

REPUBLIC OF ESTONIA INFORMATION SYSTEM AUTHORITY

# Web service integration with State Single Sign-On (GOVSSO)

Helen Raamat (Information System Authority) Aare Nurm (Nortal AS) Alar Kvell (Nortal AS) 07.06.2022



European Union European Regional Development Fund Investing in your future

# Agenda

- Introduction
- DEMO/PROD environment application process
- Q&A
- Authentication flows
- API parameters, required validations
- Testing
- Q&A

## What is GOVSSO?

#### Purpose

- To optimize cost of authentication by minimizing the usage of billable services (Mobile-ID; Smart-ID; OCSP for ID-card).
- To give better user experience when moving between different state services.

# What is GOVSSO?



### What is GOVSSO?

- Users should not differentiate when system is moved from TARA to GOVSSO
- Same Login button recommendations as for TARA

### **UI recommendation for login**

#### If TARA or GOVSSO is the only authentication option



• If there are several authentication options:



#### **UI recommendation for logout**

- Reference what service has been logged out of
- Avoid instructing to close all windows

	<u>Eesti keeles</u> <u>На русском</u>		<u>Eesti keeles</u> <u>На русском</u>
Session has ended		e-MTA session has ended	
You have signed out of e-MTA. For security reasons, please close all web browser windows. Sign in		You have signed out of e-MTA.	
REPUBLIC OF ESTONIA TAX AND CUSTOMS BOARD 880 0815 e-tax s 880 0814 e-cust All contact data ar	o <b>rt</b> services toms services	REPUBLIC OF ESTONIA TAX AND CUSTOMS BOARD 880 ( 880 ( All cr	tomer support 0815 e-tax services 0814 e-customs services ontact data_ &

#### **GOVSSO** roadmap

#### • 03.2022 – 06.2022 GOVSSO stage 2

- Feedback, refinement
- GOVSSO software ready for production
- 08.2022 GOVSSO as production service

# **Application process for DEMO and PROD environments**

- Register your e-service in our demo environment and conduct integration tests.
- Register your e-service in our production environment.
- The application forms will become available on <u>RIA website</u>.
- Submit your completed and signed applications at <u>help@ria.ee</u>.
  - The application must be signed by the legal representative of your organization.
- After registration you will receive required credentials to use GOVSSO services.

## **Considerations on selecting values**

- Client application name
  - Should be recognized by end user. Avoid technical terms.
- Client application short name
  - Should be recognized by end user. Should be relatable with application name.
- Client application logo
  - SVG format

## **Considerations on selecting values**

- Authentication return URL-s
  - One or multiple URL-s
- Logout URL-s
  - One or multiple URL-s
- Back-channel logout URL
  - Recommended to limit access to only RIA IP-address

## **Additional information**

#### <u>https://e-gov.github.io/GOVSSO/</u>

• This page is the main source for technical information

### **Questions and answers**

• Questions?

# Usage flow without GOVSSO

1			2			3			
🔒 Home page		Self-service log-in	Secure authentication for e-services		EESTI РУССКИЙ	Secure auth	entication for e-services		
SELFSERVICE									
			RIIGI AUTENTIMISTEENUS			See .	IIGI AUTENTIMISTEENUS		
i War in Ukraine v		th your country!							
		an your oound y.	iD-card	(j) smart-ib		(	Smart-ID		
nepublic of Estonia 🗸			( Smart ID			Ċ	Verification code was sent to your	Smart-ID app.	
🗱 Health and care 🗸	Life events				nerround and allely		Your control code is:		
Pensions, social € services and ~	WAR IN UKRAINE	8 I HAVE FALLEN ILL	"Continue". A ve	rification code will be sent to your Smart-ID app.	personal code and click		2080		
allowances	Here you can find the links to the official information related to war in Ukraine.	Here, you can find information and instructions on topics related to the health data of you and your family.	Personal code	EE					
Work and labor							Cancel		
Doing business 🗸	CREATING A FAMILY	ਨੂੰ THE BIRTH OF A CHILD		Continue					
Licences and Notices of Economic Activity	Here, you can find information and instructions on marriage, registered partnerships, applying for new documents after changing your name, etc.	Here, you can find information and instructions on activities and allowances related to the birth of a child.				Return to se	rvice provider		Help from smart-id.com
Disabled people			Return to service provider		Help from smart-id.com				
documents	合 I AM CHANGING MY PLACE OF RESIDENCE	🖞 I WISH TO ESTABLISH A COMPANY							
Education and Research	Here, you can find information on registration of residence, concluding contracts for electricity, water, and waste transport, changing your family physician, etc.	Here, you can find information on forms of business, registering a company, hiring employees, paying taxes, areas of activity subject to special requirements, etc.	Contraction of the second seco	financed by the Connecting Europe ility of the European Union More abo	ut the national authentication service	Company U Var Economic Harmon Development Francis	Co-financed by the Con Facility of the European	Hecting Europe More about	the national authentication service
4	~		5&6		*	7	W		i um i
Home page SELFSERVICE	RIIGIPORTAAL EESTLEE Accessibility Q	LANGUAGE: ROLE en V MATI MAASIKAS V	Secure authentication for e-services	EESTI PYCCKI		Expand menu	REPUBLIC OF ESTONIA MINISTRY OF THE INTERIOR	E	T RU MAASIKAS X <u>Sign out</u>
- Dashboard	Home / Personal data / I and my family		Ridi Ad Fer Limis Lends			Dashboard	y data		
Personal data ^	I and my family		An ID-card 🔮 Mobile-ID	(j) Smart-ID		Q			
I and my family Health care and	✓ My identity documents and photo	Submit query	Secure :	authentication for e-services		es My data	Address of the place of residence		
Allowances and pensions	✓ Me and my children: data from the Population Re	zgistry Submit query	A valid Smar "Continue". A	Riigi autentimisteenus		Residence	Iartu maakond, Kambja vald, Kuukivi Starting date: 31.12.2017	alevik, Korvenogese tee 17	
Education Work and labor relations	Changing data in Population Register	Open in new window	Personal cod	(j) Smart-ID		A Family	Children and wards		
Traffic	E Registering the birth of a child	Open in new window		Verification code was sent to your Smart-ID app. Your control code is:		Q Requesting T	'ou can change the residence data of your children a otice of residence.	nd wards together with your own reside	nce data or separately by submitting a
Housing and real estate Notarised documents and execution proceedings	Query for name statistics	Open in new window		2080		data	lame	The place of residence	d, Kuukivi alevik, Kõrvenõaese tee
Will and succession	Family event certificate (birth, marriage, divorce of	or name change) Open in new window				F	MAKI-LIIS MANNIK Personal identification code: 47302200234	17 Starting date: 31.12.2017	
Hunting and weapons	Query for relative relations	Open in new window	Return 1	to service provider	Help from smart-id.com				
My consents  Data tracker	The suitability of a name for registering a birth	Open in new window		Co-financed by the Connecting Europe Facility of the European Union	More about the national authentication service		VIATILAL STATUS I your marital status in the population register is inco onvenience to correct this data.	rrect, please contact the local governm	ent of the county centre of your
	Death information around		(restore i)						

