

AVINOR FEDERATION TECHNICAL TENDER REQUIREMENTS

Version 1.0

29. APRIL 2025

1 Document Description 3
1.1 Purpose of the document 3
1.2 Scope 3
1.3 Target Audience 3
1.4 Related Documents 3
2 Terms And Abbreviations 4
3 Authentication 5
3.1 TEK-FED-01 – Usernames 5
3.2 TEK-FED-02 – General Federation 5
3.3 TEK-FED-02-01 – Support / Selection of Identity Provider 5
3.4 TEK-FED-03 – Entra ID 6
3.4.1 TEK-FED-03-01 – Entra ID – Conditional Access 6
3.4.2 TEK-FED-03-02 – Entra ID – App registrations and authentication flow 7
3.4.3 TEK-FED-03-03 – Entra ID – Implicit Grant Flow 7
3.4.4 TEK-FED-03-04 – Entra ID – Cross Broker SSO 7
3.4.5 TEK-FED-03-05 – Entra ID – B2B Guest Users 8
3.4.6 TEK-FED-03-06 – Entra ID – Application Gallery 8
3.5 TEK-FED-04 – ADFS – Active Directory Federation Service 9
3.6 TEK-FED-04-01 – ADFS – Selection of Preferred Solution 9
3.7 TEK-FED-05 – Federation Protocol Requirements 10
3.7.1 TEK-FED-05-01 – Requirement to OpenID Connect Implementation 11
3.7.2 TEK-FED-05-02 – Requirement to “SAML 2.0 / WS-FED” Implementation 11
3.7.3 TEK-FED-05-03 – Single Logout Protocol (SLO) 11
3.7.4 TEK-FED-05-04 – Token Signing Certificate 12
3.8 TEK-FED-06 – Authentication Libraries 12
3.9 TEK-FED-07 – PKI Security 13
3.10 TEK-FED-08 – Provisioning of identities 13
3.11 TEK-FED-08-01 – Provisioning method 14

1 DOCUMENT DESCRIPTION

1.1 Purpose of the document

The purpose of this document is to describe Avinor's federation guidelines that shall be followed when establishing federation with 3rd party organizations.

1.2 Scope

The scope is to describe what kind of federation that Avinor supports.

1.3 Target Audience

This document is targeted to 3rd party organizations whom need insight in Avinor's federation guidelines.

1.4 Related Documents

A list of related documents and information is provided below.

- ADFS Design Document.

2 TERMS AND ABBREVIATIONS

Terms and abbreviations used throughout this document are described in the following table:

Term / Abbreviation	Description

Table 1.

3 AUTHENTICATION

3.1 TEK-FED-01 – Usernames

Ref	Requirement description	Classification
TEK-FED-01	The solution shall support usernames standard as described.	**S - Shall (absolute)**
Chapter Ref:	Chapter 4.1 and 4.3.4 Avinor Federation Guidelines.pdf	
Score Card:	"Entra ID" is preferred over "ADFS" and gives higher evaluation score.	

Vendors answer:
"Please use this section to describe in detail what is supported / not supported accordingly to Avinor specified requirement above."

3.2 TEK-FED-02 – General Federation

Ref	Requirement description	Classification
TEK-FED-02	The solution must be incompliance with "Avinor Federation Guidelines". You must describe if the solution/application/api shall use the requirement specified for "**Entra ID**" or "**ADFS**" for authentication and authorization.	**S - Shall (absolute)**
Chapter Ref:	Whole document of Avinor Federation Guidelines.pdf	
Score Card:		

Vendors answer:
"Please use this section to describe in detail what is supported / not supported accordingly to Avinor specified requirement above."

3.3 TEK-FED-02-01 – Support / Selection of Identity Provider

Ref	Requirement description	Classification
TEK-FED-02-01	You must select and describe if the solution/application/api shall use "Entra ID" or "ADFS" for authentication and authorization. If "**Entra ID**" is selected or supported, all requirement specified in TEK-FED-03 (inc. all sub requirements) shall be followed and answered for all corresponding subsequent requirements. If "**ADFS**" is selected or supported, all requirement specified in TEK-FED-04 (inc. all sub requirements) shall be followed and answered for all corresponding subsequent requirements. If both "**Entra ID**" and "**ADFS**" is supported, you must answer for all corresponding subsequent requirements.	**E - Evaluation**

Chapter Ref:	Whole document of Avinor Federation Guidelines.pdf	
Score Card:	"**Entra ID**" is preferred over "**ADFS**" and gives higher evaluation score.	

