MFA Service – Additional Information

Global Shared Services
GSS IT/Global Security Services
Author: Arnd Meysenburg

Version	1.1
Date	July 2017
Information class	public
Contact	Tobias Warth, GSS IT
Associated documents	

Content

1. Introduction

The scope of this document is to provide additional information for a better understanding of the MFA service, its purpose and usage.

2. Multi-Factor Authentication (MFA) Overview

The MFA service provides a multi factor authentication solution to enhance security of authorized logins on thyssenkrupp applications. Multi factor authentication means that a user is granted access to a source of information (IT systems, corporate data etc.) only after successfully giving more than one piece of evidence to an authentication mechanism. At thyssenkrupp there are two steps of authentication are used: 1. a so called **token** which consists of a software solution (e.g. smartphone app) or a hardware device generating x-digit numbers and 2. the entry of one of those generated numbers as so called One Time Password (OTP) combined with your **username and password**.

3. FAQ

1 **What is MFA and why do we need it for thyssenkrupp applications?**
The MFA service is the thyssenkrupp standard multi factor authentication solution significantly enhancing application logon security. The MFA service uses One Time Passwords (OTP) as an additional secret (factor) to be provided by the user to authenticate against the application. This approach increases the confidence with which the application knows the user´s identity, which makes the login process more secure.

2 **What is a One Time Password?**
An OTP is an mathematically unpredictable number calculated on all thyssenkrupp tokens and valid for a very short time (e.g. 30 seconds). Knowledge of this number provides a confidential second factor for the login process. The first factor is a user´s secret password, known only to that user.

3 **What is a token?**
In the context of IT security, a token refers to a device or piece of software which has been configured to calculate One Time Passwords for a group of trusted users.

4 **Where can I get support for MFA?**
Please call the GSS IT Application Support Hotline +49201844555555 or email to app-support@thyssenkrupp.com)

5 **When can I get support for MFA?**
The current availability is Monday - Friday: 2.00 a.m. - 6.00 p.m. CEST.
MFA Service is planned to be reachable all day every day by end of FY16/17.

6 **What type of tokens are there?**
There are six different tokens available to thyssenkrupp users at this time. There are four different hardware token types:

- simple LCD tokens (Feitian C200 i28)
- LCD tokens with an activation button (Feitian C200 h27)
- USB Tokens (Feitian ePass FIDO NFC)
- Advanced USB Tokens (YubiKey edge-n)

There are three supported software tokens at this time, which may be installed and used on any compatible thyssenkrupp or private device:

- Microsoft Authenticator available on Windows Phone and Apple iOS
- Google Authenticator available on Android and Apple iOS
- FreeOTP available on Android and Apple iOS

Apps on BlackBerry OS, and most other authenticator applications for Android, iOS and Windows Phone will function with thyssenkrupp MFA, however are not supported at this time.

7 **Which token type should I use?**
The intended standard is use of a supported software token app. This also presents the most convenient and flexible option.

8 **Can I still login without a token/OTP?**
Without an OTP, login is not possible if the application requires one.
In case your tokens are not available and you need to access the application, you may call GSS IT Application Support, verify your identity over the phone and will receive an OTP for login.
Be aware that this is only intended to use in exceptional cases.
Please inform Support if your token is lost, broken or stolen.

9 **How do I get a token?**
Please contact your application owner or local IT coordinator for details on MFA secured applications that you may require a token for.

10 **Can I see what tokens I already have?**
Yes, please login to the Self-Service Portal to view the token(s) assigned to you. https://mfa-portal.thyssenkrupp.com Only the GSS IT Application Support is able to remove tokens assigned to your user.

11 **I already own a token/app for private use, can I use that for thyssenkrupp?**
Yes, please refer to FAQ question 6 for details.

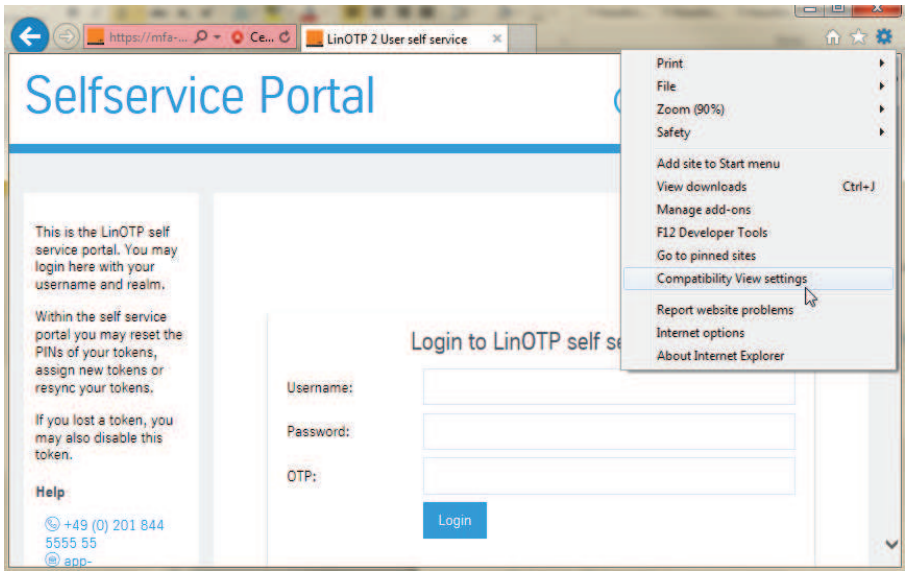
12 **How do I login if I do not have my registered token?**
Please refer to FAQ question 8 for details.

