

## Glossary

This glossary maintains the collection of definitions and abbreviations of legal, technical and general type used in context of MyData, with focus on the MyDataShare product's own, internal realisation context. References, similar terms and Finnish translations are listed under the main item where identified.

Scopes used in 2<sup>nd</sup> column of the table are:

MyData
MDS = MyDataShare
OIDC = OpenID Connect
OA = OAuth 2.0
IdM = Identity Management
Legal
CS = Computer Science

Glossary version (major, minor) is shown on the 1<sup>st</sup> page footer.

Term / abbreviation	Scope	Explanation	Example	Other terms used, References	Translation to Finnish
<b>Access consent</b>	MDS (v1)	Represents a Consent that an end-user has granted to Data Consumer to use for 1) new processing locally or 2) access the data in Data Provider.	"access_consent": "9690348d-9905-44f5-a39a-e0169a558011"	Consent token	
<b>Access Gateway AGW</b>	MDS	API Gateway component that is used to protect access to the Data Provider APIs. Responsible for authenticating and authorising the incoming requests with the Access consent information received in Authorization HTTP header.		API proxy Policy Enforcement Point (PEP)	
<b>Access token</b>	OA	Temporary credential issued by Identity Provider to perform operations against Resource Servers on behalf of Resource Owner and with the consent of the Resource Owner. Access token is always tied to a particular client application, it has limited Scope and lifetime. Access tokens are not intended to carry information about the end-user, for that use see -> ID token.			käyttötunnussanoma
<b>acr, acr claim, acr_values</b>	OIDC	Authentication Context Class Reference, result claim and request parameter used in OpenID Connect authentication requests. ACR values are set of arbitrary values that the -> Client and -> IdP agreed upon to communicate the level of authentication that happened. This is to give the client a level of confidence on the quality of the authentication (-> LoA) that took place.	"passport_social" "http://ftn.ficora.fi/2017/loa2" "http://eid.as.europa.eu/LoA/Low"		
<b>Allowed identity correlation</b>	MDS (v2)	A use case in MyDataShare ecosystem that allows using a shared, public identifier for the end-user among the federation entities. In this ID configuration the Gluu INUM claim with public subject id is provided back on the Identity token the authentication requester receives.	A group of mobility operators shares their user identities to allow ticket purchasing amongst the operators' ticket shops with a single ID.		tunnisteiden korrelaation salliva operaattorin toiminta
<b>API</b>	CS	Application Programming Interface. In this context API usually refers to RESTful API endpoints that are accessible over HTTPS.	example.com/apis/v1/exampleapi	API endpoint	ohjelmointirajapinta
<b>Audit logs</b>	CS	System-level chronological, immutable logs collected at various transaction points and locations of the ecosystem – authentication, data access, consent request & introspection events, end-user transactions etc. Form basis for human-readable -> Data access log.		Logging (IHAN) Transaction logs Audit trail	tapahtumalokitiedot, kirjausketju

Term / abbreviation	Scope	Explanation	Example	Other terms used, References	Translation to Finnish
<b>Authentication Assurance Level, AAL</b>	IdM	Intended to provide some confidence in the authentication provided by the identity provider.		Authenticator Assurance Level	tunnistamisen luottamustaso
<b>Authenticator</b>	IdM	Means used to confirm the identity of a user, that is, to perform digital authentication. A person authenticates to a computer system or application by demonstrating that he or she has possession and control of an authenticator. In the simplest case, the authenticator is a common password.	Mobile authenticators (Freja eID, SisulD beta, Google Authenticator), Bank IDs, Google/Facebook/Github social logins		tunnistusväline
<b>Authorization</b>	CS	Permission given by end-user, that all or a certain portion (segment) of his end-user information can be accessed and used by a requesting digital service (data consumer). <b>NB:</b> authorization request may lack purpose and legal terms -> not always same as -> Consent or -> Permission in the context of MyDataShare.		Permission	luvittaminen, auktorisointi
<b>Authorization code grant flow</b>	OA	OAuth 2.0 flow for confidential (and recently also public) clients to exchange an authorization code for an Access token.		See <a href="#">RFC6749</a>	
<b>Authorization endpoint</b>	MDS, OA	OAuth 2.0 and OpenID Connect API endpoint that issues an authorization code (see -> 'code') for a valid client request. Used with Authorization Code Grant flow only.			
<b>AWS</b>	CS	Amazon Web Services. Public cloud environment that is used as the deployment environment for MyDataShare Access Gateway, MyDataShare Operator Platform and MyDataShare ID.			
<b>Client</b>	OA	OAuth 2.0 client application which can request access tokens with client_id and client_secret and can make calls to Resource Server endpoints protected with OAuth 2.0.		Relying Party (OIDC)	asiakas
<b>code</b>	OA	Code used to acquire an -> Access token from -> Token endpoint. Used with Authorization code grant flow only.	"831daff2-9353-438e-9aaf-afe97518b2e0"		
<b>Consent</b>	MyData	Permission given by end-user, that all or a certain portion (segment) of her customer information can be accessed and used for predefined purposes by a digital service (and possibly by 3rd parties).		(Authorization)	(käyttölupa, käyttöluvitus)