# Usage flow with GOVSSO

1			2		3	
🔒 Home page	RIIGIPORTAAL Accessibility Q	Self-service log-in	Secure authentication for e-services	EESTI РУССКИЙ	Secure authentication for e-services	
SELFSERVICE						
ARTICLES	HEA MARIA					
🧃 War in Ukraine 🗸		ith your country!	All ID-card Mobile-ID	(EU) EU eID	10	
					(j) Smart-ID	
Republic of Estonia     K     Health and care	Life events		(j) Smart-ID		Verification code was sent to your Smart-	-ID app.
Pensions, social	WAR IN UKRAINE	🗱 THAVE FALLEN ILL	A valid Smart-ID account is required to log in to <b>eesti</b> "Continue". A verification code will be sent to your Sm	.ee. Insert your personal code and click nart-ID app.	Your control code is:	
allowances	Here you can find the links to the official information related to war in Ukraine.	Here, you can find information and instructions on topics related to the health data of you and your family.	Personal code FF		2080	
➡ Work and labor relations ~					Cancel	
Doing business 🗸	CREATING A FAMILY	5월 THE BIRTH OF A CHILD	Continue			
of Economic Activity	registered partnerships, applying for new documents after changing your name, etc.	Here, you can find information and instructions on activities and allowances related to the birth of a child.	Return to service provider	Help from smart-id com	return to service provider	Help from smart-id.com
Citizenship and			and and an and they platfind.			
	I AM CHANGING MY PLACE OF RESIDENCE  Here, you can find information on registration of residence,	I WISH TO ESTABLISH A COMPANY Here, you can find information on forms of business, registering a	Co-financed by the Connecting Europe	More about the national authentication service	Co-financed by the Connecting	Europe More about the national authentication service
Education and Research	concluding contracts for electricity, water, and waste transport, changing your family physician, etc.	company, hiring employees, paying taxes, areas of activity subject to special requirements, etc.	Development view Development view Development view		Construction Construction Construction Construction	
4			5		6	
4. A Home page SELFSERVICE	RingPortAAL Accessibility Q	LANGUAGE: ROLE en → MATI MAASIKAS →	5 Secure authentication for e-services	EESTI РУССКИЙ	6	ET RU MAASWAAS X Sign out
4 ★ Home page SELFSERVICE ■ Deshboard	RIDIPORTAAL Accessibility Q EESTLEE Accessibility Q Home / Personal data / I and my family	LANGUAGE: ROLE en V MATI MAASIKAS V	5 Secure authentication for e-services RIIGI AUTENTIMISTEENUS	EESTI РУССКИЙ	6 Expand menu Wy data	ET RU MATI MAASIKAS X Sign out
4 ♣ Home page SELFSERVICE ■ Dashboard ● Personal data ^	Riigiportaal Accessibility Q Home / Personal data / I and my family I and my family	en V MATI MAASIKAS V	5 Secure authentication for e-services RIIGI AUTENTIMISTEENUS	EESTI РУССКИЙ	6	ET RU MAASIKAS XSign.out
4 Mome page SELFSERVICE Personal data ^ Land my family Health care and	BitoportAAL     Accessibility     Q       Home / Personal data / I and my family       I and my family       ✓ My identity documents and photo	LANGUAGE: en V MATI MAASIKAS V Submit query	5 Secure authentication for e-services RIIGI AUTENTIMISTEENUS Logging in to e-population regis	ееsті русский ter	6 Expand more Subboard My data Address of the place of residence	ET RU MAASKAS X Sign out
Home page SELFSERVICE Dashboard Personal data Land my family Health care and prescriptions Allowances and pensions	REGISTANT       Accessibility       Q         Home / Personal data / I and my family       I and my family         I and my family       My identity documents and photo         Me and my children: data from the Population R	LANGUAGE: ROLE en V MATI MAASIKAS V Submit query Registry Submit query	5 Secure authentication for e-services Trigit AUTENTIMISTEENUS Riigi AUTENTIMISTEENUS Logging in to e-population register To log in to e-population register it is sufficient to co to another service. Data that will be transmitted to be	EESTI РУССКИЙ ter ntinue your session because you are logged in price:	6 Expand menu Beshbaard My data My data Address of the place of residence Address of the place of residence Contemporate Starting date: 31.12.2017	ET RU MAASIKAS X Sign out MAASIKAS X Sign out
Home page SELFSERVICE B Deshboard Personal data A  Personal data A  Land my family Health care and prescription Allowances and pensions Education	RiidPorttAAL       Accessibility       Q         Home / Personal data / 1 and my family       I and my family         I and my family       ✓ My identity documents and photo         ✓ Me and my children: data from the Population R         ② Changing data in Population Register	LANGUAGE ROLE en V MATI MAASIKAS V Submit query Registry Submit query	5 Secure authentication for e services RIGI AUTENTIMISTEENUS RIGI AUTENTIMISTEENUS Logging in to e-population register To log in to e-population register it is sufficient to co to another service. Data that will be transmitted to se First name MATI	EESTI РУССКИЙ ter ntinue your session because you are logged in rvrice: sonal code 38001085718	6         Expand menu         Image: Specific of Extreme	ET RU MAASKAS <b>X</b> Sign.out
Home page SELFSERVICE  Personal data Personal data Calorances and pensions Education Education Variance and labor relations Traffic	BitoportAAL       Accessibility       Q         Home / Personal data / 1 and my family       I and my family         I and my family       ✓ My identity documents and photo         ✓ Me and my children: data from the Population R         ② Changing data in Population Register         ③ Denisterion the birth of a child	LANGUAGE: en V MATI MAASIKAS V Submit query Registry Submit query Open in new window	5 Secure authentication for e-services Trigo Autentinisteenus Riigi Autentinisteenus Riigi Autentinisteenus Riigi autentinisteenus Riigi no e-population register it is sufficient to co to another service. Data that will be transmitted to see First name MATI EEE MATI MAASIKAS	EESTI РУССКИЙ ter ntinue your session because you are logged in srvice: sonal code 38001085718 e of birth 8/1980	Image: Constrained of Entropy         Image: Constrained of Entropy </th <th>ET RU MAASKAS Sign out</th>	ET RU MAASKAS Sign out
Home page ELEFSERWICE ELEFSERWICE E Deshoold data Personal data Personal data Allowances and pensions Education Education Education Traffic Housing and real estate	RIGPORTAAL       Accessibility       Q         Home / Personal data / Land my family       I and my family         I and my family       My identity documents and photo         Me and my children: data from the Population R         Changing data in Population Register         Registering the birth of a child	LANGUAGE en V MATI MAASIKAS V Submit query Registry Submit query Open in new window Open in new window	5 Secure authentication for e services RIGI AUTENTIMISTEENUS RIGI AUTENTIMISTEENUS Logging in to e-population register To log in to e-population register it is sufficient to co to another service. Data that will be transmitted to se First name MAASIKAS Continue session Re-authenticate	EESTI РУССКИЙ ter ntinue your session because you are logged in rrice: sonal code 30001085718 e of birth 8/1980	G         Expand mem       Image: Constraint of Entrance         Image: Constraint of Entrance       My data         Image: Constraint of Entrance       My data         Image: Constraint of Entrance       Image: Constraint of Entrance         Image: Constrate of Entrance       Image: Constraintof Entrance	ET RU MARSIKAS X Sign out