13 **What should I do if I my token was stolen or lost?**
Please refer to FAQ question 8 for details.

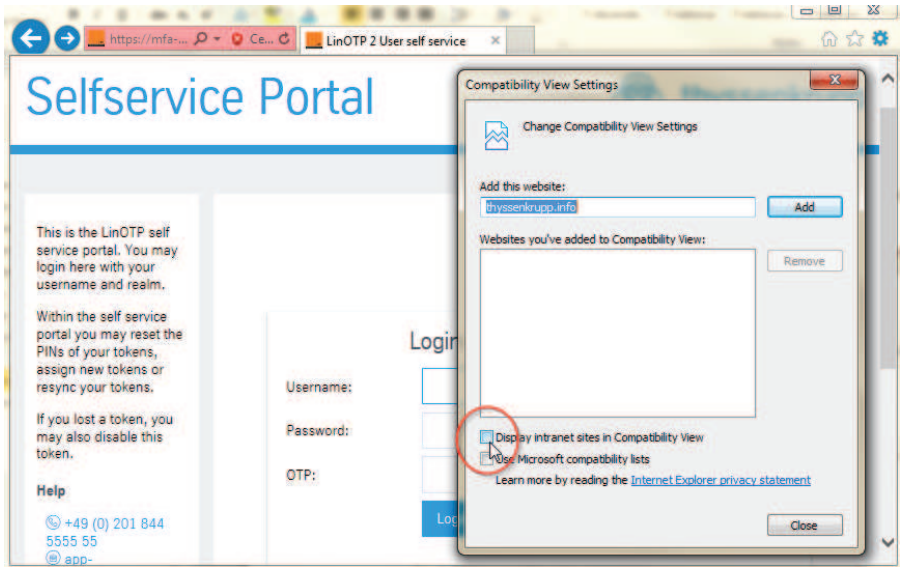
14 **What is my personal data used for?**
The MFA Service uses information already published in the global tk directory. If additional details are submitted by the user to the MFA Service (e.g. mobile phone number), this information is only stored and processed within the MFA service in order to provide the secure login options described in this document. Data storage and processing for MFA has been approved by the global workers' council (thyssenkrupp Konzernbetriebsrat, KBR) and is in line with corporate and legal data privacy requirements.

4. Known issues

1 The MFA Self-Service Portal is not displayed properly using Microsoft Internet Explorer in “Compatibility View”. If you experience this issue please turn off Compatibility View:



In the Internet Explorer, click on the TOOLS icon in the top right of the window.



Clear the “Display intranet sites in Compatibility View” checkbox and hit CLOSE.

5. MFA Service support

The regular user support of the MFA service is done by the GSS IT Application Support team:

Phone number: +49 (0) 201 844 5555 55
Mailto: app-support@thyssenkrupp.com
Support hours: Monday - Friday: 2.00 a.m. - 6.00 p.m. CEST
(24x7h support planned and is currently in the roll-out phase)
Supported languages: English, German

6. Other Documentation

Various guides are available to direct you through the initial setup of a new token and to register for OTP delivery via SMS:

- Getting started with Software tokens/apps:

software token/app

- Getting started with Hardware tokens:

hardware token

- How to register for OTP via SMS:

SMS

Getting Started with MFA – Smartphone App

Global Shared Services
GSS IT/Global Security Services
Author: Arnd Meysenburg

Version	1.1
Date	July 2017
Information class	public
Contact	Tobias Warth, GSS IT

engineering.tomorrow.together.

thyssenkrupp

Content

1 Introduction

The scope of this document is to provide comprehensive documentation for all current and future users of the thyssenkrupp MFA service. The MFA service is the thyssenkrupp standard multi factor authentication solution significantly enhancing application logon security. The MFA service uses One Time Passwords (OTP) as an additional secret to be provided by the user to authenticate against the application. This approach increases the security with which the application knows the user´s identity.

