Login and Access Management

GSEP User Knowledge Base

Exported on 06/22/2023

Table of Contents

Our R&D application manage their access rights in ZULA. This allows automatic setup and user management, including management approval, for most of the GSEP tools.

> ⚠ GSEP and ZULA are different applications, operated by different teams.
> More information regarding ZULA can be found here: https://zulaplus.e.corpintra.net/ZulaPlus/faces/pages/template/zula-home.xhtml
> Below pages are only tips and tricks how to work with ZULA from a GSEP perspective.

1 How to Login in GSEP

Try this if you have no time for reading

To login to GSEP, please use the same username as before. For JIRA and Confluence, use your Single-Sign-On Mercedes-Benz password. Follow the instructions.
If your account name starts with "S1" (some old ones start with "x"), please do a one-time login to https://supplier-portal.daimler.com/ with your Single-Sign-On Mercedes-Benz password.
If you do not know the password, reset the password there or with help from Supplier portal hotline:
07111795120 or +0080071170372

1.1 Table of Contents

1.2 Account types

Mercedes-Benz has several systems aiming at different user types. For GSEP, these user types are relevant:

- Internal Accounts: Given to users who have access to the intranet, e.g. Mercedes-Benz employees, Externals ("Extaccount" Users), Technical Users. The accounts are managed by Mercedes-Benz employees.

- Supplier Accounts: Given to users who connect applications from the intranet only. These accounts start with "x" or "S1". They are managed by the external company in the supplier portal[1]

On this page, you will find more information about these account types and how to use them to login to GSEP.

EMT or Supplier Portal User

For Non- Mercedes-Benz users, there are two ways to provide accounts to then:

- Supplier portal: The external company creates their own accounts and is able to set the email address to the companies mailbox and reset passwords.
- EMT: A Mercedes-Benz employee can create this accounts, but it is not possible to enter primary email addresses which are outside the extaccount.com domain.

GSEP will send "protected/encrypted" emails from all tools. They cannot be forwarded to an non-Mercedes-Benz mail domain. With an account created in EMT, you can only read them in a full Outlook installation within Mercedes-Benz (not in Outlook Web Access "OWA"). With an account from supplier portal, the Daimler securemail solution(see page 90) will ensure you can receive and read these mails.
We stronly suggest for non- Mercedes-Benz user, to create their accounts in the Supplier portal. This must be done by the manager of the external company.

1.3 Login with Single-Sign-On or with GSEP password

1.3.1 Overview and quick check

60% of GSEP users use only Confluence and JIRA: Since May 2021, they do no longer need a separate GSEP password

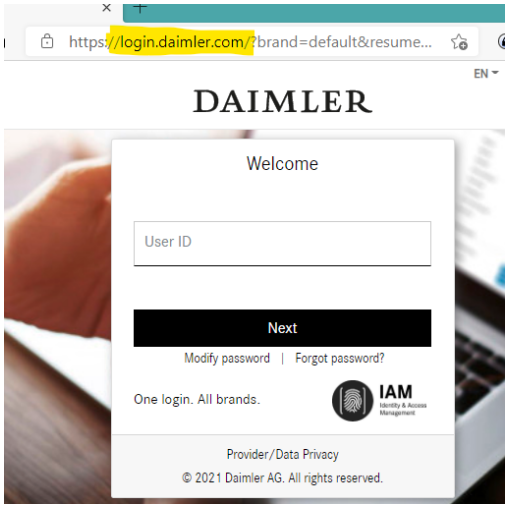
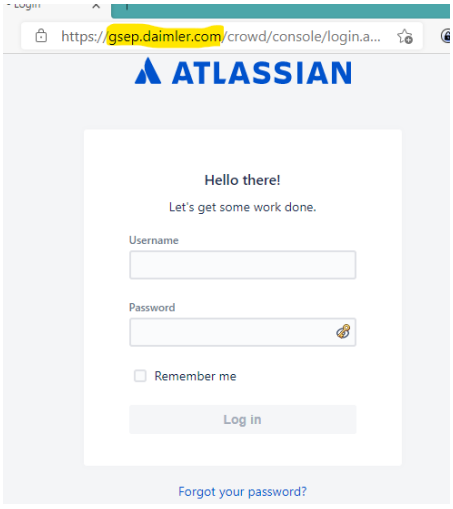
- **JIRA and Confluence** use the Mercedes-Benz **Single-Sign-On** Mercedes-Benz password with MFA
- **All other GSEP applications** (including JSD "Jira Service Desk") still use the additional GSEP password
- To access GSEP from Internet, you still need to install the GSEP certificate[2] in your browser

If you do not know your Single-Sign-On password, you will find more info below.

1.3.1.1 When to use the Single-Sign-On password or the GSEP password?

You can easily see which password is required by checking the URL during login:

1 https://supplier-portal.daimler.com/
2 https://gsep.daimler.com/confluence/x/h4tQEQ

Single-Sign-On	GSEP password
https://**login.**mercedes-benz.com 	https://**gsep.**daimler.com 

If you do not know your Single-Sign-On password, you will find more info below.

1.3.1.2 Final Test

Please check the applications you normally use:

- Can you login to Confluence: https://gsep.daimler.com/confluence/ (Single-Sign-On)
- Can you login to JIRA: https://gsep.daimler.com/jira/ (Single-Sign-On)
- Can you Login to GSEP https://gsep.daimler.com/crowd/console/user/viewprofile.action (GSEP password)

If you do not see errors, you can continue to work. With errors, we will now check your setup in smaller steps.

Note: The login to GSEP INT or STAGE might require to re-register your MFA device! This is not an error, please follow the instructions again.

1.3.2 Error handling

1.3.2.1 Do you know your Single-Sign-On password?

The Single-Sign-On password is also known as WIW or CD password:

- It is different from your Windows, AD or Outlook-Password.
- It is **not the password you got from GSEP.**

If you passed the final test above, you already know your Single-Sign-On password. If not, you can now check and reset the password.

Which type of account do you have?

Internal Account	Supplier Account
• Account name similar to user name: ABELEBR = Bruno Abele • Created by Mercedes-Benz employees in EMT: https://iam-tools.iam.corpintra.net/emt/ • Used by Mercedes-Benz employees and externals (with access to Mercedes-Benz Intranet or GEW)	• Account name starts with "x" or "S1": **x**ABCDE, **S1**abcde • Created by the supplier's manager in Supplier Portal: https://supplier-portal.daimler.com • Only used by externals (without access to Mercedes-Benz intranet)

Try to login at Mercedes-Benz; then reset the password

Internal Account	Supplier Account
Open page and login: https://login.mercedes-benz.com/ • If not successful: Use "Forgot Password?" to reset the password • On problems, contact your local User Help Desk (+49 7031 89000 for R&D Sindelfingen) • Retry This password is your Single-Sign-On Mercedes-Benz password	Open page and login: https://supplier-portal.daimler.com • If not successful: Use "Forgot Password?" to reset the password • On problems, contact the Supplier Portal support, ask for a password reset: +49 711 17 95120 or Support.Supplier-Portal@daimler.com[3] • Use the one-time passwort to login to Supplier Portal and set your new password • Retry This password is your Single-Sign-On Mercedes-Benz password

The GSEP support will not be able to help you with this, please contact only the listed help desks!

Login with MFA and register your device

For security, the login to GSEP requires a 2nd mean authentication. OIDC / PingID is the standard Mercedes-Benz technology.

Internal Account	Supplier Account
Online Guide and more details: https://login.mercedes-benz.com/password/mfa Open link to test your MFA login: https://login.mercedes-benz.com/password/mfa-settings • First time login: Follow the instructions to register a device for MFA. • If you are successful, please go back and try to login to GSEP	

3 mailto:Support.Supplier-Portal@daimler.com

Internal Account	Supplier Account
If not successful: • Contact MFA Helpdesk: +49 711 17-25005 or cuhd_support_MFA-PingID@mercedes-benz.com[4] • General Information[5] on the MFA Sharepoint	If not successful: • Contact Supplier Portal Support and ask for a PingID reset: +49 711 17 95120 or Support.Supplier-Portal@daimler.com[6] • Now click the test link again and add a new MFA device • More information on Daimler Supplier Portal (en)[7]

Note: GSEP INT and STAGE require a separate registration on https://login-int.mercedes-benz.com/password/mfa-settings

The GSEP support will not be able to help you with this, please contact only the listed help desks!

If there are still problems

If the login with MFA is successful, but you still have problems accessing GSEP, please contact GSEP Support[8] and create a web ticket.

1.3.3 Detail information about the Single-Sign-On and MFA introduction

There are NO changes in users, roles and certificates - same user name, same certificates, same roles: There is also NO change when accessing the REST API.
Please use the same account name for GSEP as before.

1.3.3.1 Why MFA and Single-Sign-On?

Multi Factor Authentication: To access Mercedes-Benz data on confidential systems, it is no longer sufficient to know a user name and passwort. A second factor must be used which must not be based on knowledge alone. The 2nd factor can be an app that is bound to your mobile phone or a YubiKey, which is not available to hackers.

Single-Sign-On allows you to use the same username and password everywhere, and maybe only login once per day - as long as you do not close your browser, you do not have to enter your passwort again on other enabled websites of the same company the whole day.

Both technologies are used at Mercedes-Benz and are configured outside of GSEP. Due to this, GSEP support is not able to help you with this functionality. Please contact the listed help desks.

1.3.3.2 Best practice on MFA devices

You should register 2 or more devices with MFA, to be able to login even if you forget or loose one device:

- Mobile phone: Use the PingID app from your app store

4 mailto:cuhd_support_MFA-PingID@mercedes-benz.com
5 https://team.sp.wp.corpintra.net/sites/05389/GAS-MFA/SitePages/General%20Information.aspx
6 mailto:Support.Supplier-Portal@daimler.com
7 https://supplier-portal.daimler.com/docs/DOC-2171
8 https://gsep.daimler.com/confluence/x/tCdKI

- Laptop/PC: Mercedes-Benz employees can use the preinstalled PingID application or download it from the PingID website
- Independent authenticator app like Google Authenticator oder Microsoft Authenticator on your phone or laptop/PC
- YubiKey

Check https://www.pingidentity.com/en/resources/downloads/pingid.html for download links.

Check IAM Services Sharepoint[9] in the Mercedes-Benz Intranet for more details.

On GEW, it is not possible to install the apps or to connect a YubiKey, but you can install it on your personal PC at your workplace (also outside Mercedes-Benz) or even on your private mobile phone.

> Tipp: Security Keys for Ping.ID are now also available through IT-Shop:
>
> - Solokey SOMU für USB-A: QEV111AI64QD
> - Yubico YubiKey5C Nano: QEV111AI64LK
>
> They also work perfectly on Windows and Mac (not only Ubuntu)

1.3.3.3 Supplier accounts

Some users have problems, especially if they are used to login with the Supplier Account and the GSEP password, without login to Supplier portal till now.

- Please use the same account name for GSEP as before. All your access rights are linked to this account. You only have to use a different password during login.
- Follow the steps listed above to ensure you can login to the supplier portal

In addition, you should check your settings in the supplier portal

- You and your manager are able to reset your Single-Sign-On passwort and change the email adress that is used for your password reset

1.3.3.4 Administration backend access in GSEP

When you want to access the administration backend of Jira and Confluence (Web Sudo) you will be asked for another password.
Please enter your **GSEP passwort** here.

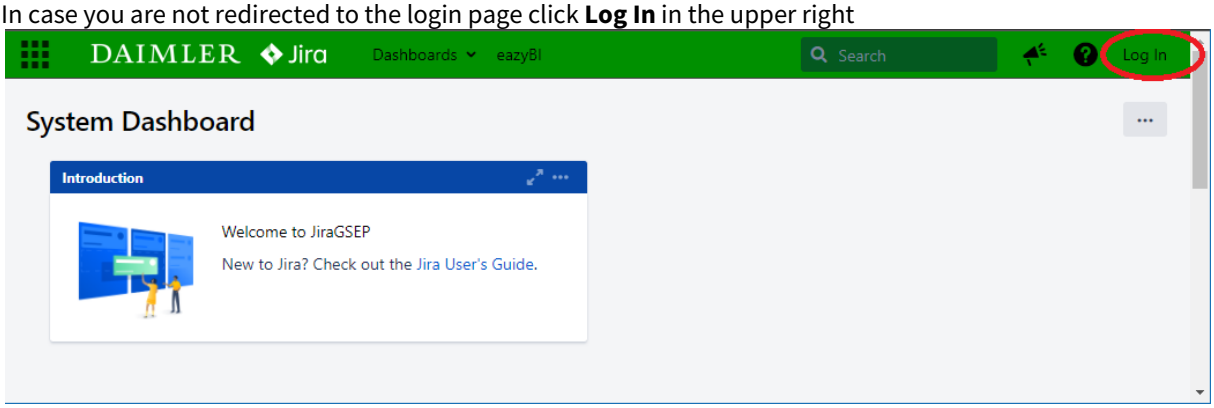
1.4 The GSEP Landing Page

Use https://gsep.daimler.com/ for easy login in the browser:

9 https://team.sp.wp.corpintra.net/sites/05389/GAS-MFA/SitePages/General%20Information.aspx

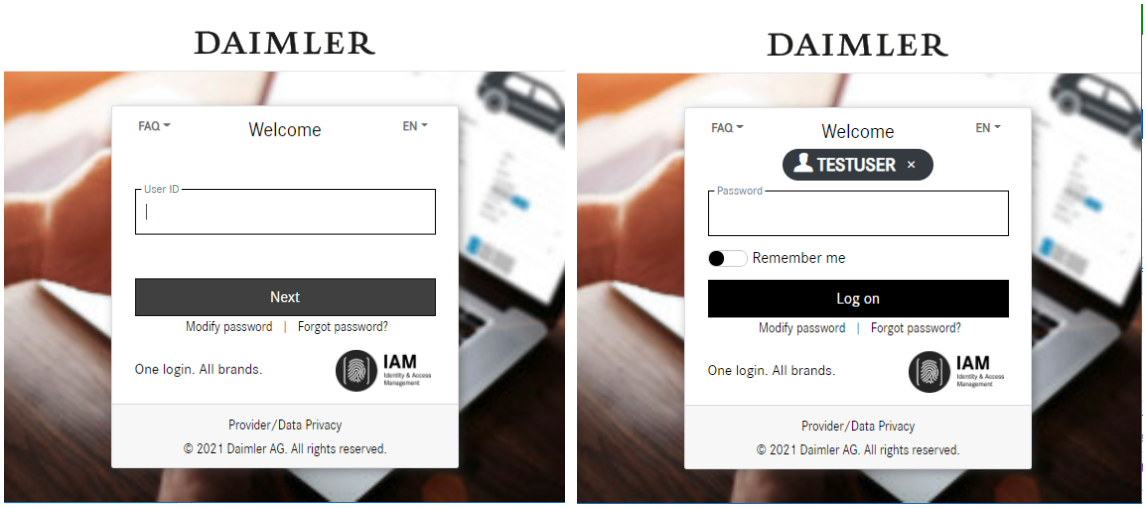
1. Open Jira[10]or Confluence[11] via direct link or via our GSEP landing page[12] (Production Environment)
   Open Jira[13]or Confluence[14] via direkt link or via our GSEP landing page[15] (Integration Environment)

2. In case you are not redirected to the login page click **Log In** in the upper right

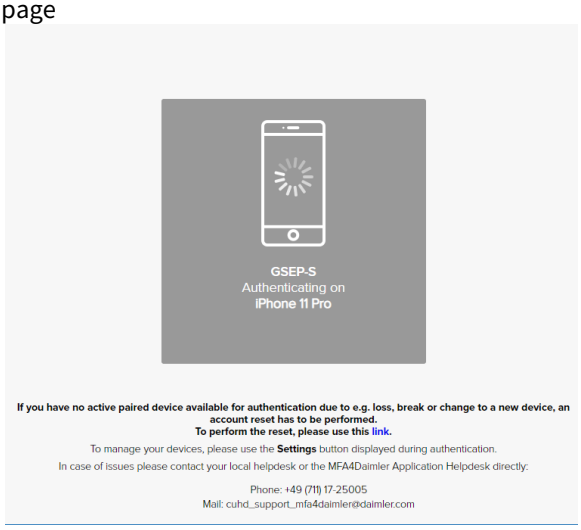


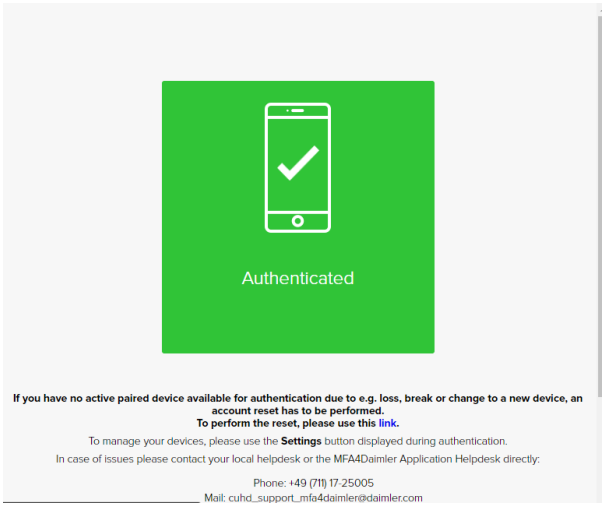
3. Please enter your **Mercedes-Benz username and password** (not the GSEP credentials) on the login page that opens automatically (https://login.mercedes-benz.com)

10 https://gsep.daimler.com/jira/login.jsp?os_destination=%2Fdefault.jsp
11 https://gsep.daimler.com/confluence/
12 https://gsep.daimler.com
13 https://gsep-int.daimler.com/jira/login.jsp?os_destination=%2Fdefault.jsp
14 https://gsep-int.daimler.com/confluence
15 https://gsep-int.daimler.com



4. Please authenticate with your second factor (PingID app on mobile or application on desktop) on the next page





5. Enjoy!

1.5 How do I authenticate in Jira and Confluence via the REST API?

1.5.1 Using Personal Access Tokens (PATs) in Jira and Confluence

> We have introduced Personal Access Tokens in Jira in July 2021 with the upgrade to Jira 8.16. These tokens are specific to GSEP and different from the access tokens from the OIDC integration guide[16] (Intranet only)!

Personal access tokens (PATs) are a secure way to use scripts and integrate external applications with your Atlassian application for personal accounts. If an external system is compromised, you simply revoke the token instead of changing the password and consequently changing it in all scripts and integrations.

For TE Account please resort to using Basic Authentication (see page 15)as this account type is not allowed to authenticate in the front end due to security policies.

1.5.1.1 How to create your Personal Access Token?

Creating Personal Access Tokens

1. Login to Jira[17]or Confluence[18]
   a. In **Jira**, select your profile picture at the top right of the screen, then choose **Personal Access Tokens**
   b. In **Confluence**, select your profile picture at top right of the screen, then choose **Settings** > Personal Access Tokens[19]
2. Select **Create token**.
3. Give your new token a descriptive name.
4. Permission level of personal access tokens is set to the level of access you currently have.
5. Optionally, for security reasons, you can set your token to automatically expire after a set number of days.
6. Click **Create** Your personal access token is created. Copy the token and store it in a safe space such as your password vault solution. You won't be able to see the token again in the web interface.

Please find additional information in the Atlassian documentation[20].

1.5.1.2 How to revoke your Personal Access Token?

If for any reason, for instance, security breach, you need to revoke your token, you can do it quickly from your Atlassian application:

Revoking Personal Access Tokens

1. In your Atlassian application go to:
   a. In **Jira** select your profile picture at the top right of the screen, then choose **Personal Access Tokens**
   b. In **Confluence**, select your profile picture at top right of the screen, then choose **Settings** > **Personal Access Tokens**
2. Select **Revoke** next to the token you want to delete.
3. Confirm your choice.
4. Your token is now revoked and can't be used for further authentication.

16 https://pages.git.daimler.com/IAM/GAS-OIDC-Integration_Guide/docs/guide/technical_authn/
17 https://gsep.daimler.com/jira/login.jsp?os_destination=%2Fdefault.jsp
18 https://gsep-stage.daimler.com/confluence/
19 https://gsep-stage.daimler.com/confluence/plugins/personalaccesstokens/usertokens.action
20 https://confluence.atlassian.com/enterprise/using-personal-access-tokens-1026032365.html

1.5.1.3 How to use Personal Access Token to authenticate with the Jira or Confluence REST API

To use a personal access token for authentication, you have to pass it as a bearer token in the Authorization header of a REST API call.

Here's an example using cURL to call the REST API with a bearer token:

```
curl -H "Authorization: Bearer <yourToken>" https://gsep.daimler.com/rest/api/content
```

1.5.2 Using Basic Authentication for accessing the Jira and Confluence REST API

You can use Basic Authentication for the REST API with your Crowd credentials both for personal and TE accounts.

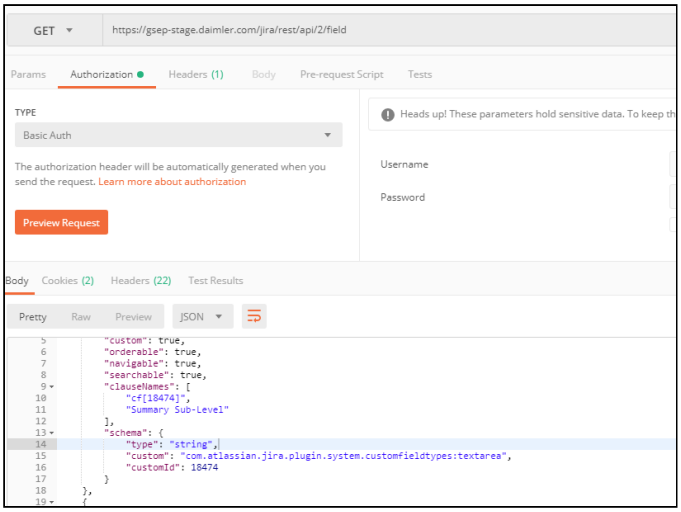
1.5.2.1 CURL Example

```
curl https://username:password@gsep.daimler.com/jira/rest/api/2/project
```

1.5.2.2 Postman[21] Example

Let's consider an example: To get all the fields in JIRA we will be using the API "https://gsep-stage.daimler.com/jira/rest/api/2/field"

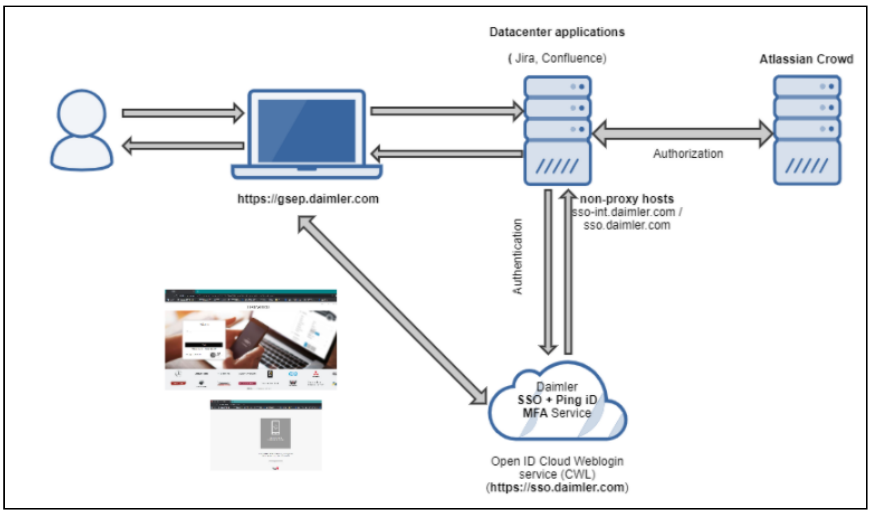
Authorization : Basic Auth - Enter The username and Password



21 https://www.postman.com/

1.6 Technical Background of the OIDC architecture in JIRA

Architecture of OIDC in JIRA



2 ALM Certificate

2.1 GSEP - Certificate Installation Guide for MAC

2.1.1 Preconditions

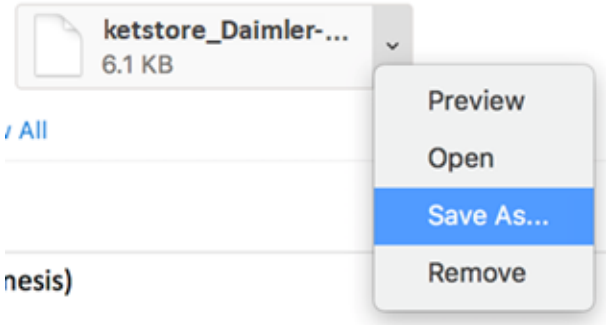
User require common ALM user-based certificate in order to access GSEP tools.

Way of Solution

Users can use the same Windows side certificate on MacBook as well to access GSEP Environment. You can just open the encrypted email contained certificate sent initially to access GSEP system and import the same on your MacBook.

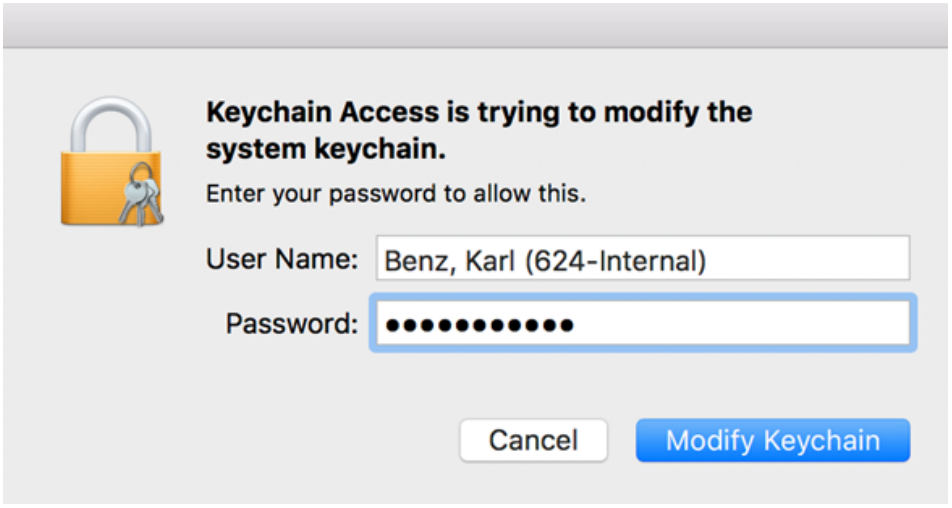
Steps to install GSEP Certificate in MAC

Step 1: Save the .pfx certificate to your desktop

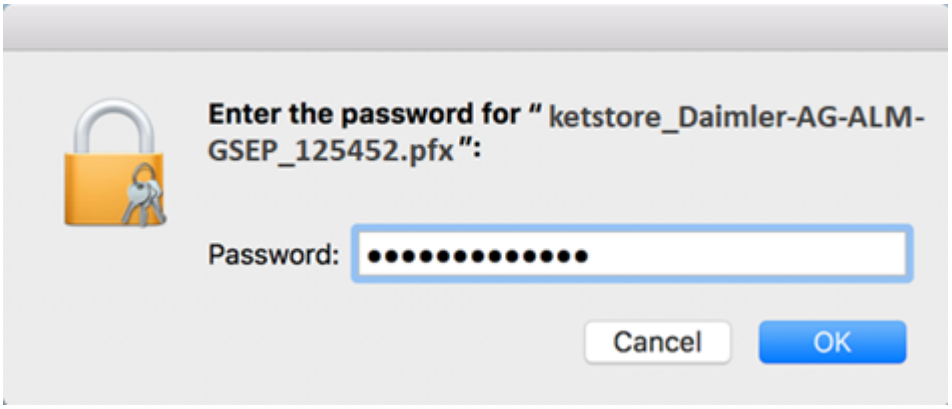


Step 2: Double-click on the certificate to open it

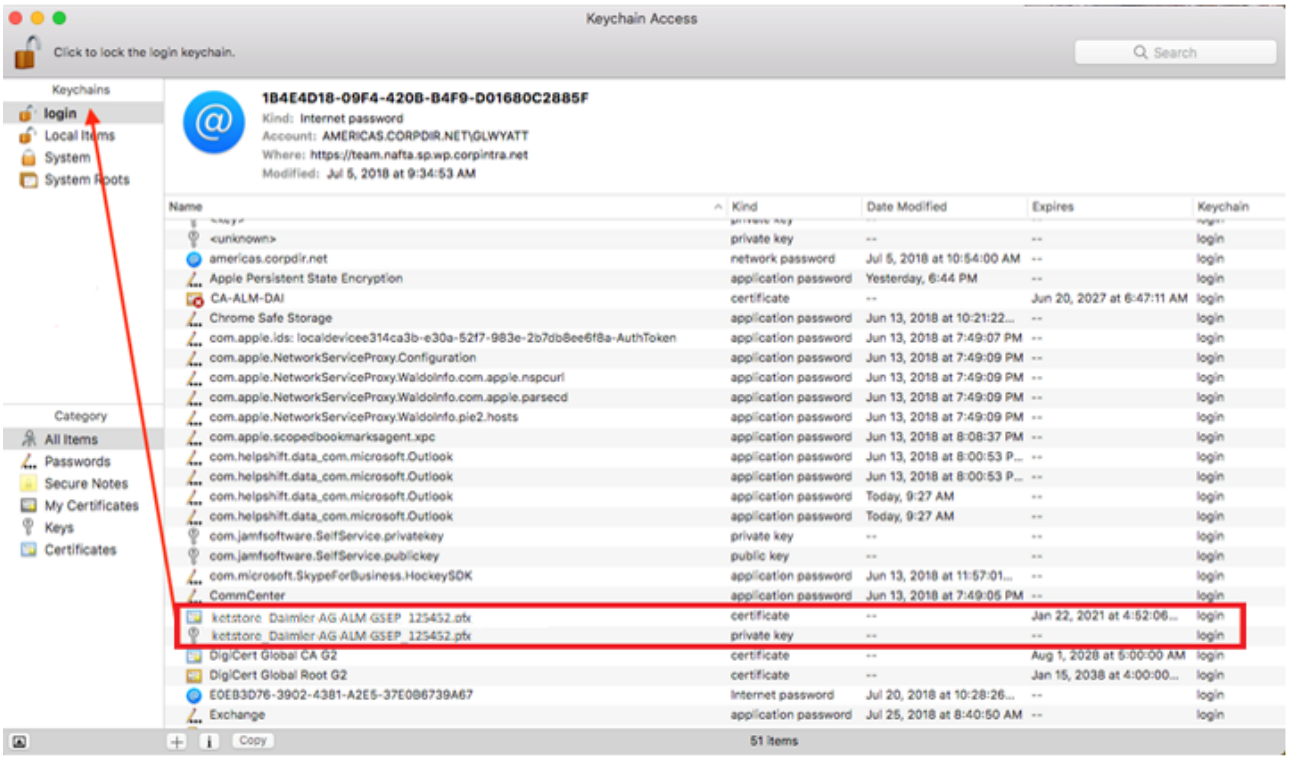
Step 3: Enter your computer password



Step 4: Enter the secret password that was sent in the encrypted email



Step 5: Drag the certificate and private key to the login keychain



Note: While installing the certificate if you got this popup then need to switch from "lokale Objekte" to "System". Then only it is possible to install the certificate.

Now open up gsep.daimler.com[22] in either the Chrome or Safari browser

22 http://gsep.daimler.com

2.2 How to prevent certificate pop-up when entering GSEP page

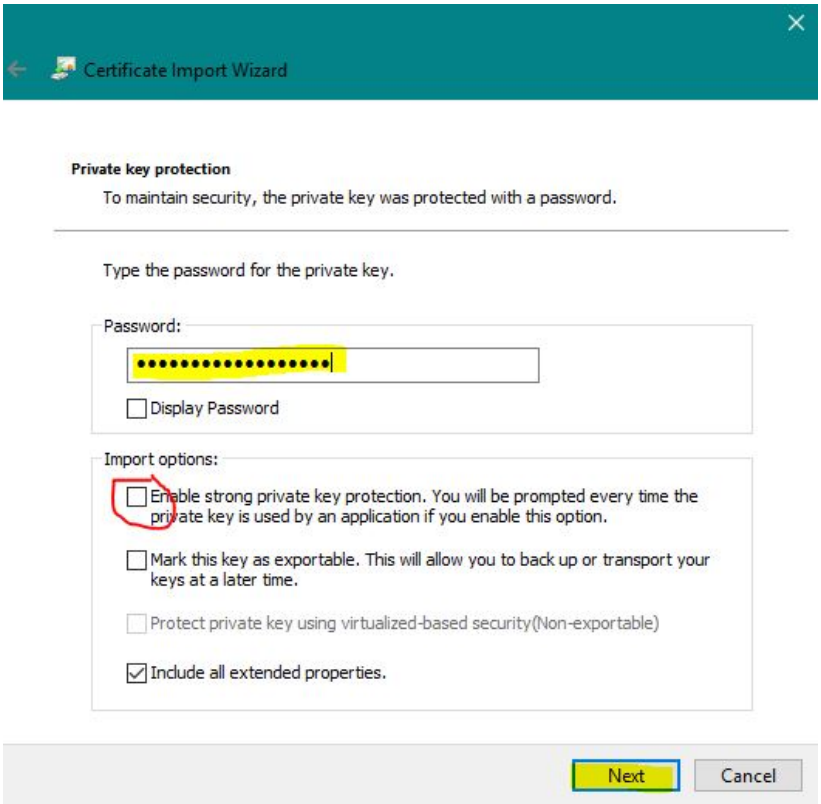
Problem: When entering the GSEP page (gsep.daimler.com[23]), the user is asked to confirm a pop-up wether it's allowed to use the certificate or not.

Solution: In order to avoid that, you have to **reinstall** the **certificate** slightly different to the User Guide that came with the registration E-Mail.

There's **no need to delete the certificate before**, if you already installed it. The process may differ depending on your operating system. Tested with Windows 10 Enterprise and Internet Explorer.

Step 1) Save the client certificate provided in the encrypted mail you got at the registration process. Title of the E-Mail should be something like "Common ALM User-Based Certificate & Password".

Step 2) Double click on the saved client certificate and click "Next" until you reach that point:



Step 3) Copy the password provided in the registration E-Mail and make sure that **"strong key protection"** is **UNchecked.**

Step 4) Click "Next", "Finish" and "Ok".

Now you should not have the pop-up when entering gsep.daimler.com[24].

23 http://gsep.daimler.com
24 http://gsep.daimler.com

2.3 How to retrieve my GSEP ALM Certificate?

From Daimler intranet:

- Go to our self service portal: https://gsep.app.corpintra.net/helpdesk/faces/portlets/SelfCertificate.xhtml
- Select the certificates you need and have them sent again to your mailbox.
- More Info: Self Service → Guide to download a Certificate to access GSEP Platform[25]

> Please check you trash and junk mail folders if you did not get the email within 10 minutes (expected: < 2 minutes). GSEP support gets a lot of tickets where the email was delivered, but deleted.
>
> - Sender: NoReply-GSEP-Pool-ID@daimler.com[26]
> - Subject: Welcome you onboard as a new member of the GSEP platform/ Willkommen an Board als neues Mitglied der GSEP Plattform

From Internet or if this is not possible, e.g. as supplier:

- please create a webticket at GSEP support to get your certificate: GSEP - How to get help[27]

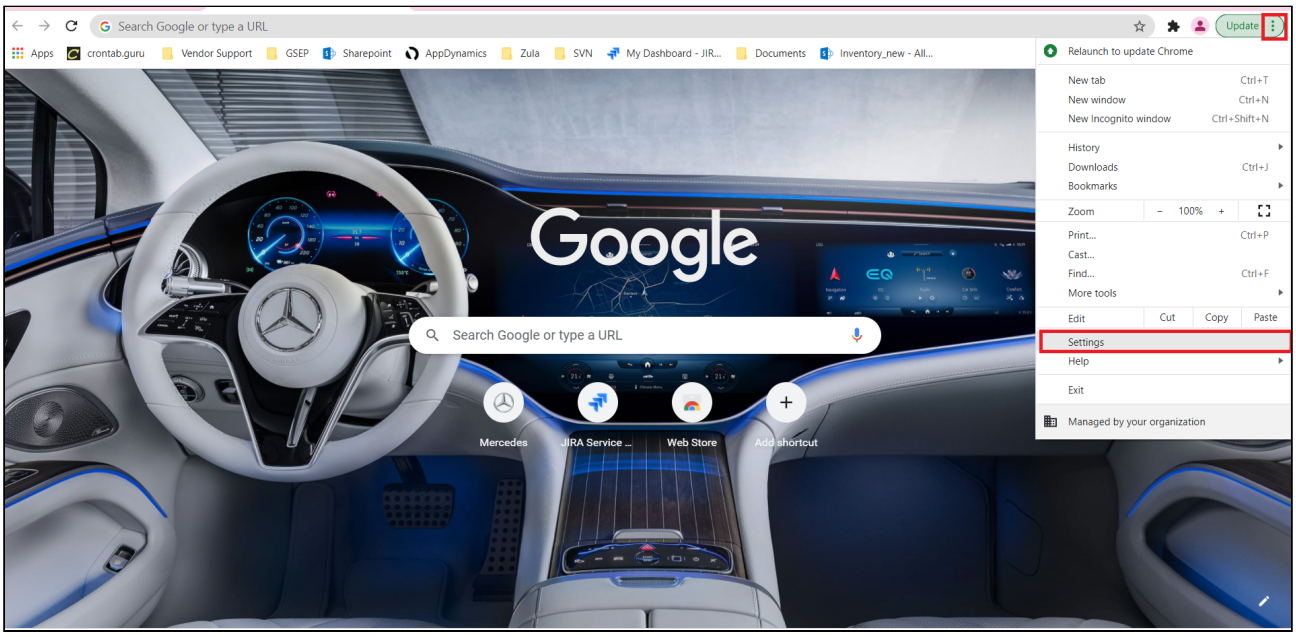
2.4 How to uninstall the GSEP certificate from a browser (Chrome, IE, Firefox and Edge)

> This guide will help you remove the GSEP certificate you have installed on your system. Please follow the relevant steps for your browser.

