TR-064 Support – Authentication

Author: AVM GmbH
Date: 2016-10-06

1   urn:X_AVM-DE_Auth-com:serviceId:X_AVM-DE_Auth1

For details please refer the SCPD files on the device.

2   History

Date	Version	Changes
2016-08-05	1	First Draft
2016-09-08	2	Changed actions, parameters, return codes
2016-10-06	3	Statevariablennames edited, Servicename edited, errorcodes added

Content

3   Action List

This chapter contains the supported actions of the service Auth which are listed inclusive arguments.

3.1   GetInfo

Read restrictive values for action parameters.
* Required rights: any

Argument name	Direction	Meaning	Data type
NewEnabled	out	2-Factor-Authentication enabled	boolean

Table 1: Argument list of action GetInfo

Return code	Description	Related argument
402	Invalid arguments	Any
820	Internal error	

Table 2: Return codes of action GetInfo

3.2 GetState

Argument name	Direction	Meaning	Data type
NewState	out		StateEnum

Table 3: Argument list of action GetState

Return code	Description	Related argument
402	Invalid arguments	Any
820	Internal error	

Table 4: Return codes of action GetState

3.3 SetConfig

Start or stop a two-factor-authentication for the current user.

Argument name	Direction	Meaning	Data type
NewAction	in		String
NewToken	out		UUID
NewState	out		StateEnum
NewMethods	out		String

Table 5: Argument list of action SetConfig

Return code	Description	Related argument
402	Invalid arguments	Any
820	Internal error	

Table 6: Return codes of action SetConfig

4 Process

Only one second factor authentication process can be active. If more than one SOAP action triggers second factor authentication, only the first SOAP action will get all parameters.
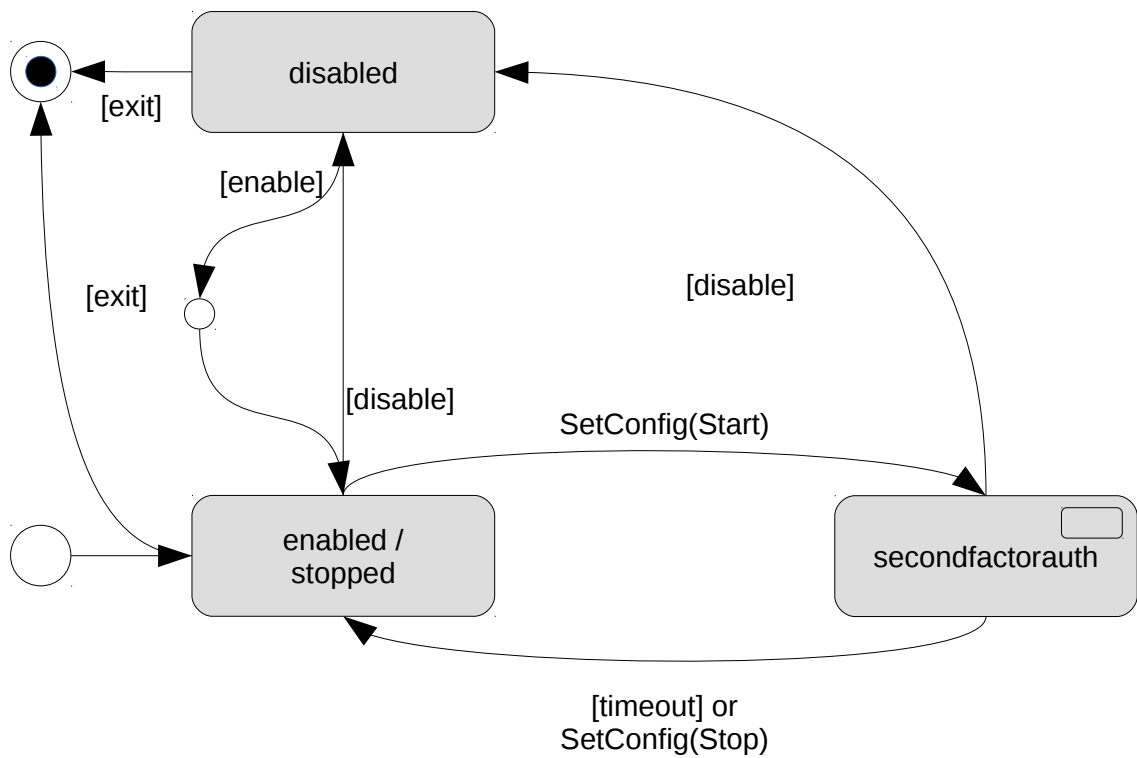
Figure 1: second factor auth state diagram

