

Instructions Internal

Date
2020-11-16
Identifier
Document id

Page
1 (10)
Version
2.4 Approved

Approved on
2020-11-16

Approved by
TeliaSonera
Internal Network
Kimmo Tuomainen

Relation
Object id.

Creator
Riitta Lapinniemi
+358408643938
riitta.lapinniemi@teliacompany.com

RSA SecurID- and MobilePASS-authentication and Pulse Secure configuration in Partner Secure User for Telia (PSU) service

Description

From this user guide you will learn how to implement MobilePASS Token and RSA software token and how to use it for authentication. Also Pulse secure configuration is presented.

Date	Page
2020-11-16	2 (10)
Identifier	Version
Document id	2.4
Relation	Approved
Object id.	

Table of contents

1 RSA SecurID installation instructions	3
1.1 RSA SecurID authentication with Software Token.....	3
1.1.1 Purpose	3
1.1.2 Install RSA SecurID Software Token from application store.....	3
1.1.3 Activating the RSA SecurID Software	3
1.2 RSA SecurID Hardware Token.....	4
1.3 Creating or changing the PIN code	4
1.4 Create PIN for the first time	4
PSU user (using Pulse Secure).....	4
PSU user (using Network Connect)	4
1.5 Creating or changing PIN for your RSA software token in the Self Service tool.....	5
1.6 Change PIN code in self-service tool	7
2 MobilePASS installation instructions	7
3 Pulse Secure.....	7
3.1 Client Installation using binary installation files	7
3.2 Creating the access profile in Pulse Secure (PSU service, external use).....	8
4 Using strong user authentication in daily work.....	8
4.1 Using SecurID Software or Hardware Token in Partner Secure User (PSU, i.e. VPN service with Pulse Secure)	8
4.2 Using MobilePASS Token in Partner Secure User (PSU, i.e. VPN service with Pulse Secure)	9
5 Version history	10

1 RSA SecurID installation instructions

1.1 RSA SecurID authentication with Software Token

1.1.1 Purpose

This is a user guide for taking a new RSA SecurID Software Token in use for the first time and how to use it then in the daily life.

- To implement this service follow the steps in 2, 3 and 4.
You only need to do these steps **once** when starting to use the service.
- In your **daily use** follow the steps in 5.
- If you forget your PIN code, you can set a new in self-service tool (see step 3).

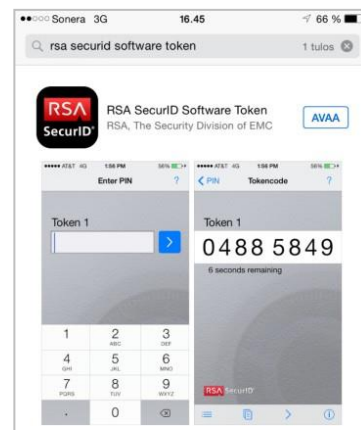
1.1.2 Install RSA SecurID Software Token from application store

Find RSA SecurID from the store and install it as follows:

Get application

1. Go the store in your mobile phone
e.g. iPhone users: App Store
2. Search with keys RSA SecurID Software Token
3. Tap download icon 
4. Tap Open (here Aava) or Install
5. In License Agreement: **Accept**

Now you have the application in your mobile phone.



1.1.3 Activating the RSA SecurID Software

1. You will receive an email from UAM-Finland (uam-finland@teliasonera.com). This email includes a link (url) that you need to open in your mobile phone.
 - If you have **TS Mobile Mail** in use, **open this email in your mobile phone** and tap the link to open it.

Or

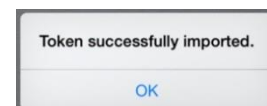
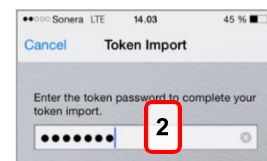
- If you don't have TS Mobile Mail in use, then you probably have some other email in use in your mobile phone, and you need to forward this email into the email you are using in your mobile phone.

Then open the email in your mobile phone and tap the link to open it.

2. In the RSA application in the 'Token Import' screen you need to enter **the token password** to complete your token import.
Token password = You have received this password in the previously mentioned email.

Type password, then tap Done.

3. 'Token successfully imported' is shown on the screen. Tap OK.

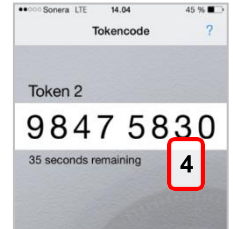


Date	Page
2020-11-16	4 (10)
Identifier	Version
Document id	2.4
Relation	Approved
Object id.	