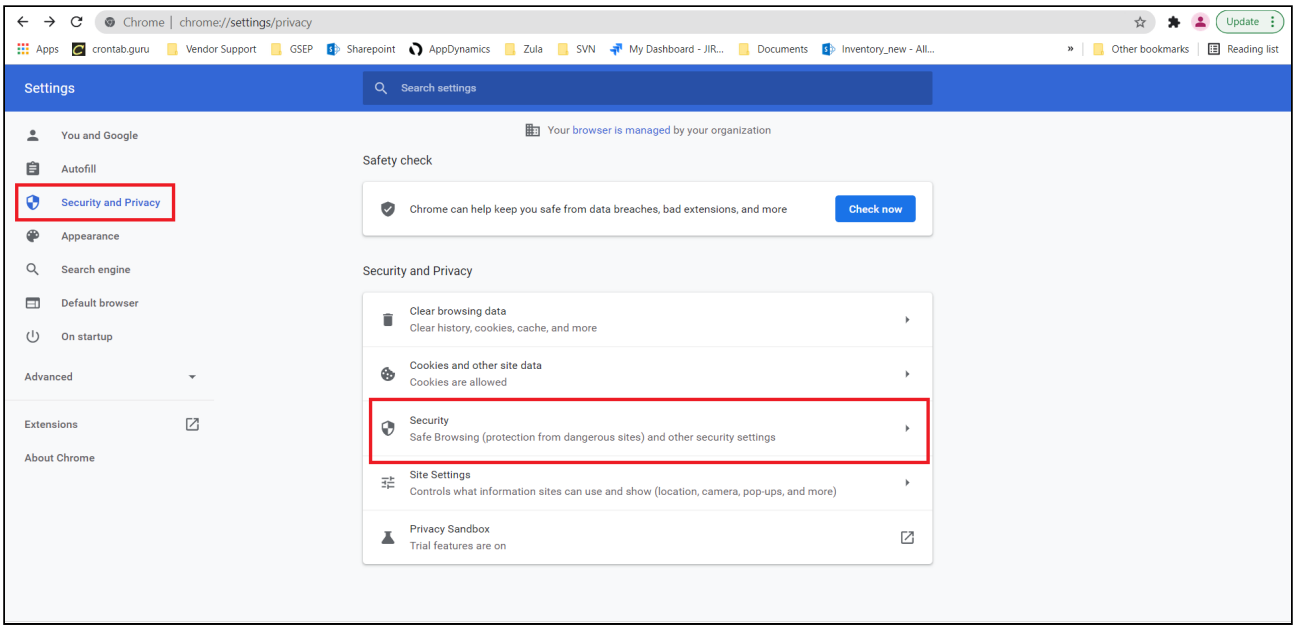
2.4.1 **Chrome:**

- Open the **Chrome** browser and click on the three dots **(...)** at the top right corner as shown below, and click on **Settings.**

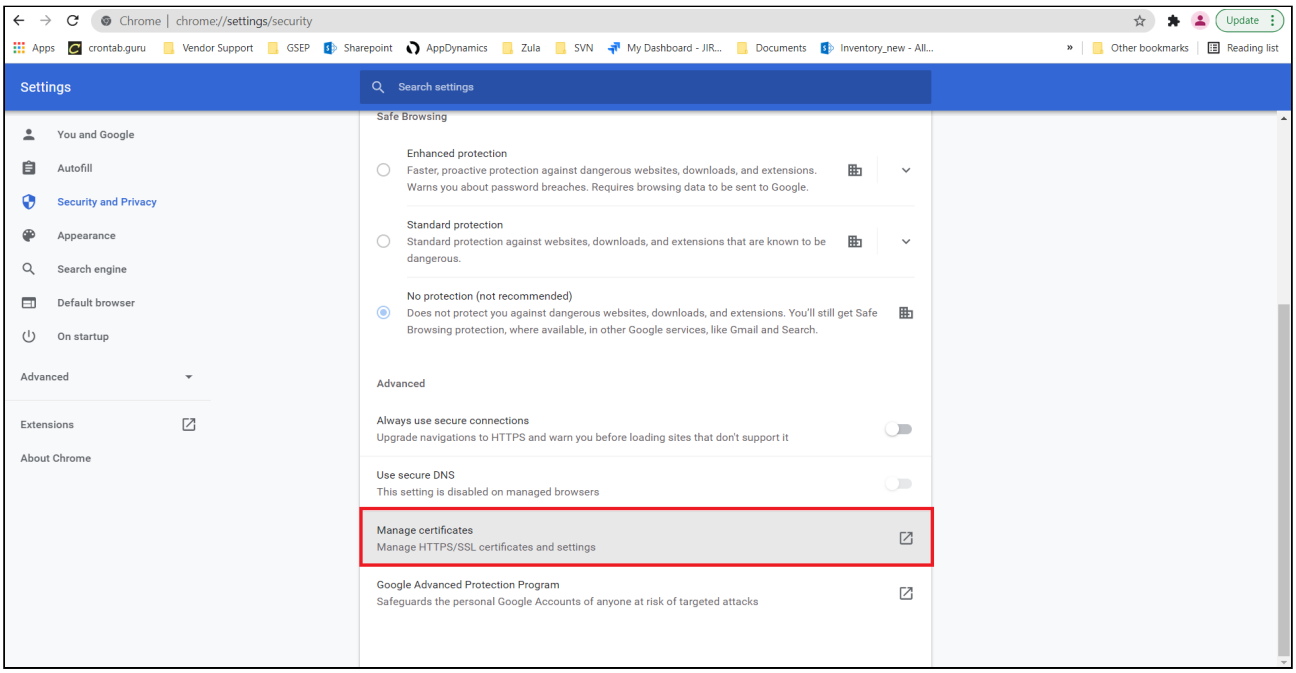
25 https://team.sp.wp.corpintra.net/sites/03009/_layouts/15/WopiFrame.aspx?sourcedoc=/sites/03009/General%20Information/User%20Guide/GSEP%20-%20Guide%20to%20download%20a%20Certificate%20to%20access%20GSEP%20Platform.docx&action=default
26 mailto:NoReply-GSEP-Pool-ID@daimler.com
27 https://gsep-int.daimler.com/confluence/display/GSEPUKB/GSEP+-+How+to+get+help



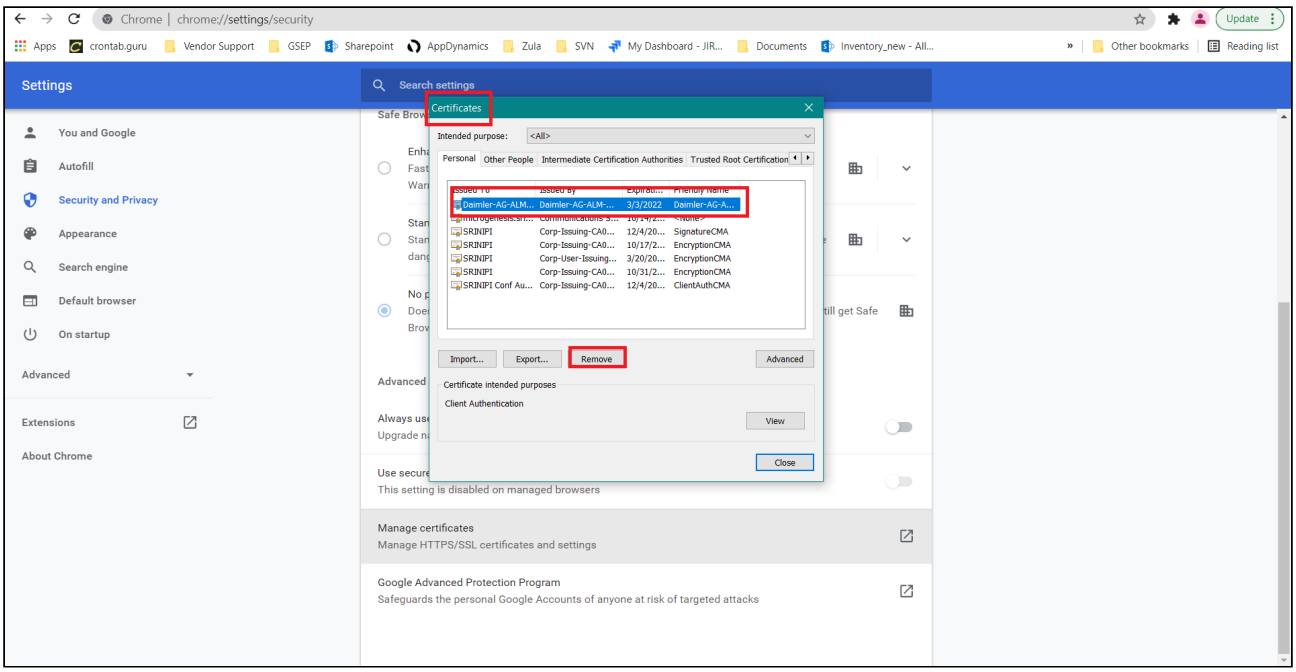
- Click on **Security and Privacy>Security :**



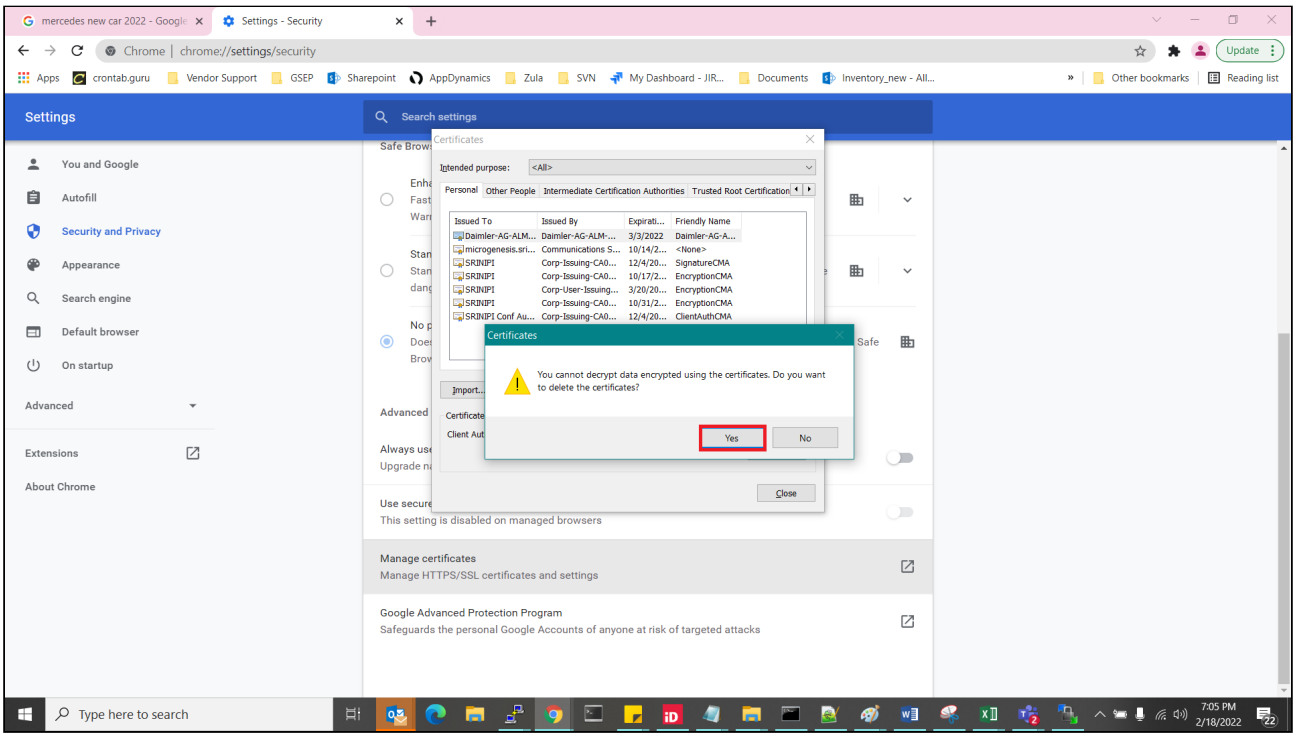
- Choose the option **Security > Manage certificates:**



- Select the GSEP Certificate on the **Certificates** screen and click on **Remove.**

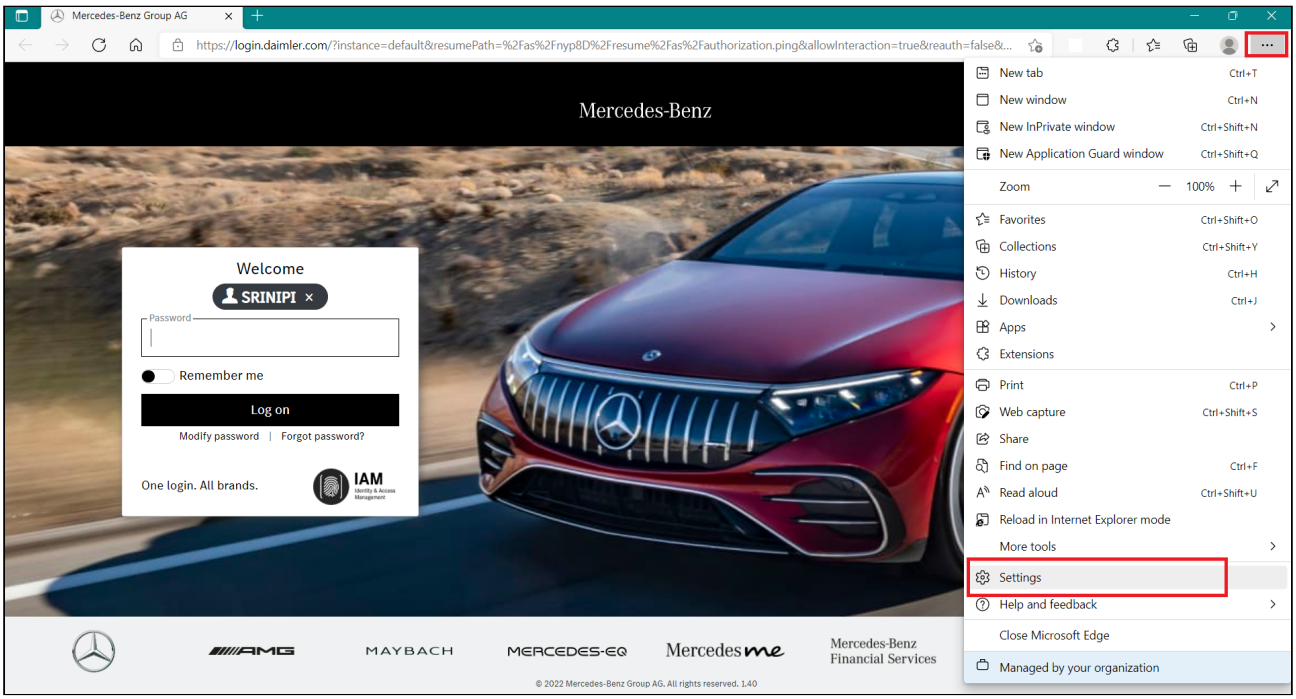


- You will get a Certificate alert popup and click on **Yes** to remove the selected certificate**:**

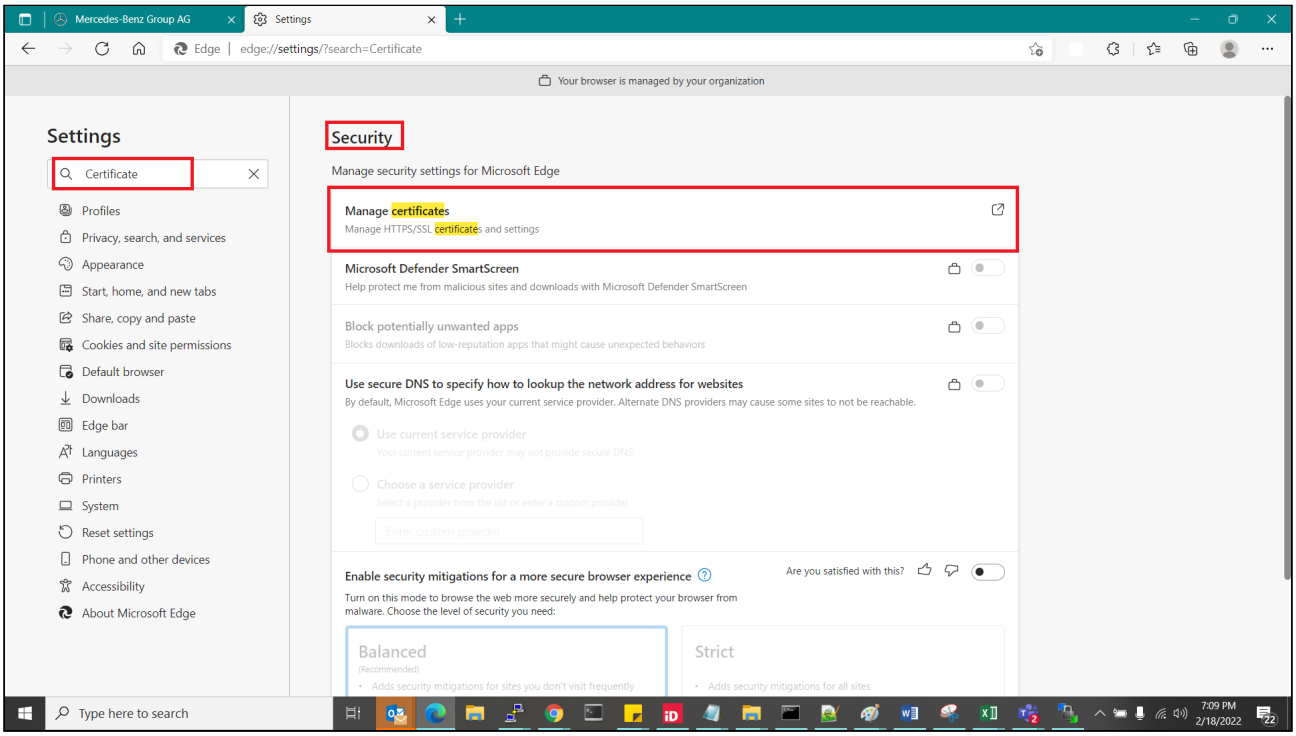


2.4.2 Internet Explorer and Edge:

- Open **Internet Explorer** and click on the three dots **(...)** at the top right corner as shown below, and click on **Settings:**



- Please search for **Security** or **Certificate,** click on **Manage Certificates** to see the below screen.

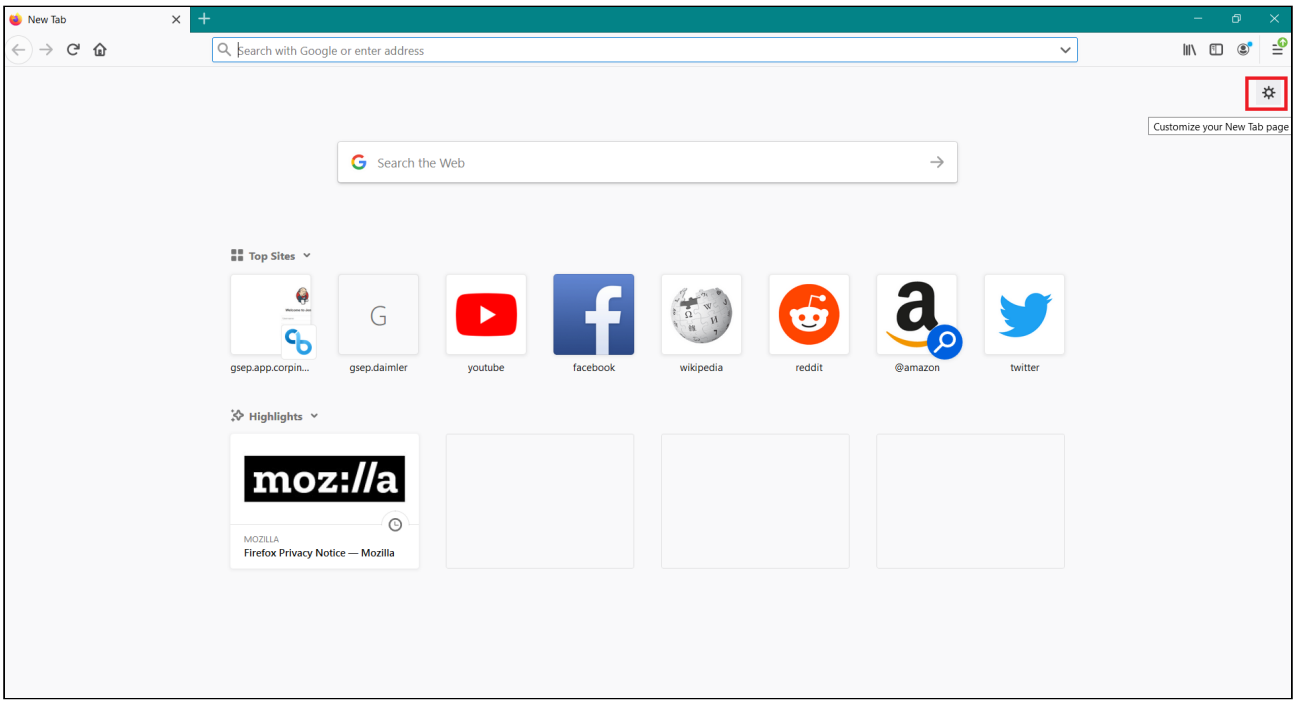


⚠ Please repeat the Chrome Browser steps 4 and 5:

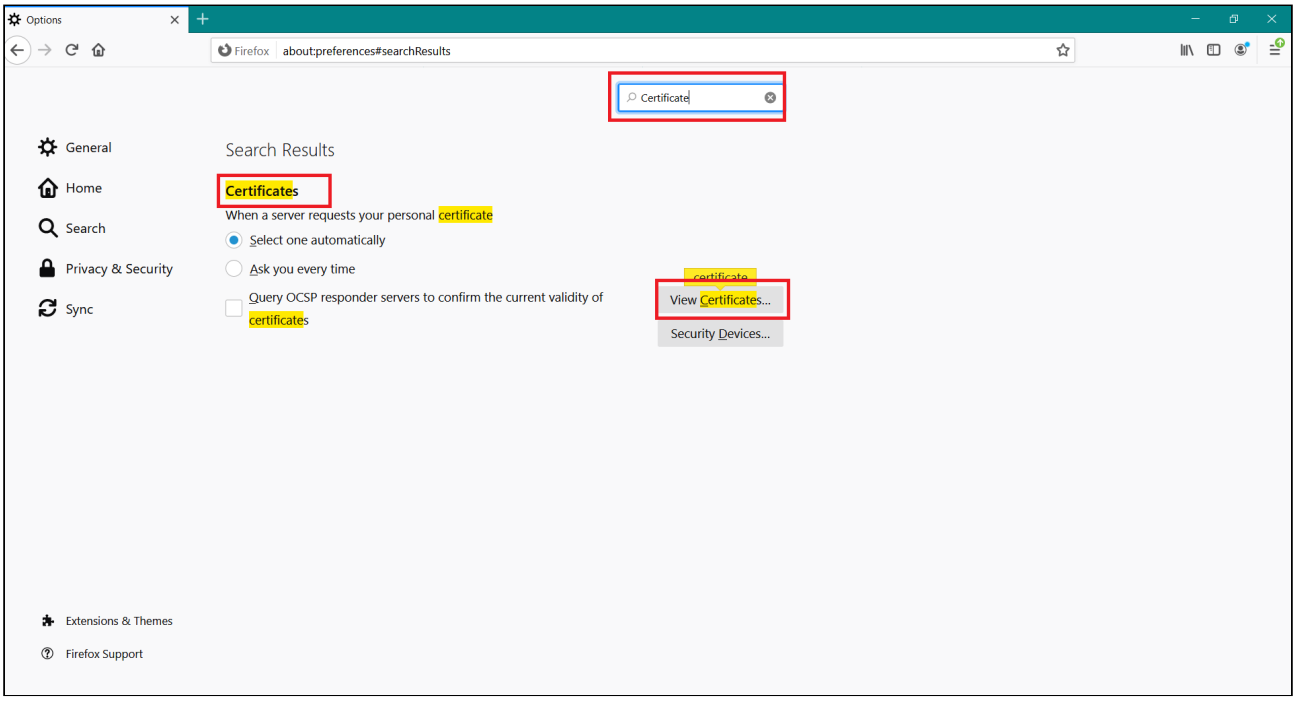
- Select the **GSEP Certificate** from the **Certificate Wizard** and click on **Remove.**
- You will get **Certificate alert** popup and click on **Yes** to remove the selected certificate.

2.4.3 Firefox:

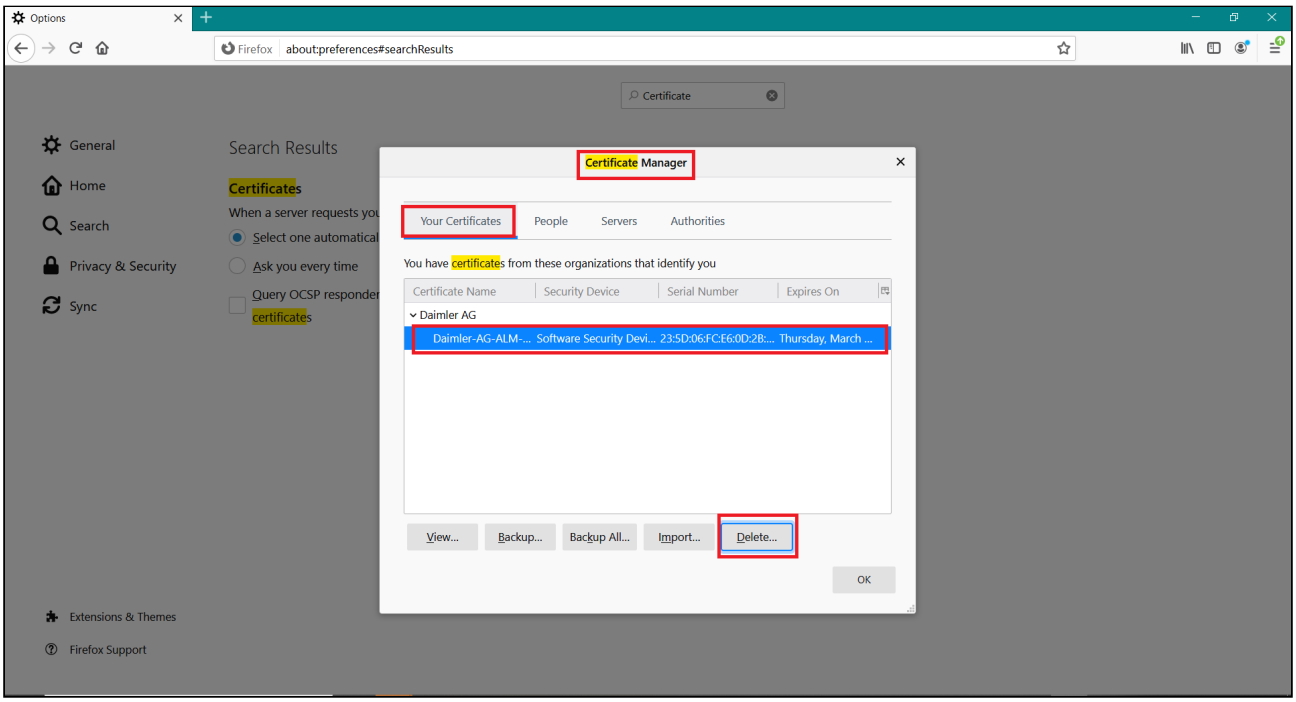
- Once you open the **Firefox** browser**,** you can see **Settings** option at the right side of the window, as shown below:



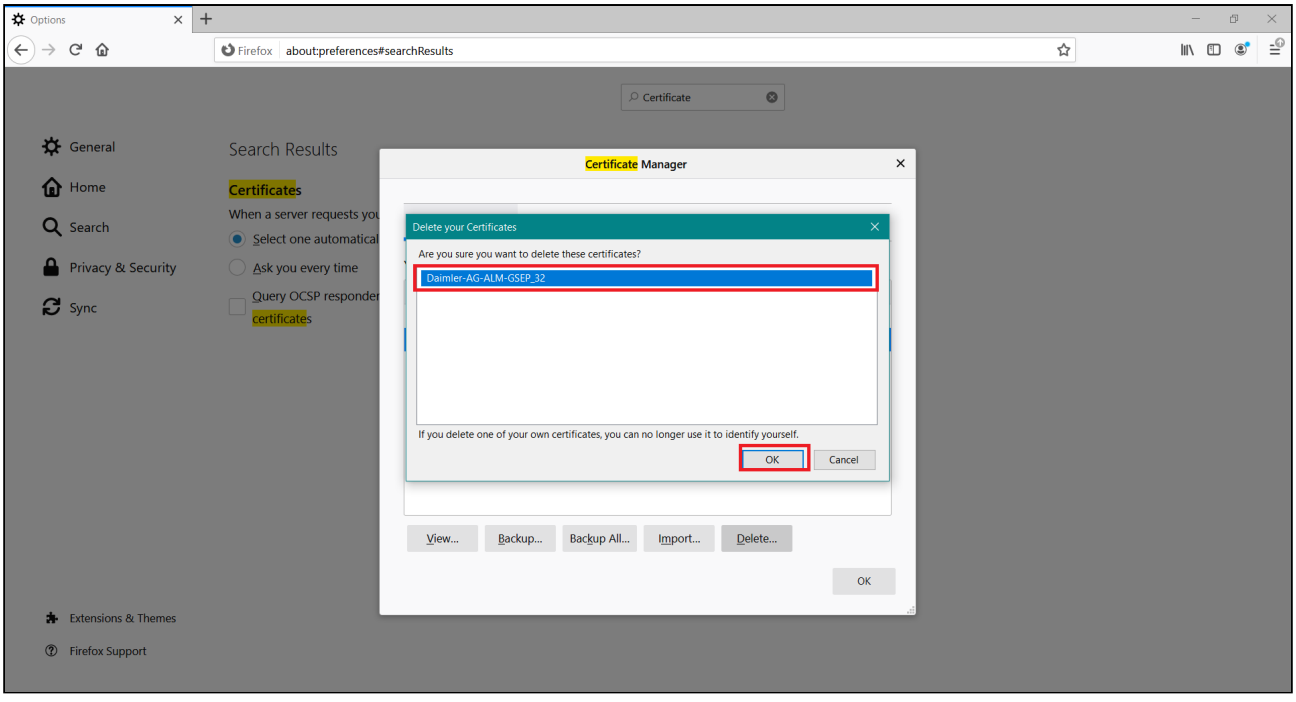
- Search for the certificate in the search bar and click on **View Certificates**:



- On the Certificate Manager screen, click on **Your Certificates** tab. Select the certificate and click **Delete** as shown below:



- You will get **Delete Your Certificates** alert popup and click on **OK** to remove the selected certificate.



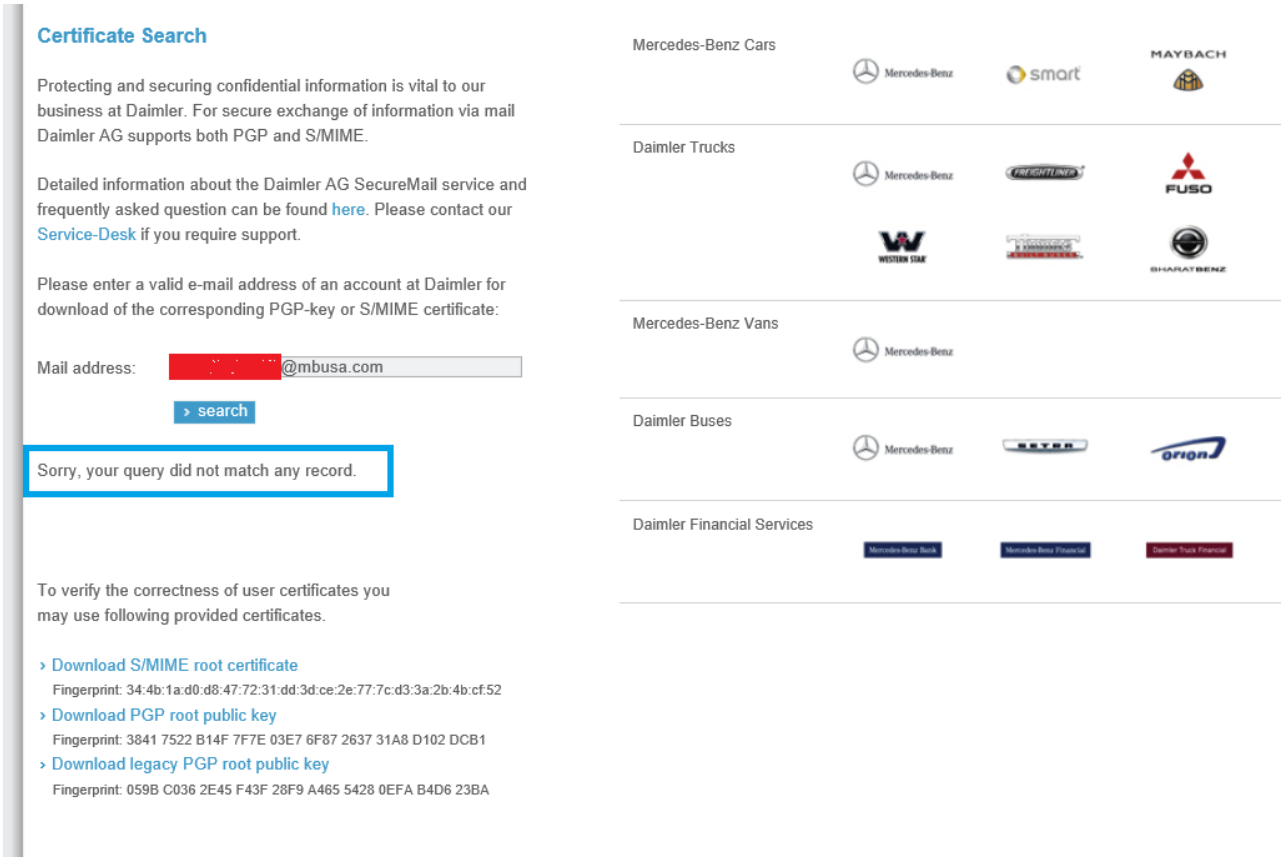
2.5 Issue while generating PGP Key for opening Encrypted/Protected email for internal Users

Issue: When user contacts GSEP and says that he/she is not able to generate PGP Key for opening encrypted or protected email where we are sending our GSEP ALM certificate.

Generally we have an option of Certificate Management Application (CMA) by default in all the Daimler hosted laptops and desktops.

User has to open the CMA from their machine and login using their WiW credentials for installing the certificate.

The encryption option will work for the employees who are internals but there are some exceptions, when user is having email ID with host name like @mbusa.com[28] or @mercedesbenz.ca[29], they may not be able to generate the PGP key to open the protected/encrypted emails.



`

If the above error is being reported then please guide the users to reach concern team as mentioned below.

==========

Who provides support for users located at Daimler location?

When users are internal and not belongs the @daimler.com[30] host name, for an example @mbusa.com[31], and they are not able to generate the PGP key then concern POC is:

KCS - Key and Certificate Service of ITI/EDC
E-Mail: encryption-service@securemail.daimler.com[32]

Phone: +49 711 17 75474
Fax: +49 711 17 28200
CISM: CISM CDCSP_KCS_SERVICE

==========

28 http://mbusa.com
29 http://mercedesbenz.ca
30 http://daimler.com
31 http://mbusa.com
32 mailto:encryption-service@securemail.daimler.com

Who provides support for partners/suppliers?