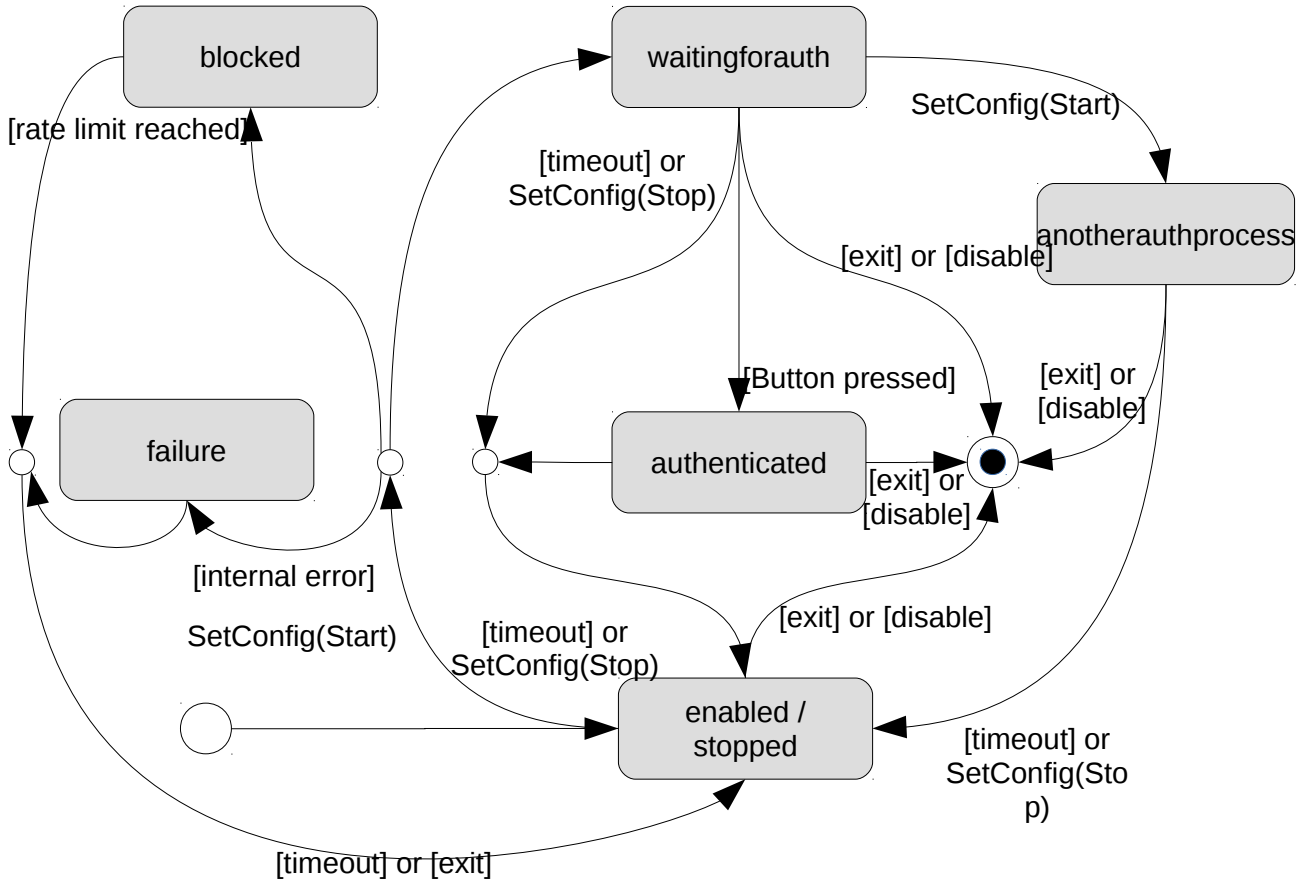| State	Description
timeout	Time out for second factor authentication; either waiting or authentication itself
exit	Exit of TR-064 service
enable	Enable second factor authentication in configuration
disable	Disable second factor authentication in configuration
secondfactorauth	Sub state diagram for second factor authentication

Table 7: state descriptions

Figure 2: second factor auth state diagram

5 Parameters

5.1 StateEnum

Value	Description
disabled	second factor authentication disabled by configuration
waitingforauth	second factor authentication waiting for user interaction to authenticate
anotherauthprocess	second factor authentication running for another user
authenticated	second factor authentication granted for current user
stopped	second factor authentication stopped and not authenticated
blocked	too many tries (limit reached)
failure	internal error occurred

Table 8: Parameter type StateEnum

6 Service States Table

Variable name	Allowed values (* == default)	Data type
Action	start, stop	String
Enabled		Boolean
Methods		String
State		StateEnum
Token		UUID

Table 9: Variable list

6.1 Action

Value	Description
start	Start second factor authentication process
stop	Stop a started second factor authentication process Possible if State has value waitingforauth or authenticated

Table 10: Parameter Action

6.2 Methods

Value	Description
button	Press any button to proceed second factor authentication
dtmf;*11234	Input the numbers *11234 as DTMF sequence using a locally cable connected phone or DECT phone.

Table 11: Parameter Methods

6.3 Return codes

The return codes may occur if second factor authentication is enabled and a protected configuration is intended to be changed.

If second factor authentication is blocked, it takes up to 60 minutes to be able to retry again.

If second factor authentication is busy, it takes up to two minutes to be able to retry again.

Value	Description
866	second factor authentication required
867	second factor authentication blocked
868	second factor authentication busy

Table 12: return codes

6.4 Token

The token shall be used to create a context for one second factor authentication process.

The token is related to a user and its configuration.

The token has to be used as part of the SOAP header for any SOAP action within the second factor authentication process.

```
<avm:token
 xmlns:avm="avm.de"
 s:mustUnderstand="1">2C0A2110-30BA-444e-8B83-566BC3F19C80</avm:token>
```

Typical scenario:

1. calling SetXYZConfig() returns 8xx, second factor authentication required

2. calling X_Auth:SetConfig(Action=start) returns
    State=waitingforauth
    Token=2C0A2110-30BA-444e-8B83-566BC3F19C80 and
    Methods=button, …

3. press the button

4. X_Auth:GetState() + SOAP-Header with Token returns
    State=authenticated

5. SetXYZConfig() with the same parameters as in step 1. and use the token inside
    the SOAP header returns with success or SOAP action specific return code.