Vendors answer:
"Please use this section to describe in detail what is supported / not supported accordingly to Avinor specified requirement above."

3.4 TEK-FED-03 – Entra ID

Ref	Requirement description	Classification
TEK-FED-03	Avinor has implemented "Entra ID / Azure Active Directory" according to Microsoft best practices. If "Entra ID" is selected as the Identity Provider, please describe how Entra ID is supported and should be implemented for the solution.	**S - Shall (absolute)**
Chapter Ref:	Chapter 4.3 - Avinor Federation Guidelines.pdf	
Score Card:		

Vendors answer:
"Please use this section to describe in detail what is supported / not supported accordingly to Avinor specified requirement above."

3.4.1 TEK-FED-03-01 – Entra ID – Conditional Access

Ref	Requirement description	Classification
TEK-FED-03-01	Conditional access polices is a security mechanism to control various signals of whom is granted access to the application. Avinor requires that it should be possible define dedicated conditional access policy for the particular app that is registered in Azure AD. This will require that the application is using a front-end and back-end architecture, where the API of the application can be protected with conditional access. Please describe if this is supported.	**S - Shall (absolute)**
Chapter Ref:	Chapter 4.3.1 - Avinor Federation Guidelines.pdf	
Score Card:		

Vendors answer:
"Please use this section to describe in detail what is supported / not supported accordingly to Avinor specified requirement above."

3.4.2 TEK-FED-03-02 – Entra ID – App registrations and authentication flow

Ref	Requirement description	Classification
TEK-FED-03-02	All app registrations towards “Azure Active Directory / Entra ID” shall follow Microsoft best practices and recommendations. Avinor prefers and recommends usage of “Authorization Code Flow”. Please describe if this flow is used and supported. If “Authorization Code Flow” is not used, please describe the OpenID Connect Flows that is used. Also describe why this flow is selected.	**E - Evaluation**
Chapter Ref:	Chapter 4.3.2 - Avinor Federation Guidelines.pdf	
Score Card:	**Using other flow than Auth. Code Flow results in lower score.**	

Vendors answer:
“Please use this section to describe in detail what is supported / not supported accordingly to Avinor specified requirement above.”

3.4.3 TEK-FED-03-03 – Entra ID – Implicit Grant Flow

Ref	Requirement description	Classification
TEK-FED-03-03	Implicit grant flow is no longer suitable authentication method due to that modern browser are planning to phase out support for third party cookies and cross domain cookies. This will cause that application will break when they attempt to get a new token during the SSO capabilities of this flow. Please confirm that your application **is not using** “Implicit grant flow”. ***Important, usage of implicit grant flow will leave to disqualification of the tender.***	**S - Shall (absolute)**
Chapter Ref:	Chapter 4.3.2.2 - Avinor Federation Guidelines.pdf	
Score Card:		

Vendors answer:
“Please use this section to describe in detail what is supported / not supported accordingly to Avinor specified requirement above.”

3.4.4 TEK-FED-03-04 – Entra ID – Cross Broker SSO

Ref	Requirement description	Classification
TEK-FED-03-04	Avinor requires the usage of “Cross Broker SSO” for all native Apple iOS / iPadOS apps developed for Avinor. This allows the end user to have single sign on their device. Please describe if this supported.	**E - Evaluation**
Chapter Ref:	Chapter 4.3.3 - Avinor Federation Guidelines.pdf	
Score Card:		

Vendors answer:
"Please use this section to describe in detail what is supported / not supported accordingly to Avinor specified requirement above."

3.4.5 TEK-FED-03-05 – Entra ID – B2B Guest Users

Ref	Requirement description	Classification
TEK-FED-03-05	Avinor support collaboration with external guest users (B2B) for registered Entra ID / Azure AD tenant's domains. The solution must support guest users from Entra ID and also support synchronization of guest users via the SCIM protocol. Please describe if this is supported or not.	**S - Shall (absolute)**
Chapter Ref:	Chapter 4.3.4 - Avinor Federation Guidelines.pdf	
Score Card:		

Vendors answer:
"Please use this section to describe in detail what is supported / not supported accordingly to Avinor specified requirement above."

3.4.6 TEK-FED-03-06 – Entra ID – Application Gallery

Ref	Requirement description	Classification
TEK-FED-03-06	Entra ID Application gallery can be used. Please describe if this is part of your solution or not.	**I - INFO**
Chapter Ref:	Chapter 4.3.5 - Avinor Federation Guidelines.pdf	
Score Card:		

Vendors answer:
"Please use this section to describe in detail what is supported / not supported accordingly to Avinor specified requirement above."