When users are external and not able to generate the PGP key for opening the encrypted email then users will have to contact below mentioned POC:

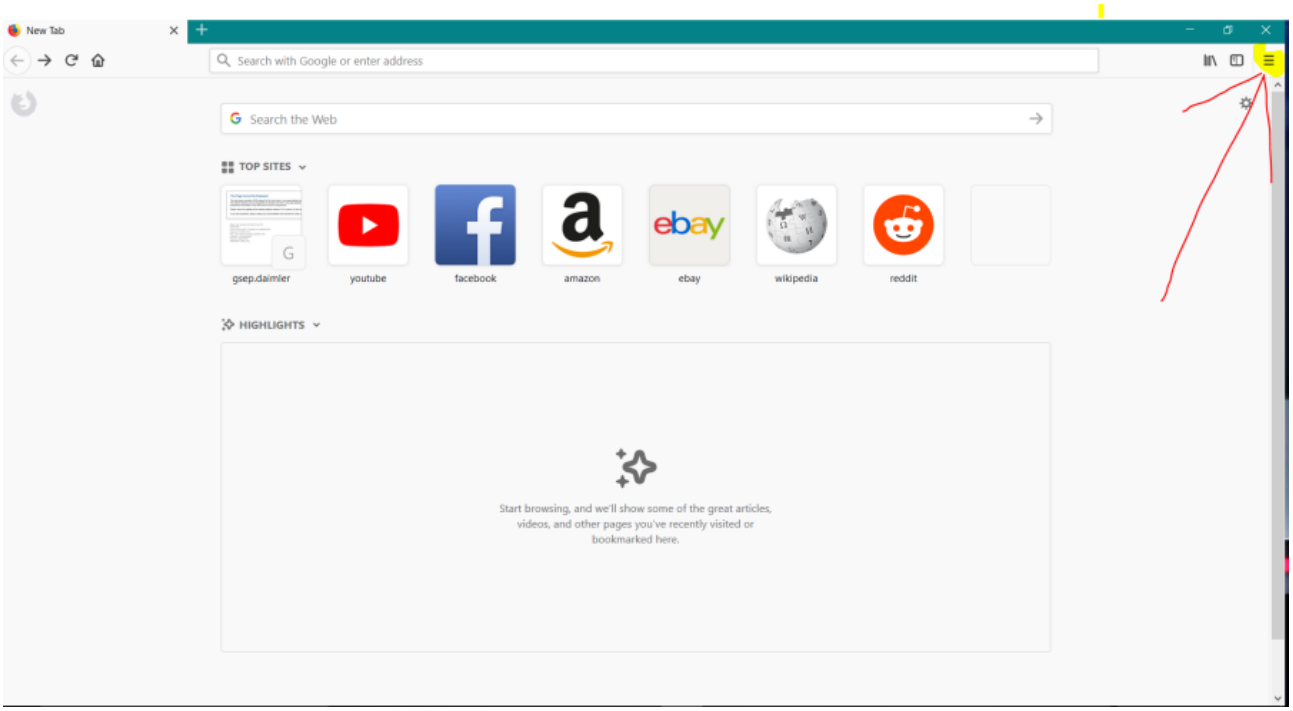
E-Mail: support@securemail.daimler.com[33]
Phone: +49 711 17 20170
Fax: +49 711 17 20171

==========

2.6 Steps to import ALM Certificate to FireFox browser

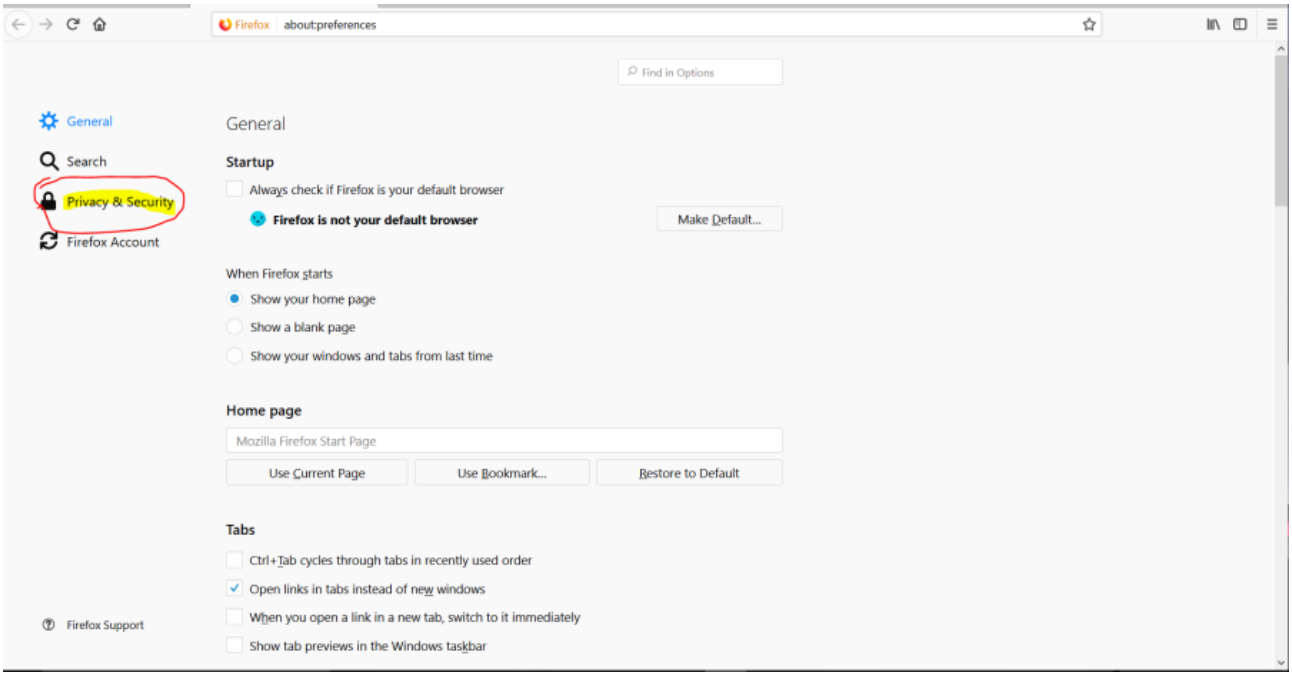
Steps to import ALM Certificate to FireFox browser

1. Open Mozilla FireFox browser and press the MENU Button shown below.

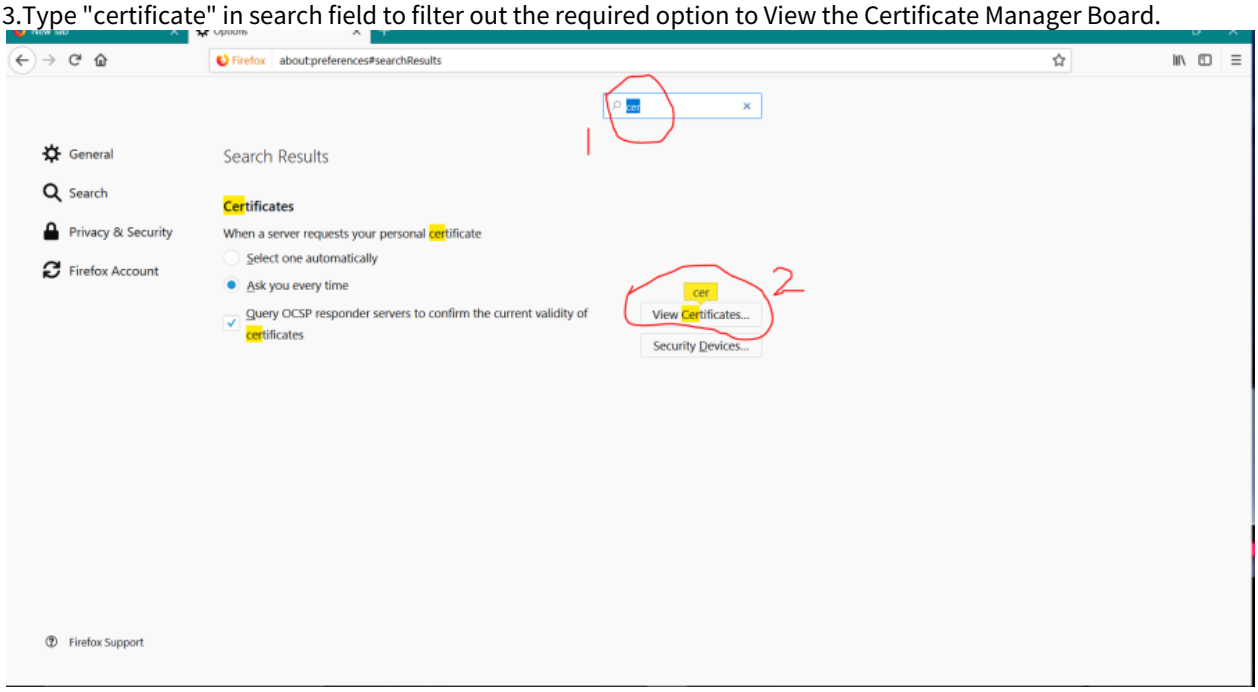


2.Select the "Privacy & Security" option

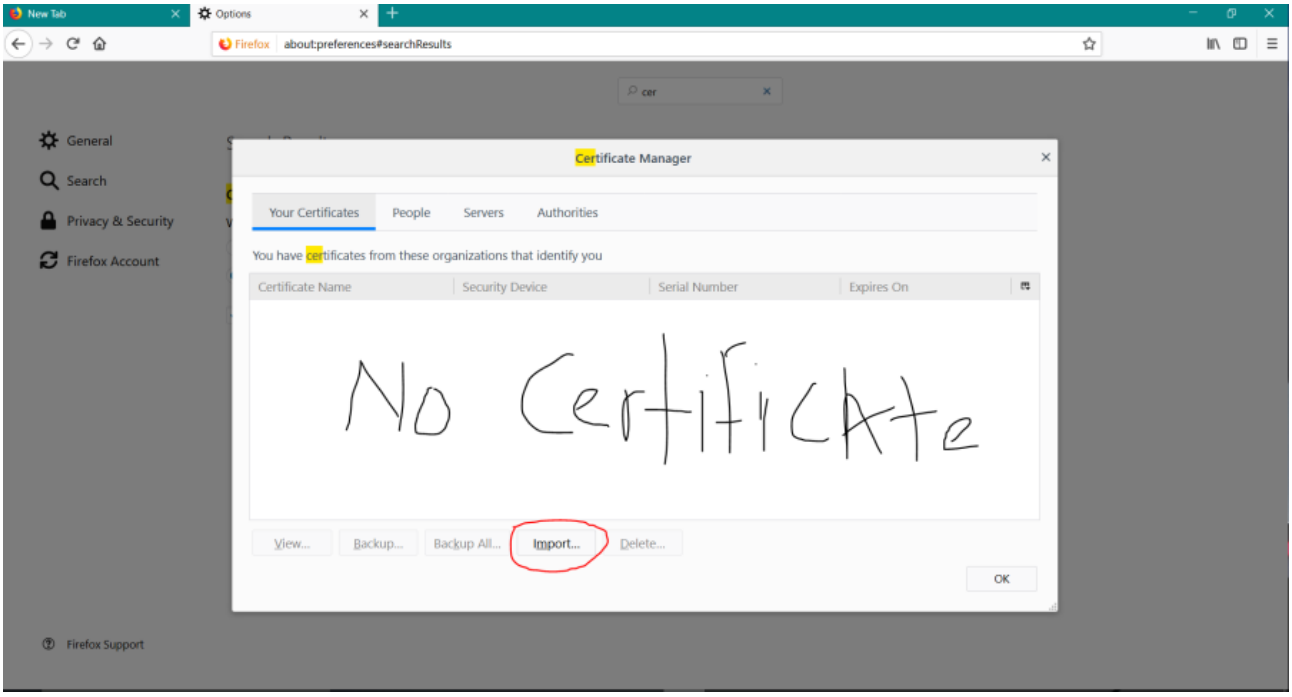
33 mailto:support@securemail.daimler.com



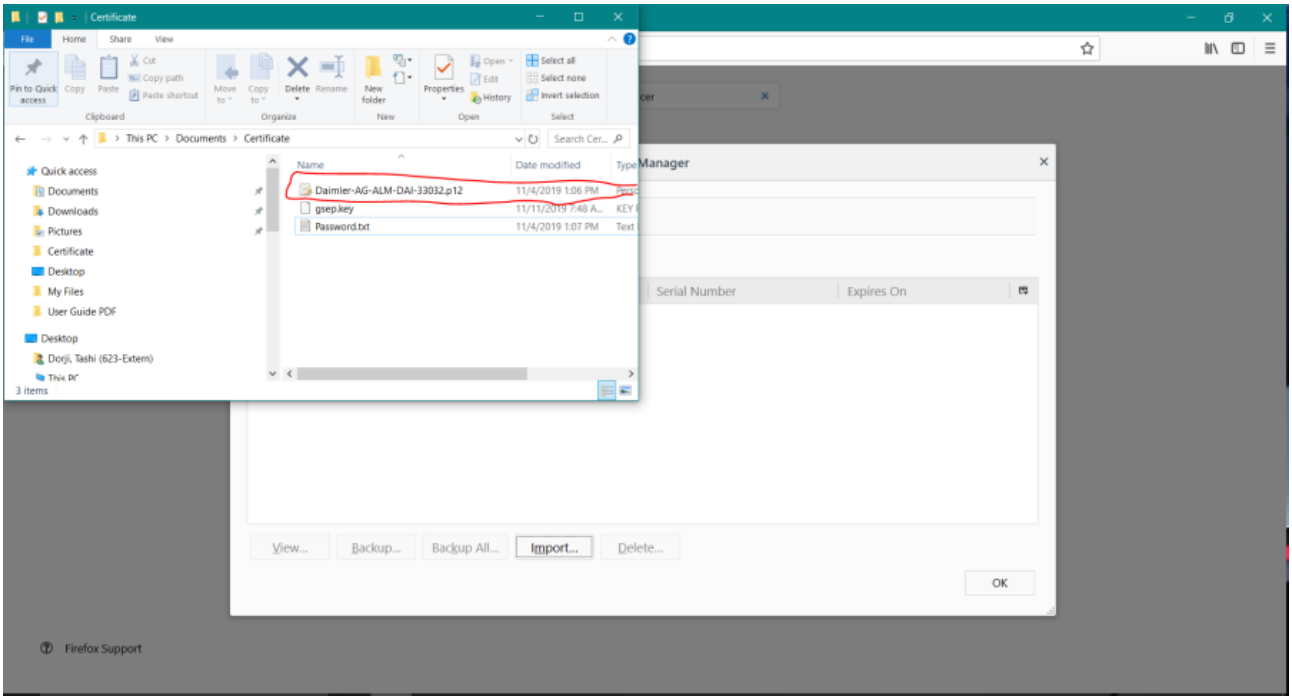
3.Type "certificate" in search field to filter out the required option to View the Certificate Manager Board.



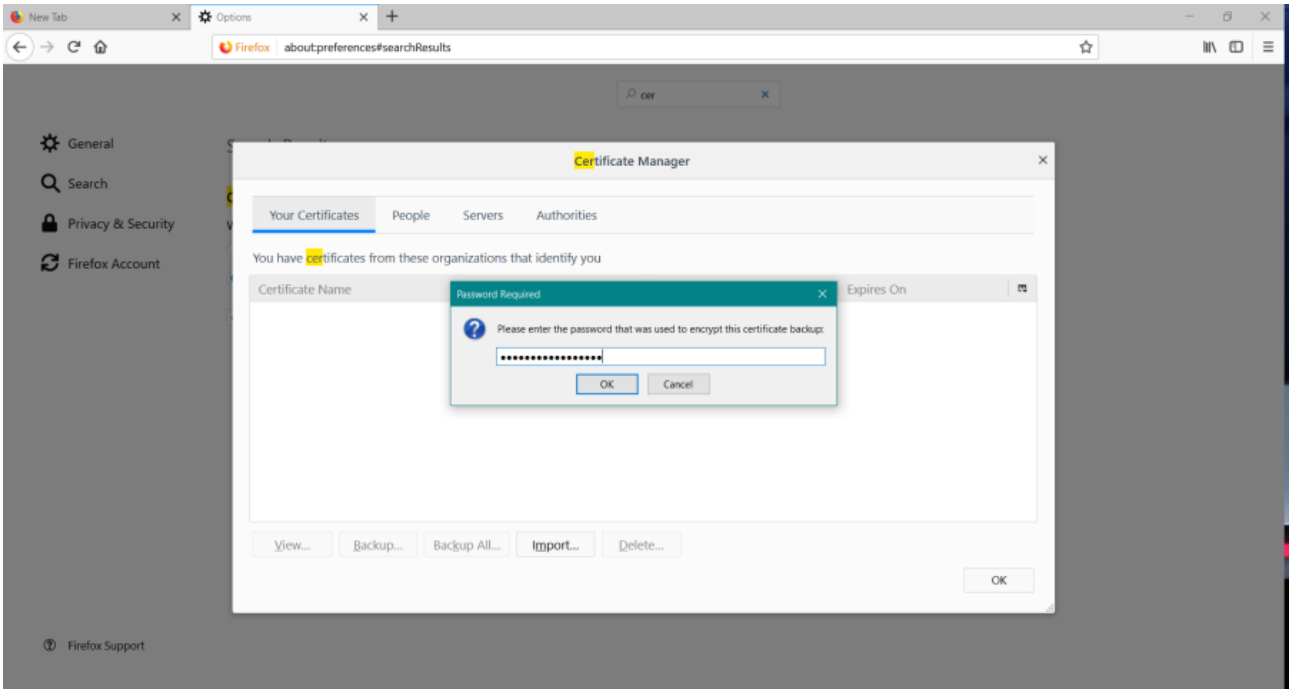
4. Click on "Your Certificates" tab. If Certificate is not listed, click on "import" button and select the GSEP certificate from the file explorer which you have received from GSEP Support via encrypted mail(save the certificate first in the local system before performing this step).



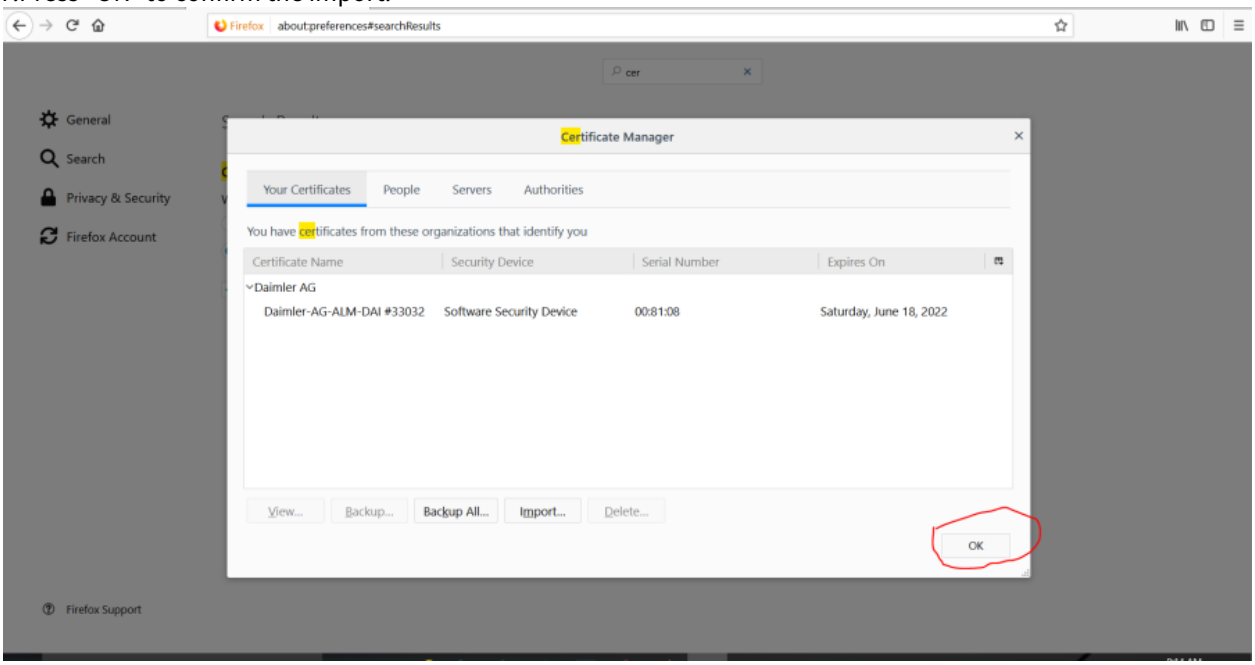
5.After that select the available certificate.



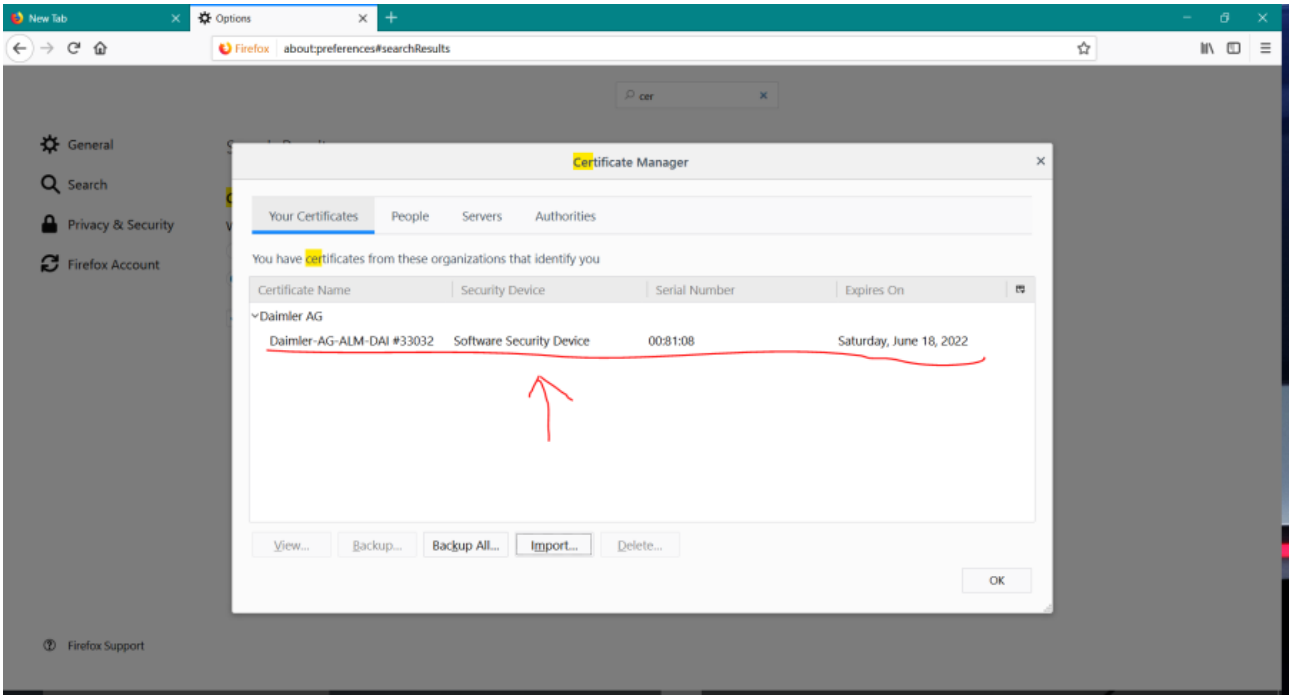
6.Enter the password which is available in the Certificate Mail content.



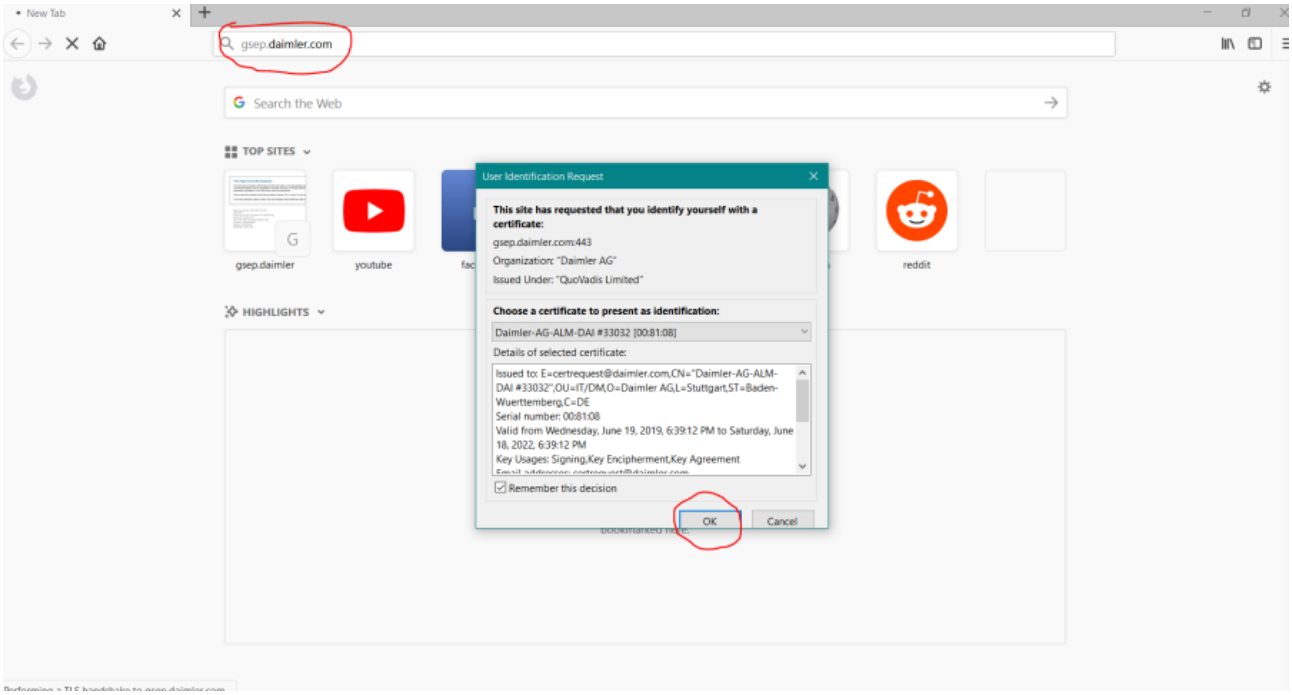
7.Press "OK" to confirm the import.



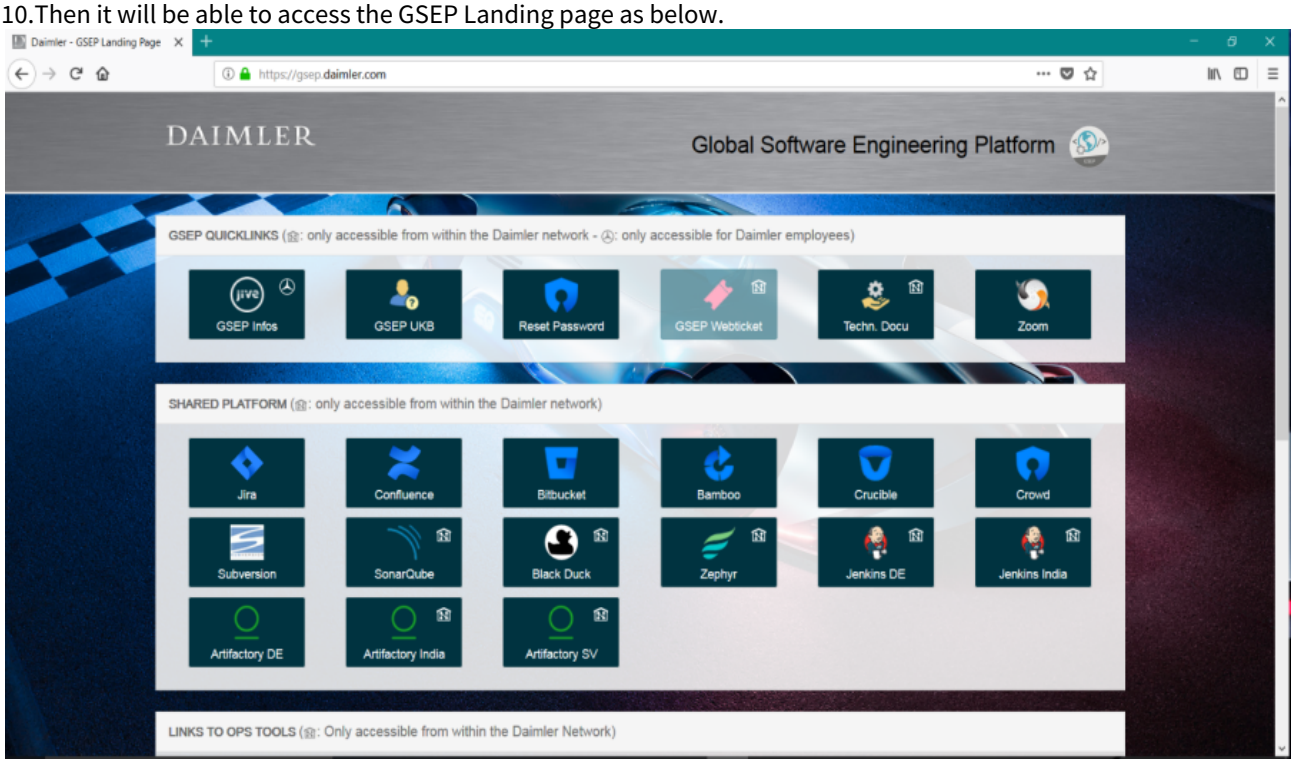
8. Once import is done, the GSEP ALM Certificate will be available like below.



9. Then go to the browser search with URL"gsep.daimler.com" and choose the imported Certificate to represent as identification.



10.Then it will be able to access the GSEP Landing page as below.

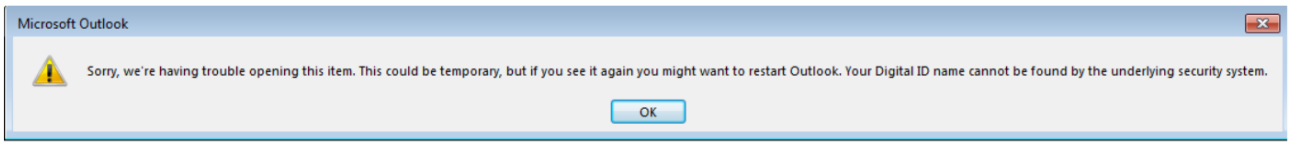


2.7 Unable to access encrypted emails (GSEP ALM certificate)

New users will receive an encrypted email from NoReply-GSEP-Pool-ID@daimler.com[34] subjected as "***Welcome you onboard as a new member of the GSEP platform/ Willkommen an Board als neues Mitglied der GSEP Plattform***"

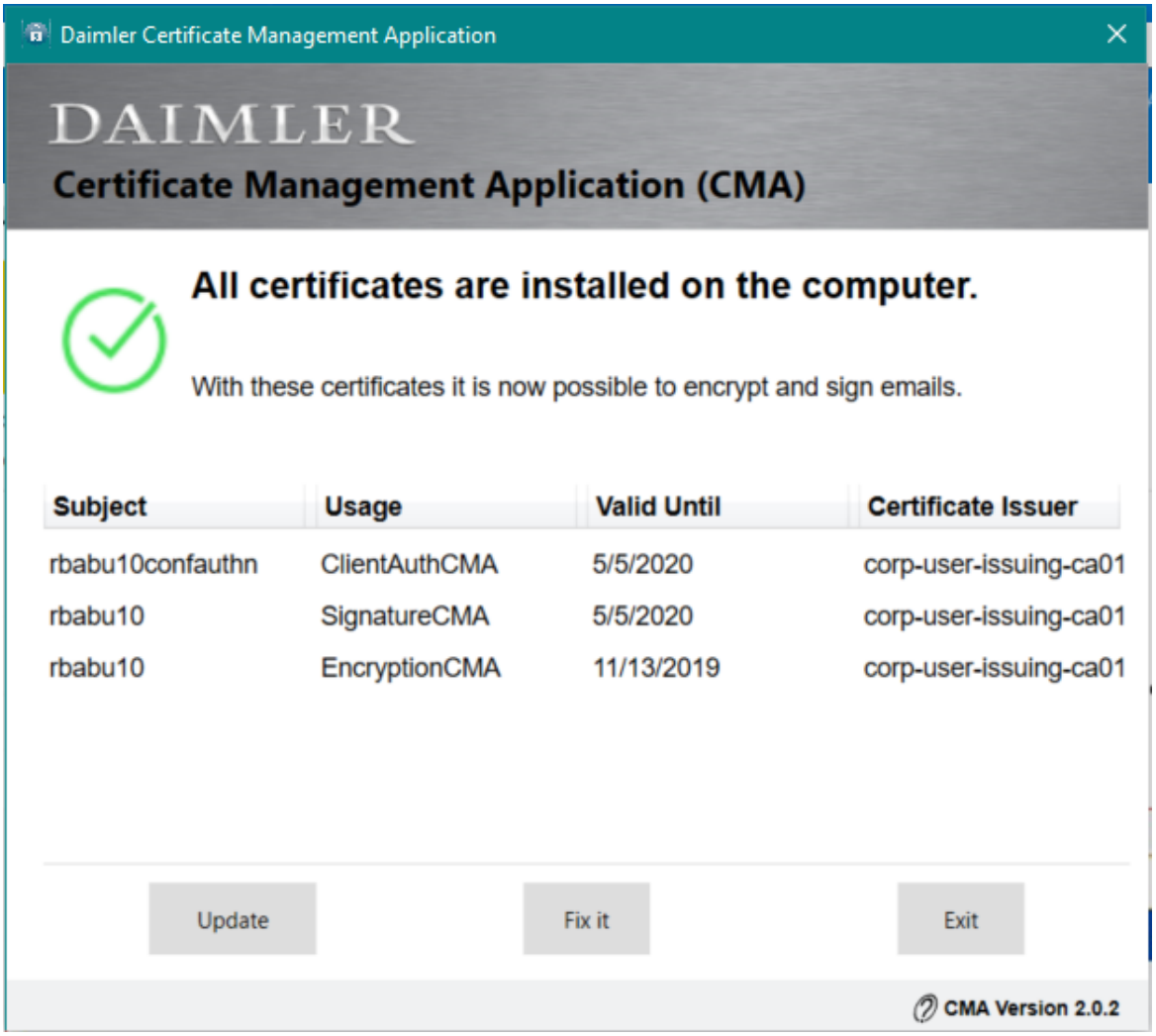
User will not be able to access encrypted email & returns with error "***Your digital ID name cannot be found by the underlying security system"***

Error screenshot:-



In order to access encrypted emails, users (*Internal/externals who are Daimler assets "Laptop & Desktops"*) has to contact their local IT team to install "**Certificate Management Application (CMA)**" on their respective machine.

34 mailto:NoReply-GSEP-Pool-ID@daimler.com


Daimler Certificate Management Application
DAIMLER
Certificate Management Application (CMA)
All certificates are installed on the computer.
With these certificates it is now possible to encrypt and sign emails.
Subject
Usage
Valid Until
Certificate Issuer
rbabu10confauthn
ClientAuthCMA
5/5/2020
corp-user-issuing-ca01
rbabu10
SignatureCMA
5/5/2020
corp-user-issuing-ca01
rbabu10
EncryptionCMA
11/13/2019
corp-user-issuing-ca01
Update
Fix it
Exit
CMA Version 2.0.2

3 Account Types and Passwords

3.1 GSEP Changing Password

3.1.1 **Summary:**

This document describes use case on **changing the password** manually for GSEP applications by log in to **Crowd's Self-Service Console** and change your password.

In order to change/ update the crowd password make sure that you are able to login with the current password.

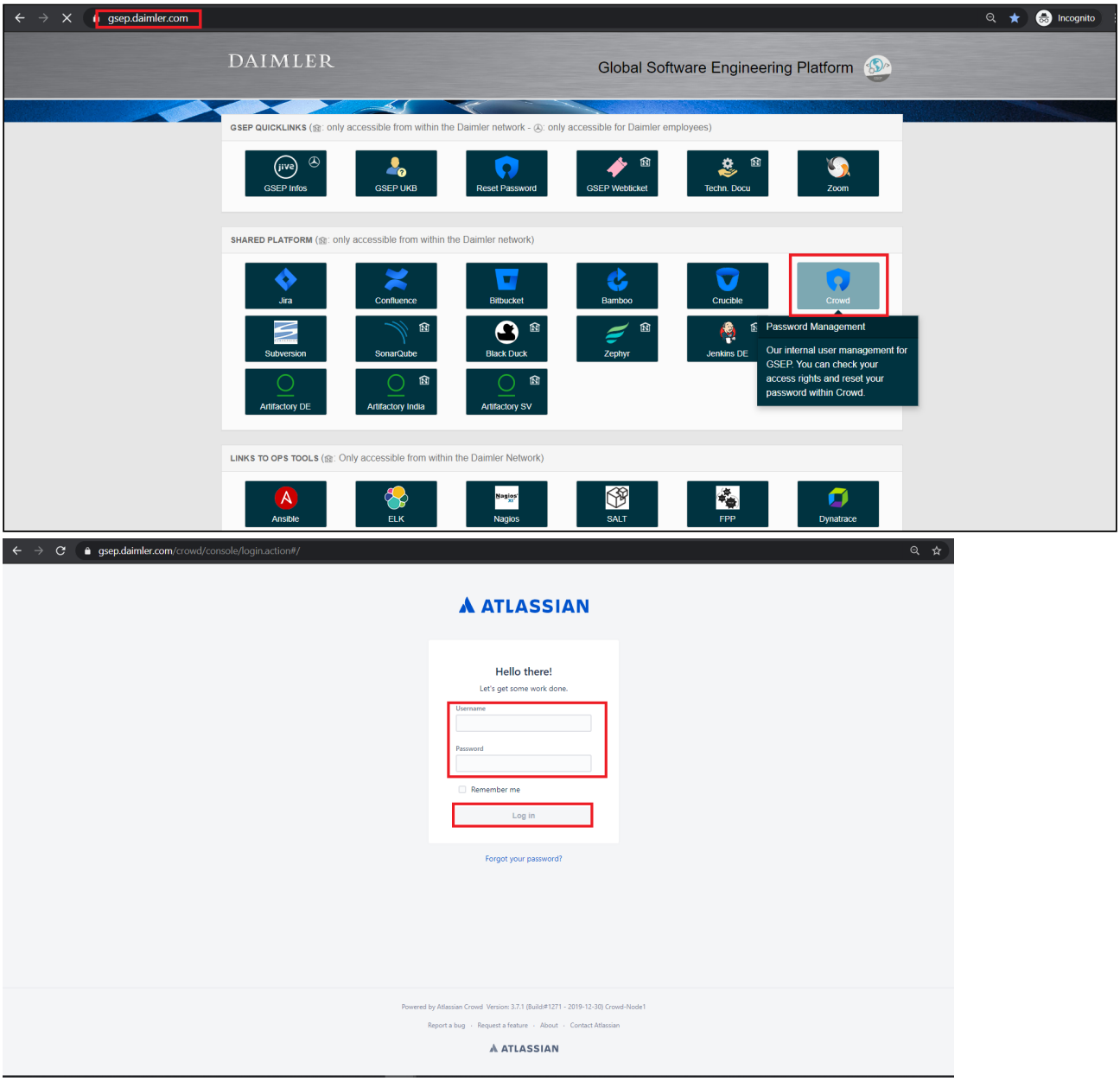
If you do not know your current password oder user id, please check GSEP Password Reset(see page 40)

3.1.2 **Kindly follow the below steps to Changing the password:**

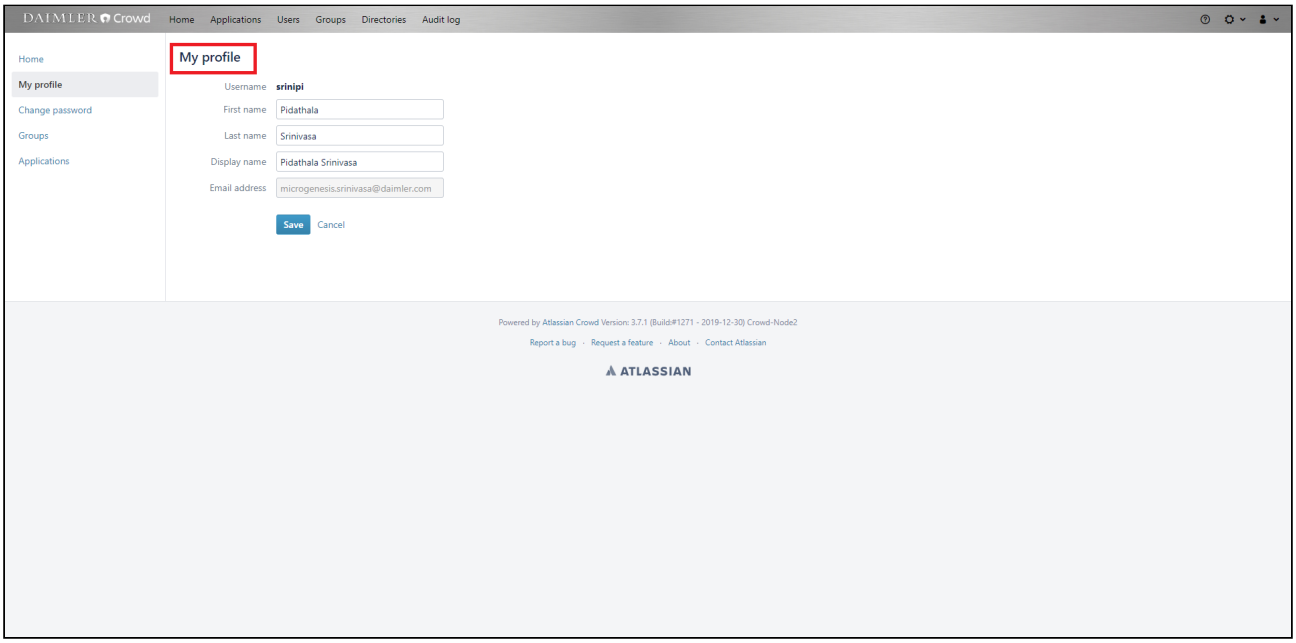
1. Please Log in to GSEP Crowd[35] from GSEP Landing page[36].

35 https://gsep.daimler.com/crowd/console/login.action#/

36 https://cism-web.es.corpintra.net/cism/forms/cism-system.es.corpintra.net/CISM_Bas%3AStdDialogs%3AStdTicket/Standard+Ticket+Selection/?cacheid=e8ea7da&format=html

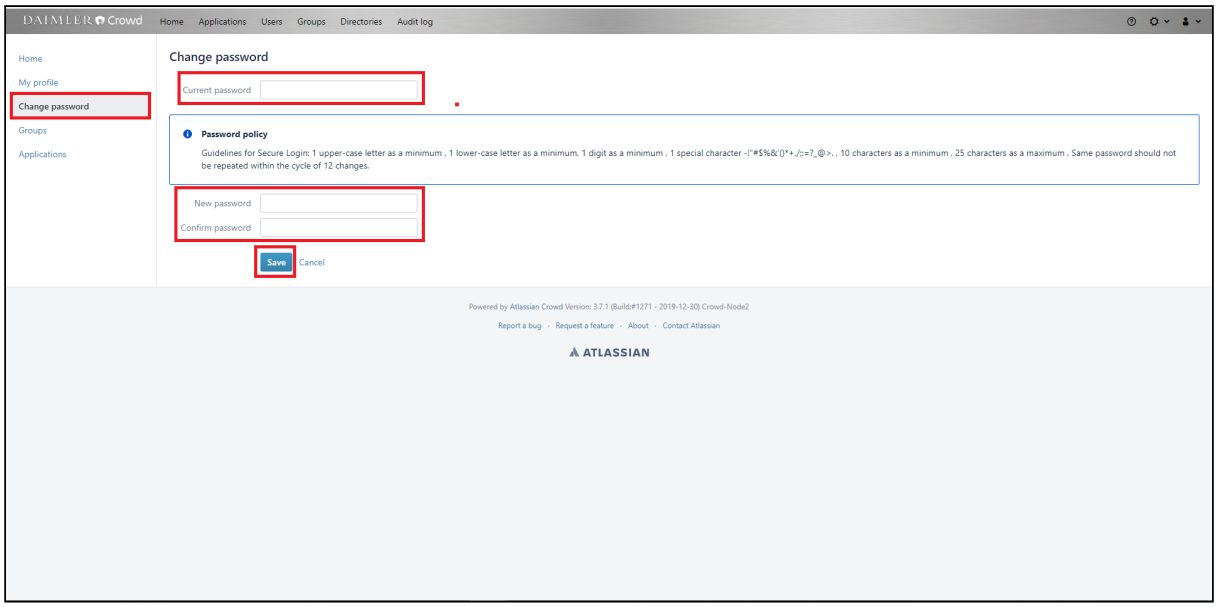


2.The **Crowd Self-Service Console** will open.