This document guides you through the initial steps, preparing and then performing your first logon using the MFA service. This guide is specific to software tokens. For using other tokens, please refer to the appropriate guide.

1. Install your chosen software token (smartphone app) onto your device
2. Please open the MFA self-service portal to register yourself
3. Contact the GSS IT Application support for your initial OTP
4. Login to the MFA self-service portal by using your 8-ID, domain password and the provided OTP
5. Register your smartphone app with MFA and proceed with the logon process

2 Getting Started

These are common, supported apps from 3rd party providers that can be used for login purposes on thyssenkrupp and other applications, e.g. G-Mail, facebook. The QR code or link will take you to the respective app store /app. Please install one to continue.

Android OS

Google Authenticator	Link to Google Play Store	
FreeOTP Authenticator	Link to Google Play Store	

Apple iOS

FreeOTP Authenticator	Link to iTunes	
Microsoft Authenticator	Link to iTunes	
Google Authenticator	Link to iTunes	

Windows Phone

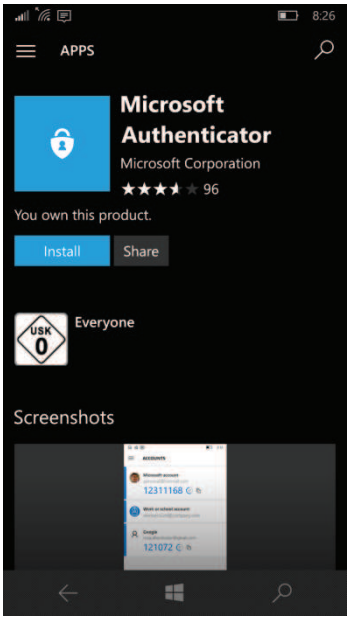
Microsoft Authenticator	Link to Microsoft Store	

Apps on BlackBerry OS, and most other authenticator applications for Android, iOS and Windows Phone will function with thyssenkrupp MFA, however are not supported at this time.

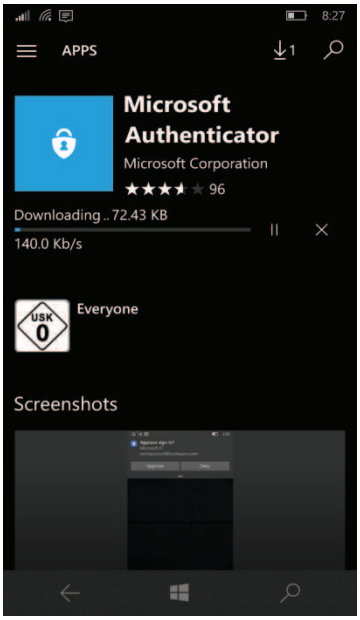
You will now be guided through the steps enabling you to use the MFA service using Windows Phone as the operating system. To prepare your smartphone, please download and install your chosen smartphone app from the app store, like any other app. For details on how to install your app on your device, please refer to the instructions provided to via the app store.

1. Download and install your apps

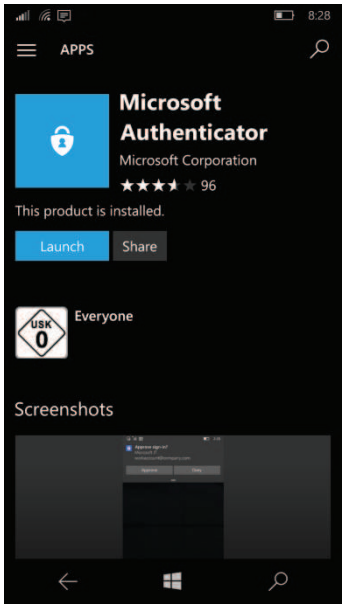
For demonstration purposes we will show how this works using the Microsoft Authenticator app



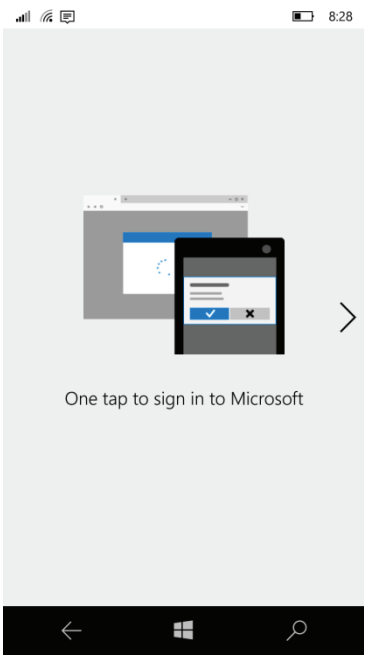
a) press “Install”