Term / abbreviation	Scope	Explanation	Example	Other terms used, References	Translation to Finnish
<b>Consent</b>	Legal	Provides the legal basis for the processing of the Personally Identifiable Information of the individual. Consent must be freely given, specific, informed and unambiguous.			suostumus
<b>Consent introspection</b>	MDS	A service request to validate a given Access consent at MyDataShare Operator Platform. Received typically from a Data Provider (but also by Data Consumers in applicable case).			
<b>Consent introspection endpoint</b>	MDS	API endpoint for incoming Consent Introspection requests at MyDataShare Operator Platform. Requires Access token with Scope consent_introspection.			
<b>Consent Management Service, CMS</b>	MDS	Functionality for; <ul style="list-style-type: none"> <li>- End-user to manage his consents (give, revoke, view, modify)</li> <li>- Data provider and data consumer to verify if consent by End-user exists for use the data for a certain purpose (a part of overall authorization)</li> <li>- Data consumer to request consents from End-users</li> <li>- Usage logging</li> </ul>			suostumuksenhallinta palvelu
<b>Consent receipt</b>	MyData	A machine-readable and human-readable artifact of the fact that Individual has given consent to data processing. An approved -> Consent request can result in delivery of a Consent receipt.			suostumuskuitti
<b>Consent request</b>	MDS (v1)	A Data Consumer initiated service request to initiate consent notice & acquisition process with an end-user. Request is managed via MyDataShare Operator Platform and the applicable Wallet application.		Consent notice (esp. on user interface context)	suostumuspyyntö
<b>Consent request endpoint</b>	MDS	API endpoint for incoming Consent requests at MyDataShare Operator Platform. Requires Access token with Scope consent_request.			
<b>Contract</b>	Legal	In personal data processing, contract is a valid legal basis when processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract (Art 6 (1)(b) GDPR).			sopimus (henkilötietojen käsittelyperusteena)
<b>Controller</b>	Legal	A natural or legal person, public authority, agency or other body which alone or jointly with others determines			rekisterinpitäjä

Term / abbreviation	Scope	Explanation	Example	Other terms used, References	Translation to Finnish
		the purposes and means of the processing of personal data (Art. 4 (7) GDPR).			
<b>Customer</b>	MDS	Usually Organization in role of a MyDataShare B2B customer. For a natural person as a customer see -> End-user.			(yritys)asiakas
<b>Data access log</b>	MDS	A human-readable history of end-user related data access events collected via reporting entities such as AGW, Wallet and CMS. This data is served to End-users via MyDataShare Wallet.			käyttölokitus
<b>Data Club</b>	MDS	A group of Data Providers and Consumers (within one or several Organizations) that can organize data sharing amongst themselves. Data Club specific Wallet instances or views will not show processing records active outside the group's Data Providers and Data Consumers.		Data Federation	dataklubi
<b>Data Consumer</b>	MDS	Service that is requesting Consent from end-user to process personal data hosted at a Data Provider on his/her behalf. Uniquely identified by a uuid value within the MyDataShare Operator Platform. Data Consumer is issued with an Access consent that it can use to perform these operations.		Data-using Service Service Provider Data Sink Sink Client	hyödyntäjäpalvelu, käyttävä palvelu
<b>Data Protection Officer DPO</b>	Legal	A natural person nominated as the privacy responsible contact person towards data subjects in an Organisation. Monitors processing of personal data and provides advice on compliance with data protection regulations.		(Chief) Privacy Officer	tietosuojavastaava
<b>Data Provider</b>	MDS	A service that can provision personal data to 3 <sup>rd</sup> party clients. Offers a set of API endpoints for Data Consumers that are protected with Access Gateway or own equivalent (see -> Direct Introspection). Uniquely identified by a uuid value within the MyDataShare Operator Platform. Data Consumers can access these endpoints with the Consent of the End-user.		Data Source Source Resource Server	luovuttajapalvelu, tietolähde, luovuttava palvelu
<b>Data Subject</b>	Legal	an identified or identifiable natural person whose personal data is processed (Art. 4 (1) GDPR).			rekisteröity
<b>Decentralised Identifier DID</b>		A W3C-defined digital identifier controlled without a central identifier issuer/provider service. Can be public		<u>W3C Recommendation</u>	hajautettu tunniste