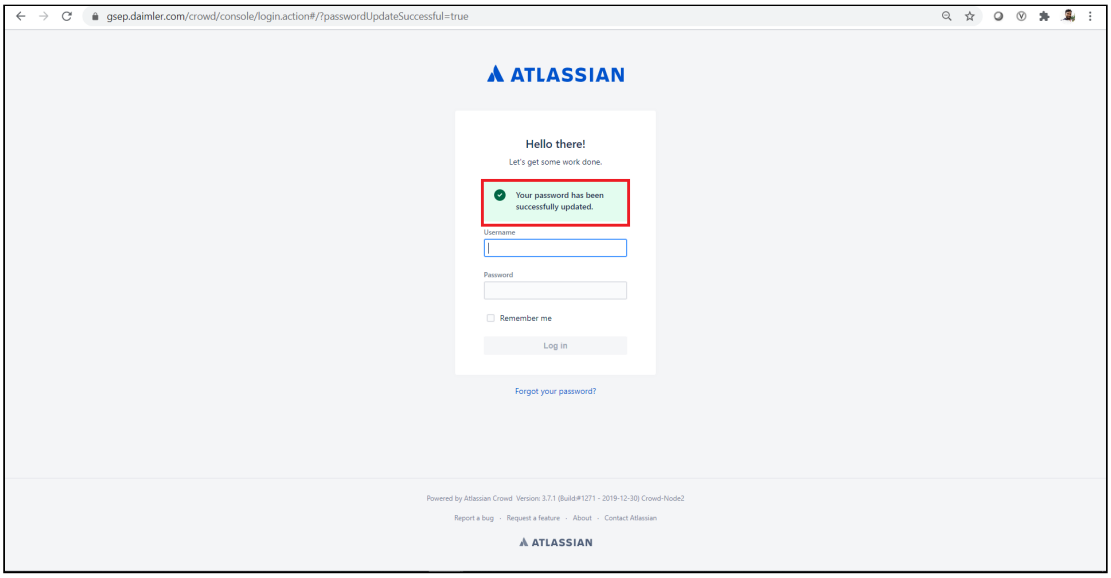
3.Click '**Change Password**' in the left-hand menu.The '**Change Password**' screen will appear, as shown in the screenshot below. Enter the following information:

- **Current Password** — Your current password.
- **New Password** — The new password you would like to start using.
- **Confirm Password** — Your new password again, to verify that you typed it correctly the first time.

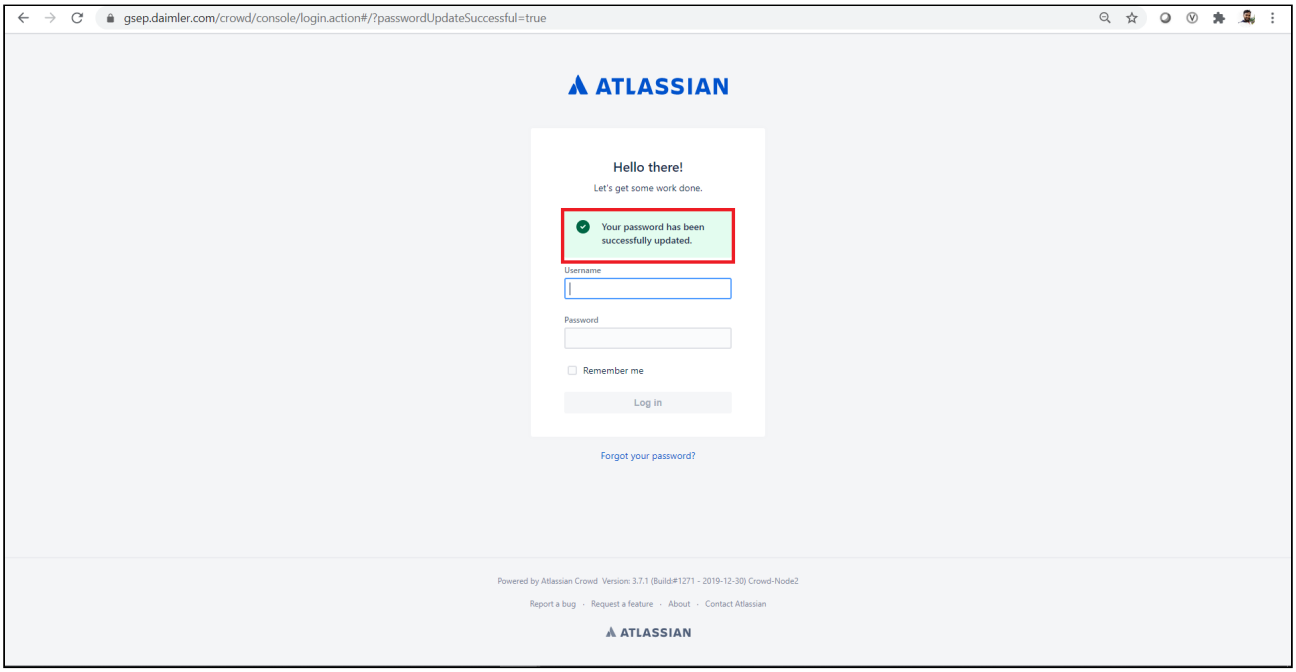


4. Click the '**Save**' button.

Note: If the change is successful, a '**Password updated**' message will appear on the screen.



5.Now you can login with new password



3.2 GSEP Password Reset

3.2.1 **Summary:**

This document describes use case on **Reset the password** manually for GSEP applications.

By following the steps below, our system will send you an email with a password reset link. The application "Crowd" handles the password for the GSEP system

The Crowd application **blocks application login** after user **entered the wrong password** more than **3** times. This block **will not be removed** when the password is reset manually.
Please contact **GSEP Support** to reset password after error message ***InvalidPasswordAttempts***.

Global Software Engineering Platform (GSEP);

- 24x7 Helpline: **+49 7031 90 89029** à Extn: 1 for GSEP
  Use one of the following links to report any GSEP Incident & Inquiry/help - MBAG Webticket(ITSM)[37], DTAG Webticket (JSM)[38] & Suppliers Webticket (CSM)[39]
  ⓘ Please follow the links on https://gsep.daimler.com/ to create GSEP support tickets or to open the UKB "How to get help"[40] page.

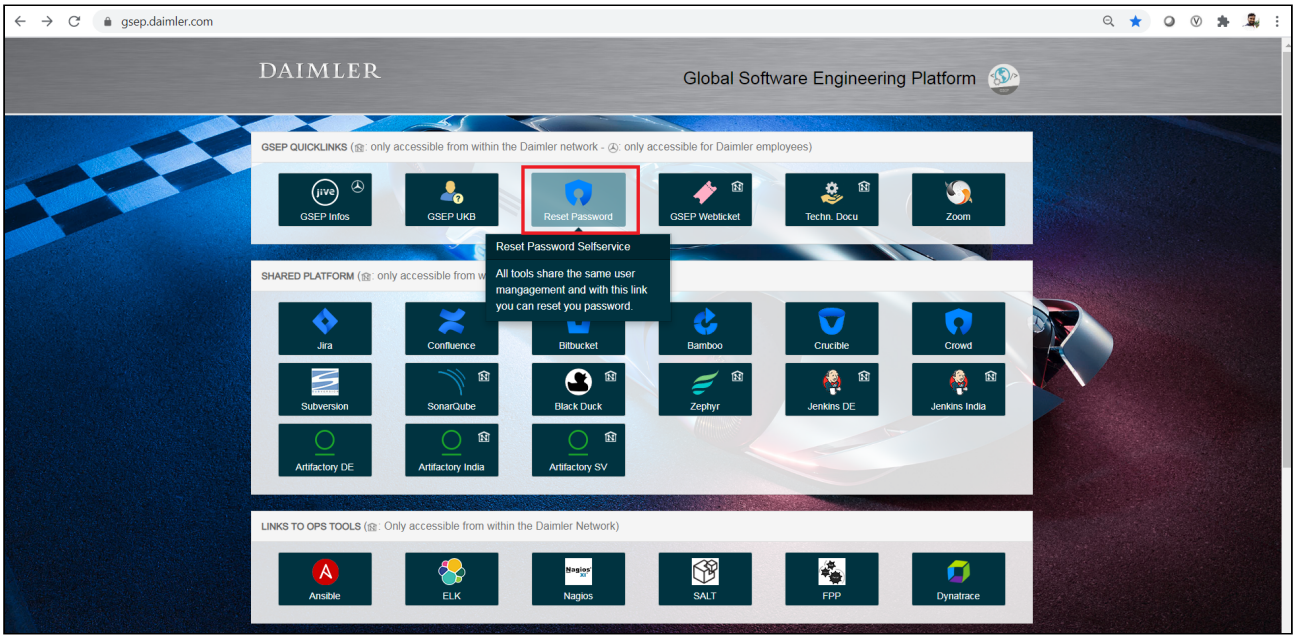
3.2.2 How to reset your password:

1. Please use the below URL to reset your password in the respective environment at any point of time (with respect to available access rights):

   i. GSEP Production: https://gsep.daimler.com/crowd/console/login.action#/forgot-password

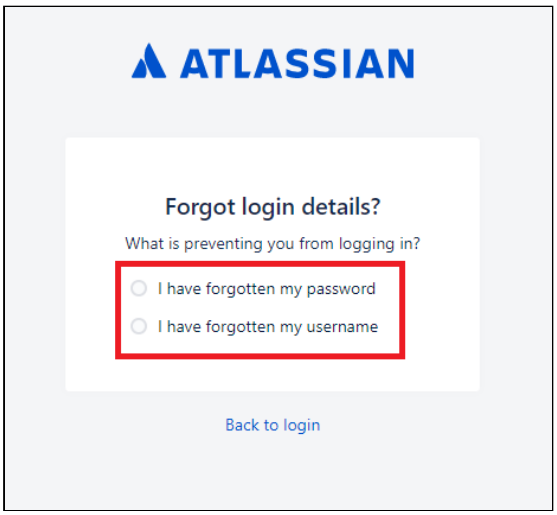
   ii. GSEP Integration: https://gsep-int.daimler.com/crowd/console/login.action#/forgot-password

Note: The same password reset link is available in the GSEP Landing page also. Please see the below screen shot.



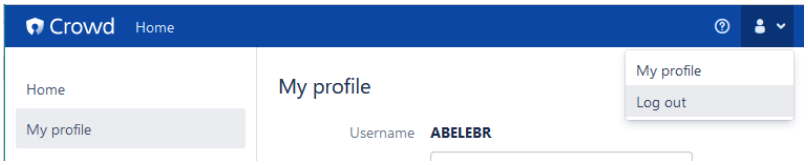
37 https://daimler.service-now.com/sp?id=sc_cat_item&sys_id=062eec1f1b0c605093b43113dd4bcbf0&sysparm_category=c68bd6491bd10410f826bb31dd4bcbb5
38 https://gsep.daimler.com/servicedesk/servicedesk/customer/portal/261
39 https://digitalservices.mercedes-benz.com/
40 https://gsep.daimler.com/confluence/x/tCdKI

2. It will routed to the respective **Forgot login details** page as below.

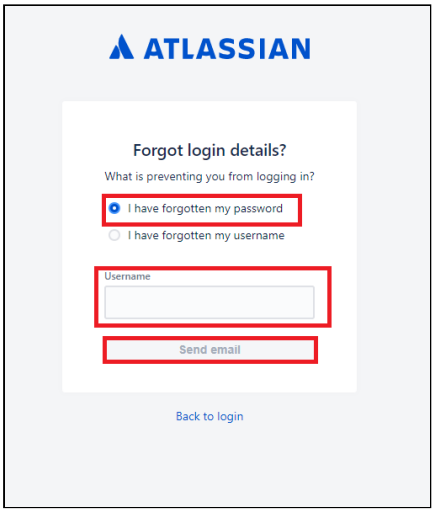


Important

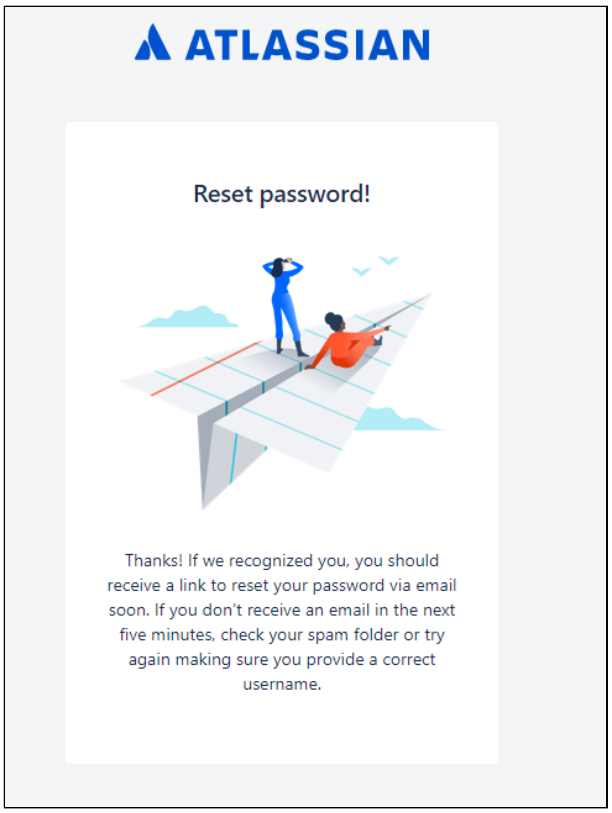
If you do not see this dialogue from above, please **logout first and then retry the link** from point 1 again:



3. Please select **" I have forgotten my password"** option from the list , enter the GSEP **User id** and click on **" Send email" .**

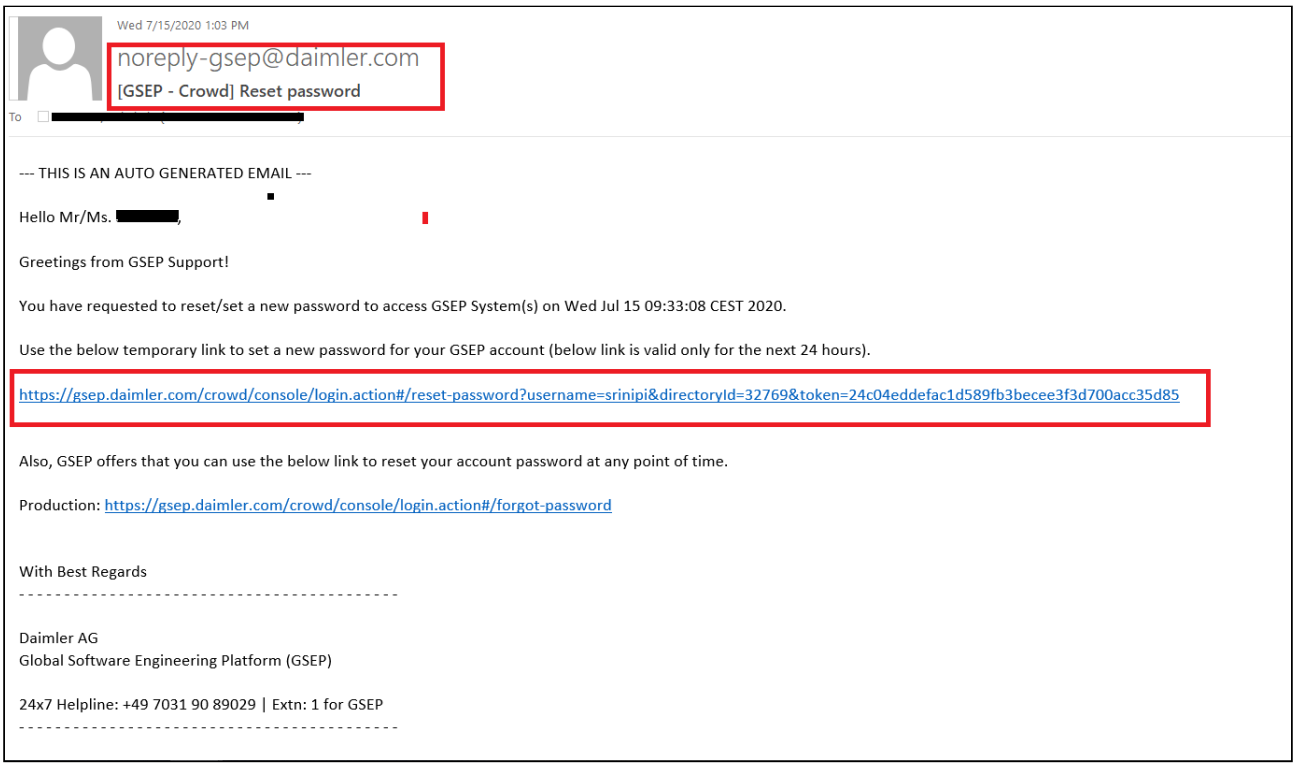


4. It will trigger an automated email to your account and you will receive the password reset link email from gsep-support@daimler.com[41] with a subject as "**[GSEP - Crowd] Reset password".**



5. Please click on the link which you received via mail which will redirect it to web browser as shown below.

41 mailto:gsep-support@daimler.com



Wed 7/15/2020 1:03 PM

noreply-gsep@daimler.com

[GSEP - Crowd] Reset password

To [redacted]

--- THIS IS AN AUTO GENERATED EMAIL ---

Hello Mr/Ms. [redacted],

Greetings from GSEP Support!

You have requested to reset/set a new password to access GSEP System(s) on Wed Jul 15 09:33:08 CEST 2020.

Use the below temporary link to set a new password for your GSEP account (below link is valid only for the next 24 hours).

https://gsep.daimler.com/crowd/console/login.action#/reset-password?username=srinipi&directoryId=32769&token=24c04eddefac1d589fb3becee3f3d700acc35d85

Also, GSEP offers that you can use the below link to reset your account password at any point of time.

Production: https://gsep.daimler.com/crowd/console/login.action#/forgot-password

With Best Regards

Daimler AG
Global Software Engineering Platform (GSEP)

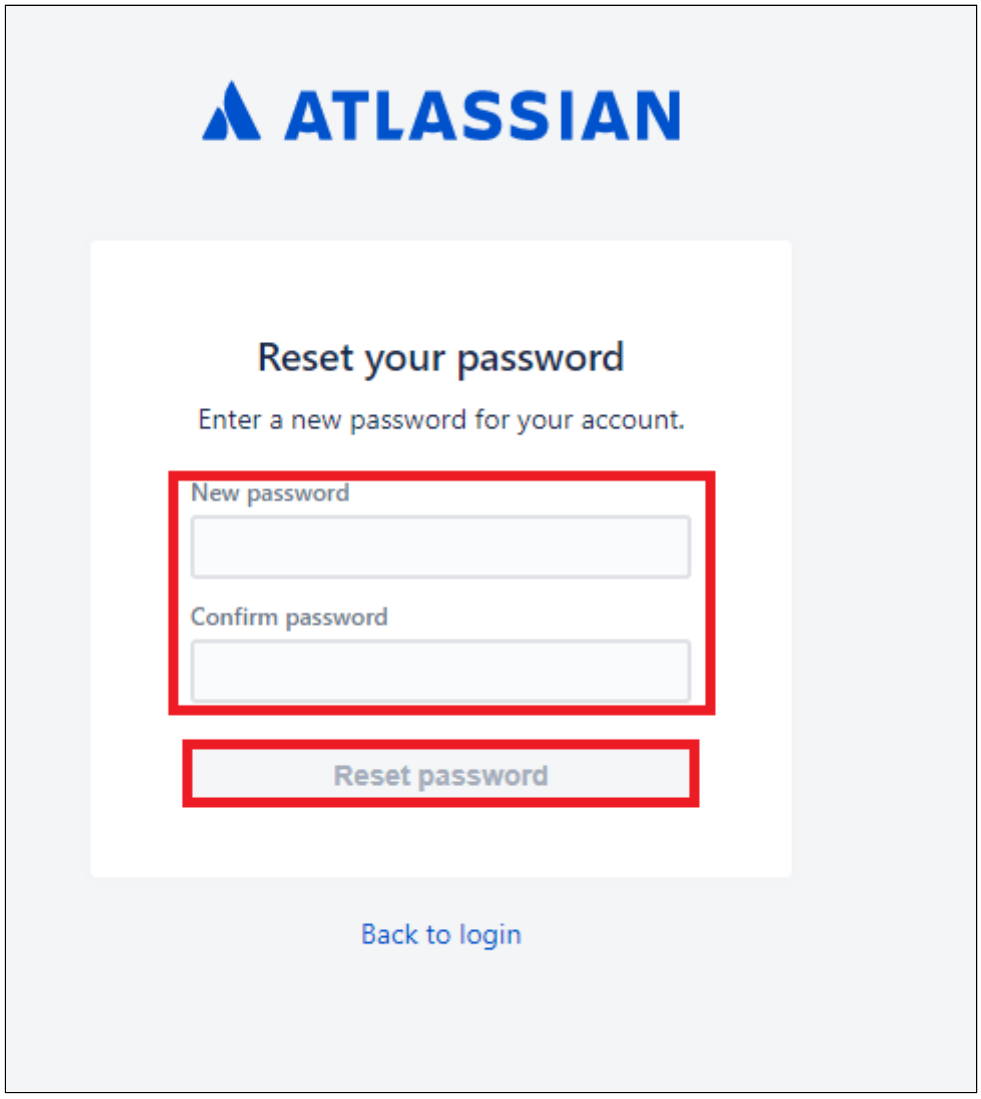
24x7 Helpline: +49 7031 90 89029 | Extn: 1 for GSEP

---

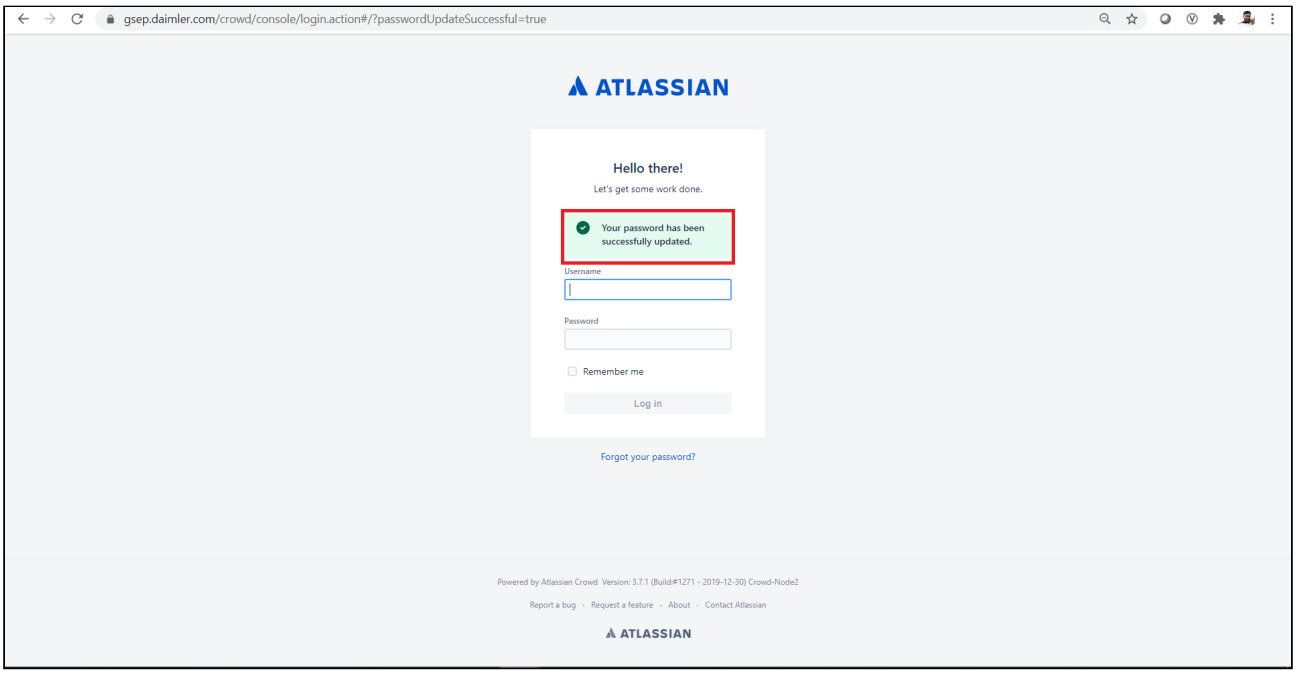
6. It will redirect to Reset your password page in the web browser. Enter the New password and Confirm Password . Once the new password is entered click on Reset password.

Password policy

Guidelines for Secure Login: 1 upper-case letter as a minimum , 1 lower-case letter as a minimum, 1 digit as a minimum , 1 special character -!"#$%&'()*+,/;:=?_@>. , 10 characters as a minimum , 25 characters as a maximum , Same password should not be repeated within the cycle of 12 changes.



Note: If the reset is successful, a '**Password updated**' message will appear on the screen. as follow.



7. Now you can login with new password

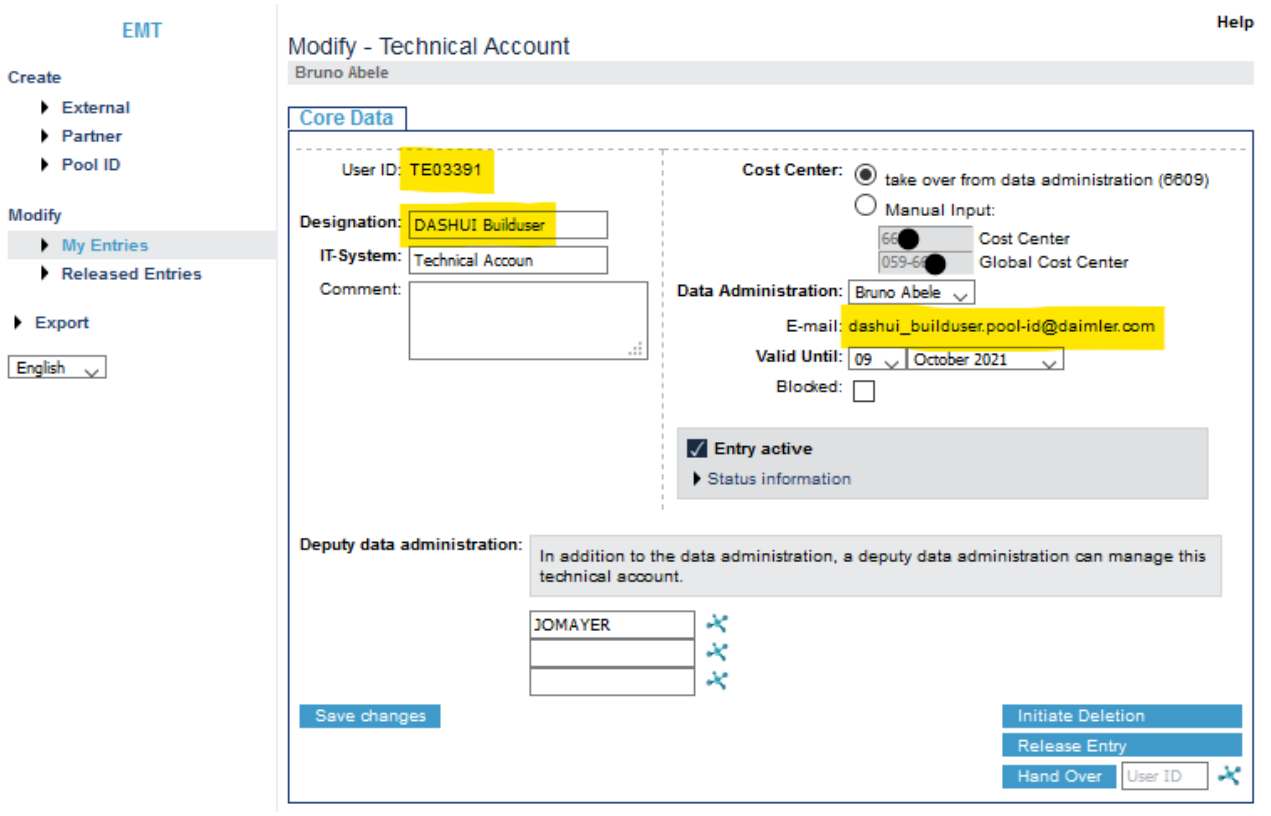
3.3 Technical Accounts in GSEP

Technical (TE) Accounts are **for non-personal access** to technical systems, e.g. for sync between applications, CI/CD pipelines or automatic downloads. TE Accounts look like **TE12345** (TE*****)

> It is not possible to use TE accounts for interactive login on gsep.daimler.com (via Single-Sign-On), they can only be used on APIs.

> If you use the same TE account for PROD processes but also for development or on developer computers, there is a risk that password changes are not handled correctly. The TE account will be locked when the users/systems do not change the password at the same time.

Please establish a password change process on your side and restrict the TE account usage to non-personal access: More info here(see page 52)!



Pool-IDs have a similar use case, but are no longer allowed, Why? Pool ID in GSEP - Creation and Management(see page 54)

3.3.1 How to create a Technical Account

A Technical TE Account can be created with the help of your local IT Team (ITK/UHD). Depending on the users location, the process is different. If in doubt, please contact your local ITK or UHD.

Please ask your ITK/UHD to **create TE account with CD + AD + Mailbox** since a valid email-id is a must in order to register an account on GSEP.
Note for ITK: After creating a TE user, it takes several hours till this user becomes visible in WAMS, where the @mercedes-benz.com[42] email address is created. Please be patient

As with any other GSEP account, the Technical Account will have a separate GSEP password in addition to the CD/ WIW and AD/EMEA/Windows password. Please use this whenever you access services on https://gsep.daimler.com.

42 http://mercedes-benz.com

3.3.1.1 Step-by-step guide (for EMEA Users)

Only internal employees can request a Technical Account

1. Request the Technical Account at your ITK.

Mail template (with example data)

Hello ITK / UHD,

I need a technical account (TE*****)/ Ich benötige einen Technischen Account (TE*****):

Owner: <your user id> e.g. GRACHR
Deputy: <other user's id> e.g. ABERNKI
Name: <a name for the technial account> SynchronizationUser
Email: Should be generated (normally synchronizationuser.pool-id@mercedes-benz.com[43])
CD: Yes
AD: Yes
Mailbox: Yes (important/Wichtig!)

I need this technical account to automate processes on GSEP.

Best wishes

2. Once the account is created, you will receive an email with an initial password (windows password).
3. Access the TE account email https://webmail.wp.corpshared.net/owa and add the new mailbox to your Outlook, see below.
4. Request access to GSEP via ZULA and get your password and certificate, see below.
5. The account can be managed via EMT,[44] see below.
6. For the first GSEP OIDC login(see page 6), you have to reset the CD password[45] of the Technical Account.

*In most locations you are **not** allowed to request accounts via UHD, Email to UHD89000 (059-NPM) <uhd89000@mercedes-benz.com[46]> or a ServiceNow ticket. This has to be done by an ITK.*

(ITK steps: start net v3.7.6.1 or higher, click link "User Management", click link "Technical account", add owner, then click EMT on right bottom side, click link "Technical Account", add user data)

3.3.1.2 Step-by-step guide (for MBRDI Users)

Only internal (Daimler) employees can request a Technical Account

43 mailto:synchronizationuser.pool-id@mercedes-benz.com
44 https://iam-tools.iam.corpintra.net/emt/
45 https://gsep.daimler.com/confluence/display/GSEPUKB/Technical+%28TE%29+Account+in+GSEP#Technical(TE)AccountinGSEP-ChangetheCDpasswordoftheTechnicalAccount(forOIDC/PingID)
46 mailto:uhd89000@mercedes-benz.com

1. Write an email to your manager (L5/above) along with business justification for approval. Use the mail template from EMEA, see above.
2. Forward the manager's approval email to MBRDI ISO Team it-security-mbrdi@mercedes-benz.com[47], for ISO approval.
3. Register an IUHD Ticket[48] by attaching the (1&2) approvals, to create the TE account.
4. Forward the ISO approved email along with the IUHD ticket number to MBRDI Wintel Team: dw_623-mbrdi-proj_iti-wintel-team@mercedes-benz.com[49].
    a. Wintel Team will create your TE account & the AD password will be shared via an encrypted email to you.
    b. Post the TE account creation, Wintel Team will ask the MBRDI EUC L2 Team to create a mailbox for the newly created TE account.
5. Add the new mailbox to your Outlook, see below.
6. Request access to GSEP via ZULA, see below.
7. The account can be managed via EMT,[50] see below.
8. For the first GSEP OIDC login(see page 6), you have to reset the CD password[51] of the Technical Account.

Here is a sample email chain as reference: RE Technical account creation 0053890158 .msg[52]

3.3.1.3 Step-by-step guide (for MBRDNA Users)

Only internal (Daimler) employees can request a Technical Account

1. MBRDNA Business Unit members should submit a request using this link[53]. If you are unable to login, then please reach the support via email (ITHelpCenter@mbrdna.atlassian.net[54]), or call the helpline (1-408-991-6666).
2. The IT Department creates the technical account in EMT, then sends an encrypted email with the TE credentials to the BU requester.
3. In case of any issues or doubt on your raised request, then please contact Mr. Wyatt, Glenn (GLWYATT), BRM from Sunnyvale with your submitted request.
4. For the first GSEP OIDC login(see page 6), you have to reset the CD password[55] of the Technical Account.
5. Skip to section 2.4. Request roles for Technical Account in ZULA.

47 mailto:it-security-mbrdi@mercedes-benz.com
48 https://servicenow.i.mercedes-benz.com/esc?id=sc_cat_item&sys_id=74f00e051b8160502f8a3113dd4bcbce&sysparm_variables=eyJzZXJ2aWNlX29mZmVyaW5nX3NlbGVjdCI6IjA4YWY2YWUxMWJiZjQ5NTAwMDJkOTkzMzliNGJjYjJjIiwic2VsZWN0X3RlbXBsYXRlIjoiOWI0ZGZkZGQxYmFkOTU1MGFmMjE3NTkzOWI0YmNiMjYiLCJzaG9ydF9kZXNjcmlwdGlvbiI6Ik1CUkRJIEluY2lkZW50IC0gIiwiZGVzY3JpcHRpb24iOiJIYXJkd2FyZSBUeXBlICA6IExhcHRvcC9wL1ZESSBcclxuXHJcbkNvbnRhY3QgTnVtYmVyIChNYW5kYXRvcnkpIDogXHJcblxyXG5Ib3N0bmFtZSA6IFxyXG5cclxuU2VyaWFsIE51bWJlciA6ICBcclxuXHJcbkFmZmVjdGVkIEFwcGxpY2F0aW9uICA6IFxyXG5cclxuSXNzdWUgaW4gRGV0YWlscyAgIDpcclxuXHJcbkFkZGl0aW9uYWwgQ29tbWVudHMgOiAgLSBBbGVhc2UgYXR0YWNoZWQgc2NyZWVuc2hvdCAoIElmIGFueSkifQ%3D%3D
49 mailto:dw_623-mbrdi-proj_iti-wintel-team@mercedes-benz.com
50 https://iam-tools.iam.corpintra.net/emt/
51 https://gsep.daimler.com/confluence/display/GSEPUKB/Technical+%28TE%29+Account+in+GSEP#Technical(TE)AccountinGSEP-ChangetheCDpasswordoftheTechnicalAccount(forOIDC/PingID)
52 https://gsep-int.daimler.com/confluence/download/attachments/398623423/RE%20%20Technical%20account%20creation%20%200053890158%20.msg?api=v2&modificationDate=1597233816000&version=1
53 https://mbrdna.atlassian.net/servicedesk/customer/portal/1/group/1/create/1
54 mailto:ITHelpCenter@mbrdna.atlassian.net
55 https://gsep.daimler.com/confluence/display/GSEPUKB/Technical+%28TE%29+Account+in+GSEP#Technical(TE)AccountinGSEP-ChangetheCDpasswordoftheTechnicalAccount(forOIDC/PingID)

3.3.2 Additional Steps

3.3.2.1 Check/Edit the Technical Account Settings in EMT

Open EMT[56], e.g. from the App Station in Social Intranet EMT App @ Social Intrane[57]t.

- Then: Select "Modify" → My Entries → Choose "Technical Accounts" in the Dropdown → Press Search
- More info here: EMT Support Page[58]

Use this to extend/reduce the validity period of the account or to find the email address of the user.

You might see a hint in EMT "Password action necessary". To fix this, you have to reset the CD password[59] of the Technical Account.

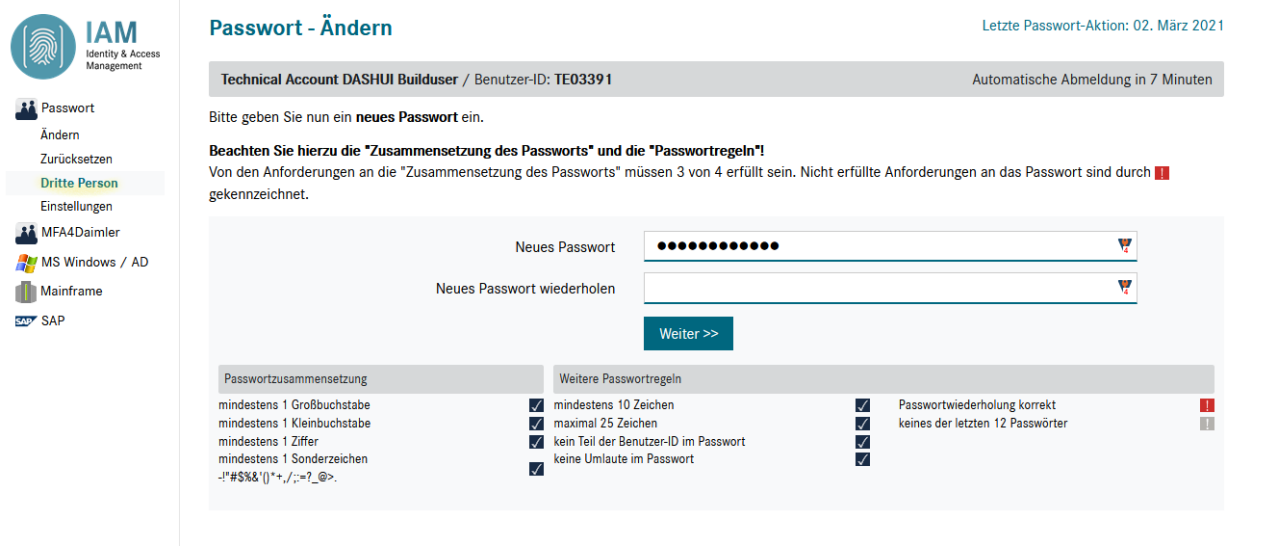
3.3.2.2 Change the CD password of the Technical Account (for OIDC/PingID)

> Newer Technical Accounts are created without the ability to change the CD password. It is not possible to use Single-Sign-On solutions on GSEP with these accounts.
> Such accounts can only be used for API access, using their GSEP password or by creating an access token like this: Generate user personal bitbucket access token[60].

You might see a hint in EMT "Password action necessary". To fix this as the owner of the Technical Account:

- Login to https://login.daimler.com/password/ with your personal ID (not the TE account!).
- Select "Password" from the menu on the left, then select "Third Person".
- Enter the user name and password of your personal ID (not the TE account!).
- Enter the user ID of your Technical Account and press Next.
- Set a new WIW password for the Technical Account:

56 https://iam-tools.iam.corpintra.net/emt/
57 https://social.intra.corpintra.net/apps/app-station?appId=604695
58 https://team.sp.wp.corpintra.net/sites/05389/IAMTools/EMT/SitePages/EMT.aspx
59 https://gsep.daimler.com/confluence/display/GSEPUKB/Technical+%28TE%29+Account+in+GSEP#Technical(TE)AccountinGSEP-ChangetheCDpasswordoftheTechnicalAccount(forOIDC/PingID)
60 https://gsep-int.daimler.com/confluence/display/GSEPUKB/Generate+user+personal+bitbucket+access+token



- If you encounter any problems, please contact WIW hotline (+49 711 1791233) to report the problem.
- You can also create a ticket via this link: https://support.iam.corpintra.net/tools/emt?issue=emt_notListed.