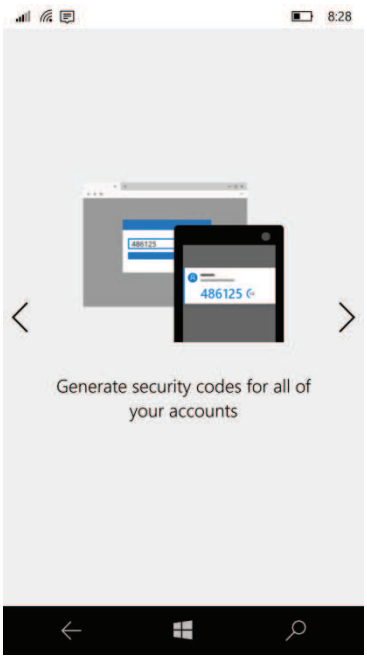
b) wait for the download to complete



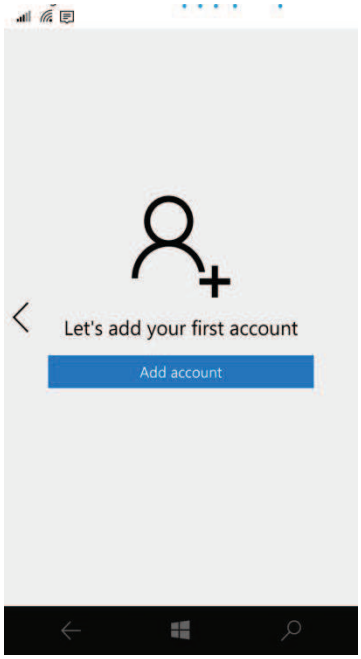
c) press “Launch”



d) swipe left or hit the arrow



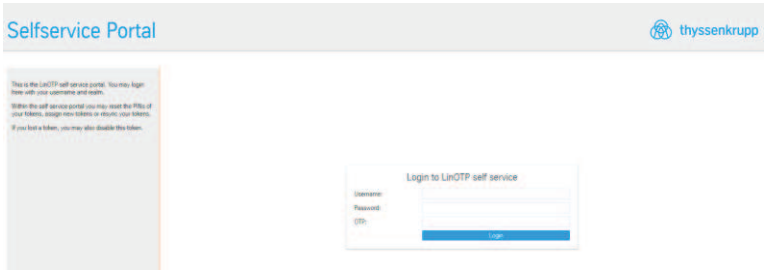
e) swipe left or hit the arrow



f) hit “Add Account” and proceed with the next step on your PC

2. Open the MFA self-service portal in your browser

Please follow the link: https://mfa-portal.thyssenkrupp.com



3. Login to the MFA self-service portal

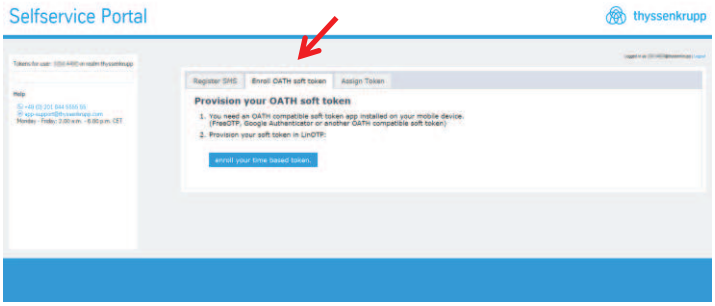
To login to the MFA portal, you need your 8-ID, your password and now also an OTP. To obtain your initial OTP:

- please call GSS IT Application Support under: +49 201 844 555555.

You must verify your identity to the agent over the phone before the OTP is provided. Please now use your 8-ID, domain password and the provided OTP

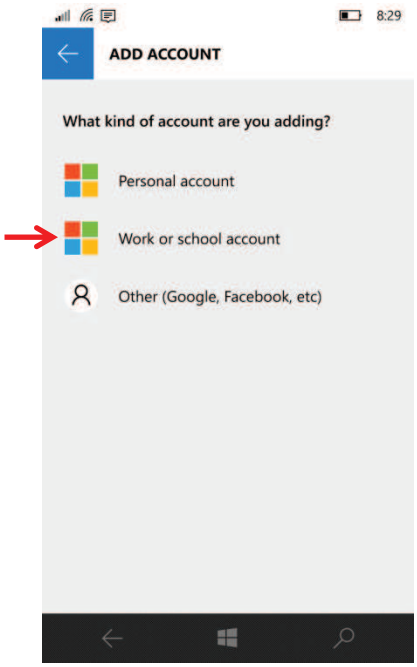
4. Register the app

To register your smartphone app, please click on the tab “Enroll OATH soft token”