Home page SELFSERVICE SELFSERVICE  Personal data Personal	BitisportAAL       Accessibility       Q         Home / Personal data / Land my family       I and my family         I and my family       My identity documents and photo         Me and my children: data from the Population R         Changing data in Population Register         Registering the birth of a child         Query for name statistics	LANGUAGE:       ROLE         en       MATI MAASIKAS >         Submit query       Submit query         Registry       Submit query         Open in new window       Open in new window         Open in new window       Open in new window	5 Secure authentication for e-services TRIGI AUTENTIMISTEENUS RIGI AUTENTIMISTEENUS	EESTI РУССКИЙ ter ntinue your session because you are logged in srvice: sonal code 38001085718 e of birth 8/1980	€       Experience of Entropy         €       Experience of Entropy         €       My data         Ø       My data         Ø       Address of the place of residence         Ø       My data         Ø       Address of the place of residence         Ø       Tartu maakond, Kambja vald, Kuukivi alevik Starting date: 31.12.2017         Register a new place of residence       Children and wards         Vou can change the residence data of your children and ware notice of residence.       Name         Name       The starter of the	ET RU MAASKAAS Sign out
Home page ELEFERNOE ELEFERNOE ELEFERNOE E Denonal data Perscription Allowances and pensions Education Education Education Under relations Traffic Housing and real estate Notaried documents and execution proceedings	RIGBPORTAAL       Accessibility       Q         Home / Personal data / Land my family       I and my family         I and my family       My identity documents and photo         Me and my children: data from the Population R         Changing data in Population Register         Registering the birth of a child         Query for name statistics         Family event certificate (birth, marriage, divorce)	LANGUAGE en     ROLE       MATI MAASIKAS ~       Submit query       Registry     Submit query       Open in new window	5 Secure authentication for e services Tig Autentinisteenus Rici Autentinisteenus Logging in to e-population register To log in to e-population register it is sufficient to co to another service. Data that will be transmitted to se First name MAASIKAS Continue session Re-authenticate National authentication service uses a single sign-on you can continue your session in other services with	EESTI РУССКИЙ ter ntinue your session because you are logged in rrvce: sonal code 30001085718 e of birth 8/1980	Expand mem       Image: Construct of Extended         Expand mem       Image: Construct of Extended         Image: Construct of Extended       My data         Image: Construct of Extended       Address of the place of residence         Image: Construct of Extended       Address of the place of residence         Image: Construct of Extended       Image: Construct of Extended         Image: Construct of Extended<	ET RU MARTMAASWAAS X Sign out K, Kõrvenögese tee 17 ds together with your own residence data or separately by submitting a he place of residence artu maakond, Kambja vald, Kuukivi alevik, Kõrvenögese tee 7 tarting date: 31.12.2017
Home page SELFSERVICE CELFSERVICE Ce Personal data	RicaportAAL       Accessibility       Q         Home / Personal data / I and my family       I and my family         I and my family       ✓ My identity documents and photo         ✓ My identity documents and photo       ✓ Me and my children: data from the Population R         ③ Changing data in Population Register         ④ Registering the birth of a child         ④ Query for name statistics         ④ Family event certificate (birth, marriage, divorce         ⑤ Query for relative relations	LANGUAGE en       ROLE MATI MAASIKAS >         Submit query         Registry       Submit query         Open in new window	5 Secure authentication for e-services Rici AUTENTIMISTEENUS Rici AUTENTIMISTEENUS	EESTI PYCCKVIЙ ter ntinue your session because you are logged in rvice: stool 38001085718 e of birth 371980 1 (SSO) solution - while logged in to one service, out re-authenticating. By clicking "Continue rring personal identification data listed above	Bender       Image: Contract of Entrant         Explored mem       Image: Contract of Entrant         Image: Contract of the blace of residence       My data         Image: Contract of the blace of residence       Image: Contract of the blace of residence         Image: Contract of the blace of residence       Image: Contract of the blace of residence         Image: Contract of the blace of residence       Image: Contract of the blace of residence         Image: Contract of the blace of residence       Image: Contract of the blace of residence         Image: Contract of the blace of residence       Image: Contract of the blace of residence         Image: Contract of the blace of residence       Image: Contract of the blace of residence         Image: Contract of the blace of residence       Image: Contract of the blace of residence         Image: Contract of the blace of residence       Image: Contract of the blace of residence         Image: Contract of the blace of residence       Image: Contract of the blace of residence         Image: Contract of the blace of residence of residence       Image: Contract of the blace of residence         Image: Contract of the blace of residence       Image: Contract of the blace of	ET RU MASKAS XSIgn.out k, Kõrvenõgese tee 17 ds together with your own residence data or separately by submitting a he place of residence artu maakond, Kambja vald, Kuukivi alevik, Kõrvenõgese tee 7 tarting date: 31.12.2017
Home page SELFSERVICE SELFSERVICE  SELFSERVICE  C Personal data Personal	RisportAL       Accessibility       Q         Home / Personal data / I and my family       I and my family         I and my family       I and my family         ✓ My identity documents and photo       ✓         ✓ Me and my children: data from the Population R         ② Changing data in Population Register         ③ Registering the birth of a child         ③ Query for name statistics         ③ Family event certificate (birth, marriage, divorce)         ④ Query for relative relations         ③ The suitability of a name for registering a birth	LANGUAGE       ROLE         en       MATI MAASIKAS >         Submit query       Submit query         Registry       Submit query         Open in new window       Open in new window         Open in new window       Open in new window         e or name change)       Open in new window         Open in new window       Open in new window         Open in new window       Open in new window	5 Secure authentication for e-services RIGI AUTENTIMISTEENUS RIGI AUTENTIMISTEENUS Note -population register it is sufficient to co to another service. Data that will be transmitted to se First name MASIKAS To Continue session Re-authenticate National authentication service uses a single sign-on you can continue your session in other services with session' you are confirming your identity and transfer to Service name B. By clicking "Re-authenticate" you are logged out from can authenticate as a new user.	EESTI РУССКИЙ ter ntinue your session because you are logged in evice: sonal code 38001085718 e of birth 3/1980 ) (SSO) solution - while logged in to one service, out re-authenticating. By clicking "Continue rring personal identification data listed above n all services related to current session and you	Generation       Image: Construct of Entrance         Construct of Entrance       My data         Image: Construct of Entrance       My data         Image: Construct of Entrance       Image: Construct of Entrance         Image: Construct of Entrance       Imag	ET RU MAASKAAS XSIQT OUT