3.3.2.3 Access the email of a Technical Account

You can access the email using WebMail: https://webmail.wp.corpshared.net/owa, login with EMEA\TExxxxxx and the password you got from UHD.

It is not possible to read encrypted mails there!

You can add the email to your Outlook as an "Additional Mail account".

- Find the "Account settings" in Outlook under the "File" menu.
- Use the SMTP address of your TE user (@@mercedes-benz.com[61]) which is listed in EMT, see above.
- Follow this (outdated) description: https://team.sp.wp.corpintra.net/sites/01223/en/DocumentsNWP/Guideline%20for%20Pool%20IDs%20and%20NPMs.pdf
- Please remember to restart Outlook after the addition: Outlook will then ask for the EMEA/Windows ID and the Windows password of the TE user.

You should be able to read encrypted mails for the TE user within Outlook!

3.3.2.4 Request roles for Technical Account in ZULA

You can request and remove application roles in ZULA in the same way as you do for personal accounts (internals, externals, suppliers etc.). Contacting GSEP support is not required for this.

- In ZULA, please select the "Technical ID" user type on the right when you create your request.
- More Info here: How to request new permissions for GSEP projects in ZULA+?(see page 69)

3.3.2.5 Get a GSEP password for a Technical Account

Technical accounts do **not** get an initial mail with password and certificate, as the owner already has GSEP access.

61 http://mercedes-benz.com

- To get the password, open the password reset page[62] on Crowd and complete the "I have forgotten my password" form.
  Important: Enter the exact TExxxx user account name! Do **not** add blanks before and after!
- The mailbox of the TE user will get an email with a password reset link. Open the link in your browser and set a new password.

To verify, go to the Crowd: My profile[63] page, log out from your current user and log in as your TE user.

3.3.2.6 Get a certificate for a Technical Account

Within the Daimler Network DCN (IP53.*), a GSEP ALM client certificate **is not required** to communicate with GSEP applications.

If you need a certificate to access GSEP from the internet, please explain your demand and request an ALM certificate for the TE account from **GSEP Support.**

The certificate will be sent to the account owner in an encrypted email.

Later, you can have that email resent to you by following these instructions. Log in with your personal account (TE account owner): How to retrieve my GSEP ALM Certificate?(see page 21)

Note: Use one of the following links to report any GSEP Incident & Inquiry/help - MBAG Webticket (ITSM)[64], DTAG Webticket (JSM)[65] & Suppliers Webticket (CSM)[66]

ⓘ Please follow the links on https://gsep.daimler.com/ to create GSEP support tickets or go to the UKB How to get help[67] page.

3.3.2.7 Ensure the password does not expire and does not get locked

If you use the TE in a CI/CD tool chain, you might ensure the password does not expire (normally after 90 days).

- Use a very long and random password for the TE (see FAQ below).
- Contact GSEP support to disable the password expiry of the TE (extend it to 31.12.2050, but GSEP support will probably only allow using the same password for a year.)

The account will still be locked if a wrong password is used multiple times to login. This lock might break your CI/CD tool chain. This is a security feature: This way, it is not possible to hack the account.

There might be situations where you are locked out if some of your servers (or test user, or local git) use the old password - this will be the most frequent cause for such problems. Keep a list of servers where you use the user/password and use different TE users for development and production use. By handling your passwords and setups with care, you will be able to prevent such account locks.

If the account is locked, please contact GSEP support and request a **reset without password change.**

3.3.3 FAQ

Q: What is a Technical Account?

---

62 https://gsep.daimler.com/crowd/console/login.action#/forgot-password
63 https://gsep.daimler.com/crowd/console/user/viewprofile.action
64 https://daimler.service-now.com/sp?id=sc_cat_item&sys_id=062eec1f1b0c605093b43113dd4bcbf0&sysparm_category=c68bd6491bd10410f826bb31dd4bcbb5
65 https://gsep.daimler.com/servicedesk/servicedesk/customer/portal/261
66 https://digitalservices.mercedes-benz.com/
67 https://gsep.daimler.com/confluence/x/tCdKI

A: In the context of Daimler IT systems and services, an Technical Account (also known as System Account) meets the following conditions:

- A Technical Account is an account used exclusively for communication between IT systems (machine-machine communication).
- Use of a Technical Account by humans is not allowed (this includes administrative tasks).
- There is always an internal employee (= Account Owner, Data Administration) responsible for the Technical Account.
- If the Technical Account has privileged rights or accesses secret, confidential or integrity critical data, the Technical Account must be managed in EMT.

Official definition of a technical account

Official Name	**Naming Scheme**	**Password Policy in Active Directory (AD)**	**Validity**	**Authentication**	**Created in**	**Mailbox**	**Login to Portal**	**Purpose**
Technical Account	**TE** *****	PW expires after max. 5 years	extension once a year via EMT	CD & AD	**CD & AD**	without or **with Mailbox** (for GSEP: with Mailbox)	No	Technical CD-User for interfaces that need Authentication via CD.

Every TE account has an Owner and a Deputy who are allowed to manage the account. The account must be extended in EMT every year.

Q: Can this TE##### account be used to log into the GSEP website?

A: Technically yes, but a TE##### account is **not** for personal use. Please login only with a personal account.

Technical accounts are intended for non-interactive system processes e.g. machine to machine communication, e.g. using an API.

Q: Can I reset the password of the Technical Account?

A: Yes.

- CD/WIW password: Use the "third person" password reset at https://login.daimler.com/password/other-person, login as your personal user (not the TE user).
- Windows/EMEA password:
  - Send an email/ticket to your UHD to request a password reset (Important: make it very clear it is not about your personal user, but the TExxxxx user).
    It is NOT possible to reset the Windows password via https://login.daimler.com/password/ad
- You can change and reset the GSEP password of a technical account in the same way as any other GSEP account: GSEP Password Reset(see page 40)

Q: Can I change the email address for the Technical Account?

A: Please contact your ITK/UHD for this. In EMEA and most other locations, the email address is generated and it is not possible to use an address that already exists (e.g. not your own and not a supplier-provided email

address).

Q: Where can I ask more questions about TE##### accounts?

A: Ask your local IT Team (ITK/UHD).

3.4 Pool ID in GSEP - Creation and Management

No longer supported, please use this new account type → Technical (TE) Account in GSEP[68]
In general, it is not possible to request GSEP project access for PoolIDs in ZULA!

RD defines the allowed usage scenarios for Pool IDs here https://social.cloud.corpintra.net/docs/DOC-401636 (DE). This includes "test accounts for application tests", but GSEP does not allow pool ids today due to this policy below. I see a small gap in the GSEP rules when the pool id would be used only on test data (non-confidential). Still, we do not allow Pool IDs, and as a TE user cannot use MFA login, GUI automation is very limited in GSEP.

IT IS NOT ALLOWED TO USE POOL IDs IN GSEP!

See Policy A22: https://erd.app.corpintra.net/ERD/Home/RuleProfile/85125

5.3.2.17. Non-privileged non-personalized user accounts must only be used if:

- accountability for the particular business process does not require the distinction of the individual user and usage of personalized user accounts is not feasible
- they do not have administrative rights,
- they do not access information that is classified as secret or confidential and do not modify integrity-critical information

68 https://gsep.daimler.com/confluence/x/v4LCFw

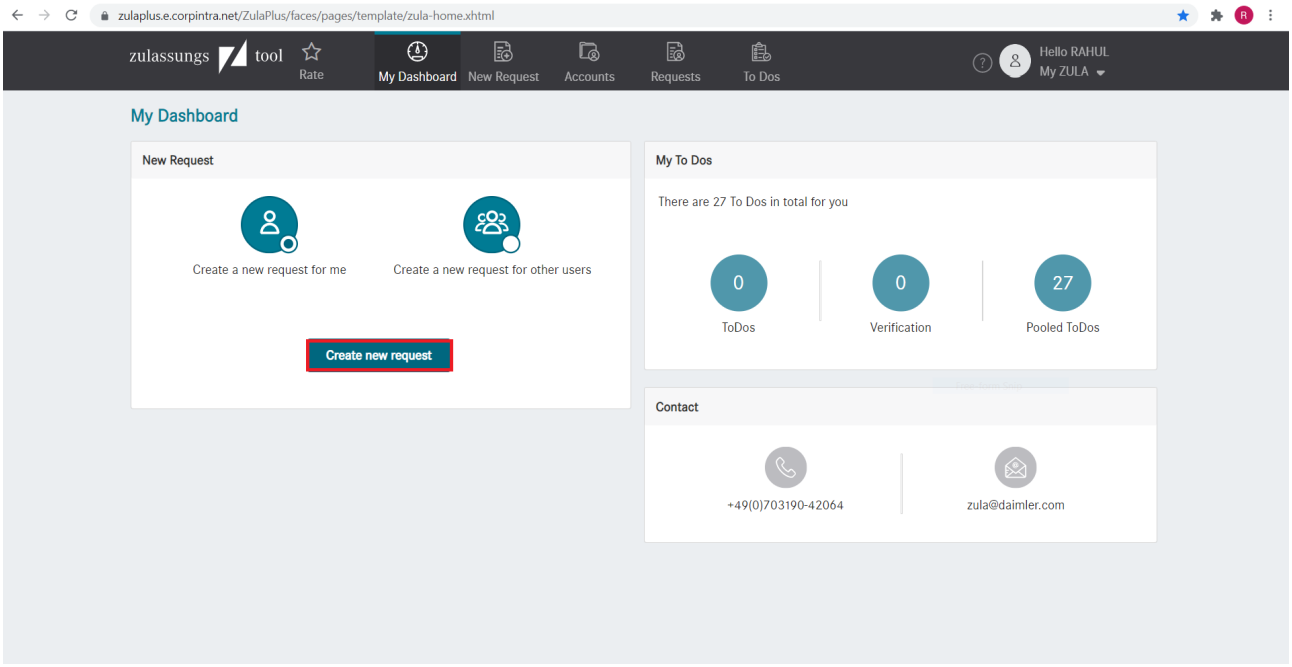
4 Access Management in ZULA

4.1 GSEP SANDBOX Access Approval Process

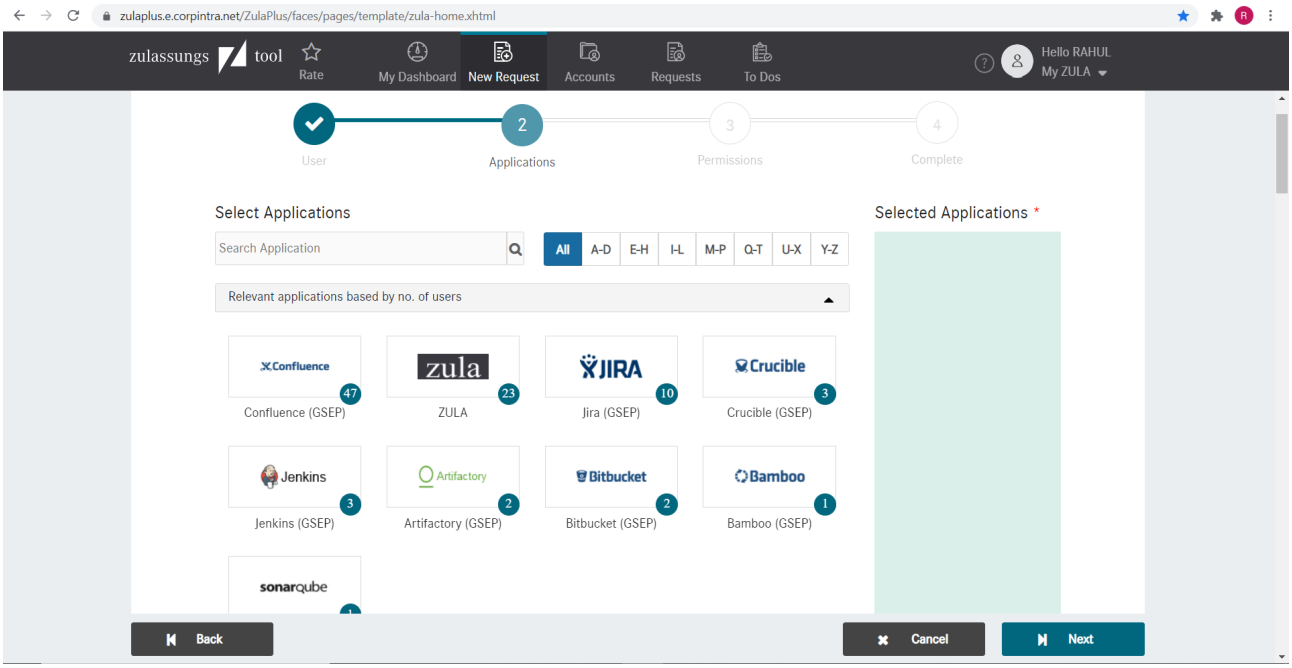
Please follow the below guide to request access for "**SANDBOX**" Project for GSEP Applications in Zula.

Zula Link : https://zulaplus.e.corpintra.net/ZulaPlus/faces/pages/template/zula-home.xhtml

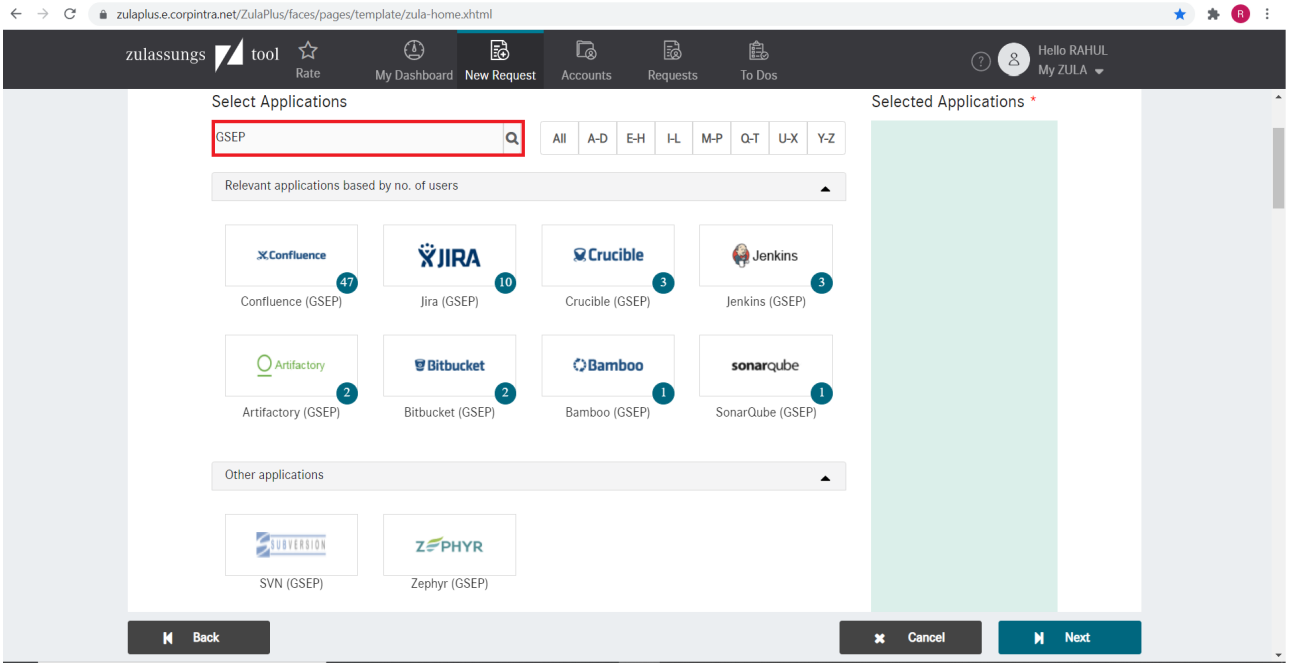
Step 1: Create a new request.



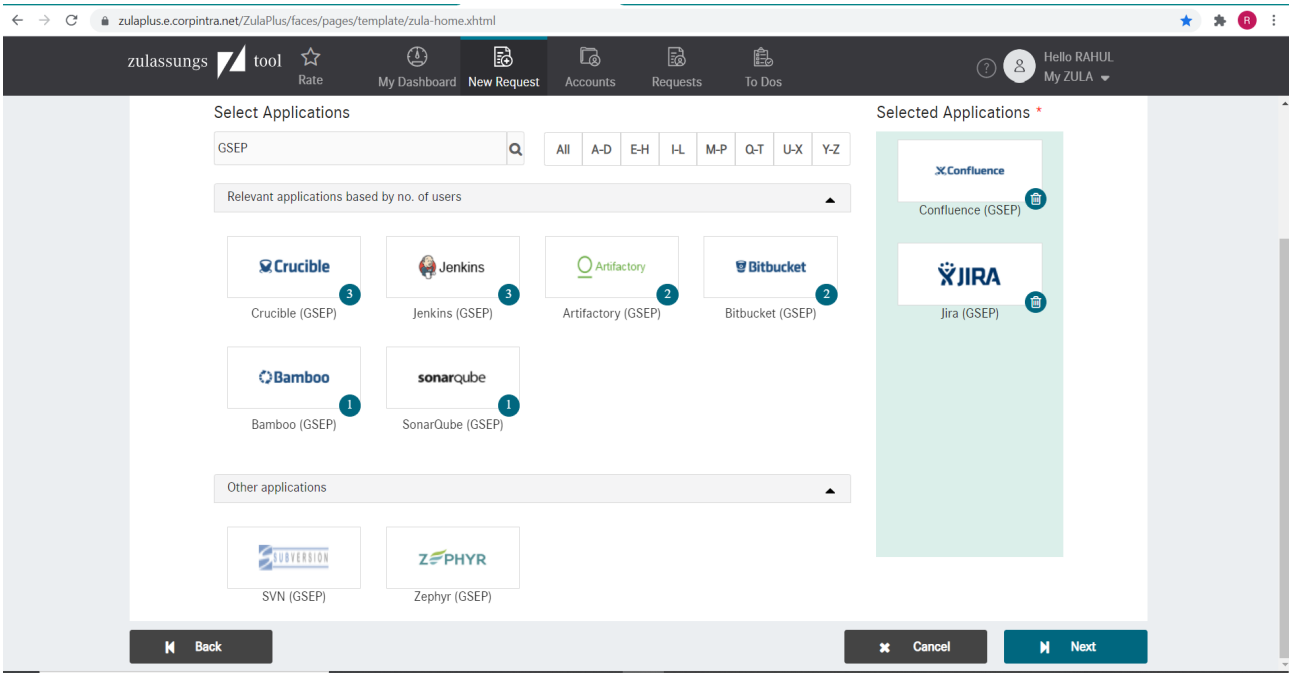
Step 2:You are presented with a list of all applications for that permissions that can be requested.



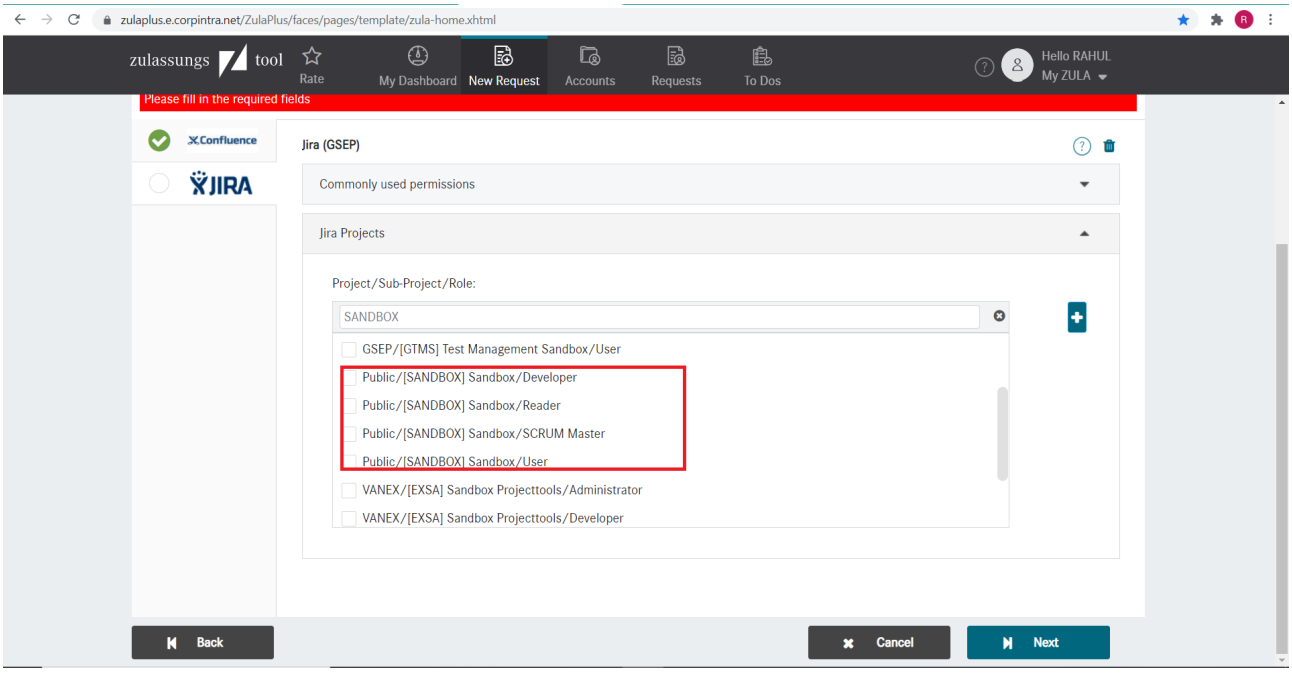
Step 3: Add "GSEP" to the search box and click the magnifying glass icon to filter all GSEP applications.



Step 4: Add all necessary applications to your shopping basket.



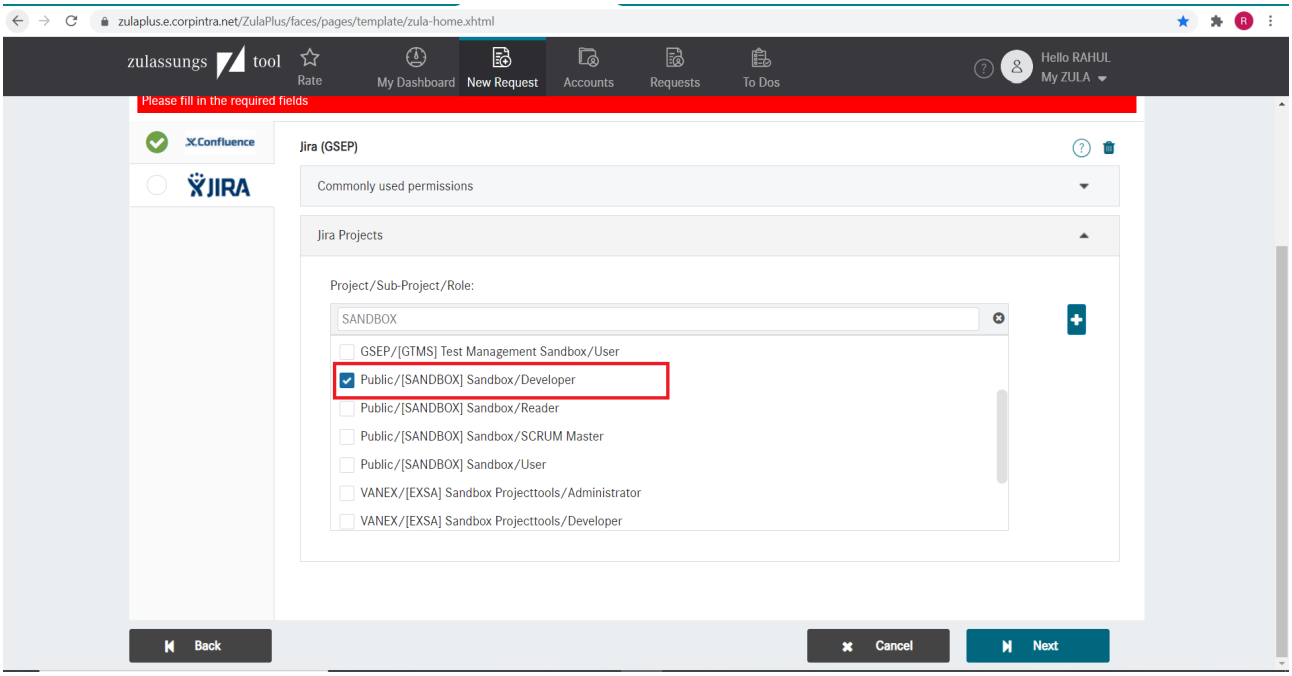
Step 5: Search for the SANDBOX project in the search box for each application.



Step 6: Select the necessary permissions for SANDBOX project.

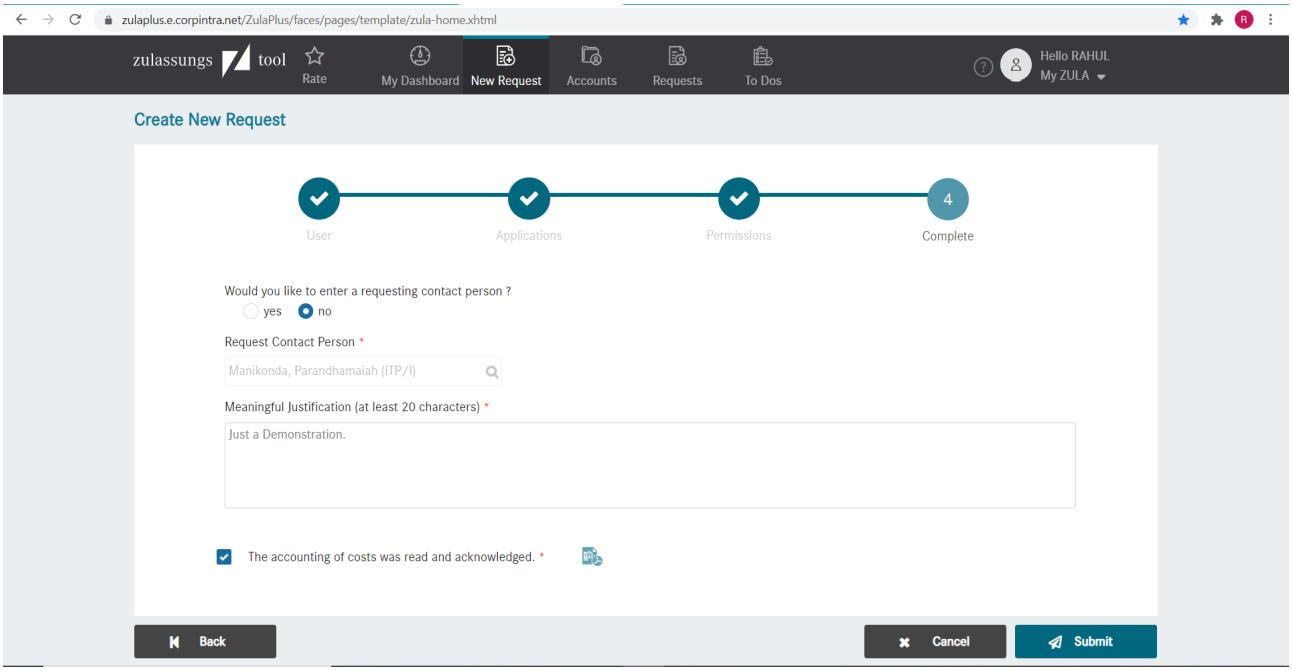
You can find the current permission matrix for all our applications at https://team.sp.wp.corpintra.net/sites/03009/General%20Information/GSEP_Permission-Matrix.xlsx?Web=1

After adding the necessary permissions for all selected applications please go to the next page via the "Next" button.



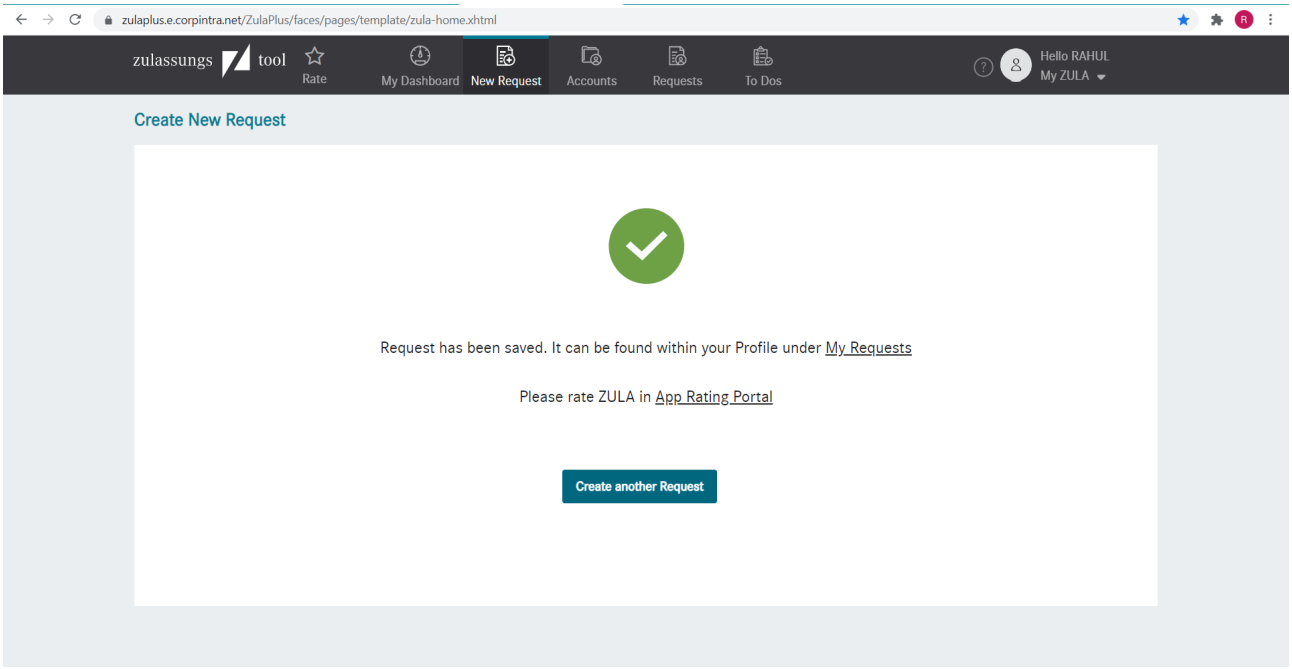
Step 7: Don't forget to add your request justification (at least 20 letters) along with the name of the contact person if needed.

In the bottom select the checkbox just to confirm the cost associated with the GSEP Application and submit the request.



Step 9: Your request is sent to the project approver and you can view the status of your Zula request within your Profile under My Request.

After the approval your permissions will be automatically granted and you will have access to the "SANDBOX" Project in the chosen tools.



Step 10: Start working.

4.2 How to delegate the “Request Decisions” in Zula

This document describes about, how to enable Zula Delegate to Approve the Zula Requests on Behalf of Zula Approver.

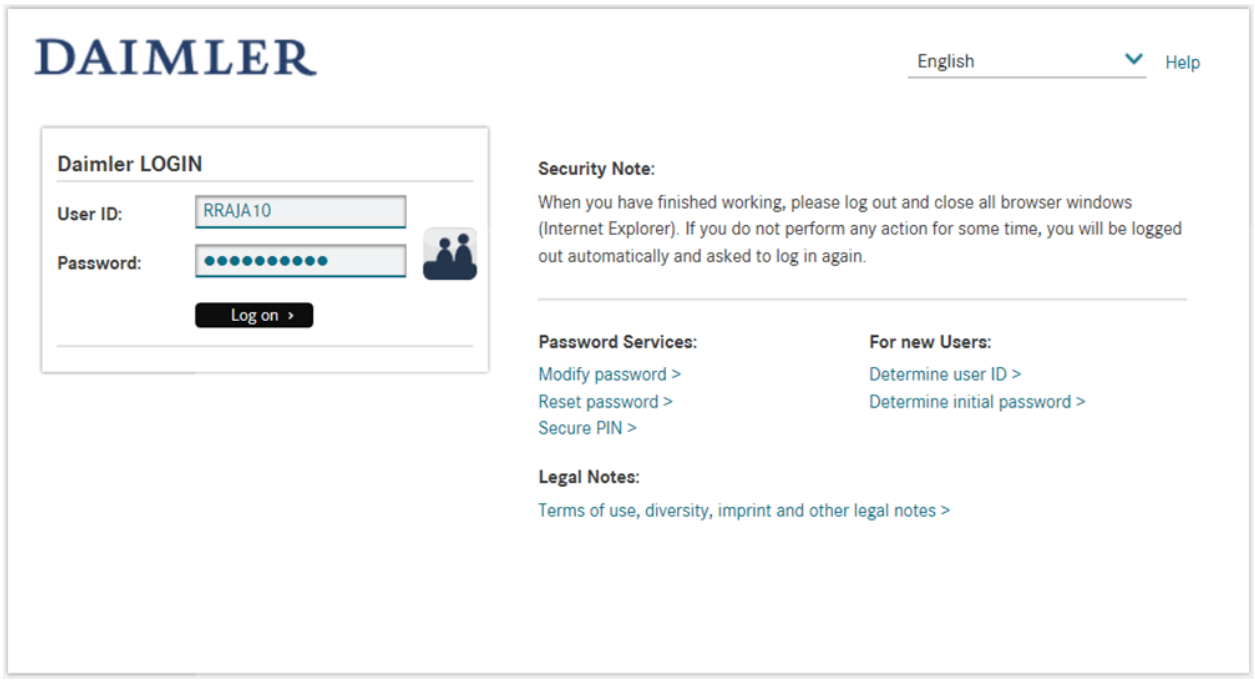
Prerequisites:-

The Authority/Deputized (E4/E5 Manager) of the project should be an existing approver to approve the access requests in Zula.

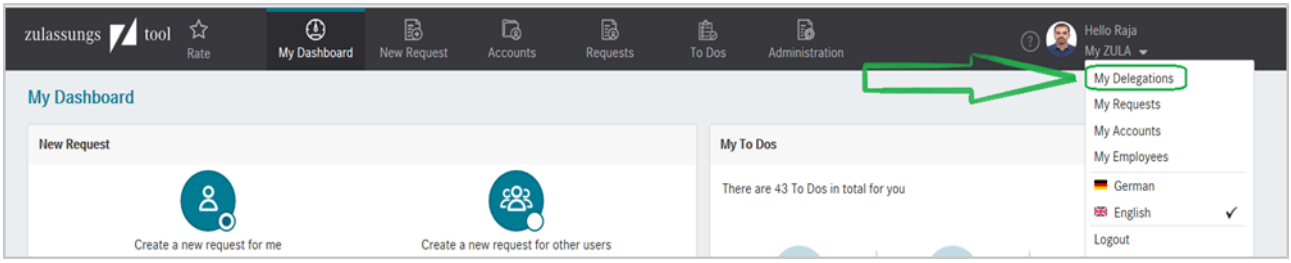
Way of Solution

Step 1: - Login into Zulaplus thru à Link[69]

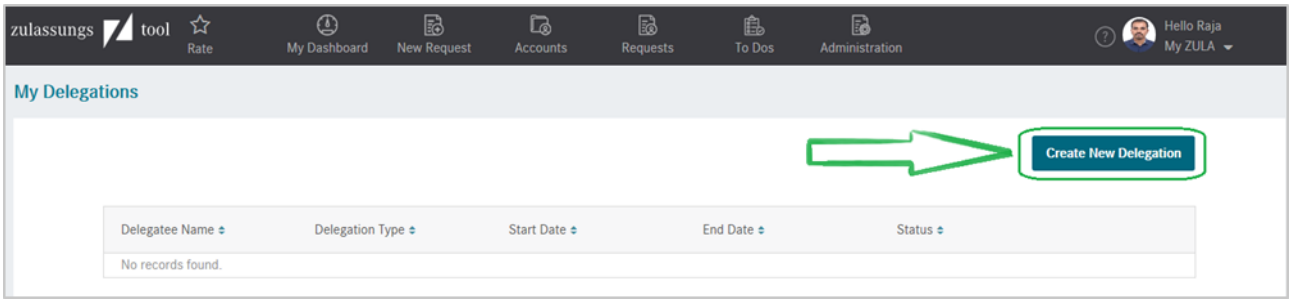
69 https://zulaplus.e.corpintra.net/ZulaPlus/faces/pages/template/zula-home.xhtml



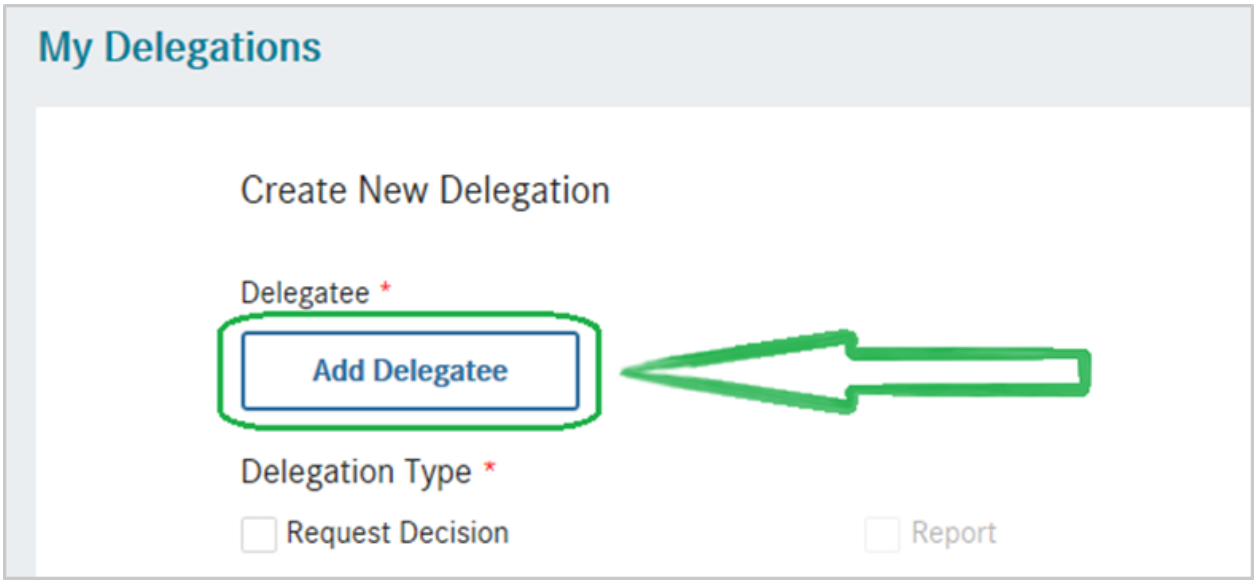
Step 2: - Please select **My Delegations** as shown in the below image.