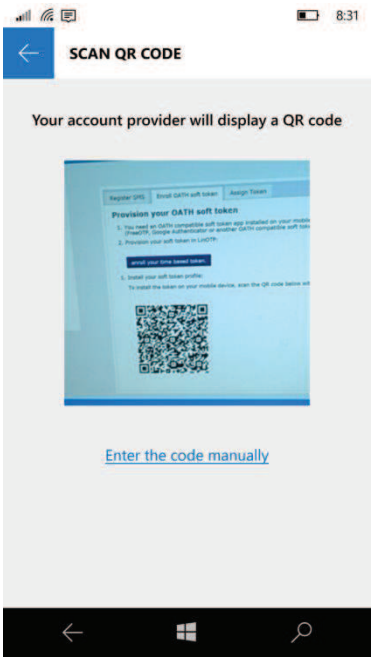


Click on “enroll your time based token”

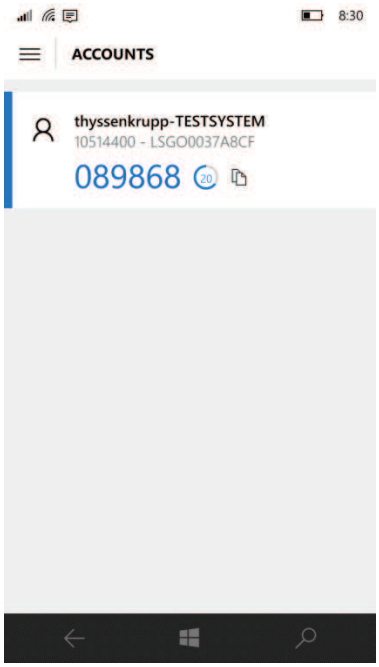
A QR code is shown for you to scan using your smartphone app:



a) Activate “Work or school account”



b) Now scan the QR code



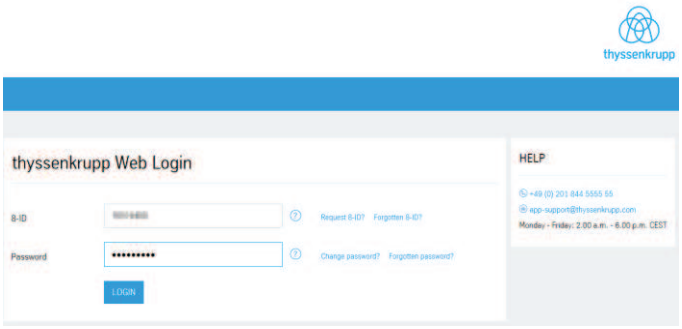
c) A 6 digit One Time Password (OTP) is displayed on your smartphone

5. Proceed with the regular login process

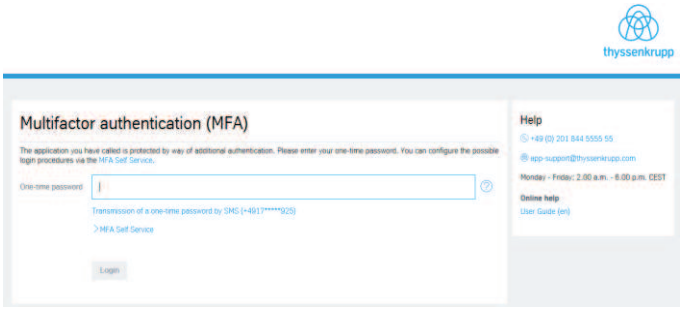
Now you are able to use this token for the regular login process on applications secured by the MFA service. Please be aware that any OTP is valid for 30 seconds only and a new OTP may need to be entered if login fails.

3 Regular login process

1. **Start your browser and open the link to your target application**
2. **The application will present a login page**



Please enter your 8-ID and domain password as usual. The MFA screen is shown, requesting your OTP:



Please use your smartphone app to obtain a valid OTP, enter it into the “Single-use password” field and hit “Login”.

4 MFA Service support

The regular user support of the MFA service is done by the GSS IT Application Support team:

Phone number: +49 (0) 201 844 5555 55
Mailto: app-support@thyssenkrupp.com
Support hours: Monday - Friday: 2.00 a.m. - 6.00 p.m. CEST
(24x7h support planned and is currently in the roll-out phase)
Supported languages: English, German

Getting Started with MFA – Hardware Tokens

Global Shared Services
GSS IT/Global Security Services
Author: Arnd Meysenburg

Version	1.1
Date	July 2017
Information class	public
Contact	Tobias Warth, GSS IT

engineering.tomorrow.together.

thyssenkrupp

Content

1 Introduction

The scope of this document is to provide comprehensive documentation for all current and future users of the thyssenkrupp MFA service. The MFA service is the thyssenkrupp standard multi factor authentication solution significantly enhancing application logon security. The MFA service uses One Time Passwords (OTP) as an additional secret to be provided by the user to authenticate against the application. This approach increases the security with which the application knows the user´s identity.