Term / abbreviation	Scope	Explanation	Example	Other terms used, References	Translation to Finnish
		(see -> Public DID) or just for peer connections (-see > Peer DID).			
<b>Description (service registration)</b>	MDS	Free-text form service-level description of the Data Provider and Data Consumer, and for the latter also of intended personal data processing that the Data Consumer is set to execute.		Service Description	palvelukuvaus
<b>Digital signature</b>	CS	A mathematical scheme for verifying the authenticity of digital messages or documents.		Electronic signature	digitaalinen allekirjoitus
<b>Direct introspection</b>	MDS	A mechanism where Data Provider validates the requests from Data Consumers directly against MyDataShare Operator Platform APIs (no Access Gateway in middle).		AGW-less integration	
<b>EC2</b>	CS	AWS Elastic compute cloud service that offers the possibility to run virtual servers in the cloud.		Elastic Computing Cloud	
<b>Electronic ID, eID</b>	IdM	A digital solution for proof of identity of citizens or organizations, for example in view to access services provided by government authorities, banks or other companies etc. Many electronic identity services also give users the option to sign electronic documents (see -> digital signature).			
<b>End-user</b>	MDS	Person using digital service(s) in MyDataShare ecosystem		Individual, Data Subject, End-customer, Resource Owner (OAuth 2.0)	loppukäyttäjä, henkilöasiakas, yksilö
<b>Federation Assurance Level, FAL</b>	IdM	Describes aspects (e.g. strength) of the assertion and federation protocol used in a given authentication transaction.			
<b>Gluu</b>	CS	Open-source Java based access management solution that is used to implement the OpenID Connect compliant MyDataShare ID identity provider.		<a href="https://gluu.org">https://gluu.org</a>	
<b>ID token</b>	OIDC	ID token is a security token granted by the -> OpenID Provider that contains information about an -> End-user. This information tells your client application that the user is authenticated, and can also give you additional information like their username or locale.		Identity token <a href="https://openid.net/specs/openid-connect-core-1_0.html">https://openid.net/specs/openid-connect-core-1_0.html</a> - IDToken	tunnistussanoma

Term / abbreviation	Scope	Explanation	Example	Other terms used, References	Translation to Finnish
<b>Identification Assurance Level, IAL</b>	IdM	Confidence level related to end-user identity proofing process.			identiteetin todentamisen luottamustaso
<b>Identity</b>	IdM	An attribute or set of attributes that uniquely describe a subject within a given context.			Identiteetti, yksilöllisyys
<b>Identity federation</b>	IdM	Federated identity management (FIdM) is an arrangement that can be made between multiple organizations to let subscribers use the same identification data to obtain access to the networks of all the organizations in the group. The use of such a system is sometimes called identity federation.	ORCID, Google ID, Office 365, Github		Federoitu tunnistaminen
<b>Identity linking</b>	IdM	Linking the digital identifiers of an identity in multiple federated identity providers to a digital identifier of the same identity in the MyDataShare ID identity provider.	eDuuni ID		identiteettien yhdistäminen
<b>Identity non-correlation</b>	MDS	A use case in MyDataShare ecosystem that uses only MyDataShare ID -stored pairwise identifiers of the end-user among the peer entities. The authentication requester only receives the end-user's pairwise identifier, so that doesn't allow correlation in context.			pseudonyymitunnisteisiin perustuva (yksityisyyden suojaava) toimintatapa
<b>Identity Provider IdP</b>	IdM	Identity Provider solution that is used to offer Identity Provisioning and Access Management services.			Identiteetinhallintapalvelu
<b>Implicit grant flow</b>	OA OIDC	OAuth 2.0 & OpenID Connect flow for non-secure (such as a web browser) clients' Access token requests. Suggested replacement: authorization code flow + PKCE extension.		Recommended replacement see <a href="#">RFC 7636</a>	
<b>Individual</b>	MDS	See -> End-user		person	yksilö, henkilö
<b>Introspection</b>	OA OIDC MDS	Mechanism offered by Identity Provider and MyDataShare Operator Platform to examine the contents and validity of OAuth 2.0 access tokens and in latter, Access consents and/or Permission tokens.			
<b>Introspection API</b>	OA, OIDC, MDS	API endpoint that is used for introspection requests			
<b>Keychain</b>	MDS	A grouping of all individual's identifiers within MyDataShare ID. A Wallet user's keychain contains both her identifying and pairwise identifiers.			Avainnippu, tunnistenippu