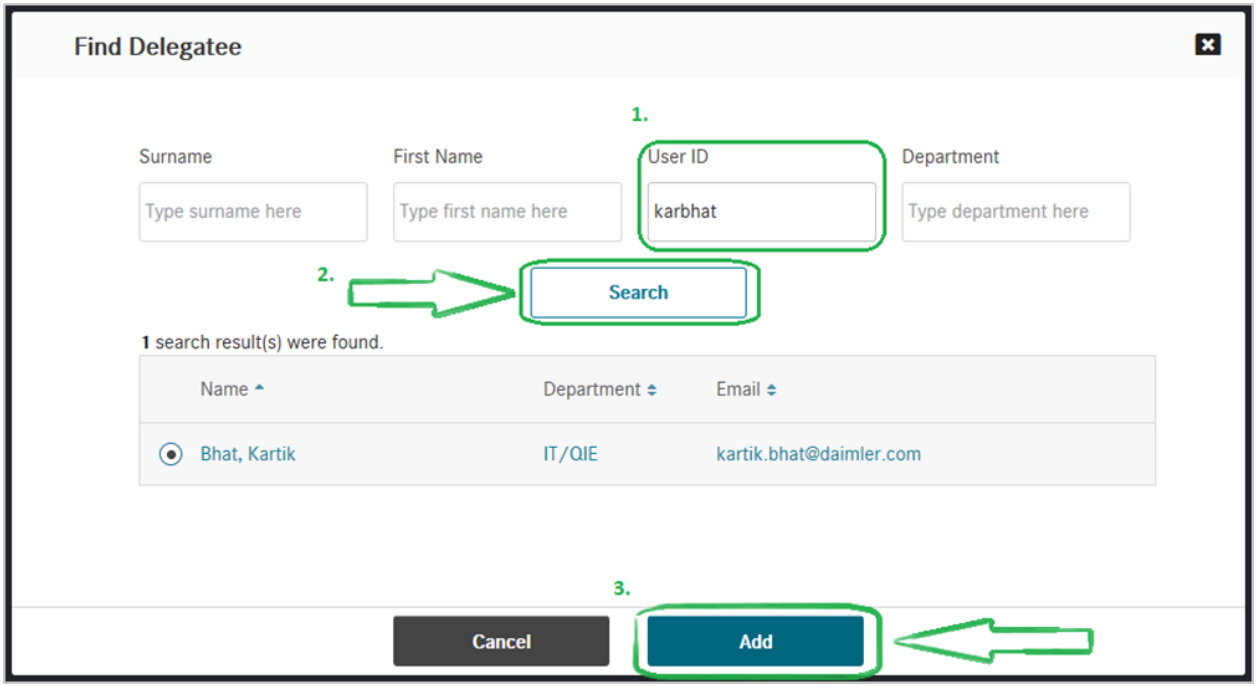
Step 3: - Click on **Create New Delegation** as shown in the below image.



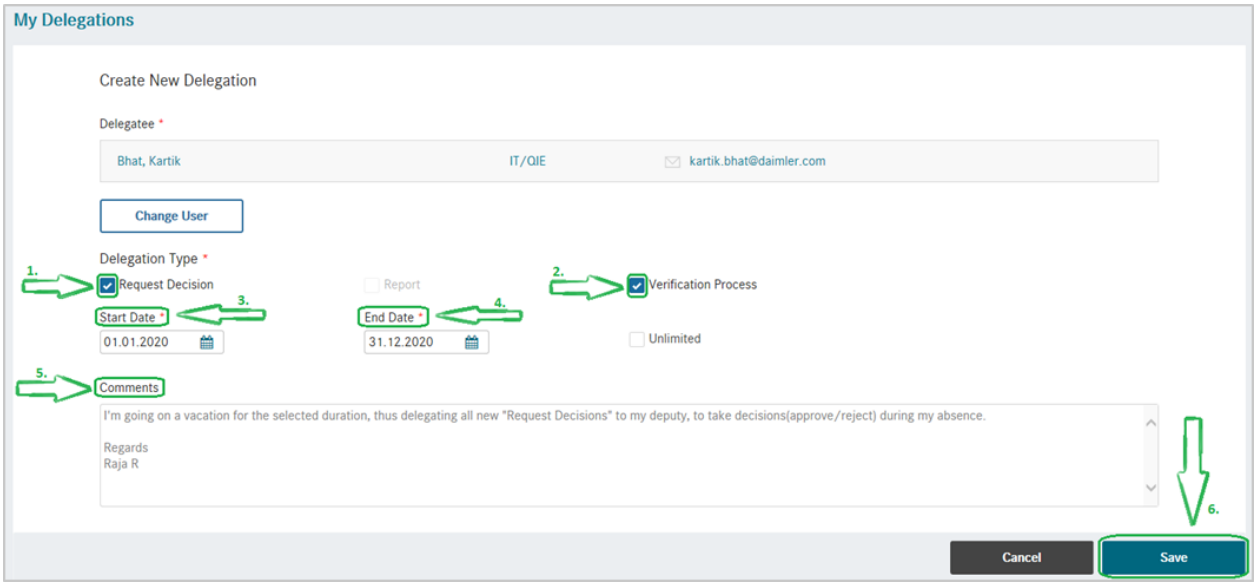
Step 4: - Click on **Add Delegatee**.



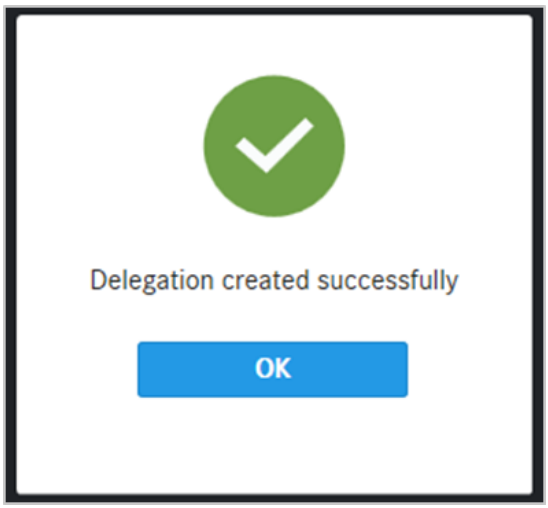
Step 5: - Enter the Delegatee's **User ID**, **Search** & **Add** it as shown in the below image.



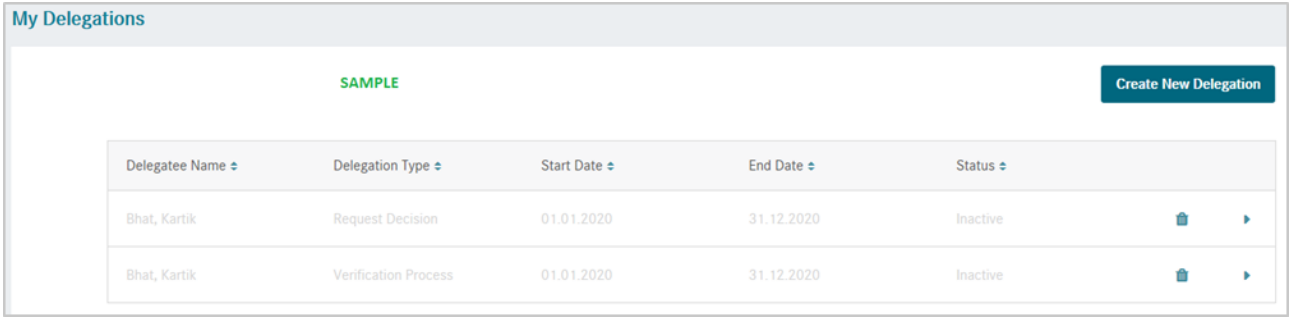
Step 6: - Choose the **Duration** you wanted your delegatee to approve the Zula requests on behalf of you, select the **Delegation Type** & click on the **Save** button as shown in the below image.



Step 7: - **Delegation created successfully**.



Step 8: - Now the Delegatee can approve the Zula requests on behalf of the Primary Zula Approver.



Note: Only the new requests can be approved by the Delegate, old requests(which was already awaiting for the approval in Primary Approver's queue cannot be visible in Delegate's list to approve the requests).

4.2.1 **Only Intranet users can open this link..**

4.3 How to Delete/Cancel GSEP Accesses

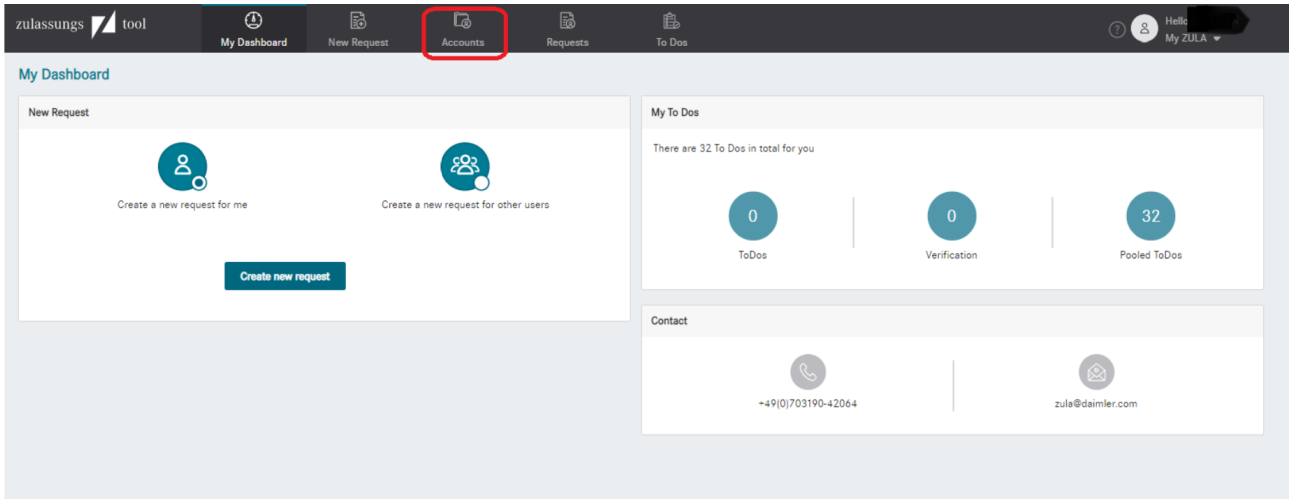
All rights are managed in ZULA:
https://zulaplus.e.corpintra.net/ZulaPlus/faces/pages/template/zula-home.xhtml

By using three methods, we can revoke/remove the access.

1. The approver of your project can remove/revoke rights from users in ZULA only if he has raised a access request before on behalf of that user.
2. The user himself can also remove/revoke his own rights in ZULA.
3. If you would like to remove accesses/delete a user account for someone else who had left your project or the organization, submit a GSEP Incident.
   *Use one of the following links to report any GSEP Incident & Inquiry/help - MBAG Webticket(ITSM)[70], DTAG Webticket (JSM)[71] & Suppliers Webticket (CSM)[72]
   ⓘ Please follow the links on https://gsep.daimler.com/ to create GSEP support tickets or to open the UKB "How to get help"[73] page.

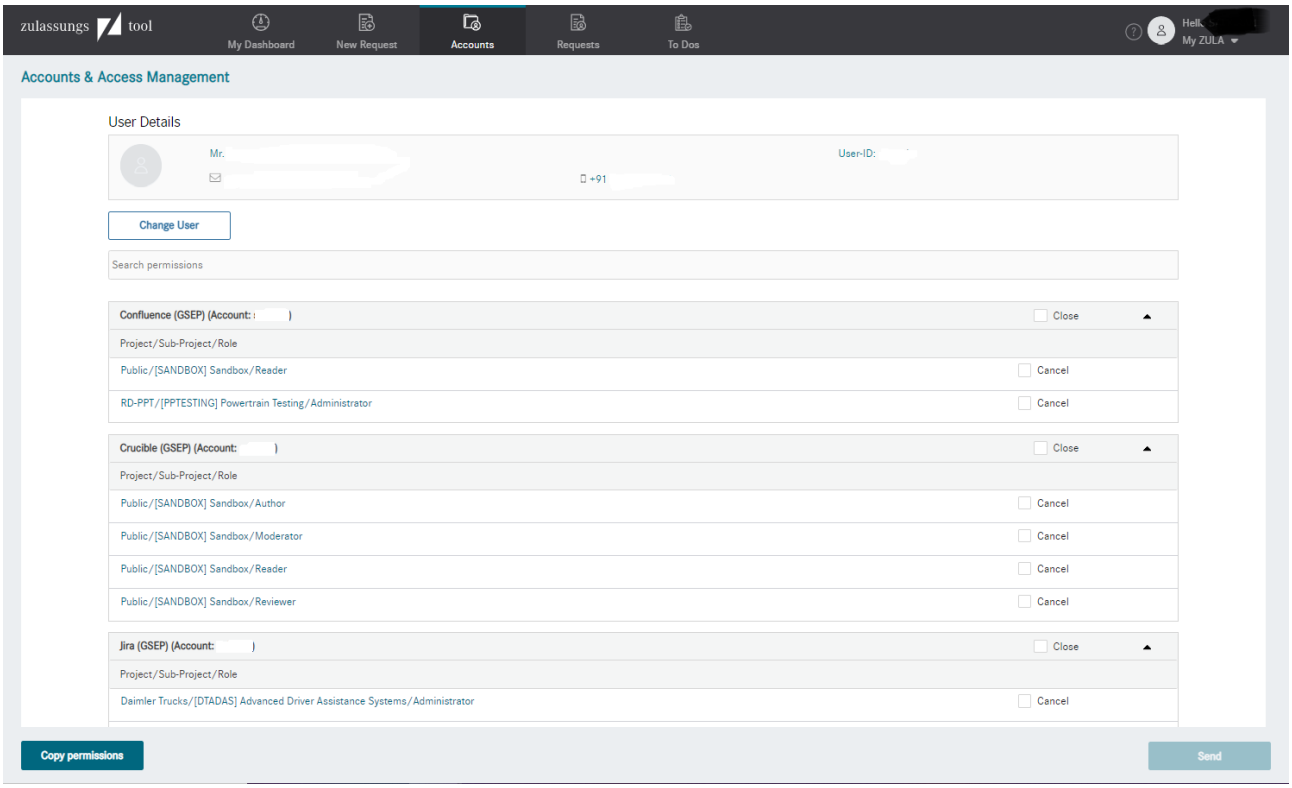
Below process shows that, how user himself can remove his own rights in ZULA.

Step-1:- We have to login into Zula Tool and click on "Accounts" option.

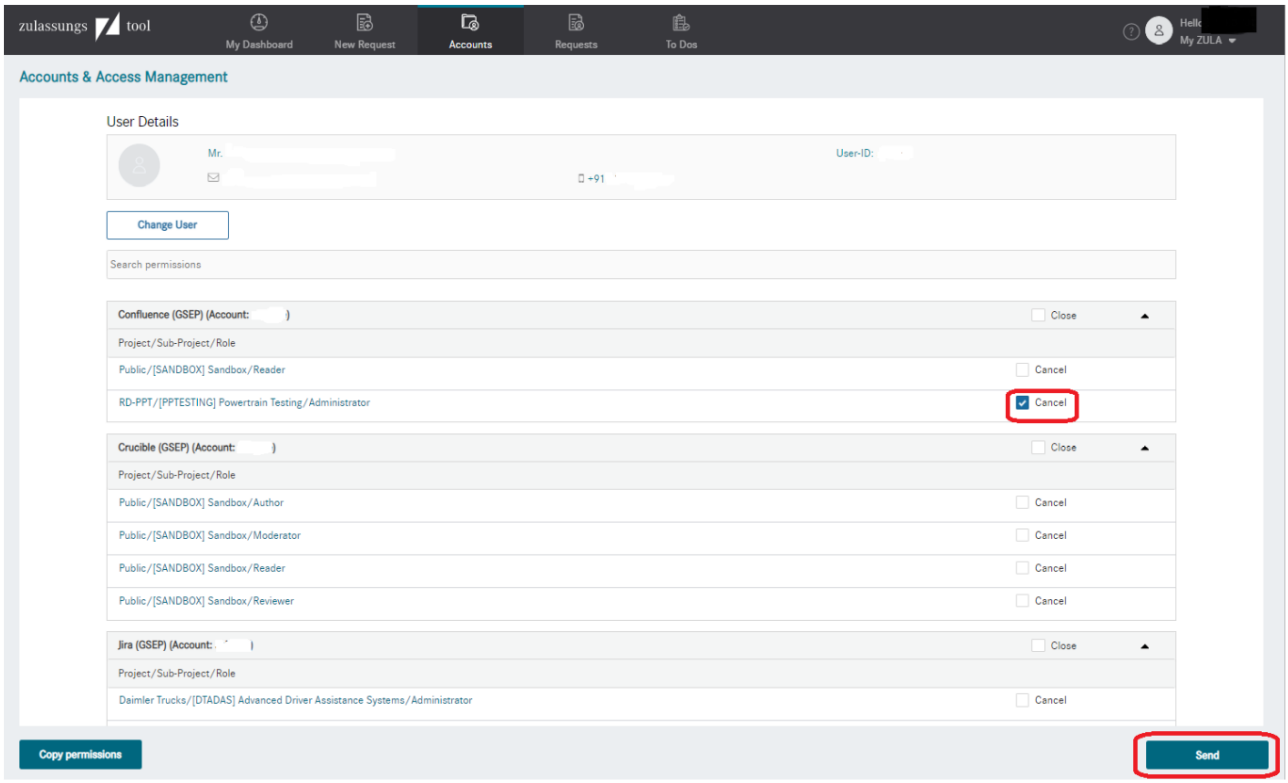


70 https://servicenow.i.mercedes-benz.com/esc?id=sc_cat_item&sys_id=062eec1f1b0c605093b43113dd4bcbf0
71 https://gsep.daimler.com/servicedesk/servicedesk/customer/portal/261
72 https://digitalservices.mercedes-benz.com/
73 https://gsep.daimler.com/confluence/x/tCdKI

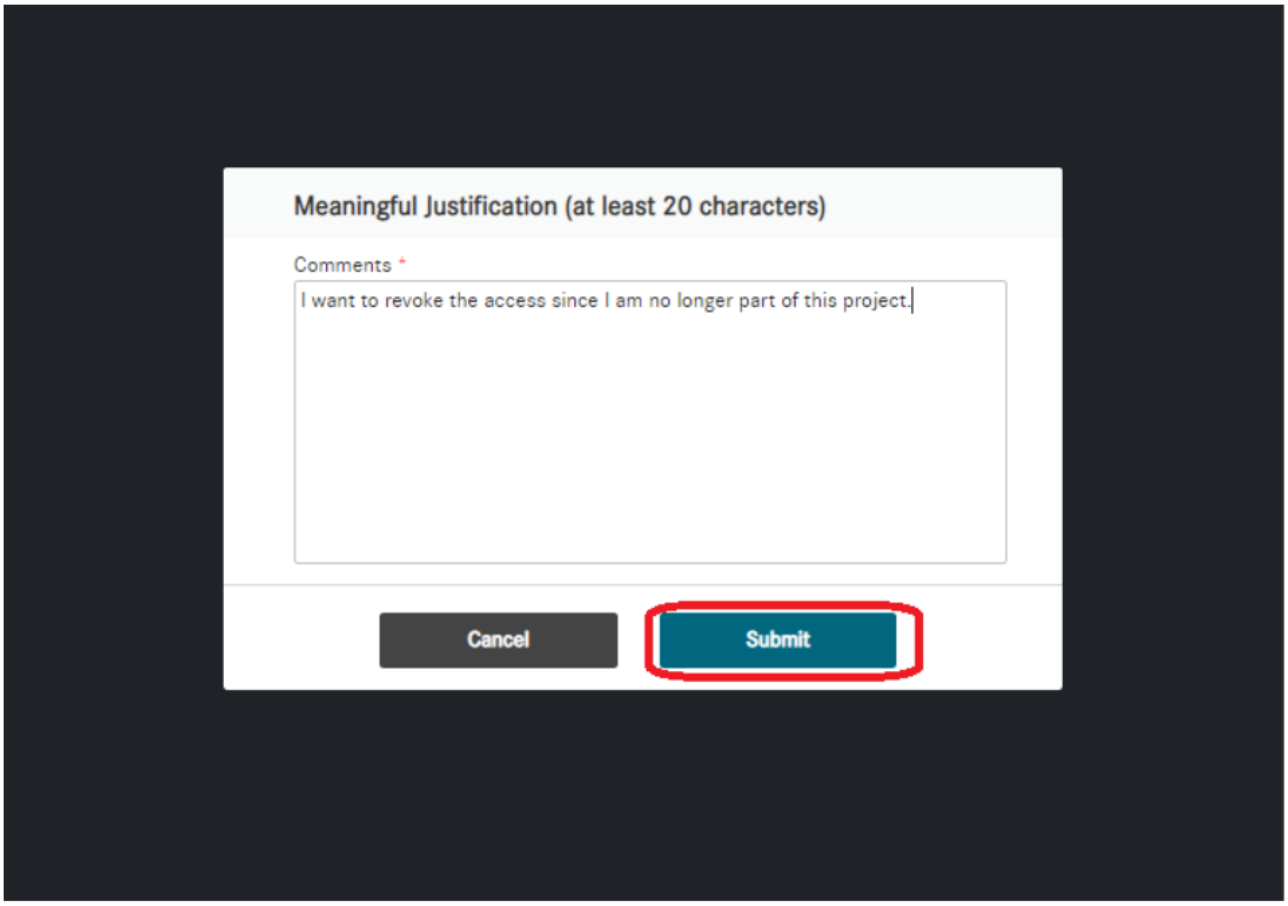
Step-2:- Then it will show the list of access that currently we have.



Step-3:- For example if we want to remove admin access for the Confluence Project(PPTESTING), Then you need to select the "Cancel" check-box or click on “Close” to close the account i.e. specific to the applications and click on "Send" option as below.



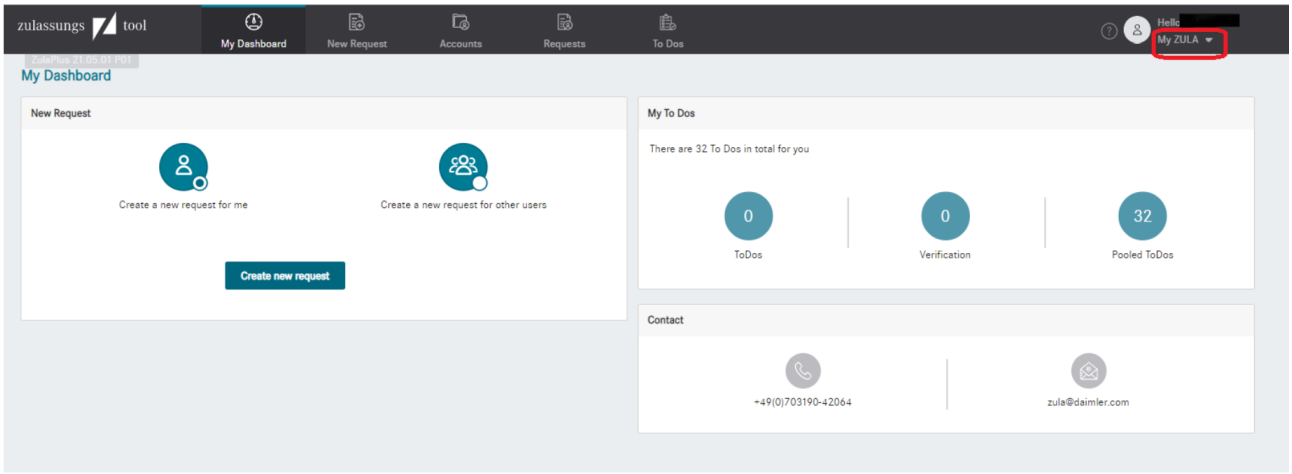
Step-4:- Then new window will pop-up/open's as below and asks us to enter the Justification for removal/revoke of access. After entering the justification click on Submit.



Step-5:- Then access for the requested project will be revoked/removed.

<u>If we are a manager then we can remove/delete the accesses of your employee by just one click via Zulaplus Portal</u>

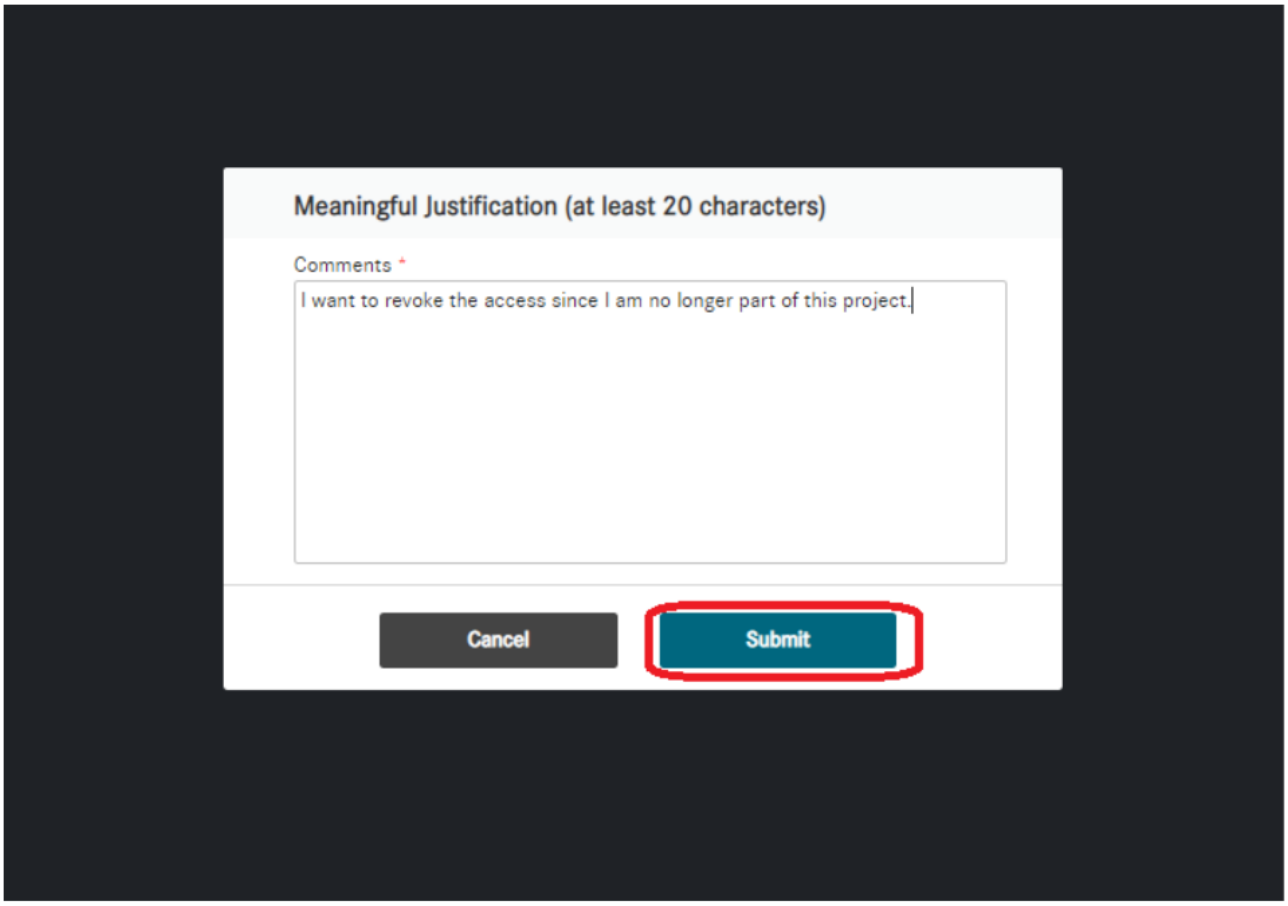
Step-1:- We have to click on “My Zula” on the top right corner on the portal as show in below image.



Step-2:- We have to click on “Manage Employees” option from the drop down. Where it will show you the user's with role of access he has access for project.

Step-3:- Then we have to select the user account to execute access removal/account deletion. Remember we can only revoke/remove for whom we have already raised a request on behalf of them.

Step-4:- Then new window will pop-up/open's as below and asks us to enter the Justification for removal/revoke of access. After entering the justification click on Submit.



Note:-

- A user is offboarded when he has no rights in GSEP anymore.
- At this moment, there will be no costs for the former GSEP user.

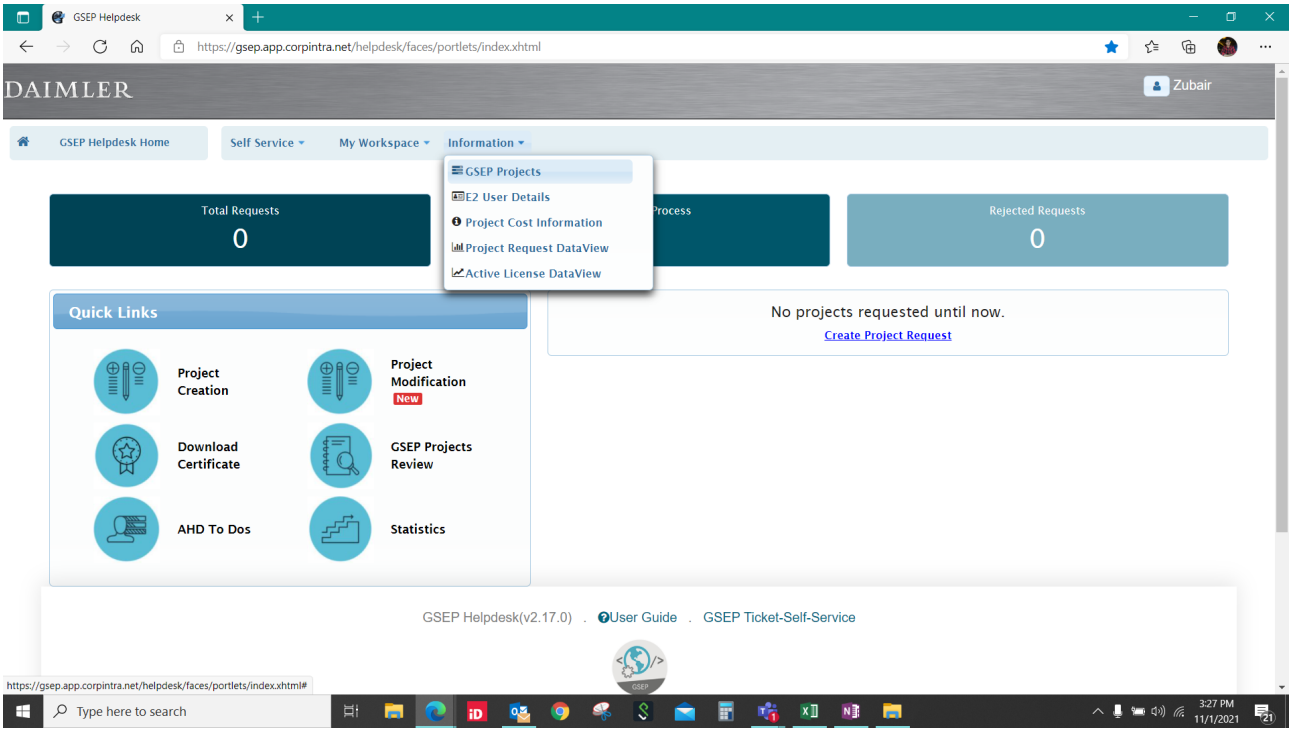
ServiceNow KB article - KB0349943[74]

4.4 How to find the ZULA Approver

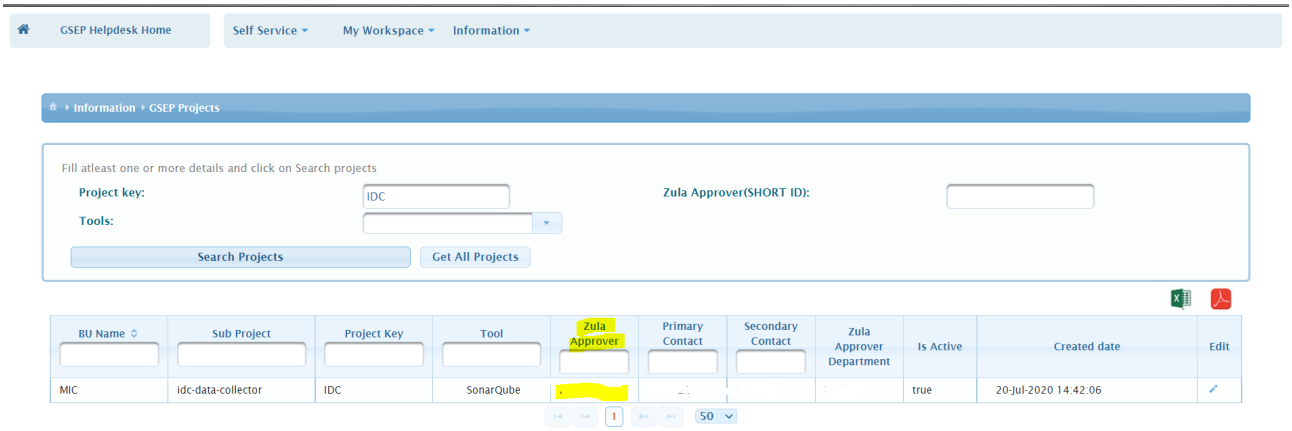
For every project in GSEP details like the Admin, Deputy Admin, ZULA Approver is provided in the GSEP Helpdesk (corpintra.net)[75]. Please follow the below mentioned steps to find the ZULA Approver.

- Click on GSEP Helpdesk (corpintra.net)[76] , and navigate to Information > GSEP Projects.

74 https://servicenow.i.mercedes-benz.com/esc?id=kb_article&table=kb_knowledge&sys_kb_id=158377671b7099101d67a7953b4bcb84
75 https://gsep.app.corpintra.net/helpdesk/faces/portlets/index.xhtml
76 https://gsep.app.corpintra.net/helpdesk/faces/portlets/index.xhtml



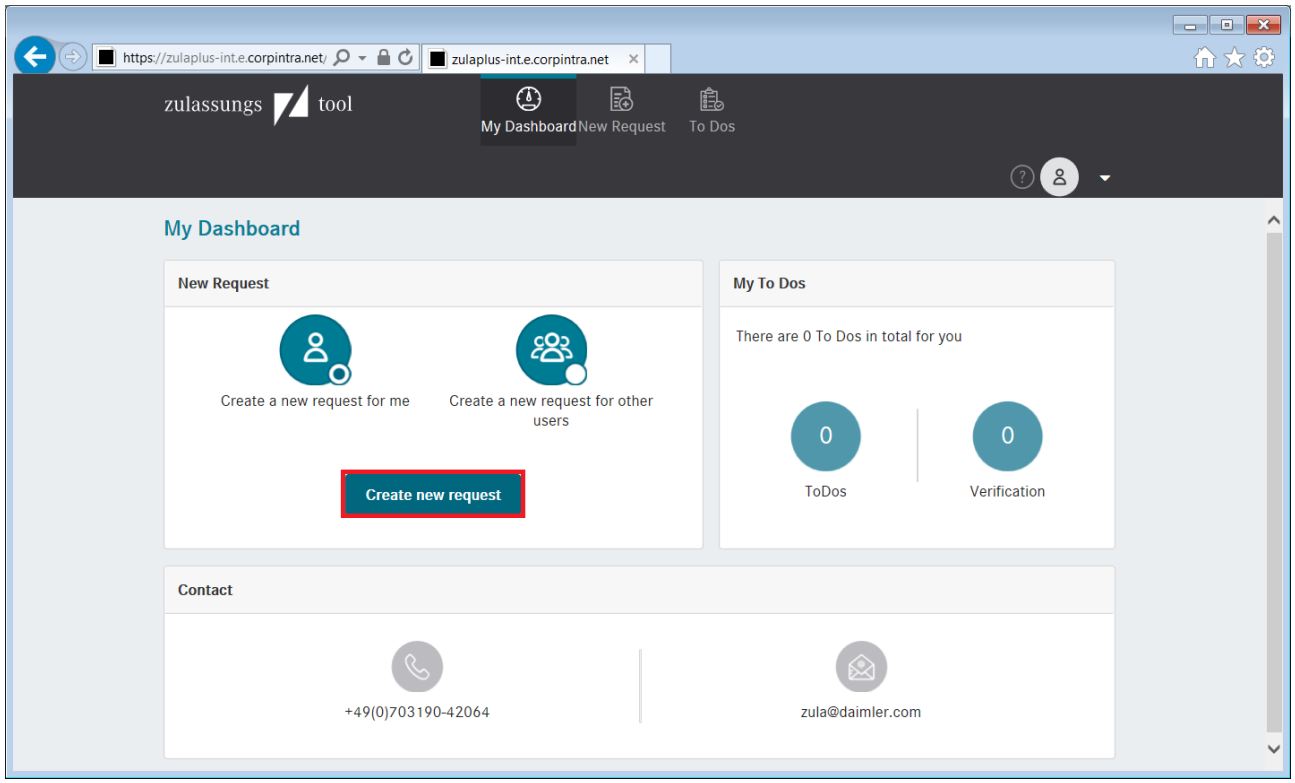
- Enter the Project Key Details and Click on Search Projects. The search results will display the ZULA Approver details.



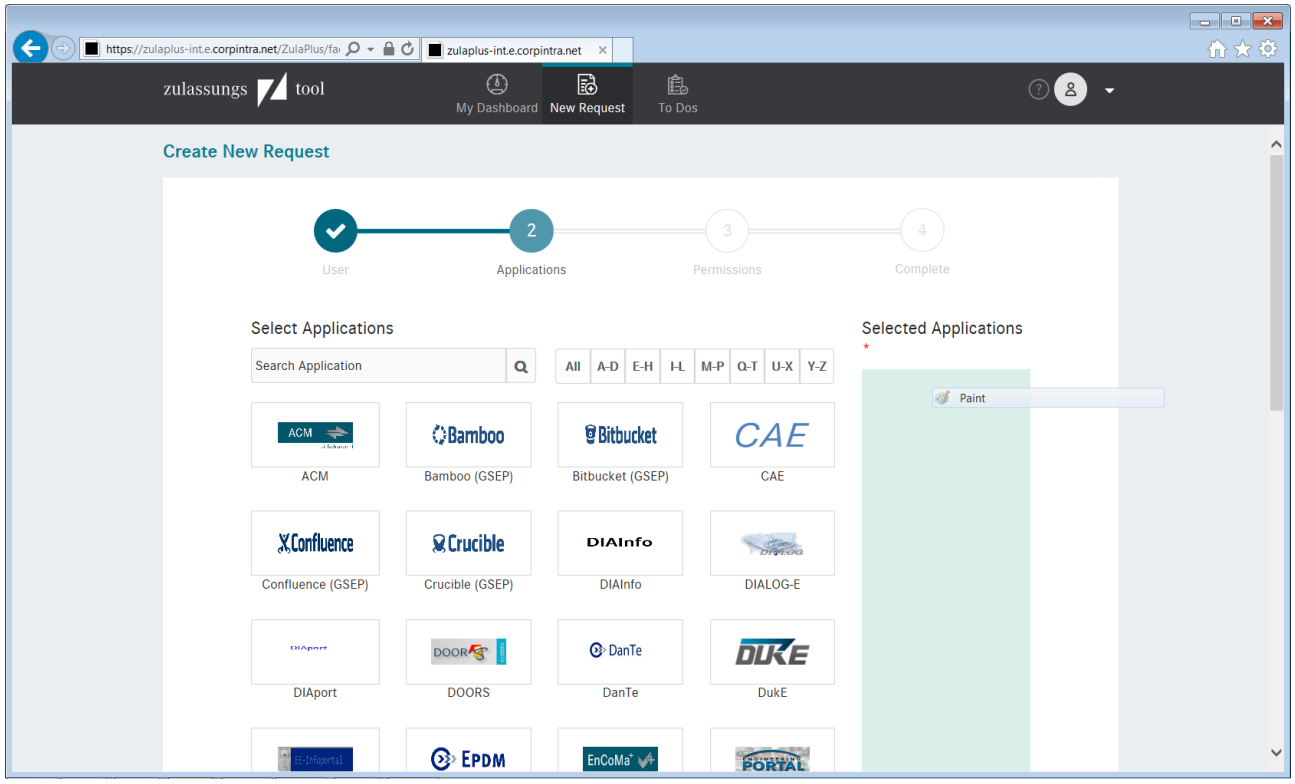
4.5 How to request new permissions for GSEP projects in ZULA+?