#### **GOVSSO** session continuation

Secure authentication	Secure authentication for e-services			РУССКИЙ
	NTIMISTEENUS			
RUNCO CERTA	Logging in to e-population reg to another service. Data that First name MATI Surname MAASIKAS Continue session	opulation register gister it is sufficient to continue yo t will be transmitted to service: Personal code EE3800108 Date of birth 1/8/1980 Re-authenticate	our session because you are	logged in
	National authentication serv you can continue your sessi session" you are confirming to Service name B. By clicking "Re-authenticate can authenticate as a new u	vice uses a single sign-on (SSO) s on in other services without re-au your identity and transferring per " you are logged out from all servi iser.	olution - while logged in to or thenticating. By clicking "Cor sonal identification data liste ices related to current sessio	ne service, ntinue d above n and you
Return to service prov	vider		1	Help from id.ee
Bingens Utin Brocks Hopped	Co-financed by the Connecting European Union	g Europe Facility of the	More about the national au service	thentication

# **GOVSSO** logout

Secure authenticati	on for e-services	EESTI РУССКИЙ
Riigi Aut	TENTIMISTEENUS	
Катольс от Сатема Манатаку от тые Кателон	You have been logged out from e-p You are still logged in to the following services: eesti.ee Log out all Continue session	oopulation register
	By clicking "Log out all" you are logged out from all servic terminated. By clicking "Continue session" you are able to keep workin	es listed above and your session is ng in all services listed above. <u>Help from id.ee</u>
Evergeeu Liver Beseteneerd Fand	Co-financed by the Connecting Europe Facility of the European Union	More about the national authentication service

### **GOVSSO flow demonstration**

- Authentication
  - Single service
  - Two services
- Session update
- Logout
  - One service
  - Logout all

#### **GOVSSO** authentication flow: new session



#### **GOVSSO** authentication flow: session exists



#### **GOVSSO** session update



## **GOVSSO** logout



# /.well-known/openid-configuration endpoint

```
"issuer": "https://govsso-demo.ria.ee/",
"authorization_endpoint": "https://govsso-demo.ria.ee/oauth2/auth",
"token_endpoint": "https://govsso-demo.ria.ee/oauth2/token",
"jwks_uri": "https://govsso-demo.ria.ee/.well-known/jwks.json",
"subject_types_supported": [
    "public"
1,
"response types supported": [
    "code"
1,
"claims supported": [
    "sub",
    "acr".
    "amr",
    "at hash",
    "aud",
    "auth time",
    "exp",
    "iat",
    "iss",
    "jti",
    "nonce",
    "birthdate",
    "family name",
    "given_name",
    "sid"
],
```

# /.well-known/openid-configuration endpoint

```
"grant_types_supported": [
    "authorization_code"
],
"response_modes_supported": [
    "query"
],
"scopes_supported": [
    "openid"
1,
"token_endpoint_auth_methods_supported": [
    "client secret basic"
Ъ,
"id_token_signing_alg_values_supported": [
    "RS256"
],
"request_uri_parameter_supported": false,
"claims_parameter_supported": false,
"backchannel_logout_supported": true,
"backchannel_logout_session_supported": true,
"ui_locales_supported": [
    "et",
    "en",
    "ru"
1,
```

# /.well-known/openid-configuration endpoint

```
"acr_values_supported": [
    "low",
    "substantial",
    "high"
],
    "claim_types_supported": [
    "normal"
],
    "service_documentation": "https://e-gov.github.io/GOVSSO/",
    "end_session_endpoint": "https://govsso-demo.ria.ee/oauth2/sessions/logout"
```

}

# /.well-known/jwks endpoint



#### Key usage

 Client application should buffer the public key (it needs to be buffered together with kid value). It needs to compare the kid value from JWT header with buffered kid value.

HEADER:	
{ "alg": "RS256", "kid": "public:4a91f86b-340c-4c3a-a3c1-204a74449e1d", "typ": "JWT" }	

#### Key usage

 If key values from JWT header and buffer match, buffered key can be used. If not, client application needs to make request to public signature key endpoint and select key corresponding to kid value received from JWT header and buffer it.

GET https://govsso.ria.ee/oauth2/auth?

redirect\_uri=https%3A%2F%2Fclient.example.com%2Fcallback&
scope=openid&
state=hkMVY7vjuN7xyL15&|
response\_type=code&
client\_id=58e7ba35aab5b4f1671a&
ui\_locales=en&
nonce=fsdsfwrerhtry3qeewq&
acr\_values=substantial

URL element	compulsory	example	explanation
protocol, host, port and path	yes	https://govsso.ria.ee/oauth2/auth	<pre>/oauth2/auth is the OpenID Connect-based authentication endpoint of the GOVSSO service (the concept of 'authorization' originates from the OAuth 2.0 standard protocol). The URL is provided from OIDC server public discovery service: https://govsso.ria.ee/.well-known/openid-configuration as authorization_endpoint parameter.</pre>
client_id	yes	client_id=58e7ba35aab5b4f1671a	Client identifier. The client identifier is issued by RIA upon registration of the client application as a user of the authentication service.
redirect_uri	yes	<pre>redirect_uri=https%3A%2F%2Fclient.example.com%2Fcallback</pre>	Redirect URL ([OAUTH] "3.1.2. Redirection Endpoint"). The redirect URL is selected by the institution. The redirect URL may include the query component. URL encoding should be used, if necessary [URLENC]. It is not permitted to use the URI fragment component ( # and the following component; [URI] "3.5. Fragment"). The URL protocol, host, port and path must match one of the pre-registered redirect URLs of given client application registration metadata (see client_id parameter).

