[
    {
        "id": "5a83f8cc3042ec0001854dd2",
        "userId": "945a788f91874e9a94f0eca51a8ce03c",
        "processingPurposeId": "4",
        "attribute": {
            "name": "birthDate"
        },
        "consent": {
            "dateConsented": "2018-01-13T08:52:28.560Z",
            "locale": "en_GB",
        }
    }
]
```

DELETE all consents for attribute birthDate for a user

```
DELETE
http://www.ongo.com/api/consents/v1/users/945a788f91874e9a94f0eca51a8ce0
3c/attribute_consents/attributes/birthDate
```

Delete all consents for a user

```
DELETE
http://amsdemo1a01:8045/api/consents/v1/users/945a788f91874e9a94f0eca51a
8ce03c/attribute_consents/attributes
```

Consentable Document

Schema

This endpoint and associated documentation will be made available with the forthcoming GA release.

It will resemble processing purpose to a certain extend.

Document Consent

Schema

This endpoint and associated documentation will be made available with the forthcoming GA release.

It will resemble attribute consents to a certain extend.