On 26.04.2018 the Zulassungstool (Zula) was relaunched with a new user interface. Please follow the guide below to request new permissions for GSEP projects at https://zulaplus.e.corpintra.net/ZulaPlus/faces/pages/template/zula-home.xhtml

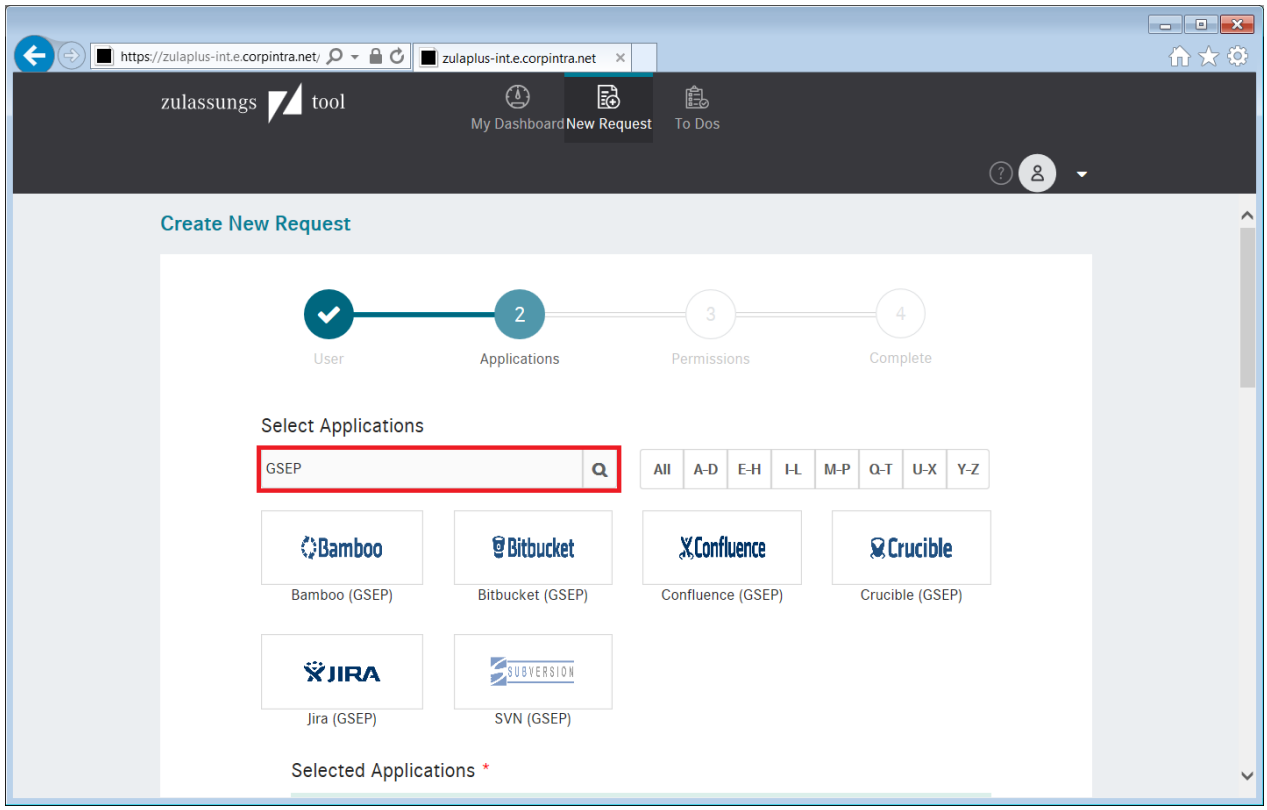
Step 1: Create a new request.



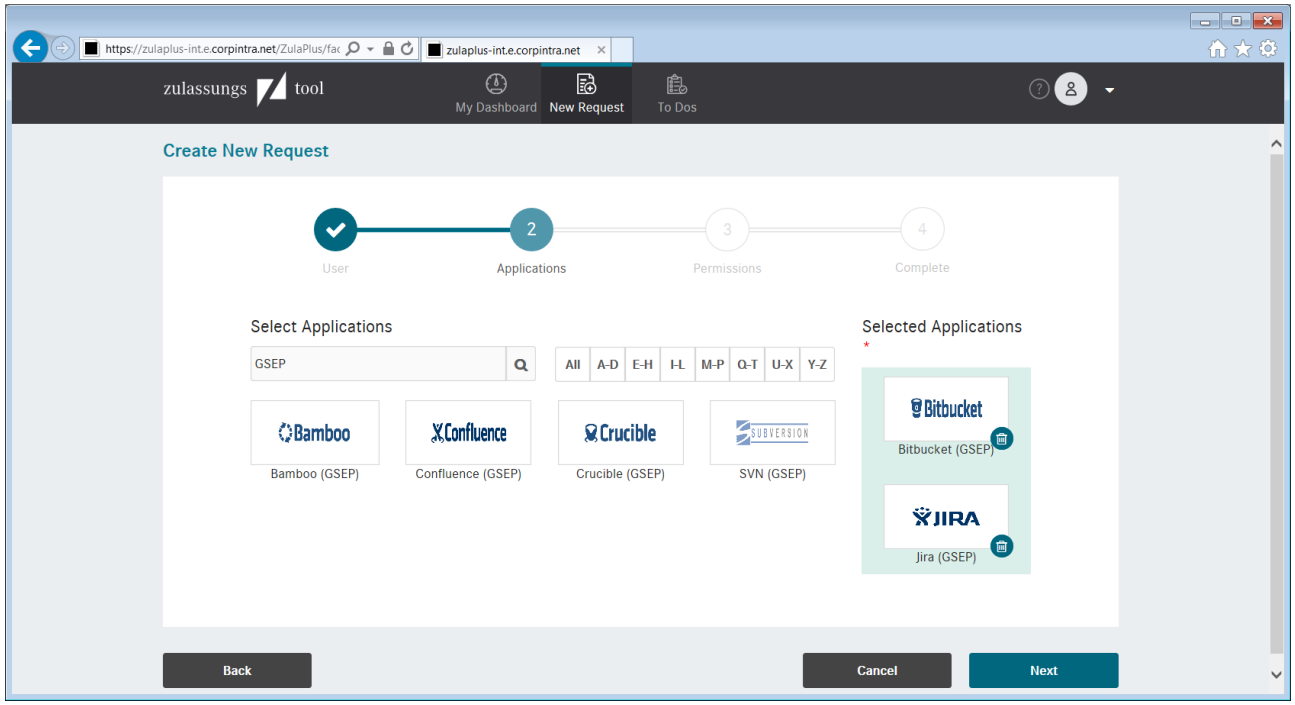
Step 2:You are presented with a list of all applications for that permissions that can be requested.



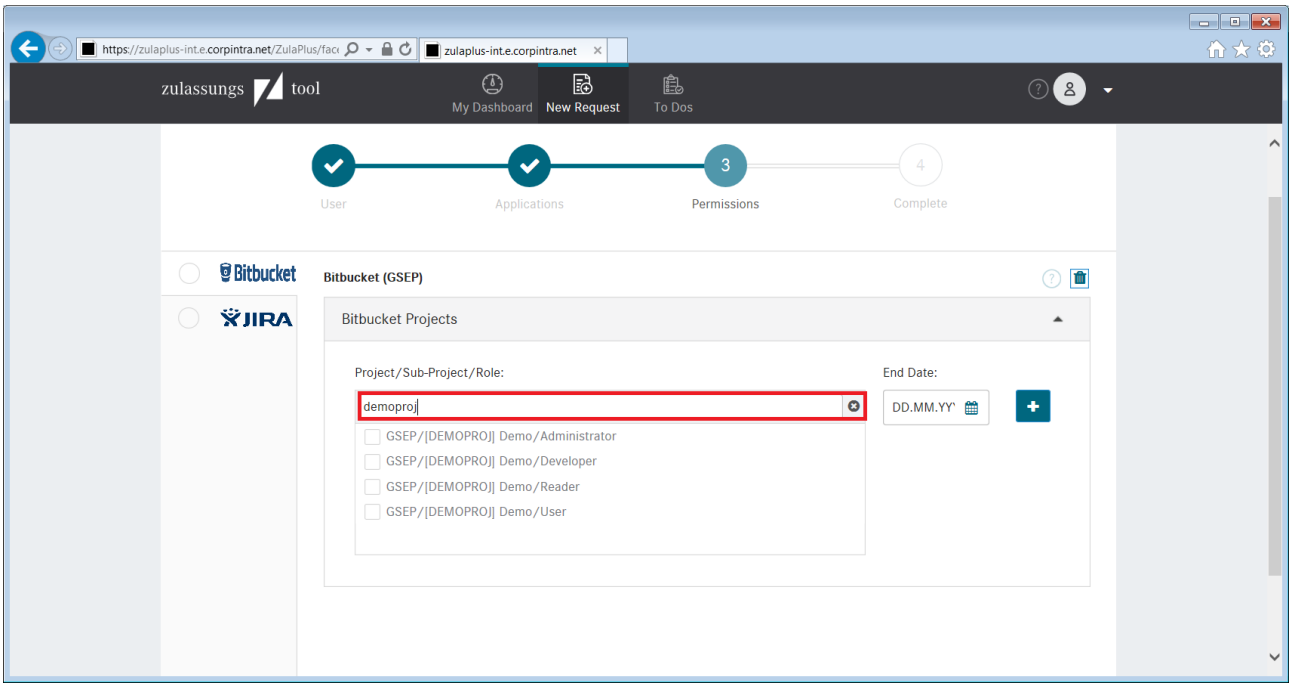
Step 3: Add "GSEP" to the search box and click the magnifying glass icon to filter all GSEP applications



Step 4: Add all necessary applications to your shopping basket.

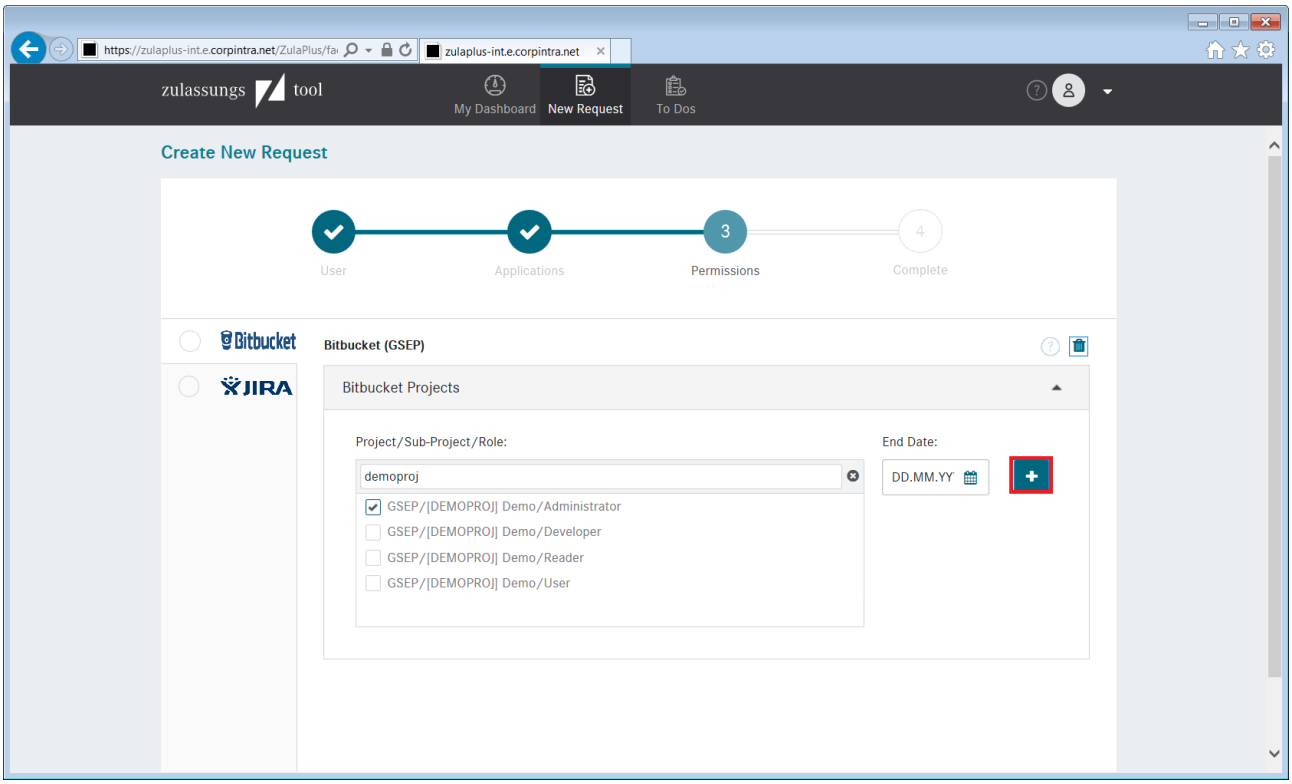


Step 5: Search for the project in the search box for each application, e.g. "demoproj"

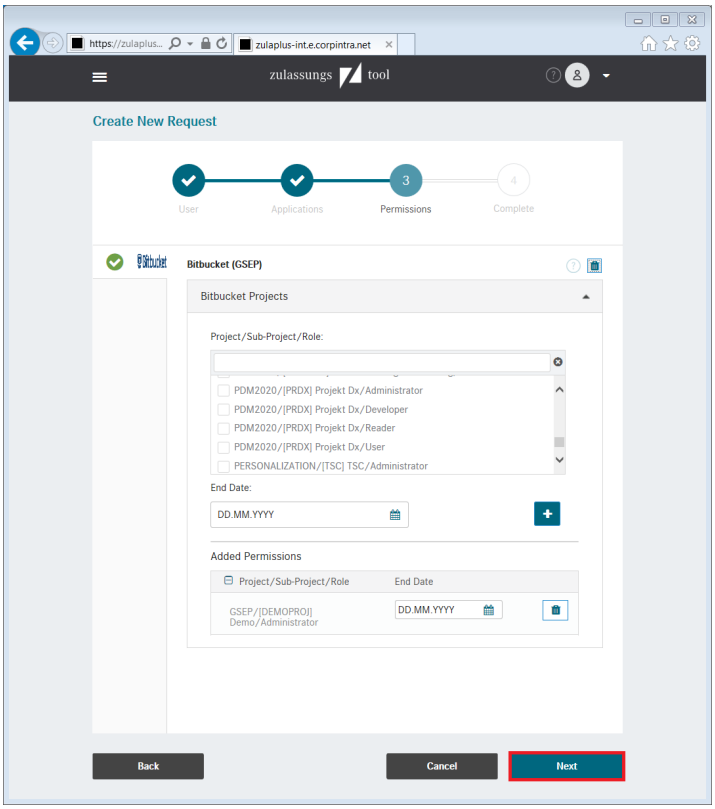


Step 6: Select the necessary permissions for each project and add them via the plus button. Multiple permissions for several projects can be selected in one request.

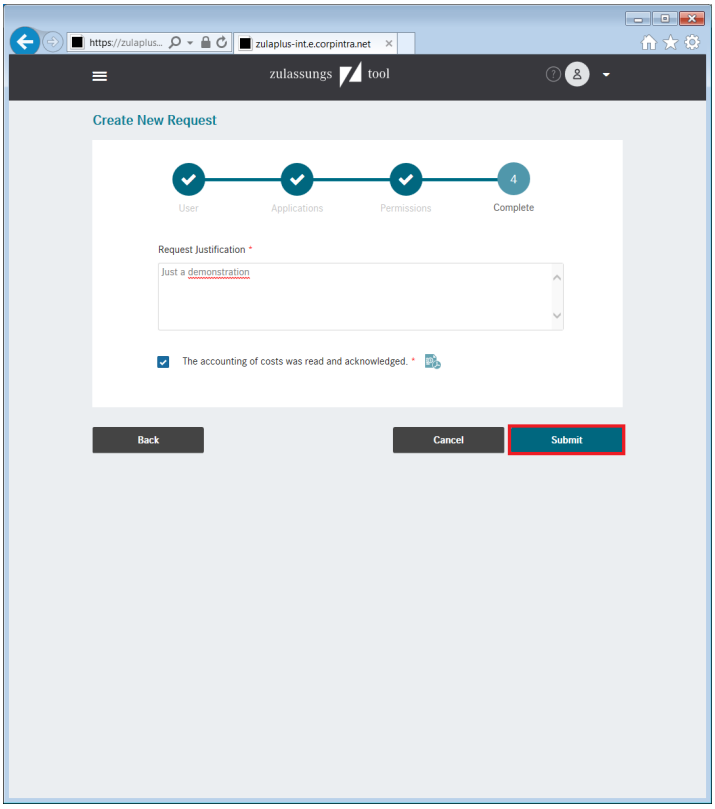
You can find the current permission matrix for all our applications at https://team.sp.wp.corpintra.net/sites/03009/General%20Information/GSEP_Permission-Matrix.xlsx?Web=1



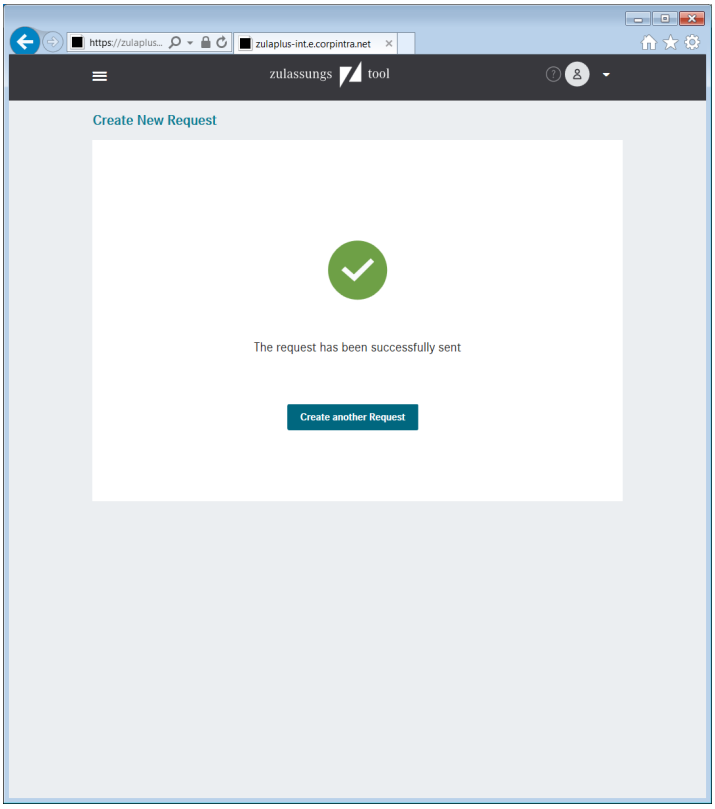
Step 7: After adding all your necessary permissions for all selected applications please go to the next page via the "Next" button.



Step 8: Don't forget to add your request justification (at least 20 letters) and submit your request.



Step 9: Your request is sent to the project approver. After the approval your permissions will be automatically granted and you have access to the chosen tools.



Step 10: Start working.

ServiceNow KB article- KB0349943[77]

4.6 List project access of users via confluence macro

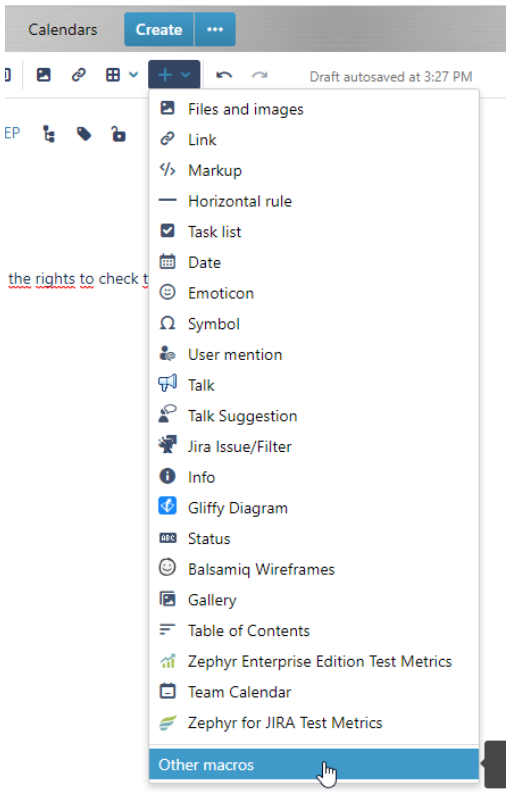
4.6.1 Problem

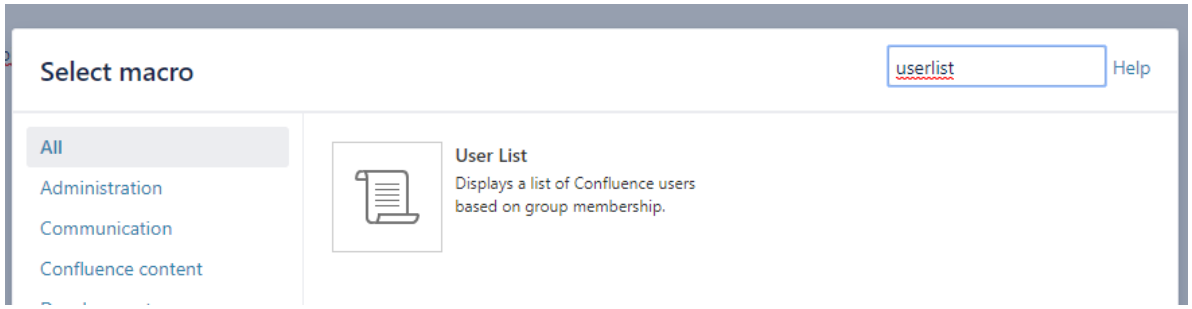
I want to know who has actually access to my Jira, Confluence, Bitbucket, ... projects but I do not have the rights to check the access in ZULA.

4.6.2 Solution

Go to a confluence page and ad the **User List** macro:

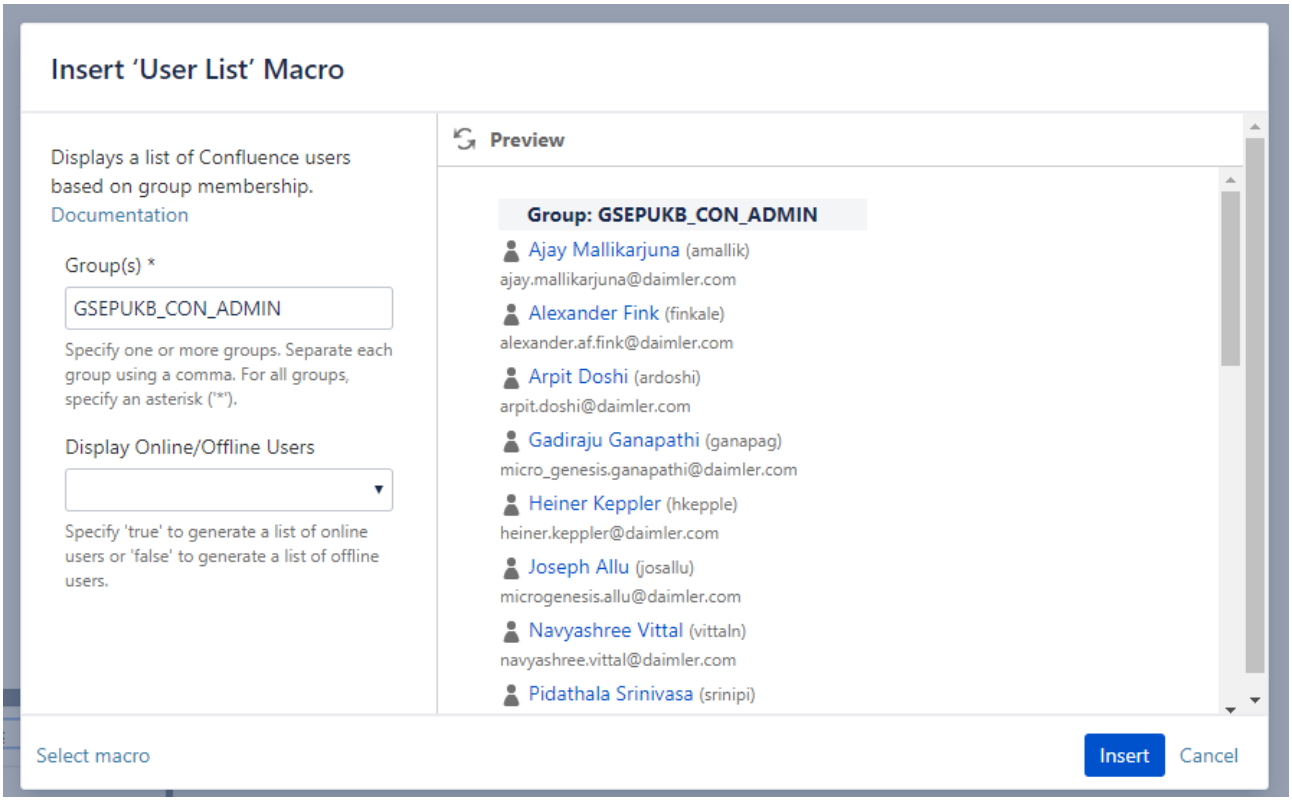
77 https://servicenow.i.mercedes-benz.com/esc?id=kb_article&table=kb_knowledge&sys_kb_id=158377671b7099101d67a7953b4bcb84





(Shortcut: type "{user" to have the autocomplete)

Now add the groups you are interested in into the Group(s)* field:



(You can get a good overview on the groups when you go to your group page in Crowd: https://gsep.daimler.com/crowd/console/user/viewgroups.action)

Schema: PROJECTKEY_TOOL_ROLE

You can add groups from all our tools. Here we only use confluence as the tool to show this list in a convenient way.

The result is a list that shows all people in the group. The list is showing the actual rights that are queried when a user clicks on a page.

4.6.2.1 Result

No results were found for groups : GSEPUKB_CON_ADMIN

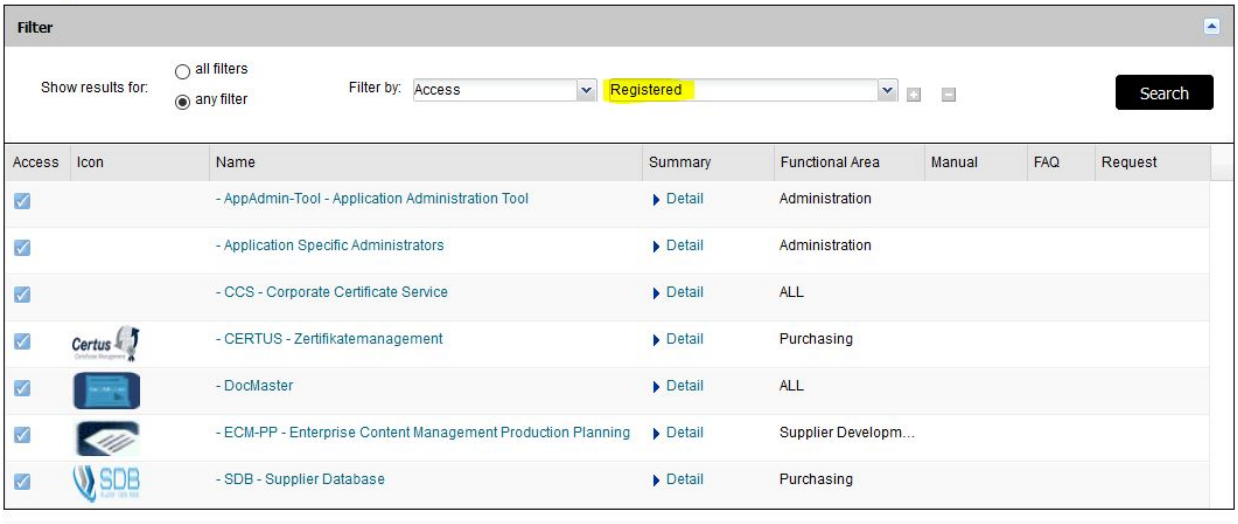
4.7 User not visible in ZULA/ Application to Engineering Portal

If you are not visible in ZULA as a supplier, the reason might be that you are not registered to the Engineering Portal.

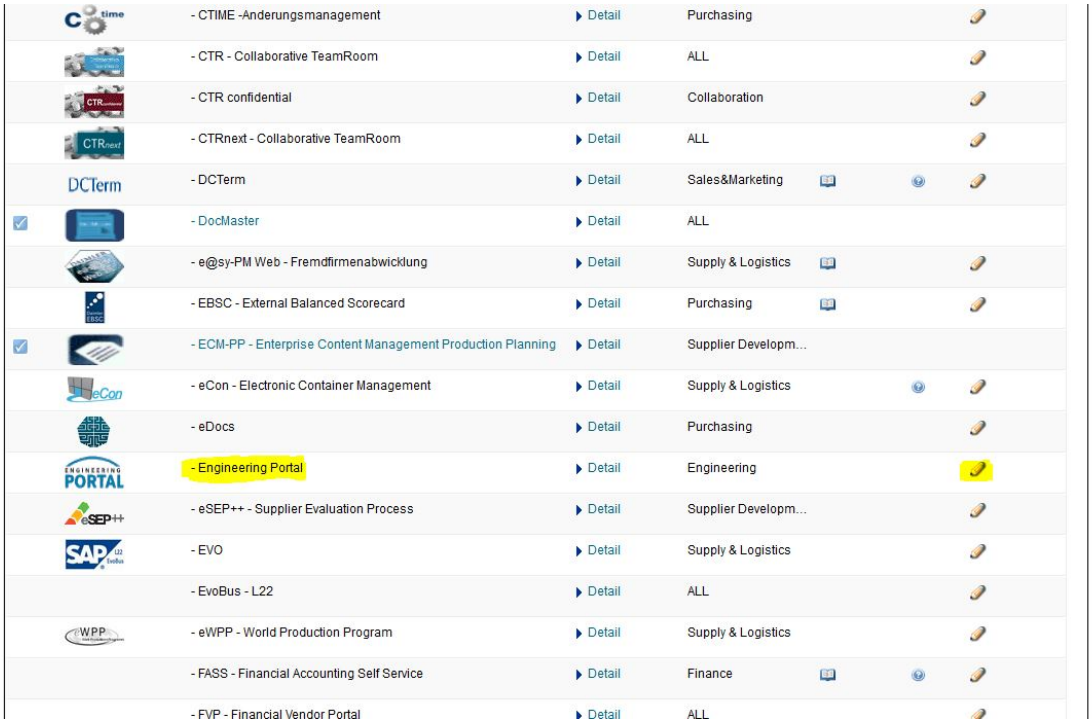
1.) Go to the Supplier Portal https://supplier-portal.daimler.com, log in and go to main page and Scroll down to "Applications".

2.) Change the filter from "Registered" to "All" and click "Search".

Your Applications



3.) Scroll down to "Engineering Portal", click on the pencil and accept the Popup.



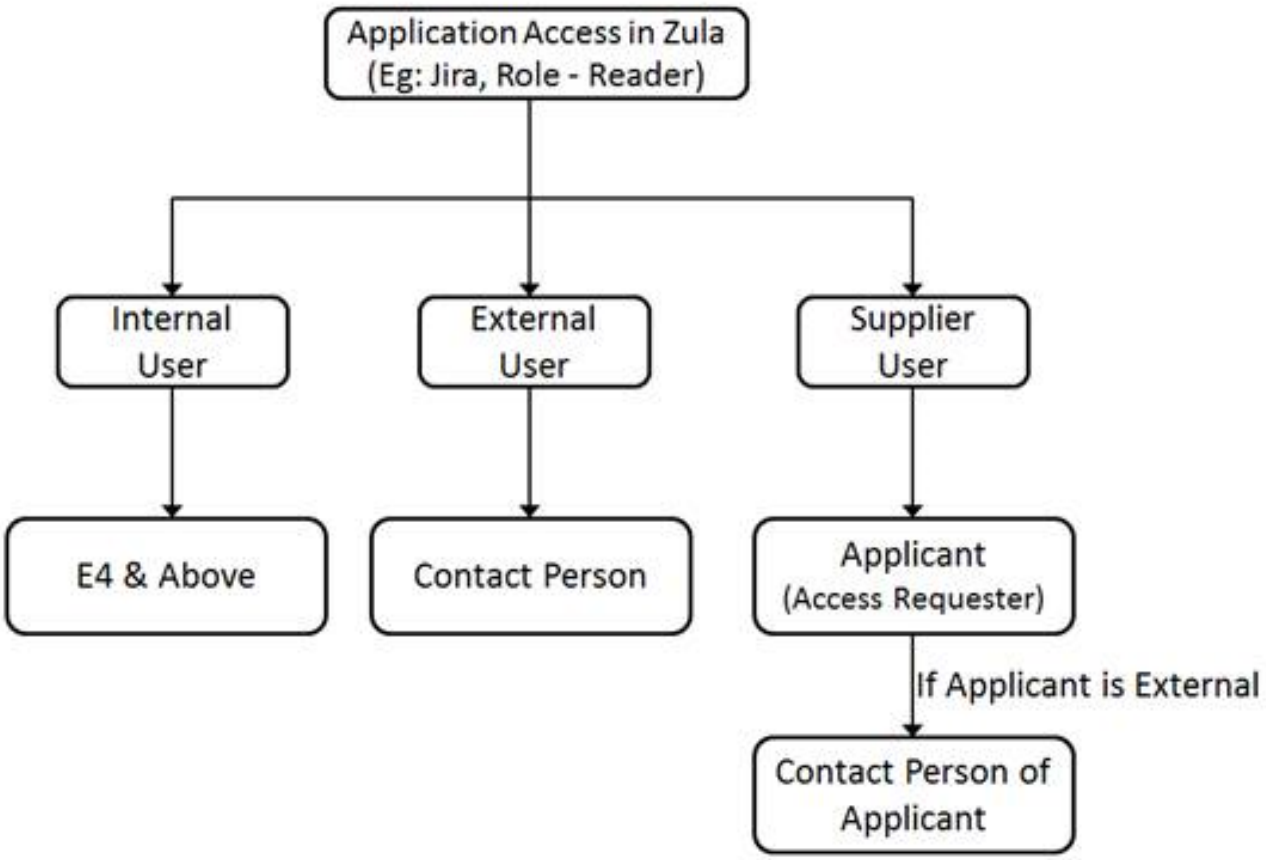
4.) State the reason for approval and click "Next".

5.) Now you have to wait for approval through an administrator (estimated 1 week).

4.8 Zula-Mercedes Access Validation Process

4.8.1 As per Mercedes-Benz Information Security Mandate, every system/ application users accesses has to be verified by the respective Mercedes-Benz Line Manager(s) with a regular interval (i.e. to extend/revoke their existing accesses).

Below is the standard workflow/hierarchy of GSEP Accesses verification thru Zula (i.e. once in every 6 months) -



Please Note: If the accesses are not-validated or not-actioned by the Line Manager(s) within the defined time-frame, then all the existing accesses will be revoked automatically by the system.

Post that, the users who still needs access to GSEP application(s), they have to submit a fresh request thru Zulaplus[78] to get back their revoked access (i.e. the regular on-boarding process has to be followed).

Additional Info / FAQ -

Q 1) How one can change their point of contact person(manager) name if it is incorrectly assigned in Zula & what is the process?

> **Ans:** To change the contact person for a user, the correct contact person(manager) needs to do this change in the system "**EMT**".
>
> Zula is just fetching such information from Corporate Directory(CD) & they are not responsible for data modification in CD. (User information will be fetched from Corporate Directory & Supplier Directory during every Zula sync, this includes their contact persons aswell).

Q 2) How an end users can directly reach to Zula-Support for their quires/concerns related to Zula?

78 https://zulaplus.e.corpintra.net/ZulaPlus/faces/pages/template/zula-home.xhtml

Ans: Anyone can reach Zula-Support directly with their quires related to Zula. **Zula SPOC** (Single Point of Contact) → Helpline **+49 7031 90 42064** or write to zula@mercedes-benz.com[79] (to get a faster response/ direct answers from Zula).

Q 3) Access Types and Reviewal Frequency?

Ans: Access Types – **Standard Permissions** and **Privileged Permissions**

Frequency of Reviewal – once in **6months** for standard permissions and once in **3months** for privileged permissions.

ServiceNow KB Article- KB0349943[80]

79 http://mercedes-benz.com
80 https://servicenow.i.mercedes-benz.com/esc?id=kb_article&table=kb_knowledge&sys_kb_id=158377671b7099101d67a7953b4bcb84

5 Permission Matrix

The official Permission Matrix can be found in our Sharepoint:

https://team.sp.wp.corpintra.net/sites/03009/General%20Information/GSEP_Permission-Matrix.xlsx

It contains the mapping between the Groups and Roles to the actual Rights that are associated.

There are tabs for each tool, so you can easily find our the rights for Jira or Confluence.

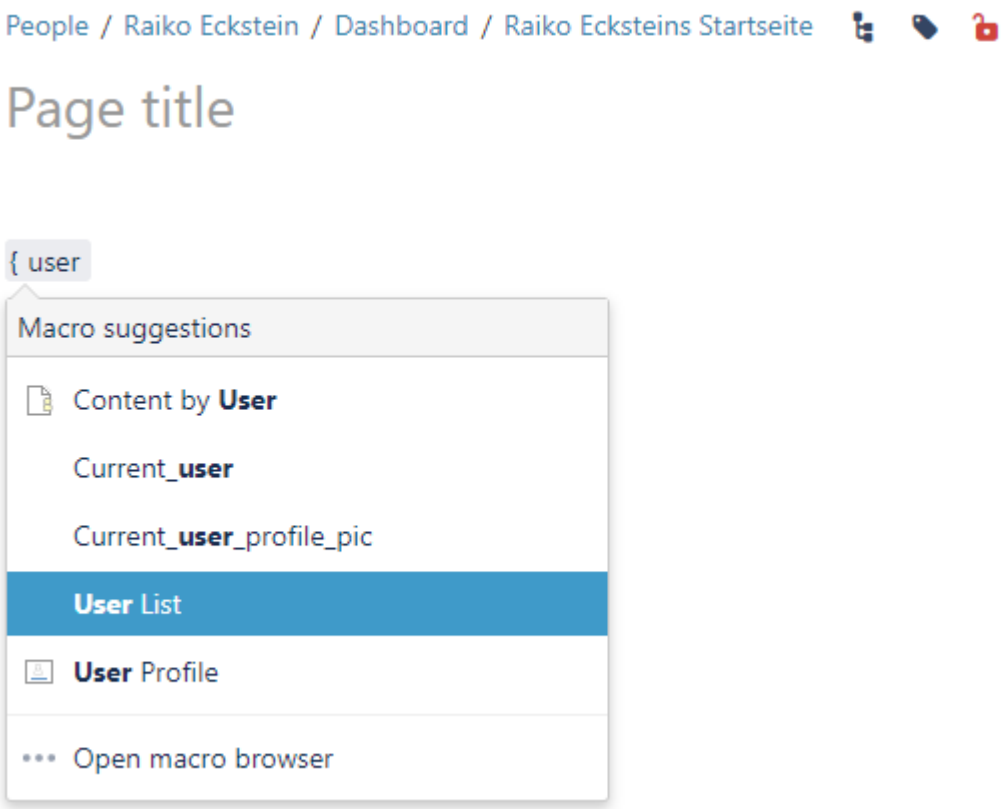
6 Who has access to my project's data?

6.1

6.2 Atlassian Tools

For Altassian tools, you can check the members of the access groups in Confluence.

- Create a new page, e.g. "Project access rights" in Confluence. This example also works if you do not save the new page.
- Type "{ User List" and select the suggested macro.



1.