scope yes		The authentication scope. Space delimited list of requested scopes. openid scope is compulsory to signal that this is an OIDC authentication request. In the default scope of openid GOVSSO will issue ID Tokens with the following attributes:	
	yes	<pre>scope=openid</pre>	<pre>sub (physical person identifier) given_name family_name birthdate</pre>
			Presence of given attribute values will depend on the amount of information that is returned within TARA ID Tokens.
state	yes	<pre>state=hkMVY7vjuN7xyL15</pre>	Security code against false request attacks (cross-site request forgery, CSRF). Read more about formation and verification of state under "7.3 Protection against false request attacks".
response_type	yes	response_type=code	Determines the manner of communication of the authentication result to the server. Only value code is allowed as only authorization code flow is supported by GOVSSO

ui_locales	no	ui_locales=et	Selection of the user interface language. The following languages are supported: et , en , ru . By default, the user interface is in Estonian language. The client can select the desired language. This will also set the GUI language for TARA service views.
nonce	no	nonce=fsdsfwrerhtry3qeewq	A unique parameter which helps to prevent replay attacks based on the OIDC protocol ([OIDC- CORE] "3.1.2.1. Authentication Request").
acr_values	no	acr_values=substantial	The minimum required level of authentication based on the eIDAS level of assurance (LoA). Allowed values are: low, substantial, high. high is used by default if the value has not been set in request. GOVSSO will store the authentication level of assurance in the SSO session object as an Authentication Context Class Reference (acr) claim, from TARA ID Token response. Upon each GOVSSO authentication request, GOVSSO will check that the requested level of assurance (acr_values parameter value) is lower or equal to the acr claim value of the GOVSSO session. If the SSO session acr value (level of assurance) is lower than requested, the previous GOVSSO session is automatically terminated and a new authentication is requested from TARA. After successful authentication a new SSO session is created.

#### **GOVSSO flow: Authentication response**

GET https://govsso.ria.ee/oauth2/auth?

• Sent request

redirect\_uri=https%3A%2F%2Fclient.example.com%2Fcallback&
scope=openid&
state=hkMVY7vjuN7xyL15&|
response\_type=code&
client\_id=58e7ba35aab5b4f1671a&
ui\_locales=en&
nonce=fsdsfwrerhtry3qeewq&
acr\_values=substantial

• "Response" is returned through HTTP 302 redirect

HTTP GET https://client.example.com/callback?

Received response

code=71ed5797c3d957817d31&
state=hkMVY7vjuN7xyL15

## **GOVSSO flow: Authentication response**

URL element	example	explanation
protocol, host, port and path	https://client.example.com/callback	Matches the redirect_uri value sent in the authentication request.
code	code=71ed579	The authorization code to request the ID Token.
state	<pre>state=hkMVY7vjuN7xyL15</pre>	Security code against false request attacks. The security code received in the authentication request is mirrored back. Read more about forming and verifying state from 'Protection against false request attacks'.

#### **GOVSSO flow: Authentication error response**

HTTP GET https://client.example.com/callback?

error=invalid\_scope& error\_description=Required+scope+%3Copenid%3E+not+provided.+GOVSSO+does+not+allow+this+request+to+be+processed& state=hkMVY7vjuN7xyL15

- If user cancels authentication in GOVSSO same mechanism is used to return the cancel action.
  - error=user\_cancel
- Error description should be used only for debugging

#### **GOVSSO flow: ID Token request**

- HTTPS is obligatory and GOVSSO certificate (chain) must be trusted
- TLS 1.2 is used (TLS 1.3 will come in future)
## **GOVSSO flow: ID Token request**

POST /oauth2/token HTTP/1.1 Host: govsso.ria.ee Content-Type: application/x-www-form-urlencoded Authorization: Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW

grant\_type=authorization\_code&
code=Splx10BeZQQYbYS6WxSbIA&
redirect\_uri=https%3A%2F%2client.example.com%2Fcallback

- The body of the HTTP POST request must be presented in a serialized format based on the OpenID Connect protocol.
- ID Token must be requested within 30 seconds after GOVSSO has issued authorization code

#### **GOVSSO flow: ID Token request authentication**

- Request must include the Authorization request header
- The value is formed of the word Basic, a space, and a string <client\_id>:<client\_secret> encoded in the Base64 format.

## **GOVSSO flow: ID Token request**

Parameter	parameter type	example	explanation
protocol, host, port and path	query	https://govsso.ria.ee/oauth2/token	GOVSSO server token endpoint URL. Published in GOVSSO discovery endpoint token_endpoint parameter value.
grant_type	body	<pre>grant_type=authorization_code</pre>	The authorization_code value required based on the protocol. [OIDC-CORE] "3.1.3.1. Token Request"
code	body	<pre>code=Splxl0BeZQQYbYS6WxSbIA</pre>	The authorization code received from the authentication service.
redirect_uri	body	<pre>redirect_uri=https%3A%2F%2client.example.com%2Fcallback</pre>	The redirect URL sent in the authentication request.

#### **GOVSSO flow: ID Token response**

#### Sent request

POST /oauth2/token HTTP/1.1 Host: govsso.ria.ee Content-Type: application/x-www-form-urlencoded Authorization: Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW

grant\_type=authorization\_code&
code=Splx10BeZQQYbYS6WxSbIA&
redirect\_uri=https%3A%2F%2client.example.com%2Fcallback

HTTP/1.1 200 OK Content-Type: application/json Cache-Control: no-store Pragma: no-cache

Received response

"access\_token": "EKN-4fXC4n1RdkegKk-M0DRxZ8RwJYZ\_EwW-9zLCYcA.7GT7Xq2deLvWzrrFq6f0DNwL6INW2PYRDPPEFMbws1o",
"token\_type": "Bearer",
"expires\_in": 3600,
"id\_token": "eyJhbGci0iJSUzI1NiIsImtpZCI6InB1YmxpYzoyMDQ0YmV10C03MmY0LTQxYTMtYTR1

## **GOVSSO flow: ID Token response**

Parameter	explanation
access_token	OAuth 2.0 access token. With the access token the client application can request authenticated user's data from userinfo endpoint. Not used in GOVSSO because GOVSSO session management is purely ID Token dependent. All user data is already available in the ID Token.
token_type	OAuth 2.0 access token type with bearer value. Not used in GOVSSO.
expires_in	The validity period of the OAuth 2.0 access token. Not used in GOVSSO.
id_token	ID Token, encapsulated in JWS Compact Serialization form ([JWS] chapter 3.1). The ID Token itself is issued in JSON Web Token [JWT] format .