3.5 TEK-FED-04 – ADFS – Active Directory Federation Service

Ref	Requirement description	Classification
TEK-FED-04	If "ADFS" is selected as Identity Provider for the solution, you must describe if the configuration will follow one of these two design choices: - ADFS Preferred Primary Solution - ADFS Preferred Secondary Solution The selected design choice must be incompliance with all requirements as specified in the relevant chapter for the design choice.	**S - Shall (absolute)**
Chapter Ref:	Chapter 4.4.1 and 4.4.2 - Avinor Federation Guidelines.pdf	
Score Card:		

Vendors answer:
"Please use this section to describe in detail what is supported / not supported accordingly to Avinor specified requirement above."

3.6 TEK-FED-04-01 – ADFS – Selection of Preferred Solution

Ref	Requirement description	Classification
TEK-FED-04-01	You must select and describe if the solution shall use "**ADFS Preferred Primary Solution**" or "**ADFS Preferred Secondary Solution**". The configuration design must follow one of these two design choices that is selected for the solution. The selected design choice must be incompliance with all requirements as specified in the relevant chapter for the design choice.	**E - Evaluation**
Chapter Ref:	Chapter 4.4.1 and 4.4.2 - Avinor Federation Guidelines.pdf	
Score Card:	ADFS Preferred Primary Solution will result in higher score.	

Vendors answer:
"Please use this section to describe in detail what is supported / not supported accordingly to Avinor specified requirement above."

3.7 TEK-FED-05 – Federation Protocol Requirements

Ref	Requirement description	Classification
TEK-FED-05	Avinor supports two types of federation protocols: **Modern Authentication Protocol** - OpenID Connect (OIDC) **Legacy Authentication Protocol** - SAML 2.0 - WS-FED Avinor prefers and recommends only to use “OpenID Connect” protocol as modern authentication mechanism. Selecting legacy protocols (SAML 2.0 or WS-FED) should be avoided. You must select and describe what authentication protocol the solution shall use. If “**OpenID Connect (OIDC)**” is selected or supported all requirement specified in TEK-FED-05-01 (inc. all sub requirements) shall be followed and answered for all corresponding subsequent requirements. If “**SAML 2.0 / WS-FED**” is selected or supported all requirement specified in TEK-FED-05-02 (inc. all sub requirements) shall be followed and answered for all corresponding subsequent requirements. If both “**OpenID Connect (OIDC)**” and “**SAML 2.0 / WS-FED**” is supported, you must answer for all corresponding subsequent requirements. **Important!** If the tender solution from Avinor has specified that a native app to “Apple iOS” or “Android” devices shall be included in the delivery, then “**OpenID Connect (OIDC)**” must be selected for the whole solution. Therefore, this requirement will change from “E - evaluation” to “**S - shall**” requirement. Be aware of that Avinor do not support native apps with other protocols than with “**OpenID Connect (OIDC)”**	**E** **-** **Evaluation**
Chapter Ref:	Chapter 4.5 - Avinor Federation Guidelines.pdf	
Score Card:	Selection of OpenID Connect protocol will result to higher score.	

Vendors answer:

“Please use this section to describe in detail what is supported / not supported accordingly to Avinor specified requirement above.”

3.7.1 TEK-FED-05-01 – Requirement to OpenID Connect Implementation

Ref	Requirement description	Classification
TEK-FED-05-01	If the solution has selected "OpenID Connect" as preferred protocol for this delivery, the solution shall support all specified OIDC requirement that Avinor has specified. Please document that the compliance of these requirements.	**S - Shall (absolute)**
Chapter Ref:	Chapter 5.1 including all sub chapters - Avinor Federation Guidelines.pdf	
Score Card:	Selection of OpenID Connect protocol will result to higher score.	

Vendors answer:
"Please use this section to describe in detail what is supported / not supported accordingly to Avinor specified requirement above."

3.7.2 TEK-FED-05-02 – Requirement to "SAML 2.0 / WS-FED" Implementation

Ref	Requirement description	Classification
TEK-FED-05-02	If the solution has selected "SAML 2.0 / WS-FED" as preferred protocol for this delivery, the solution shall support all specified SAML 2.0 / WS-FED requirement that Avinor has specified. Please document that the compliance of these requirements.	**S - Shall (absolute)**
Chapter Ref:	Chapter 5.2 and sub chapters - Avinor Federation Guidelines.pdf	
Score Card:	Selection of SAML 2.0 / WS-FED protocol will result to lower score.	