This document guides you through the initial steps, preparing and then performing your first logon using the MFA service. This guide is specific to hardware tokens. For using other tokens, please refer to the appropriate guide.

1. Login to the MFA self-service portal by using your 8-ID, domain password and an OTP
2. Register your new hardware token with the MFA service

2 Getting Started

Hardware tokens are provided by thyssenkrupp GSS IT for use with the thyssenkrupp MFA Service. To obtain a hardware token for an application, please contact the respective application owner. Often, hardware tokens are provided to users through application rollout projects.

2.1 First time token use

If you have **never used the MFA service** before, automatic enrollment provides a fast and very easy way to start using it:

Please proceed to login to your application as usual and use your hardware token to obtain the One Time Password (OTP) now requested by the application.

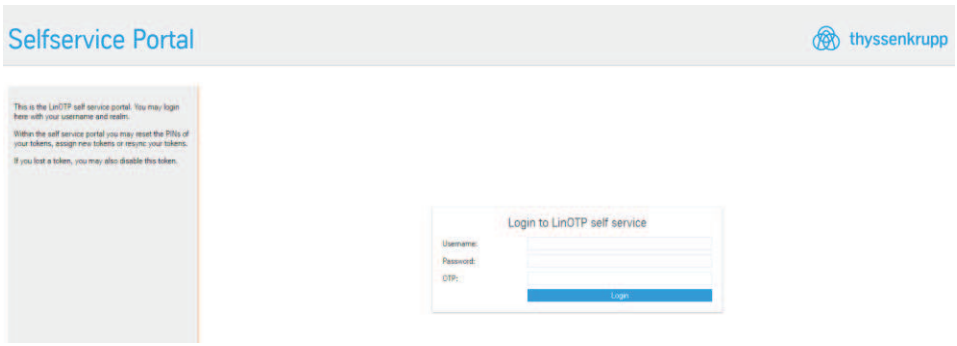
Once login is completed, your hardware token is automatically registered to your 8-ID, no further action is required.

2.2 Register a hardware token

If you have received a hardware token and have already registered your 8-ID for MFA usage, you need to register the new hardware token through the MFA self-service portal as follows:

1. **Please open the MFA self-service portal in your browser**

   Follow this link https://mfa-portal.thyssenkrupp.com to the MFA self-service portal.

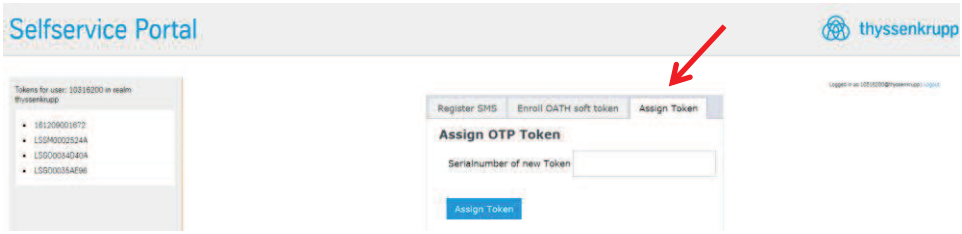


2. **Login to the MFA self-service portal**
   To login to the MFA portal, you need your 8-ID, your password and also an OTP. To obtain your initial OTP:
   - Use your existing token, smartphone app or SMS service
   - OR call GSS IT Application Support under: +49 201 844 555555.

   You must verify your identity to the agent over the phone before the OTP is provided. Please now use your 8-ID, domain password and the provided OTP.

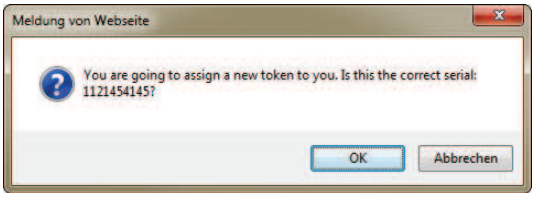
3. Register your new token

To register your hardware token, please click on the tab “Assign Token”.



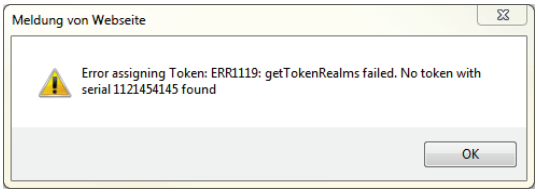
Please enter the serial number printed on the rear of your hardware token. In most cases it is identified by “S/N:” Please only enter the number.

Click on “Assign Token”, a pop-up window is shown, requesting you to validate the entered serial number.