- id\_token is only value that should be used
- Unknown parameters must be ignored

```
"jti": "663a35d8-92ec-4a8d-95e7-fc6ca90ebda2",
"iss": "https://govsso.ria.ee/",
"aud": [
 "sso-client-1"
],
"exp": 1591709871,
"iat": 1591709811,
"sub": "EE60001018800",
"birthdate": "2000-01-01",
"family name": "O'CONNEŽ-ŠUSLIK TESTNUMBER",
"given name": "MARY ÄNN",
"amr": [
 "mID"
1,
"acr": "high",
"at_hash": "AKIDtvBT2JS_02tk1_DvuA",
"nonce": "POYXXoyDo49deYC3o5_rG-ig3U4o-dtKgcym5SyHfCM",
"sid": "f5ab396c-1490-4042-b073-ae8e003c7258",
```

ID Token element (claim)	example	explanation
jti	"jti":"663a35d8-92ec-4a8d-95e7- fc6ca90ebda2"	ID Token unique identifier ([JWT] "4.1.7. jti (JWT ID) Claim").
iss	"iss":"https://govsso.ria.ee/"	Issuer Identifier, as specified in [OIDC-CORE].
aud	<pre>"aud": [ "sso-client-1" ] or "aud": "sso-client-1"</pre>	Unique ID of a client application in GOVSSO client database. ID belongs to the client that requested authentication (the value of client_id field is specified in authentication request). String or array of strings. A single aud value is present in GOVSSO tokens.
ехр	"exp": 1591709871	The expiration time of the ID Token (in Unix epoch format).
iat	"iat": 1591709811	The time of issue of the ID Token (in Unix epoch format).

sub	"sub": "EE60001018800"	The identifier of the authenticated user (personal identification code or eIDAS identifier) with the prefix of the country code of the citizen (country codes based on the ISO 3166-1 alpha-2 standard). The subject identifier format is set by TARA authentication service ID Token [TARA] "4.3.1 Identity token". NB! in case of eIDAS authentication the maximum length is 256 characters.
birthdate	"birthdate": "2000-01-01"	The date of birth of the authenticated user in the ISO_8601 format. Only sent in the case of persons with Estonian personal identification code and in the case of eIDAS authentication.
given_name	"given_name": "MARY ÄNN"	The first name of the authenticated user (the test name was chosen because it consists special characters).
family_name	"family_name": "O'CONNEŽ-ŠUSLIK TESTNUMBER"	The surname of the authenticated user (the test name was selected because it includes special characters).
amr	"amr": [ "mID" ]	Authentication method reference. The authentication method used for user authentication. A single amr value is present in GOVSSO tokens. Possible values: mID - Mobile-ID idcard - Estonian ID card eIDAS - European cross-border authentication smartid - Smart-ID Available authentication methods depend on TARA authentication service and the list may be extended in the future [TARA] "4.1 Authentication request".

nonce	<pre>"nonce": "POYXXoyDo49deYC3o5_rG- ig3U4o-dtKgcym5SyHfCM"</pre>	Security element. The authentication request's nonce parameter value. Value is present only in case the nonce parameter was sent in the authentication request.
acr	"acr": "high"	Authentication Context Class Reference. Signals the level of assurance of the authentication method that was used. Possible values: low, substantial, high. The element is not used if the level of assurance is not applicable or is unknown.
at_hash	"at_hash": "AKIDtvBT2JS_02tk1_DvuA" The access token hash calculated as described in OIDC specification [OIDC-CORE].	
sid	"sid": "f5ab396c-1490-4042-b073- ae8e003c7258"	Session ID - String identifier for a GOVSSO session. This represents a session of a User Agent. Different sid values are used to identify distinct sessions at GOVSSO.

# **ID Token signature validation**

- Verifying the signature
  - RS256 signature algorithm is currently used
  - For the signature verification the GOVSSO public signature key must be used.
  - The used algorithm and public signature key is published at the public signature key endpoint /.well-known/jwks

## **ID Token signature validation**

- **1**. Read the kid value from the JWT header.
- 2. Validate the signature using the key corresponding to kid value from the JWT header.

# **ID Token validation**

- Verifying the issuer of token
  - The iss value of the ID Token element must match the issuer value in /.well-known/openid-configuration
  - In DEMO this value should be <a href="https://govsso-demo.ria.ee/">https://govsso-demo.ria.ee/</a>
- Verifying the addressee of the tokens
  - The client application must verify whether the token received was issued for them. For this purpose, it must be made sure that the aud value of the ID Token element matches the client\_id issued upon registration of the client application.

# **ID Token validation**

#### Verifying the validity of the tokens

- The verification is done using iat and exp elements in the ID Token. The client application uses its own clock to verify the validity. The following details should be verified:
  - that token issuing time has been reached:
    - iat <= (current time + permitted difference between clocks)</li>
  - that the "expired" time has not been reached:
    - exp > (current time permitted difference between clocks)
- The application must choose the permitted difference between clock values.

## **ID Token acr level validation**

- Acr value in ID token must be on equal or higher level than requested
- In case it was not specified in acr\_values parameter at request, it must be equal to value high

## **ID Token nonce validation**

• Nonce value must be the same that was used in the request

## If ID Token validation is successful

- ID Token must be stored for session update flow
- ID Token information can be used for authentication

- Session update should be done 2 minutes before the id\_token expiration
- Session update request should be done in background (with JavaScript)

GET https://govsso.ria.ee/oauth2/auth?

redirect\_uri=https%3A%2F%2client.example.com%2Fcallback&
scope=openid&
state=hkMVY7vjuN7xyL15&|
response\_type=code&
client\_id=58e7ba35aab5b4f1671a&
ui\_locales=en&
nonce=fsdsfwrerhtry3qeewq&
acr\_values=substantial&
prompt=none&
id\_token\_hint=eyJhbGci0iJSUzI1NiIsImtpZCI6InB1YmxpYzo...TvE

URL element	compulsory	example	explanation
protocol, host, port and path	yes	https://govsso.ria.ee/oauth2/auth	<pre>/oauth2/auth is the OpenID Connect-based authentication endpoint of the GOVSSO service (the concept of 'authorization' originates from the OAuth 2.0 standard protocol). The URL is provided from OIDC server public discovery service: https://govsso.ria.ee/.well-known/openid-configuration as authorization_endpoint parameter.</pre>
client_id	yes	client_id=58e7ba35aab5b4f1671a	Client identifier. The client identifier is issued by RIA upon registration of the client application as a user of the authentication service.
redirect_uri	yes	redirect_uri=https%3A%2F%2Fclient.example.com%2Fcallback	Redirect URL ([OAUTH] "3.1.2. Redirection Endpoint"). The redirect URL is selected by the institution. The redirect URL may include the query component. URL encoding should be used, if necessary [URLENC]. It is not permitted to use the URI fragment component ( # and the following component; [URI] "3.5. Fragment"). The URL protocol, host, port and path must match one of the pre-registered redirect URLs of given client application registration metadata (see client_id parameter).