- In the next **"Tokencode"** view you see 'Token X' title and 8 changing digits in the field. You have 60 seconds to use the code until it changes to another.

When you want to authenticate with RSA SecurID Software Token you add the 8 number tokencode after the PIN to form the Passcode (Passcode = PIN + 8 digit changing Tokencode).

You find the code when you open the application in your mobile phone. On the right you see the icon in iPhone.



1.2 RSA SecurID Hardware Token

If you already have or just have received an RSA SecurID Hardware Token (keychain) you can use it until the token is outdated (see date in the token's back). The only difference to Software Token is that the HW Token code has only 6 digits instead of 8 digits.



1.3 Creating or changing the PIN code

1.4 Create PIN for the first time

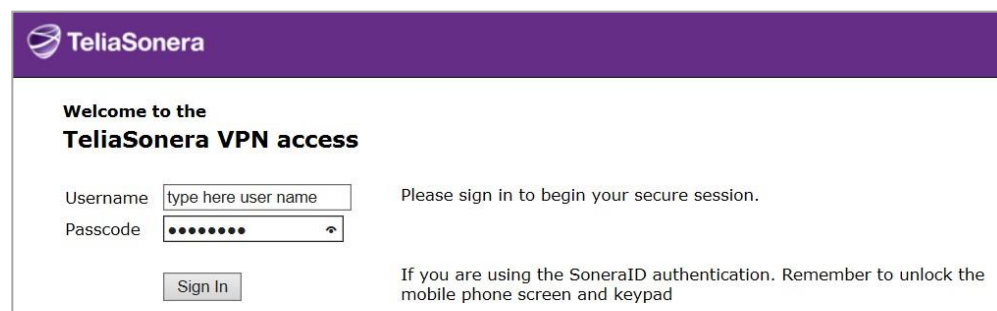
When you login to Telia Company remote access services for the **first time**, the services will require you to create your PIN code.

PSU user (using Pulse Secure)

- Install Pulse Secure and create a new profile according to chapter 4.
- When you initiate the VPN External Access connection the Pulse client guides you to set your Pin code and asks the Tokencode and then the Passcode (with the fresh set pin).

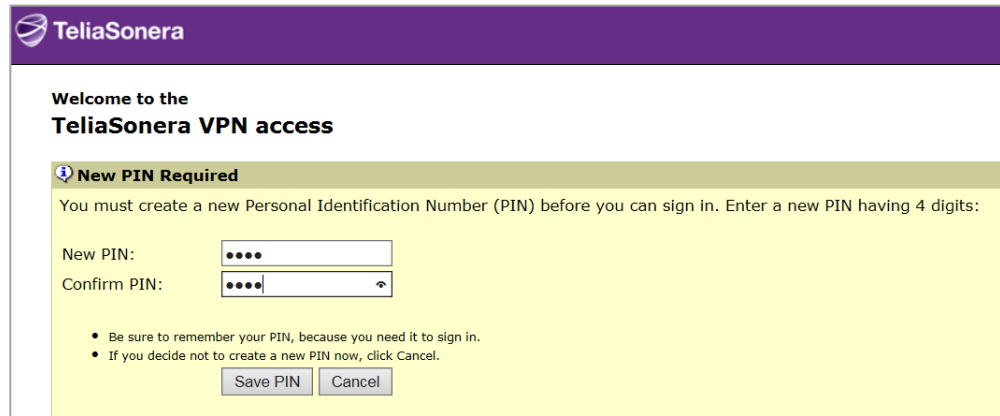
PSU user (using Network Connect)

- Use your browser and go to <https://tscafi.teliasonera.com/pulse> (for external users)
- Type your TCAD user name
in Passcode type only 8 changing numbers from RSA software token
(or 6 digits from RSA hardware token)



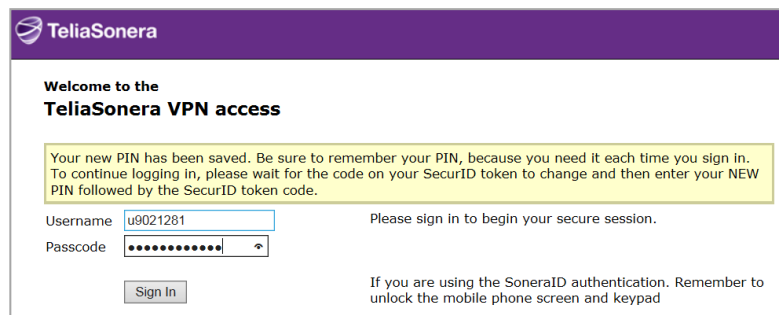
- Type a New PIN code
Type the same PIN code again to confirm it