Term / abbreviation	Scope	Explanation	Example	Other terms used, References	Translation to Finnish
<b>Legal (service registration)</b>	MDS	Free-text form, simple-language legal description of the personal data processing that Data Consumer is set to execute. Should be based on full privacy policy and include a link to it.			hyödyntäjäpalvelun tietosuojaa koskeva kansantajuinen yhteenveto
<b>Legal basis</b>	Legal	A legal basis of personal data processing according to GDPR. Six listed bases are: (for the performance of a) contract, (based on individual's) consent, legitimate interest of the controller, vital interest (of the data subject), public interest, (fulfilment of) legal obligation.			henkilötietojen käsittelyperuste
<b>Level of Assurance, LoA</b>	IdM	Aggregate degree of confidence in processes (IAL+AAL+FAL) leading up to, and including an End-user authentication.		See <a href="#">NIST 800-63-3</a>	luottamustaso
<b>Linked information</b>	IdM	Information about or related to an individual that is logically associated with other information about the individual.			henkilöllisyyteen liitetty (muu) tieto
<b>MFA</b>	IdM	Multi-factor authentication - authentication where user's identity is authenticated using 2 or more parallel -> Authenticators	<a href="https://www.youtube.com/watch?v=Q8OzabuNwHI">https://www.youtube.com/watch?v=Q8OzabuNwHI</a>	2-factor authentication (2FA)	kaksivaiheinen tunnistaminen
<b>MyDataShare ID</b>	MDS	OpenID Connect compliant Identity Provider that is used to offer Access Management services to protect access to Wallet application and MyDataShare Operator Platform's APIs. In case of -> Single sign-on use of MyDataShare ID by the relying party, it protects access to its resources/services too.			MyDataShare - tunnistamiskerros
<b>MyDataShare Operator Platform, MOP</b>	MDS	MyDataShare Operator ties together end-users, Data Providers and Data Consumers by offering Data Consumers the ability to enter into Contracts with, and/or request Consents from End-users.		Policy Server Policy Decision Point (XACML) Authorization Server aka AS (OAuth 2.0)	MyDataShare - operaattorikerros, omadataoperaattori
<b>OAuth 2.0</b>	OA	Standard protocol defined in <a href="#">RFC 6749</a> to authorise access to API endpoints offered by Resource Servers.			
<b>OpenID Connect, OIDC</b>	OIDC	Authentication mechanism profile built on top of OAuth 2.0 that allows the implementation of single sign-on and sign-out mechanisms and to pass Identity information in a secure and standards compliant manner.		<a href="https://openid.net/connect/">https://openid.net/connect/</a>	