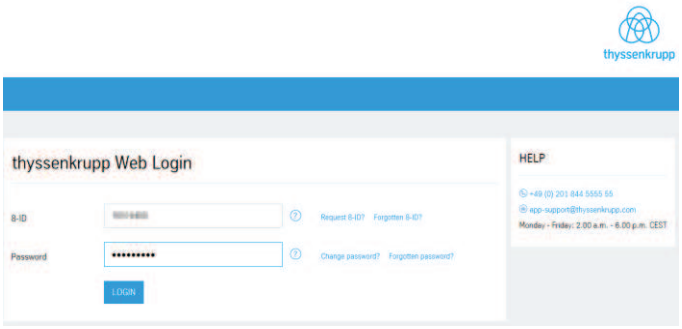
Please verify that you have entered the correct serial number and click OK. On the left side, your connected token will occur showing the serial number of the token.

Note:
If you have entered an invalid serial number, or entered a previously registered serial number, an error message is displayed. In this case, please contact GSS IT Application Support for assistance.

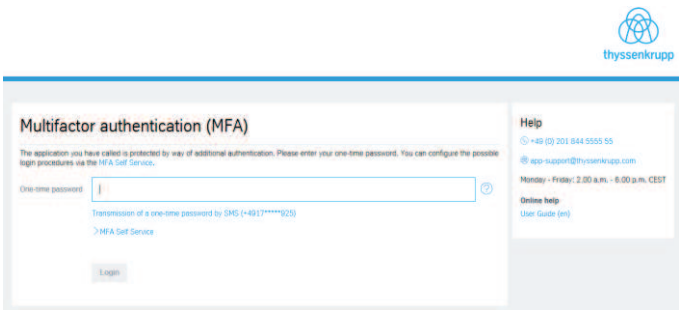


3 Regular login process

1. **Start your browser and open the link to your target application**
2. **The application will present a login page**



Please enter your 8-ID and domain password as usual. The MFA screen is shown, requesting your OTP:



Please use your hardware token (see below for details) to obtain a valid OTP password. Enter it into the “Single-use password” field and hit “Login”.

In general there are three ways to obtain an OTP from a hardware token, this depends on the type of token provided to you:

a) Read your OTP on the display of your token, then enter it
b) Press the button on your token to activate the OTP display, then enter it
c) Select the “Single-use password” field on screen using your mouse, then press the button on your inserted USB token to send an OTP directly to your application

4 MFA Service support

The regular user support of the MFA service is done by the GSS IT Application Support team:

Phone number: +49 (0) 201 844 5555 55
Mailto: app-support@thyssenkrupp.com
Support hours: Monday - Friday: 2.00 a.m. - 6.00 p.m. CEST
(24x7h support planned and is currently in the roll-out phase)
Supported languages: English, German

Getting Started with MFA – SMS Service

Global Shared Services
GSS IT/Global Security Services
Author: Arnd Meysenburg

Version	1.0
Date	July 2017
Information class	public
Contact	Tobias Warth, GSS IT
Associated documents	

Content

1 Introduction

The scope of this document is to provide comprehensive documentation for all current and future users of the thyssenkrupp MFA service. The MFA service is the thyssenkrupp standard multi factor authentication solution significantly enhancing application logon security. The MFA service uses One Time Passwords (OTP) as an additional secret to be provided by the user to authenticate against the application. This approach increases the security with which the application knows the user´s identity.

The preferred and most secure method of MFA assisted logins uses a token to provide OTPs. Only where use of a token is impractical or impossible, SMS may be used to obtain OTP for application logins.

This document guides you through the initial steps, preparing and then performing your first logon using the MFA service. This guide is specific to OTPs provided via SMS. For using personal tokens, please refer to the appropriate guide.

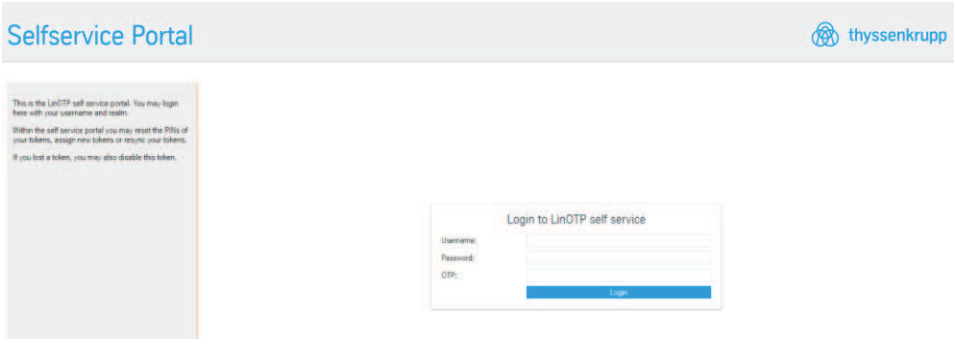
1. Login to the MFA self-service portal by using your 8-ID, domain password and the provided OTP
2. Register a mobile phone number for SMS delivery of your OTPs