			The authentication scope. Space delimited list of requested scopes.
			openid scope is compulsory to signal that this is an OIDC authentication request.
			In the default scope of openid GOVSSO will issue ID Tokens with the following attributes:
scope	ves	scope=openid	sub (physical person identifier)
	-		given_name
			tam11y_name
			birthdate
			Presence of given attribute values will depend on the amount of information that is returned
			within TARA ID Tokens.
state	yes	<pre>state=hkMVY7vjuN7xyL15</pre>	security code against faise request attacks (cross-site request forgery, USRF). Read more
			about formation and vehication of state under 7.5 Protection against faise request attacks .
response type	ves	response type=code	Determines the manner of communication of the authentication result to the server. Only
(coponec_type )	900	. coponise_cype code	value code is allowed as only authorization code flow is supported by GOVSSO
ui_locales n			Selection of the user interface language. The following languages are supported: et , en ,
	no	ui_locales=et	ru. By default, the user interface is in Estonian language. The client can select the desired
			language. This will also set the GUI language for TARA service views.

acr_values	no	acr_values=substantial	The minimum required level of authentication based on the eIDAS level of assurance (LoA). Allowed values are: low, substantial, high. high is used by default if the value has not been set in request. GOVSSO will store the authentication level of assurance in the SSO session object as an Authentication Context Class Reference (acr) claim, from TARA ID Token response. Upon each GOVSSO authentication request, GOVSSO will check that the requested level of assurance (acr_values parameter value) is lower or equal to the acr claim value of the GOVSSO session. If the SSO session acr value (level of assurance) is lower than requested, the previous GOVSSO session is automatically terminated and a new authentication is requested from TARA. After successful authentication a new SSO session is created.
prompt	yes	prompt=none	Signals GOVSSO server that it MUST NOT display any authentication or consent view to the user. An error is returned if user is not already authenticated in GOVSSO or the client application does not have pre-configured consent for the requested scope, acr_values or does not fulfill other conditions for processing the request. The error code will typically be login_required, interaction_required, or another code defined in OIDC standard ([OIDC-CORE] "3.1.2.6. Authentication Error Response").
id_token_hint	yes	<pre>id_token_hint=eyJhbGciOiJSUzI1NiIsImtpZCI6InB1YmxpYzoTvE</pre>	ID Token previously issued by GOVSSO being passed as a hint about the user's current or past authenticated session with the client application. If the user identified by the ID Token is logged in or is logged in by the request, then GOVSSO returns a positive response; otherwise, it WILL return an error. Encryption of the id_token_hint parameter is not supported in GOVSSO.

#### **GOVSSO flow: Session update response**

Sent request

GET https://govsso.ria.ee/oauth2/auth?

redirect\_uri=https%3A%2F%2client.example.com%2Fcallback&
scope=openid&
state=hkMVY7vjuN7xyL15&|
response\_type=code&
client\_id=58e7ba35aab5b4f1671a&
ui\_locales=en&
nonce=fsdsfwrerhtry3qeewq&
acr\_values=substantial&
prompt=none&
id\_token\_hint=eyJhbGci0iJSUzI1NiIsImtpZCI6InB1YmxpYzo...TvE

- "Response" is returned through HTTP 302 redirect
- Received response

GET https://client.example.com/callback? code=71ed5797c3d957817d31&

state=hkMVY7vjuN7xyL15

## **GOVSSO flow: Session update response**

URL element	example	explanation	
protocol, host, port and path	https://client.example.com/callback	Matches the redirect_uri value sent in the authentication request.	
code	code=71ed579	The authorization code to request the ID Token.	
state	<pre>state=hkMVY7vjuN7xyL15</pre>	Security code against false request attacks. The security code received in the authentication request is mirrored back. Read more about forming and verifying state from 'Protection against false request attacks'.	

#### **GOVSSO flow: Session update error response**

GET https://client.example.com/callback?

error=authentication\_required&
error\_description=Authenticated+subject+does+not+match+provided+id\_token\_hint&
state=hkMVY7vjuN7xyL15

#### If error code is received session should be terminated on client side immediately

## **ID Token request and validation**

- New ID Token must be requested as in authentication
- Same validation rules must be applied before updating the session status on client side
- New ID Token must be stored to use in next session update

GET https://govsso.ria.ee/oauth2/sessions/logout?

id\_token\_hint=eyJhbGciOiJSUzI1NiIsImtpZCI6InB1YmxpYzo3Njc2MG...VkDzh0LYvs
post\_logout\_redirect\_uri=https%3A%2F%2Fclient.example.com%2Fcallback&
state=0dHJpYnV0ZXMiOnsiZGF0ZV9vZ19iaXJ&
ui\_locales=et

URL element	compulsory	example	explanation
protocol, host, port and path	yes	https://govsso.ria.ee/oauth2/sessions/logout	<pre>/oauth2/auth is the OpenID Connect-based logout endpoint of the GOVSSO service. Described in OIDC session management specification [OIDC-SESSION] "2.1. OpenID Provider Discovery Metadata" The URL is provided from OIDC server public discovery service: https://govsso.ria.ee/.well-known/openid-configuration end session endpoint parameter.</pre>
			Redirect URL. The redirect URL is selected by the institution. The redirect URL may include the query component. URL encoding should be used, if necessary [https://en.wikipedia.org/wiki/Percent-encoding. It is not permitted ([OAUTH] "3.1.2. Redirection Endpoint") to use the URI fragment component ( # and the following component; [URI] "3.5. Fragment". The URL protocol, host, port and path must match one of the pre-registered redirect
post_logout_redirect_uri	yes	redirect_uri=https%3A%2F%2Fclient.example.com%2Fcallback	URLs of given client application. Client application is determined by the contents of the ID Token (token audience must belong to a registered GOVSSO client application). Different from OIDC session management specification, this parameter is considered mandatory in GOVSSO. In GOVSSO user logout flow we expect that the user is always redirected back to the client application that initiated the logout process. The post_logout_redirect_uri should point to the client application front page or a client application internal redirect url.

id_token_hint	yes	<pre>id_token_hint=eyJhbGciOiJSUTvE</pre>	ID Token previously issued by GOVSSO being passed as a hint about the user's current or past authenticated session with the client application. If the user identified by the ID Token is not logged in or is logged in by the request, then GOVSSO returns a positive response; otherwise, it WILL return an error. <b>id_token_hint encryption is not supported.</b>
state	no	state=hkMVY7vjuN7xyL15	Security code against false request attacks (cross-site request forgery, CSRF). Length of state parameter must be minimally 8 characters. Read more about formation and verification of state under 'Protection against false request attacks'. If included in the logout request, the TARA passes this value back to the RP using the state query parameter when redirecting the user agent back to the client application. Using the state parameter is not mandatory for login callbacks. It is expected that the user was already logged out of the client application before calling GOVSSO logout endpoint.
ui_locales	no	ui_locales=et	Selection of the user interface language. The following languages are supported: et , en , ru . By default, the user interface is in Estonian language. If the user was logged into a single client application, then no GUI prompt will be displayed to the user.