Click Save PIN button

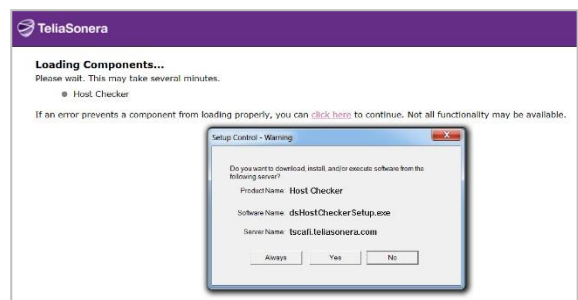
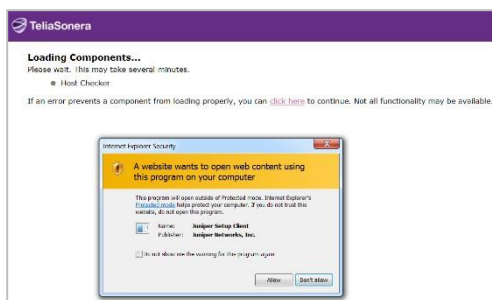


Now you have set a new PIN code.

- To log in type your user name
Then type Passcode: PIN + 8 changing digits from RSA software token (or 6 digits from RSA hardware token) and click Sign In button



- If the 'Loading Components...' views are shown select Allow and Always to proceed.



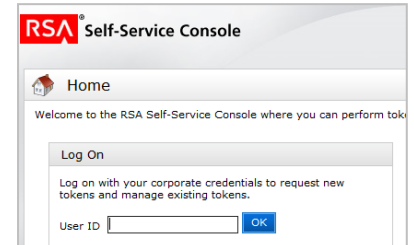
1.5 Creating or changing PIN for your RSA software token in the Self Service tool

If you have access to the RSA Self Service Console you can use it to set the PIN code for your RSA software (or hardware) token. You only need to do it once, before you start to

use the remote service.

If you don't remember your PIN code, please contact IT Service Desk and they can help you by resetting the PIN code.

1. In your TS7 computer or in an external pc after logging on to the access service go to RSA Self-Service Console: <https://excalibur.dave.sonera.fi:7004/console-selfservice>



The screenshot shows the 'RSA Self-Service Console' Home page. It includes a 'Log On' section with a text input field for 'User ID' and an 'OK' button. The text above the input field says 'Log on with your corporate credentials to request new tokens and manage existing tokens.'

2. Type your TCAD user name in 'User ID' field and click OK.



The screenshot shows the 'RSA Secure Logon' page. It has a 'Log On' section with 'User ID' (u9021281) and 'Authentication Method' (Passcode) dropdown menus. There are 'Cancel' and 'Log On' buttons.

3. In Authentication Method select **Passcode** and **Log On**.

4. In **Passcode** field you need to type the **Tokencode** from your mobile phone or from the RSA hardware token:
Open RSA SecurID app from your mobile phone and type the current token numbers in Passcode, and click **Log On**.



This screenshot is similar to the previous one but shows the 'Passcode' field filled with eight asterisks. The 'Log On' button is highlighted.

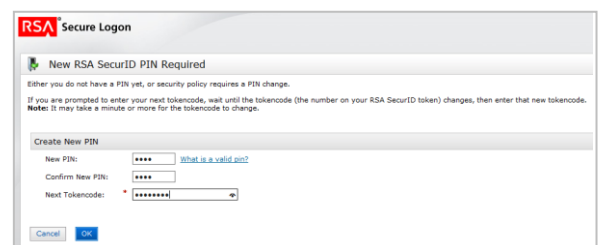
5. **New PIN:**
Type the PIN code that you want to use when authenticating.

Confirm New PIN: Type the same PIN again

Next Tokencode: Type the next Tokencode from your mobile phone (or hardware token), and click OK.

Now you have created a PIN code that you will from now on use always together with the changing Tokencode in your mobile phone (or hardware token), whenever Passcode is asked.

Passcode = PIN + 8 digit tokencode from RSA software token (or 6 digit code from RSA hardware token)



The screenshot shows the 'New RSA SecurID PIN Required' page. It has a 'Create New PIN' section with fields for 'New PIN', 'Confirm New PIN', and 'Next Tokencode'. There are 'Cancel' and 'OK' buttons.