Term / abbreviation	Scope	Explanation	Example	Other terms used, References	Translation to Finnish
<b>OpenID Provider, OP</b>	OIDC	Identity Provider compliant with -> OpenID Connect, an OAuth 2.0 profile	<a href="https://openidconnect.net">https://openidconnect.net</a>		
<b>Organisation</b>	MDS IdM	Company, NGO, cooperative, association or public sector organisation offering a set of Data Consumers and/or Data Providers in the context of MyDataShare Operator Platform. Identified by a set of identifiers (e.g. Business ID, Company ID, DID). NOT a natural person.		Legal entity, Entity	organisaatio, juridinen henkilö
<b>Pairwise identifier</b>	OIDC, MDS	A pseudonym, pairwise OpenID Connect identifier created for an authenticated end-user by the MyDataShare ID and provided back to Data Consumer or Data Provider behind the original authentication request.			yhteyskohtainen pseudonyymi tunniste
<b>Peer DID</b>	IdM	A DID created only for use within a pairwise connection. Private, not resolvable through a DID Registry.	did:peer:1zQmZMy7zYqNwU6UhmCwx5Xepf2VLs5S4HLewwgf2ai9Zuwa	Pairwise DID <a href="https://openssi.github.io/peer-did-method-spec/index.html">https://openssi.github.io/peer-did-method-spec/index.html</a>	yhteyskohtainen hajautettu tunniste
<b>Permission</b>	IdM	See -> Authorization			luvitus
<b>Permission token</b>	MDS	A MyDataShare issued token similar to -> Consent token but generalised to cover also other legal processing bases (including consent). Permission token is validated against the -> Consent introspection endpoint.		Policy token	luvitussanoma
<b>Person</b>	IdM	Natural Person identified by a set of identifiers (e.g. SSN, tax number, verified email address, (peer) DID).			(tunnistettu) luonnollinen henkilö
<b>Personal data</b>	IdM, CS	Information related to the End-user and stored in different digital services. This can be Personal information (PI), Personal identifiable information (PII) and also service specific, end-user related information like reservations, usage history of the service, etc. - whatever services store.		End-user Information	henkilötieto
<b>Processing base</b>	Legal	A literal of valid processing basis the Organisation must provide at registration of a Data Consumer, along with free form -> Description and -> Legal texts.	"contract" "consent" "public interest"		käsittelyperuste
<b>Processing notification</b>	MDS	A data consumer processes personal data using legal ground other than individual's consent may notify the End-user about the processing to meet its public or own requirements for data processing transparency.			henkilötietojen käsittelystä ilmoittaminen

Term / abbreviation	Scope	Explanation	Example	Other terms used, References	Translation to Finnish
<b>Processing record</b>	MDS (v2)	A data object stored within MyDataShare to persist permissions and policy details of personal data processing between the parties involved. Processing record has a state, and only <i>active</i> state results in passing a -> Consent introspection request (in case of consent or contract based processing).			Käsittelytallenne, 'suostumustallenne'
<b>Processor</b>	Legal	A natural or legal person, public authority, agency or any other body which processes personal data on behalf of the data controller (Art. 4 (8) GDPR).			(rekisterinpitäjän osoittama) henkilötiedon käsittelijä
<b>Public DID</b>	IdM	A -> DID that is public and can be discovered and resolved through utilities such as a DID Registry and a DID Resolver.	did:eth:1zQmZMygzYqNwU6Uhmewx5Xepf2VLp5S4HLSwwgf2aiKZuwa	Anywise DID	julkinen hajautettu tunnistus
<b>RDS</b>	CS	AWS Relational Database Service that offers the possibility to run managed relational database instances with different database engines in the cloud.			
<b>Relying party, RP</b>	OIDC	An entity that relies upon the subscriber's authenticator(s) and credentials or a verifier's assertion of a claimant's identity, typically to process a transaction or grant access to information or a system.	omavero.fi Github hel.fi		asiointipalvelu
<b>Scope</b>	OA OIDC	Associated with OAuth 2.0 access tokens and determines the set of operations that can be performed with the given access token.	"access_token" "consent_introspection" "user_info"		
<b>Service</b>	MDS CS	Abstraction of a Data Provider or Data Consumer instance uniquely identified by an UUID value within the MyDataShare Operator Platform.			sähköinen (asiointi)palvelu
<b>Signicat</b>	CS	Commercial OpenID Connect compliant ID Broker solution that exposes a set of strong authentication mechanisms (e.g. FTN, BankID, Smart-ID, Finnish Mobile Certificate) through a single standards compliant interface.			
<b>Single sign-on, SSO</b>	IdM	An access control property of a system where a single authentication provides access to multiple services, by passing the authentication token seamlessly to configured services.			kertakirjautuminen
<b>Step-up authentication</b>	IdM	Process where an authenticated End-user is requested to re-authenticate with higher-than-current LoA (AAL) due to demands of ongoing transaction. Done via			

Term / abbreviation	Scope	Explanation	Example	Other terms used, References	Translation to Finnish
		suitable MyDataShare ID -provided authentication provider.			
<b>Token endpoint</b>	OA, OIDC, MDS	API endpoint in MyDataShare ID that issues -> Access tokens			
<b>Trusted Client</b>	MDS	A -> Client that has been registered and issued valid credentials to access the MyDataShare ecosystem's APIs		MDS Client	
<b>(MyDataShare) Wallet</b>	MDS	End-user web application that gives end-users the possibility to manage Consent requests, Consents and other data processing information related to MyDataShare Operator Platform.	<a href="https://muntiedot.fi">muntiedot.fi</a> lompakkopalvelu	Privacy dashboard	(omadata)lompakko, suostumuslompakko