#### **GOVSSO flow: Logout response**

Sent request

GET https://govsso.ria.ee/oauth2/sessions/logout?

id\_token\_hint=eyJhbGci0iJSUzI1NiIsImtpZCI6InB1YmxpYzo3Njc2MG...VkDzh0LYvs
post\_logout\_redirect\_uri=https%3A%2F%2Fclient.example.com%2Fcallback&
state=0dHJpYnV0ZXMiOnsiZGF0ZV9vZ19iaXJ&
ui\_locales=et

- "Response" is returned through HTTP 302 redirect
- Received response GET https://client.example.com/callback?state=H0dHJpYnV0ZXMiOnsiZGF0ZV9vZ19iaXJ

#### **GOVSSO flow: Logout error response**

• If the logout request processing is unsuccessful error will be shown to user in GOVSSO.

#### **GOVSSO flow: Back-channel logout request**

POST /back-channel-logout HTTP/1.1
Host: client.example.com
Content-Type: application/x-www-form-urlencoded

logout\_token=eyJhbGci0iJSUzI1NiIsImtpZCI...p-wczlqgp1dg

## **GOVSSO flow: Back-channel logout request**

Parameter	compulsory	example	explanation
protocol, host, port and path	yes	<pre>https://client.example.com:443/back- channel-logout</pre>	Client application must authorize access to GOVSSO to an internal URL and port. Access to the port should be limited based on IP address. The port must be protected with TLS. GOVSSO must trust the logout endpoint server certificate.
logout_token	yes	<pre>logout_token=eyJhbGci0iJSUzqgp1dg</pre>	GOVSSO sends a JWT token similar to an ID Token to client applications called a Logout Token to request that they log out. Logout Token will give the client application exact information about the session (see the sid claim in ID Token) that should be logged out. The token is signed by GOVSSO with the same secret key that is used for singing issued ID Tokens.

#### **Logout Token structure**

```
"aud": [
   "sso-client-1"
],
"events": {
   "http://schemas.openid.net/event/backchannel-logout": {}
},
"iat": 1591958452,
"iss": "https://govsso.ria.ee/",
"jti": "c0cfc91a-cdf5-4706-ad26-847b3a3fb937",
"sid": "9038c51d-719f-40e1-9322-a7920a2087c8"
```

#### **Logout Token structure**

Logout Token element (claim)	compulsory	example	explanation
iss	yes	"iss": "https://govsso.ria.ee/"	Issuer Identifier, as specified in [OIDC-CORE].
events	yes	<pre>"events": {   "http://schemas.openid.net/event/backchannel- logout": {} }</pre>	Claim whose value is a JSON object containing the member name http://schemas.openid.net/event/backchannel-logout. This declares that the JWT is a Logout Token. The corresponding member value MUST be a JSON object and SHOULD be the empty JSON object {}. OIDC-BACK "2.4. Logout Token"
aud	yes	<pre>"aud": [ "sso-client-1" ] or "aud": "sso-client-1"</pre>	Audience(s), as specified in [OIDC-CORE].
iat	yes	"iat": 1591958452	Issued at time, as specified IN [OIDC-CORE].
jti	yes	"jti": "c0cfc91a-cdf5-4706-ad26-847b3a3fb937"	Unique identifier for the token, as specified in [OIDC-CORE].
sid	yes	"sid": "f5ab396c-1490-4042-b073-ae8e003c7258"	Session ID - String identifier for a GOVSSO session. This represents a session of a User Agent. Different sid values are used to identify distinct sessions at GOVSSO.

## **Logout Token validation**

- Signature of the Logout Token must be verified the same way as ID Token
- Issuer must be verified
- Audience must be verified
- Validity must be verified
  - The verification is done using the iat claim value of the Logout Token.
    - iat <= (current time + permitted difference between clocks)</li>
  - The application must choose the permitted difference between clocks value.

- If Logout Token validation is successful client application session must be ended.
- Issued Logout Tokens are linked to ID Tokens via the sid claim. Each client application is expected to internally keep track of the ID Token sid claim and client application session relations. The client application must log out client application sessions that contain the same sid value.
#### **GOVSSO flow: Logout response**

• If client application response HTTP status code is not 200, GOVSSO will perform retry with the same Logout Token.

# Testing

- For authentication:
  - TEST ID-cards or LIVE ID-cards with uploaded authentication certificates in DEMO OCSP service can be used. To upload the certificate, follow instructions here: <u>https://demo.sk.ee/upload\_cert/</u>.
  - Smart-ID automatic test numbers: <u>https://github.com/SK-EID/smart-id-documentation/wiki/Environment-technical-parameters#test-accounts-for-automated-testing</u> or personal DEMO account: <u>https://github.com/SK-EID/smart-id-documentation/wiki/Smart-ID-demo#getting-started</u> can be used.

# Testing

- For authentication:
  - Mobile-ID automatic test numbers: <u>https://github.com/SK-</u> <u>EID/MID/wiki/Test-number-for-automated-testing-in-DEMO</u> can be used.
  - For eIDAS Czech Republic or Sweden can be used
    - Follow instructions on their sites for authentication

## Testing

- Ensure that all validation rules for tokens are in place
- Session termination on timeout, back-channel logout
- User cancellation on authentication
- Errors on authentication, session update, logout

### **Testing and debugging tools**

- Browser developer tools
- <u>https://jwt.io/</u>

### List of endpoints for DEMO environment

Link	Comment
https://govsso-demo.ria.ee/	GOVSSO endpoint for DEMO service (OIDC issuer URL)
https://govsso.ria.ee/	GOVSSO endpoint for PROD service (OIDC issuer URL)
/.well-known/openid-configuration	Public endpoint for GOVSSO server OpenID Connect configuration information.
/.well-known/jwks.json	JSON Web Key Set document for GOVSSO service. Publishes at minimum the public key that client applications must use to validate ID Token and Logout Token signatures
/oauth2/auth	OAuth 2.0 authorization endpoint. Used for GOVSSO session update requests and authentication requests.
/oauth2/token	GOVSSO endpoint to obtain ID Token
/oauth2/sessions/logout	GOVSSO client application initiated logout endpoint

#### **Additional information**

<u>https://e-gov.github.io/GOVSSO/</u>

#### **Questions and answers**

• Questions?



REPUBLIC OF ESTONIA INFORMATION SYSTEM AUTHORITY

# Thank you!