- You can now log off from RSA self-service console: click **Log Off** in the upper right corner of the window.

1.6 Change PIN code in self-service tool

If you feel your pin code has become exposed and you need to change it, you can reset it by going in the Self-Service Console.

First sign in to the remote access service PSU

and then go to url <https://excalibur.dave.sonera.fi:7004/console-selfservice>.

Sign in with your user name and Passcode (pin + 8 or 6 digits). Then select **Change PIN**.

If you forget this PIN code, you need to call the Service Desk and ask for resetting the pin.

Token Serial Number:	created on Sep 8, 2016 1:58:16 PM EEST
PIN:	Change PIN
Expires On:	Jul 31, 2018 3:00:00 AM EEST request replacement

2 MobilePASS installation instructions

After idm approval an enrollment email is sent to users tcad registered email address. Follow the instructions to install the MobilePASS application and to activate the MobilePASS token.

Link to user guide: [Text and video user guides MobilePASS](#)

3 Pulse Secure

3.1 Client Installation using binary installation files

Windows user accounts must have administrator right to download and install software. Windows users, MAC OSX users and Linux users can install the VPN client from below binary installation files.

Binary installation file name	Installed application
PulseSecure.X64.msi	Pulse Secure for Windows 7,8,10, 64-bit
PulseSecure.X86.msi	Pulse Secure for Windows 7,8, 32-bit
PulseSecure.dmg	Pulse Secure for MAC OS X 10.10-10.12, 64-bit
Pulse-5.3R3.i386.rpm Pulse-5.3R3.x86_64.rpm	Pulse Secure for Linux quick start guide

(Red hat) Pulse-5.3R3.i386.deb Pulse-5.3R3.x86_64.deb (Debian/Ubuntu)	
---	--

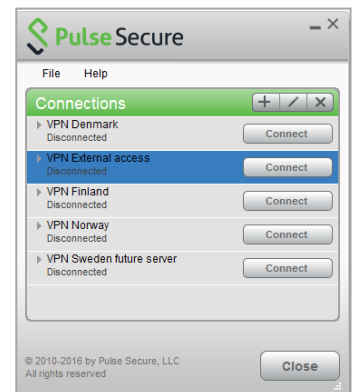
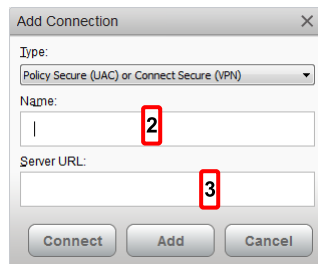
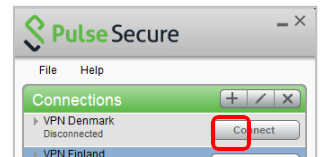
Install the Pulse client from <https://web2.storegate.com/share/gkpKV7U> (To follow the link. press CTRL+click)

The latest info regarding different remote accesses and pulse clients:
<http://howto.access.teliacompany.com/>

3.2 Creating the access profile in Pulse Secure (PSU service, external use)

If there is not a profile available when you open Pulse Secure client, you can create it easily as follows:

1. In Pulse Secure window Add Connection (+ sign) in the Connections area in the upper part of window.
2. Name: type name for the connection, e.g. 'VPN External access'
Server URL: type tscafi.teliasonera.com
3. Click **Add**, and now you have added the profile.



4 Using strong user authentication in daily work

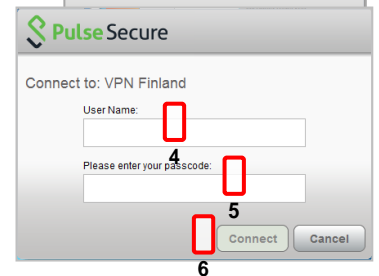
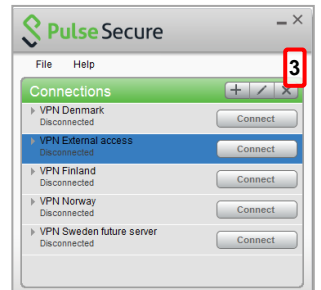
You can use your strong authentication with RSA SecurID or with MobilePASS token for authentication with tcad-userid.