2 Getting Started

SMS OTP are provided by thyssenkrupp GSS IT for use with the thyssenkrupp MFA Service. To register a mobile phone for use with an application, please follow this simple registration process:

1. **Please open the MFA self-service portal in your browser**

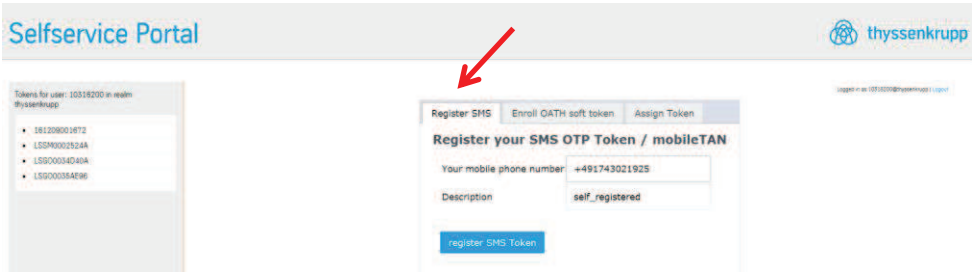
   Follow this link https://mfa-portal.thyssenkrupp.com to the MFA self-service portal.



2. **Login to the MFA self-service portal**
   To login to the MFA portal, you need your 8-ID, your password and also an OTP. To obtain your initial OTP:
   - Use your existing hardware token or smartphone app
   - OR call GSS IT Application Support under: +49 201 844 555555.

   You must verify your identity to the agent over the phone before the OTP is provided. Please now use your 8-ID, domain password and the provided OTP.

3. **Register your mobile phone number**
   To register your mobile number, please click on the tab “Register SMS”. If you have already registered a phone number for OTP via SMS or a number has been automatically imported from the central tk directory, please verify this number shall be used, or enter the number you wish to use for OTP via SMS.



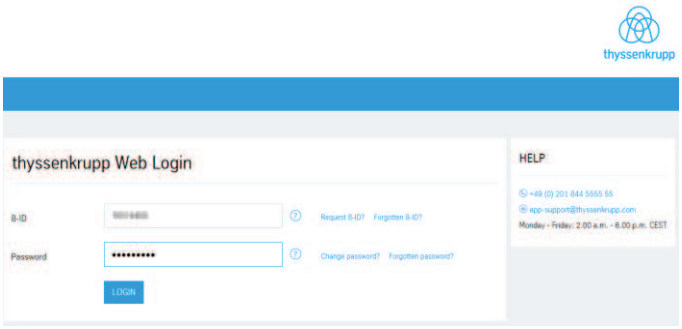
   Please also ensure that the mobile phone number is recorded in the following format, without brackets, spaces or leading zeroes:

   (e.g.) +49172123456

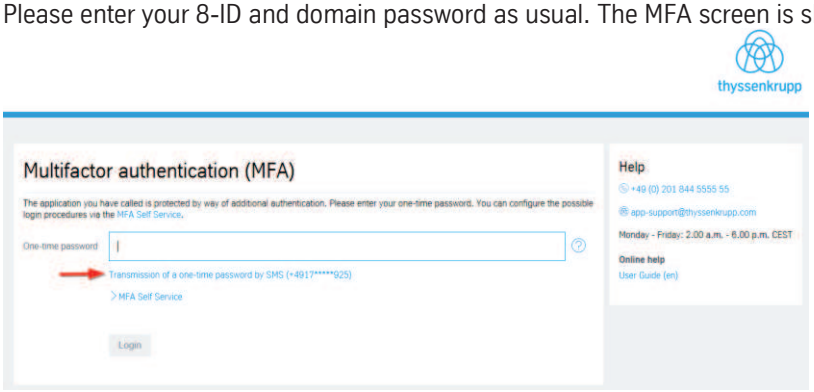
   Please do not change the information in the “Description” field and click on “register SMS Token” to complete the registration process.

3 Regular login process

1. **Start your browser and open the link to your target application**
2. **The application will present a login page**



Please enter your 8-ID and domain password as usual. The MFA screen is shown, requesting your OTP:



To trigger OTP delivery via SMS, please click on “Transmission of a one-time password by SMS[…]”, wait for the OTP to be delivered to your phone and enter it into the “One-time password” field.
Hit “Login”.

4 MFA Service support

The regular user support of the MFA service is done by the GSS IT Application Support team:

Phone number: +49 (0) 201 844 5555 55
Mailto: app-support@thyssenkrupp.com
Support hours: Monday - Friday: 2.00 a.m. - 6.00 p.m. CEST
(24x7h support planned and is currently in the roll-out phase)
Supported languages: English, German