Vendors answer:
"Please use this section to describe in detail what is supported / not supported accordingly to Avinor specified requirement above."

3.7.3 TEK-FED-05-03 – Single Logout Protocol (SLO)

Ref	Requirement description	Classification
TEK-FED-05-03	The solution shall support "Single Logout Protocol (SLO)" for the selected federation protocol according to the specified requirement by Avinor.	**S - Shall (absolute)**
Chapter Ref:	Chapter 5.3 - Avinor Federation Guidelines.pdf	
Score Card:	Selection of SAML 2.0 / WS-FED protocol will result to lower score.	

Vendors answer:
"Please use this section to describe in detail what is supported / not supported accordingly to Avinor specified requirement above."

3.7.4 TEK-FED-05-04 – Token Signing Certificate

Ref	Requirement description	Classification
TEK-FED-05-04	The solution must support to automatically read and trust the current valid "Token Signing Certificate" that is published to the respective selected federation protocol trust endpoint. Each protocol trust endpoint has its own requirement that must be followed as specified in Avinor's requirement. **Trust endpoint for Open ID Connect** .Well Known Configuration **Trust endpoint for SAML2.0 / WS-FED** federationmetadata.xml	**S** **-** **Shall (absolute)**
Chapter Ref:	Chapter 5.4 - Avinor Federation Guidelines.pdf	
Score Card:	Selection of OpenID Connect protocol will result to higher score.	

Vendors answer:
"Please use this section to describe in detail what is supported / not supported accordingly to Avinor specified requirement above."

3.8 TEK-FED-06 – Authentication Libraries

Ref	Requirement description	Classification
TEK-FED-06	Authentication to identity platforms, such as "Entra ID" and "ADFS" may require many different sign-in methods, security, and compliance requirements for the application. Authentication Libraries enables developers to acquire security tokens, support multiple sign-in methods etc. from Entra ID or ADFS without having to develop this from scratch. Avinor highly recommends usage of MSAL authentication library. Please document what authentication library the solution will use.	**E** **-** **Evaluation**
Chapter Ref:	Chapter 5.5 and sub chapters - Avinor Federation Guidelines.pdf	
Score Card:	Usage of MSAL will result in higher score	

Vendors answer:
"Please use this section to describe in detail what is supported / not supported accordingly to Avinor specified requirement above."

3.9 TEK-FED-07 – PKI Security

Ref	Requirement description	Classification
TEK-FED-07	The solution must support and follow the current PKI security and certificates requirements as specified by Avinor to ensure best practice during federation. Minimum requirement must be supported regards to: - Certificate requirements - PKI Channel Protocols - PKI Chiper Suites - PKI Security Test Avinor requires that all web applications must comply certificate security test with rate Grade A at "Qualys SSL Labs"	**S - Shall (absolute)**
Chapter Ref:	Chapter 6 and sub chapters - Avinor Federation Guidelines.pdf	
Score Card:		

Vendors answer:
"Please use this section to describe in detail what is supported / not supported accordingly to Avinor specified requirement above."

3.10 TEK-FED-08 – Provisioning of identities

Ref	Requirement description	Classification
TEK-FED-08	The solution shall support one or more of the protocols for user provisioning according to the specified requirements. You must select and describe what user provisioning protocol the solution will use. **Modern provision protocol** - SCIM - REST method. **Legacy provisioning protocol** - SOAP If the supplier does not support user provisioning accordingly, the supplier shall establish this in cooperation with Avinor.	**S - Shall (absolute)**
Chapter Ref:	Chapter 4.6 - Avinor Federation Guidelines.pdf	
Score Card:		

Vendors answer:
"Please use this section to describe in detail what is supported / not supported accordingly to Avinor specified requirement above."

3.11 TEK-FED-08-01 – Provisioning method

Ref	Requirement description	Classification
TEK-FED-08-01	You must select and describe what provisioning protocol that the solution will use. **Modern provision protocol** - SCIM - REST method. **Legacy provisioning protocol** - SOAP Avinor prefers SCIM as preferred solution. The selected protocol must be incompliance with all requirements as specified in the relevant chapter for the design choice.	**E** **-** **Evaluation**
Chapter Ref:	Chapter 4.6 and sub chapters - Avinor Federation Guidelines.pdf	
Score Card:	Selection of SCIM protocol will result to higher score.	

Vendors answer:
"Please use this section to describe in detail what is supported / not supported accordingly to Avinor specified requirement above."

--- o0o ---