4.1 Using SecurID Software or Hardware Token in Partner Secure User (PSU, i.e. VPN service with Pulse Secure)

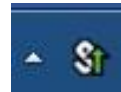
This is how you use RSA SecurID Software/Hardware Token in your daily life for authentication in Pulse Secure VPN client:

1. Check that the Internet connection is ON.

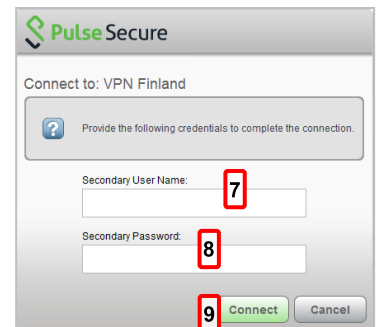
2. Open Pulse Secure
Start – All Programs – Pulse Secure –Pulse Secure
3. **Click the Connect** button after the profile name.
Note: If you don't have a suitable profile visible here, you can create it. See the chapter 4.
 1. Choose **realm SecurID**
4. In **User Name**: type your TCAD user name
5. **Passcode:**
Open RSA SecurID app in your mobile phone (or use your RSA Hardware Token).
Type here the RSA token's **PIN code** and after that the **changing number** (8-digit Tokencode from your mobile phone or 6-digit code from hw Token)
e.g. **123490807162** or **1234885667**
6. Click **Connect** button
7. In **Secondary User Name**: type again your TCAD user name
8. In **Secondary Password**: type your TCAD password
9. Click **Connect** button
10. Wait. Soon your VPN connection is ON.



6. Click **Connect** button
7. In **Secondary User Name**: type again your TCAD user name
8. In **Secondary Password**: type your TCAD password
9. Click **Connect** button
10. Wait. Soon your VPN connection is ON.



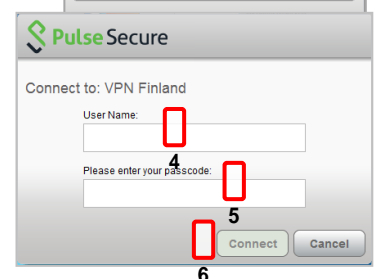
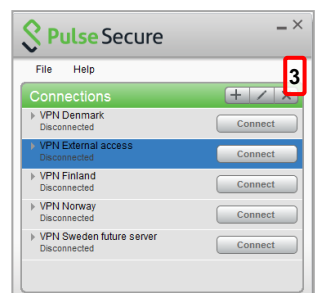
You can see the information on the Task bar:



4.2 Using MobilePASS Token in Partner Secure User (PSU, i.e. VPN service with Pulse Secure)

This is how you use MobilePASS Token in your daily life for authentication in Pulse Secure VPN client:

11. Check that the Internet connection is ON.
12. Open Pulse Secure
Start – All Programs – Pulse Secure –Pulse Secure
13. **Click the Connect** button after the profile name.
Note: If you don't have a suitable profile visible here, you can create it. See the chapter 4.
 2. Choose **realm MobilePASS**
14. In **User Name**: type your TCAD user name (4)
15. **Passcode:**
Open MobilePASS app in the device you installed it (phone or computer).
Enter PIN code you've configured for the MobilePASS
Type the 8-digit MobilePASS generated passcode
e.g. **12345678** (5)
16. Click **Connect** button (6)



Instructions Internal

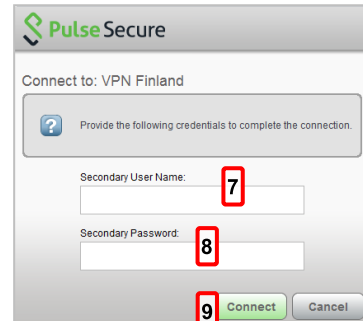
Date
2020-11-16
Identifier
Document id

Page
10 (10)
Version
2.4 Approved

Relation
Object id.

17. In **Secondary User Name**: type again your TCAD user name (7)
18. In **Secondary Password**: type your TCAD password (8)
19. Click **Connect** button (9)
20. Wait. Soon your VPN connection is ON.

You can see the information on the Task bar:

5 Version history

Versions	Status	Date	Modified by	Comments
0.1	Draft	2015-05-28	Kimmo Tuomainen	
1.0	Draft	2015-06-11	Riitta Lapinniemi	
2.0	Approved	2015-09-02	Riitta Lapinniemi	Updates
2.1	Approved	2016-09-16	Riitta Lapinniemi	Updates
2.1a	Approved	2016-11-28	Kimmo Tuomainen	Corrections
2.1b	Approved	2017-10-13	Sari Nikkilä	Split SPP/PSU instructions
2.4	Approved	2020-11-16	Kimmo Tuomainen	Links corrected