- In the macro settings dialogue, add the respective group name, in format PROJECTKEY_APP_ROLE
  You can add multiple groups, separated by komma.
    a. PROJECTKEY: Can be derived from the URL, e.g. DASHD from https://gsep.daimler.com/confluence/display/DASHP/
    b. APP:
        i. JIR for Jira (Available Roles: ADMIN, DEVELOPER, READER, SCRUM MASTER, USER)
        ii. CON for Confluence (Available Roles: ADMIN, AUTHOR, MODERATOR, READER)
        iii. STA for Bitbucket (Available Roles: ADMIN, DEVELOPER, READER)

iv. SNR for SonarQube (Available Roles: ADMIN, READER, REVIEWER, USER)

- Example:
  No results were found for groups : DASHD_CON_ADMIN,DASHD_CON_MODERATOR

6.3 Confluence

On every Confluence page, there is a '...' button on the right side at top of the page. In this menu, you can select "People who can view."

This reflects the access to the confluence project, and also checks the restrictions for this page or parent pages.

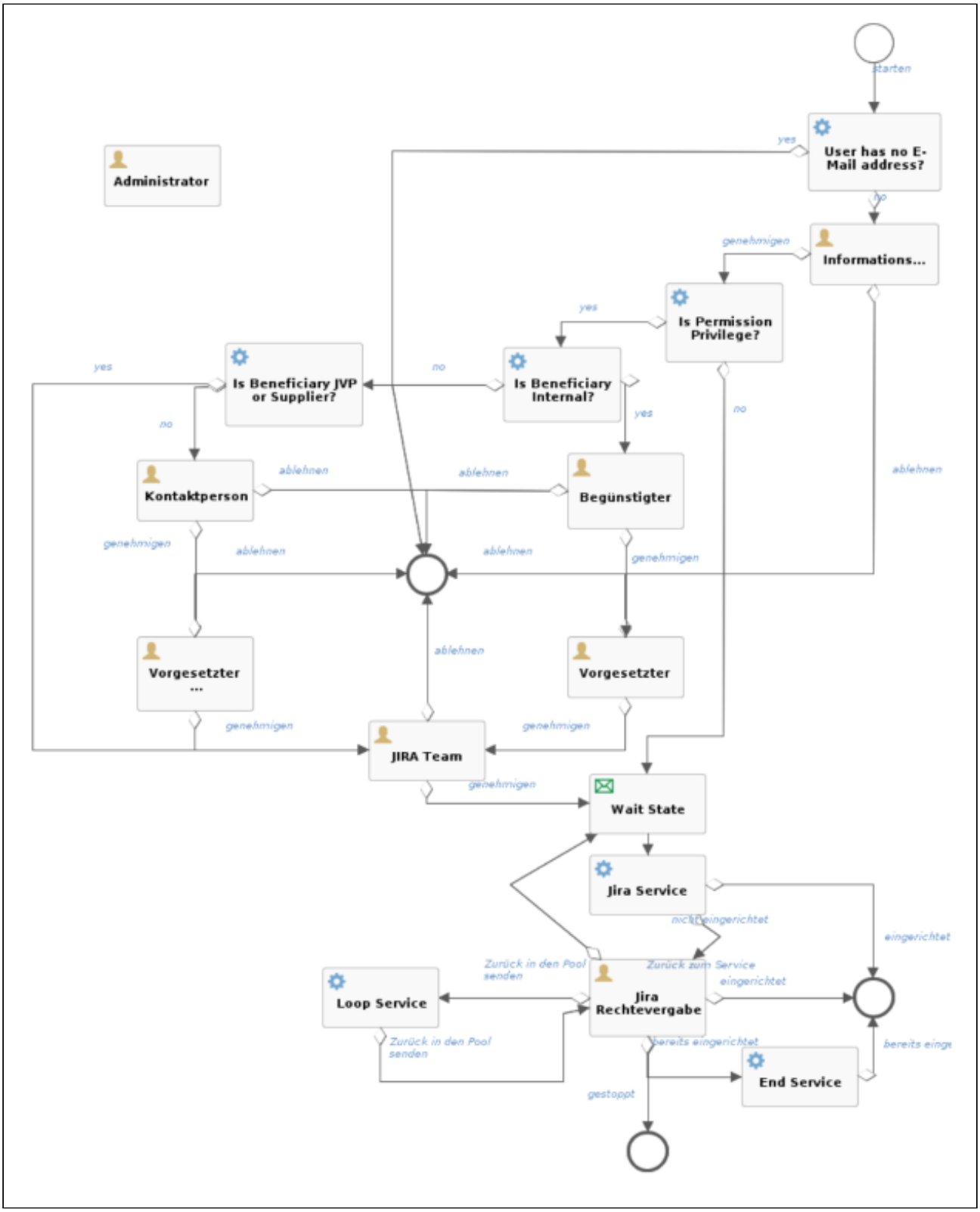
7 Technical process flow for account Activation and Deactivation

This document explains the detailed technical process flow for a User account Activation (commissioning) & Deactivation (de-commissioning). The below process has been outlined for one application (JIRA), but the same process implies to all the GSEP applications.

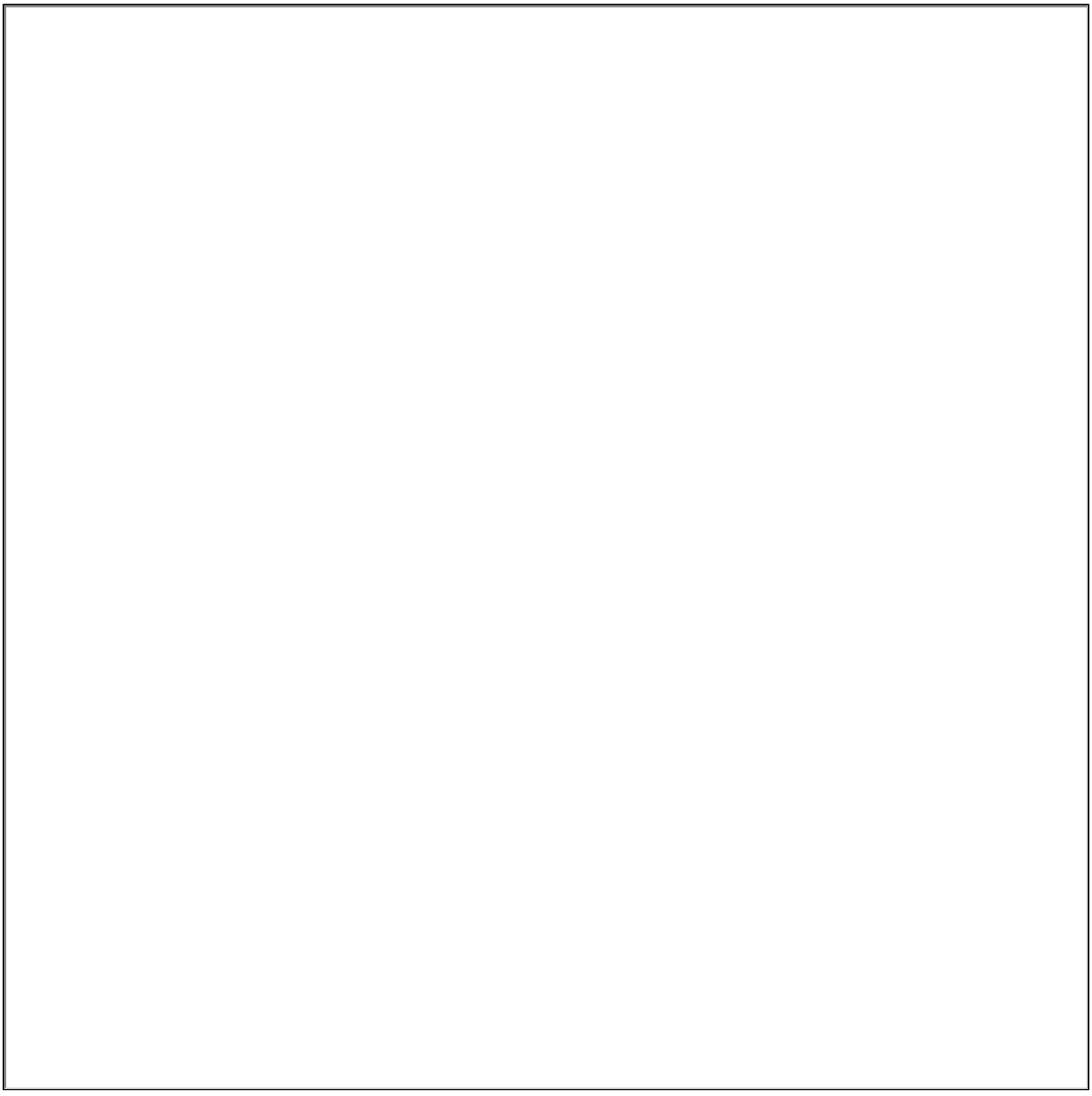
7.1 New User Request

Internal & External Users: The request can be raised by the User him/herself or any Intranet users can raise on his/her behalf.

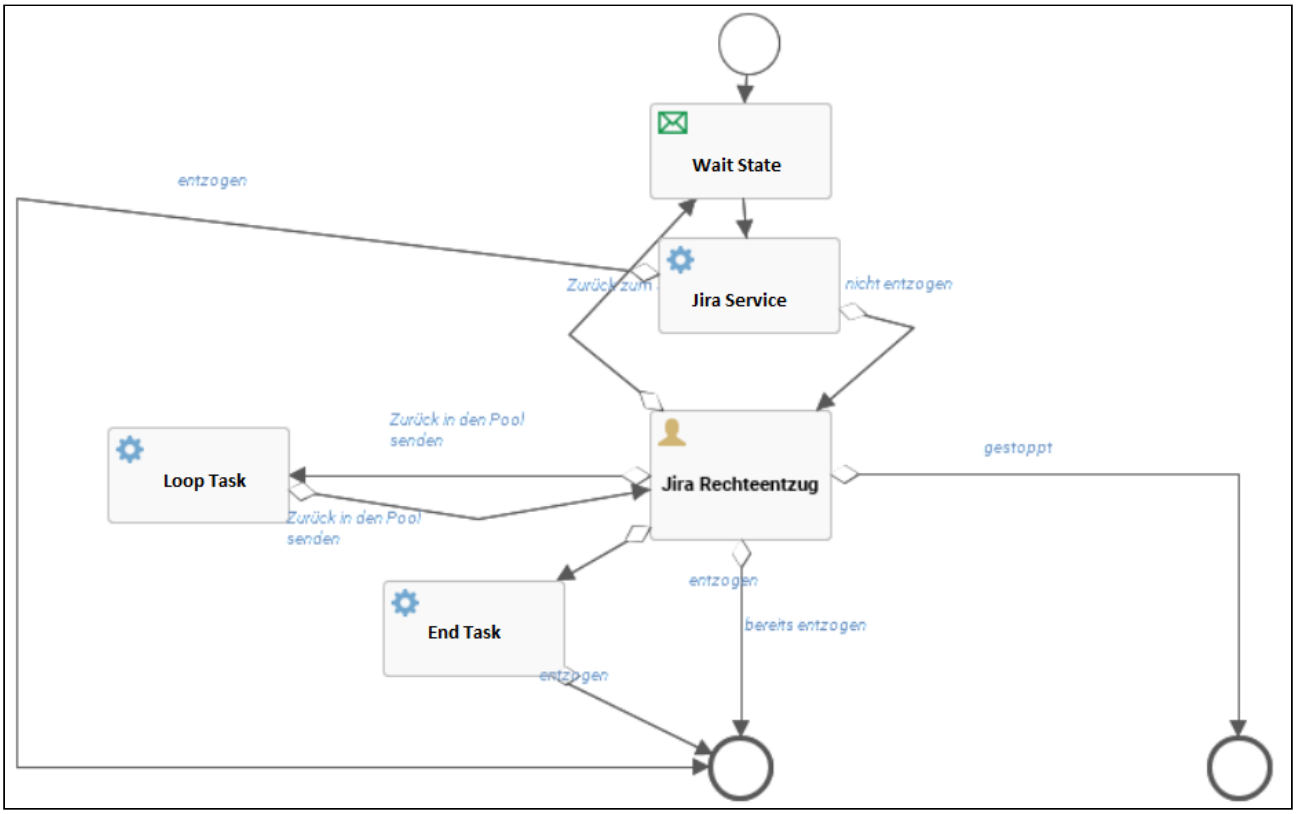
Supplier Users: The user's "Daimler Point of Contact" has to raise the access request.


starten
User has no E-Mail address?
yes
no
Administrator
genehmigen
Informations...
Is Permission Privilege?
yes
no
Is Beneficiary JVP or Supplier?
Is Beneficiary Internal?
yes
no
no
ablehnen
Kontaktperson
ablehnen
Begünstigter
ablehnen
genehmigen
ablehnen
ablehnen
genehmigen
Vorgesetzter ...
ablehnen
Vorgesetzter
genehmigen
genehmigen
JIRA Team
genehmigen
Wait State
Jira Service
nicht eingerichtet
eingerichtet
Zurück in den Pool senden
Zurück zum Service
Loop Service
Jira Rechtevergabe
eingerichtet
Zurück in den Pool senden
bereits eingerichtet
bereits eingr
gestoppt
End Service

7.2 **Cancellation Request**



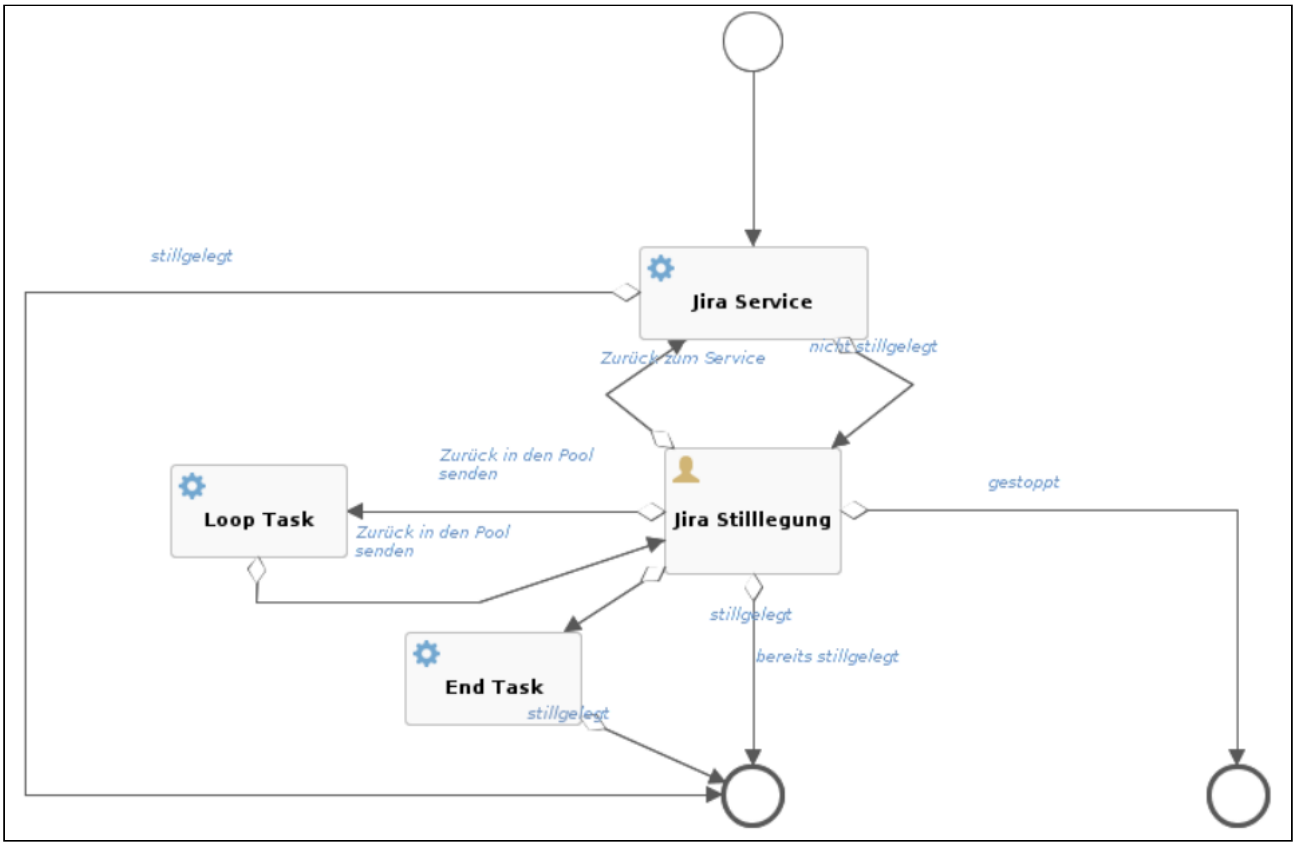
7.3 Extension Request



7.4 User Account Closure Request

Internal & External Users: The request can be raised by the User him/herself and also can be initiated by his/her supervisor.

Supplier Users: The user's "Daimler Point of Contact" has to initiate the closure request.


stillgelegt
Jira Service
Zurück zum Service
nicht stillgelegt
Zurück in den Pool senden
Loop Task
Zurück in den Pool senden
Jira Stilllegung
gestoppt
stillgelegt
bereits stillgelegt
End Task
stillgelegt

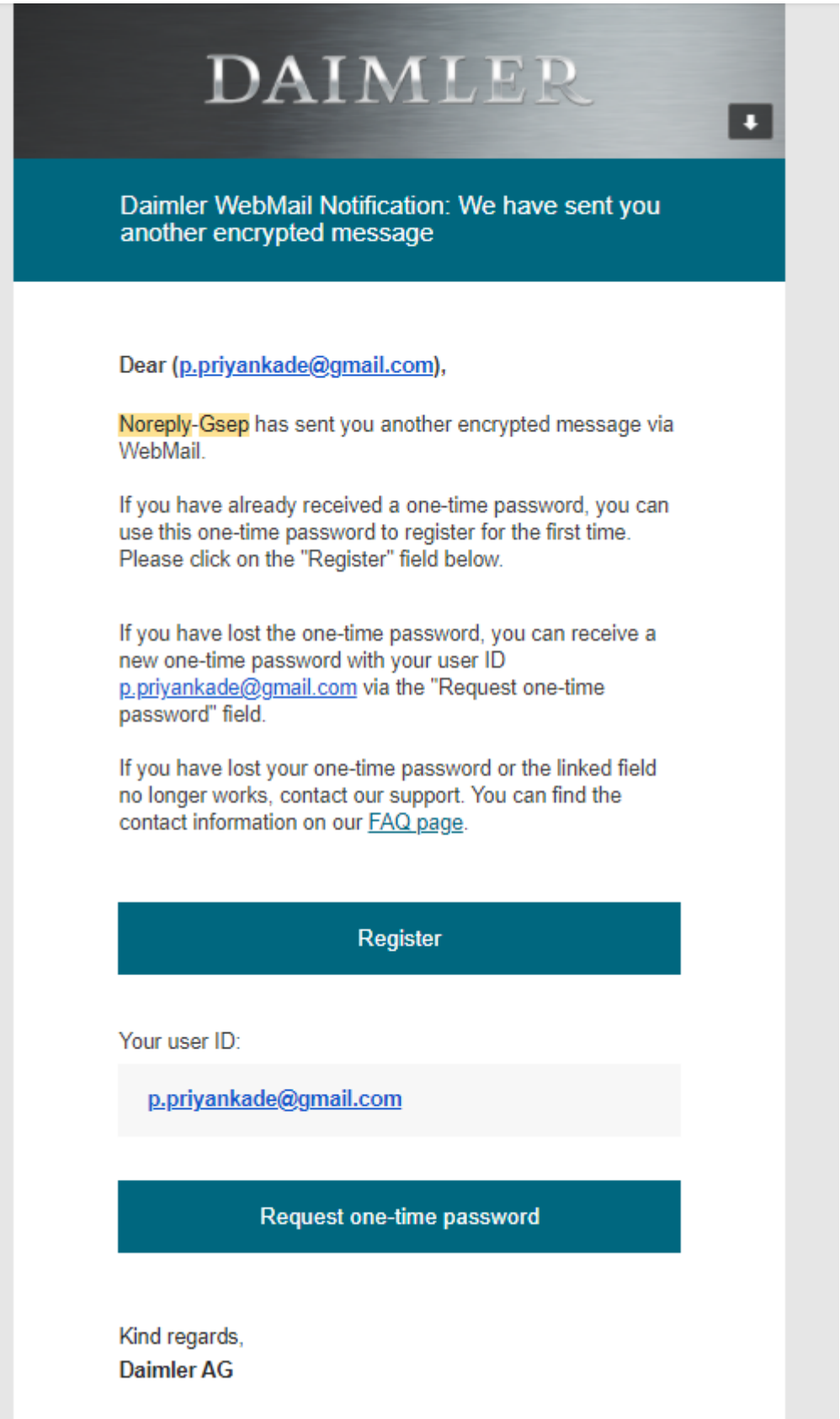
8 GSEP-Email Encryption for GSEP

GSEP-Email Encryption for GSEP					
Draft Version 1.1					
Author	Date	Version	Relevant Chapters	Changes	Support Unit accepted by
Priyanka De	18 Nov 2021	1.0	Draft	All	
Gokul.R	08 Dec 2021	1.1	Updated	All	

Official documentation on "How-to guide for WebMail 2020" – Guidelines for receiving and replying to encrypted emails from the Daimler group: https://webmail.daimler.com/WebMail_HowtoGuide_EN.pdf

Step 1: Registering on Webmail

- If this is the first time a Daimler employee has sent you an encrypted email, you must first register on WebMail.



DAIMLER

Daimler WebMail Notification: We have sent you another encrypted message

Dear (p.priyankade@gmail.com),

Noreply-Gsep has sent you another encrypted message via WebMail.

If you have already received a one-time password, you can use this one-time password to register for the first time. Please click on the "Register" field below.

If you have lost the one-time password, you can receive a new one-time password with your user ID p.priyankade@gmail.com via the "Request one-time password" field.

If you have lost your one-time password or the linked field no longer works, contact our support. You can find the contact information on our FAQ page.

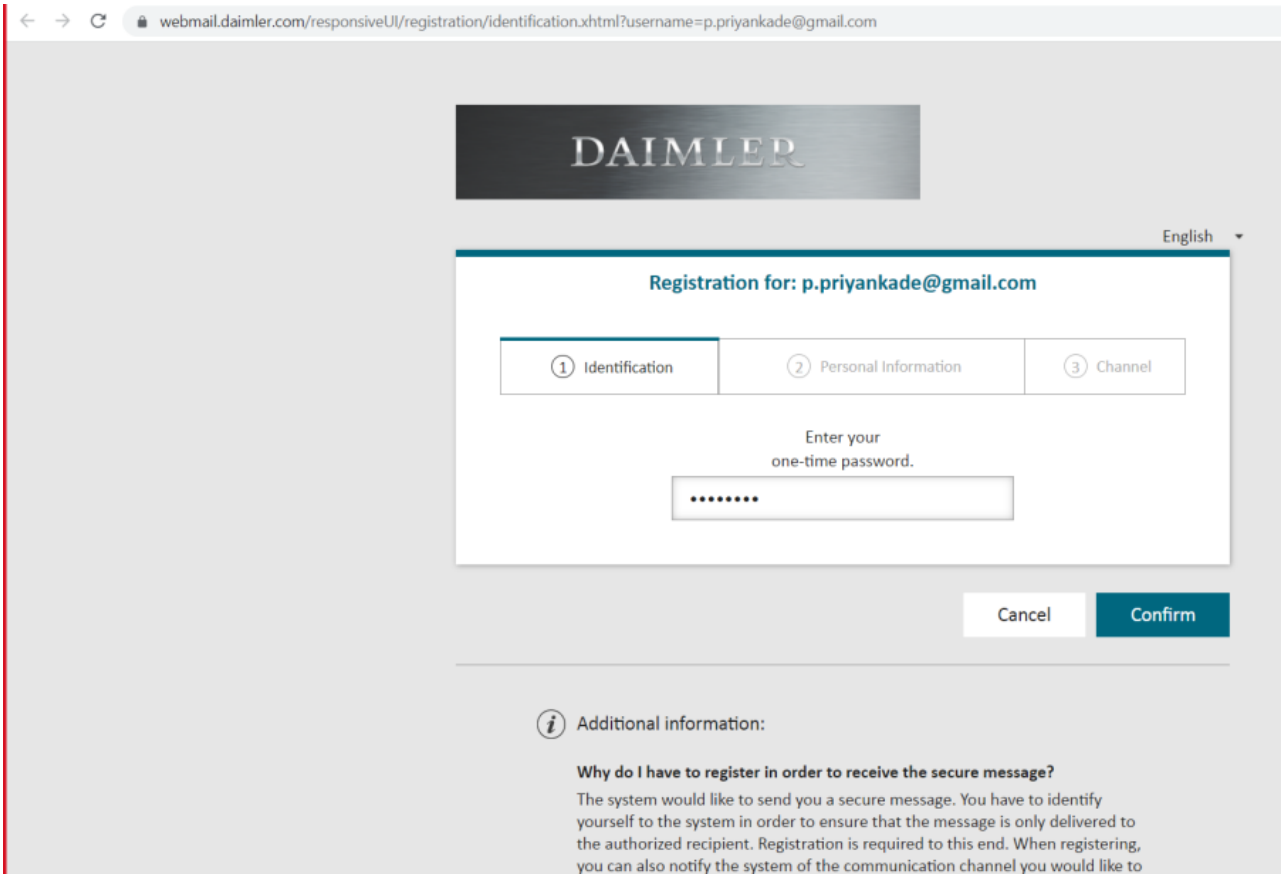
Register

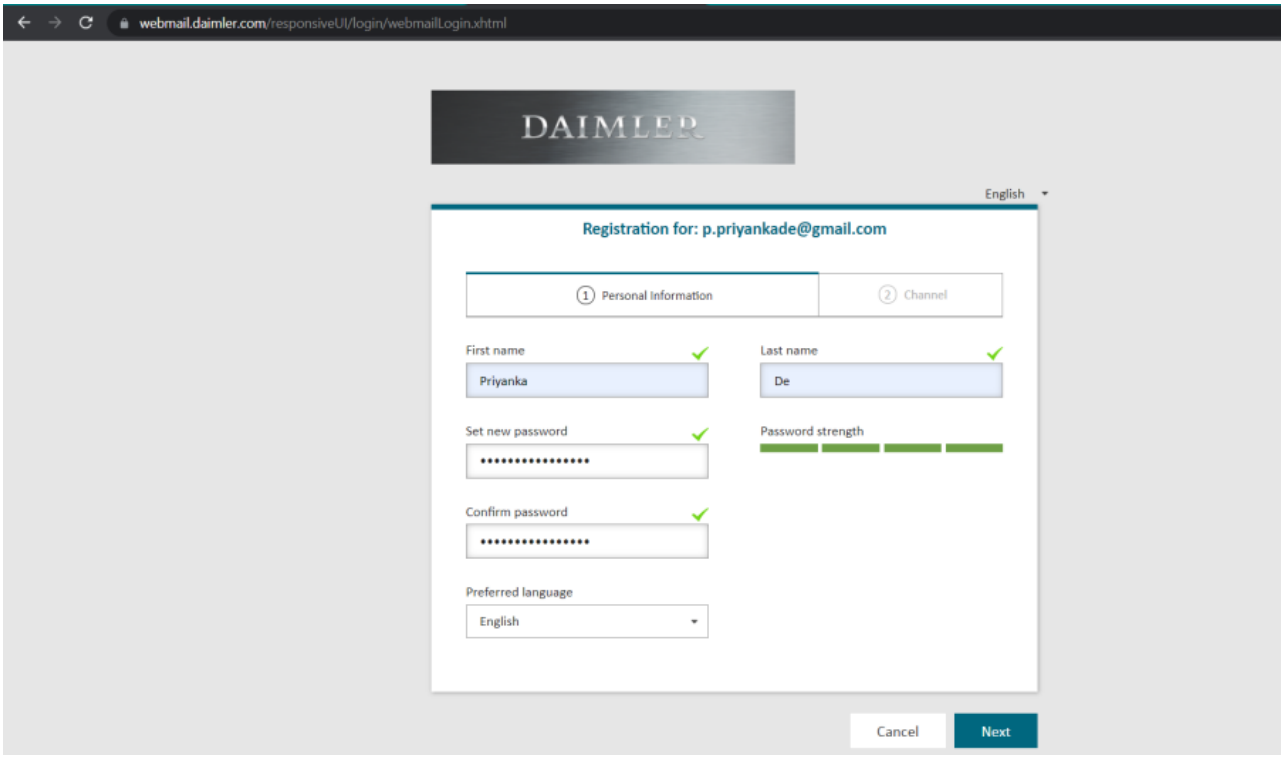
Your user ID:

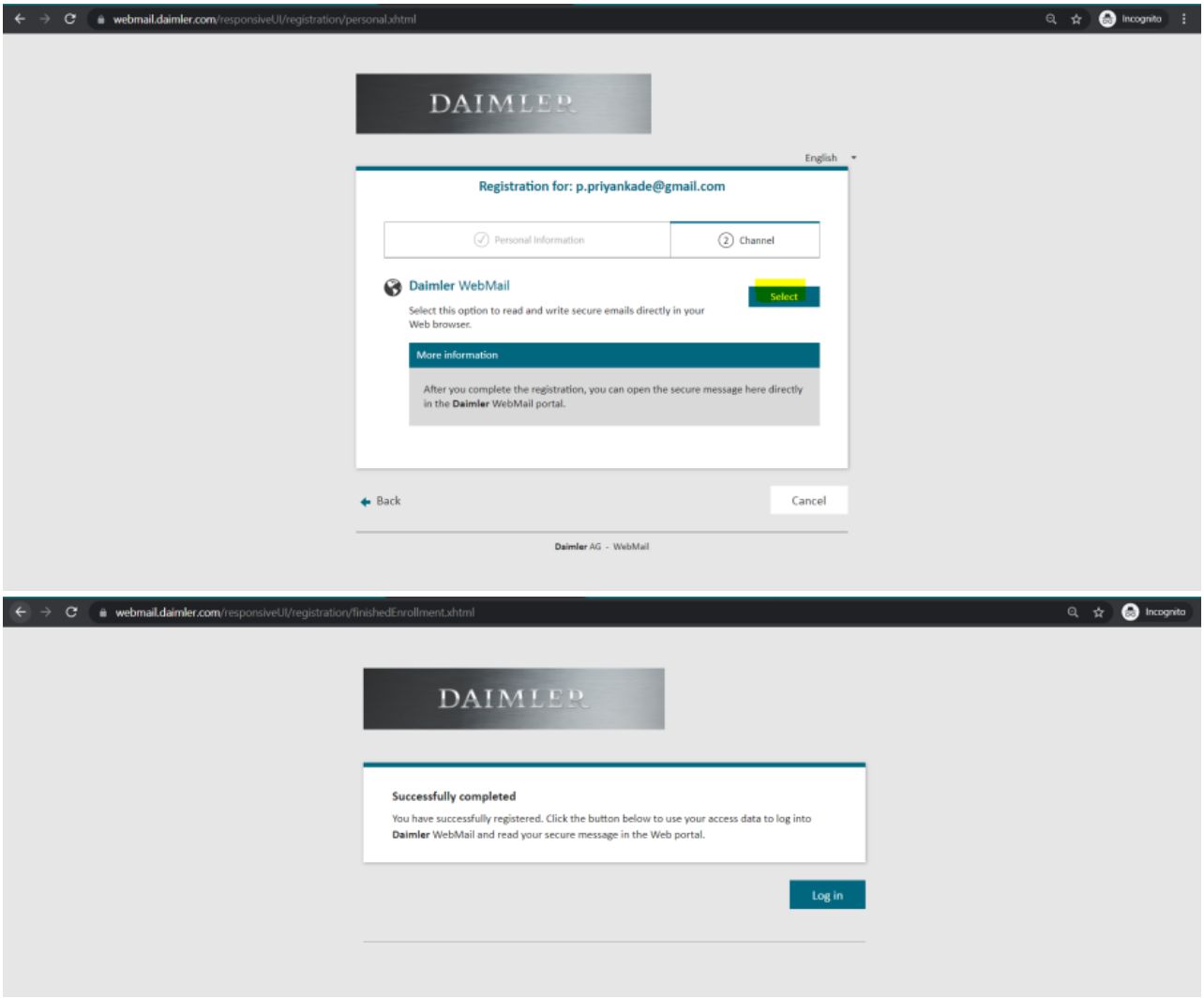
p.priyankade@gmail.com

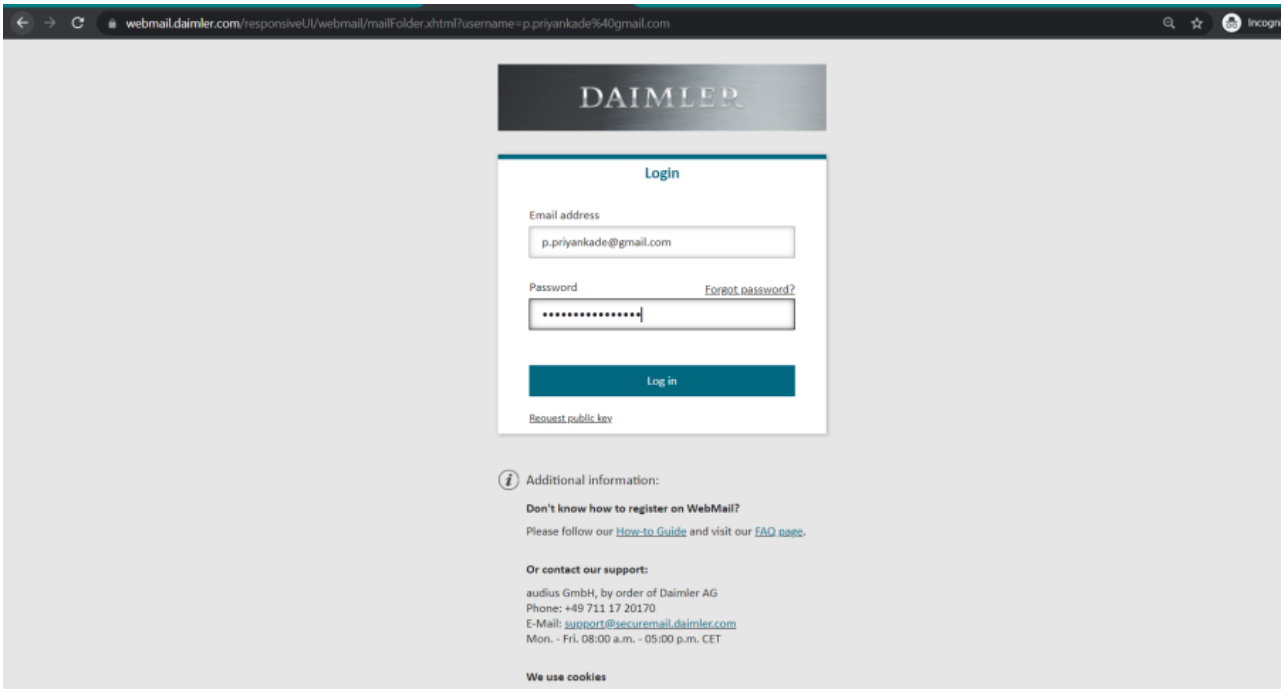
Request one-time password

Kind regards,
Daimler AG

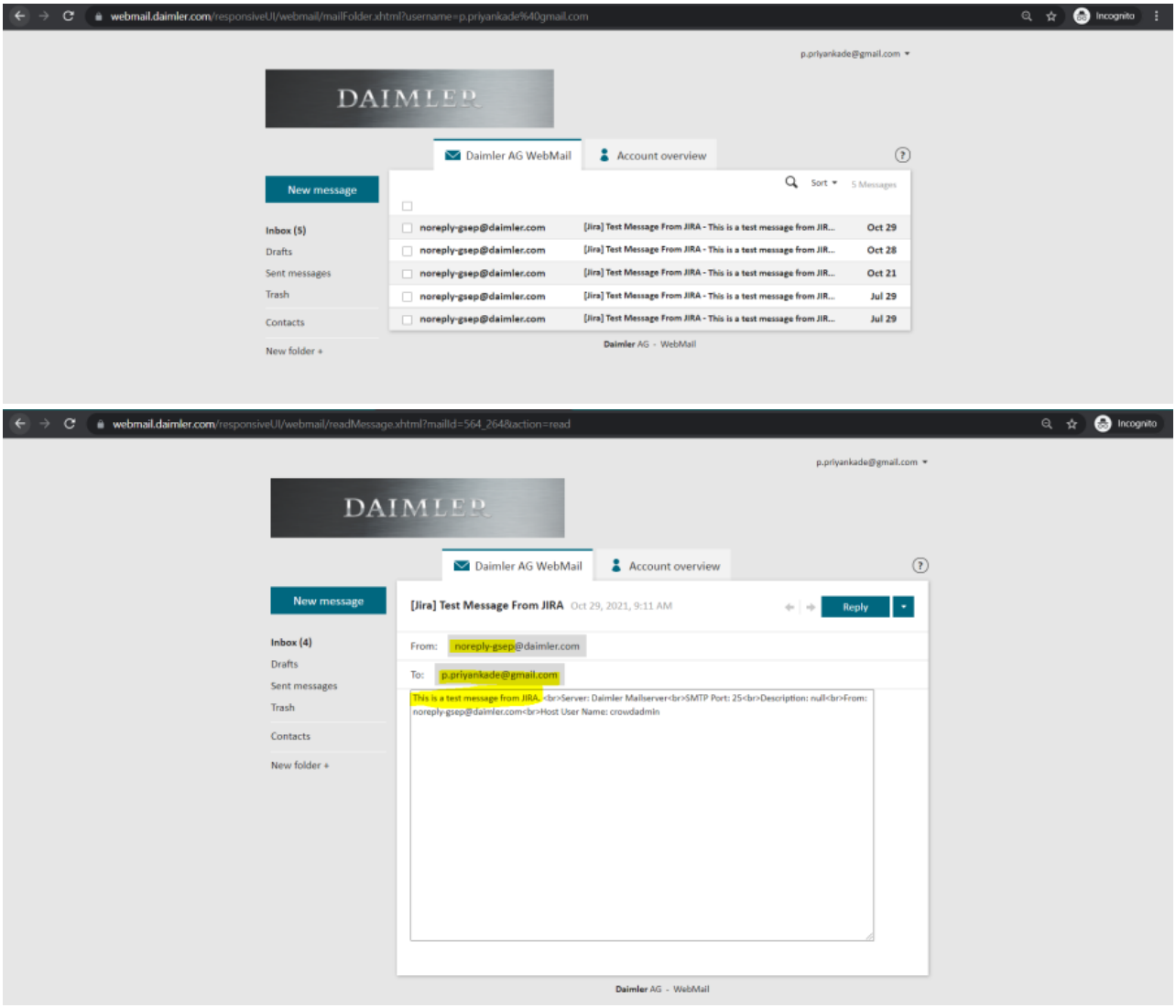

webmail.daimler.com/responsiveUI/registration/identification.xhtml?username=p.priyankade@gmail.com
DAIMLER
English
Registration for: p.priyankade@gmail.com
1 Identification
2 Personal Information
3 Channel
Enter your
one-time password.
Cancel
Confirm
Additional information:
Why do I have to register in order to receive the secure message?
The system would like to send you a secure message. You have to identify
yourself to the system in order to ensure that the message is only delivered to
the authorized recipient. Registration is required to this end. When registering,
you can also notify the system of the communication channel you would like to


webmail.daimler.com/responsiveUI/login/webmailLogin.xhtml
DAIMLER
English
Registration for: p.priyankade@gmail.com
1 Personal Information
2 Channel
First name
Priyanka
Last name
De
Set new password
Password strength
Confirm password
Preferred language
English
Cancel
Next

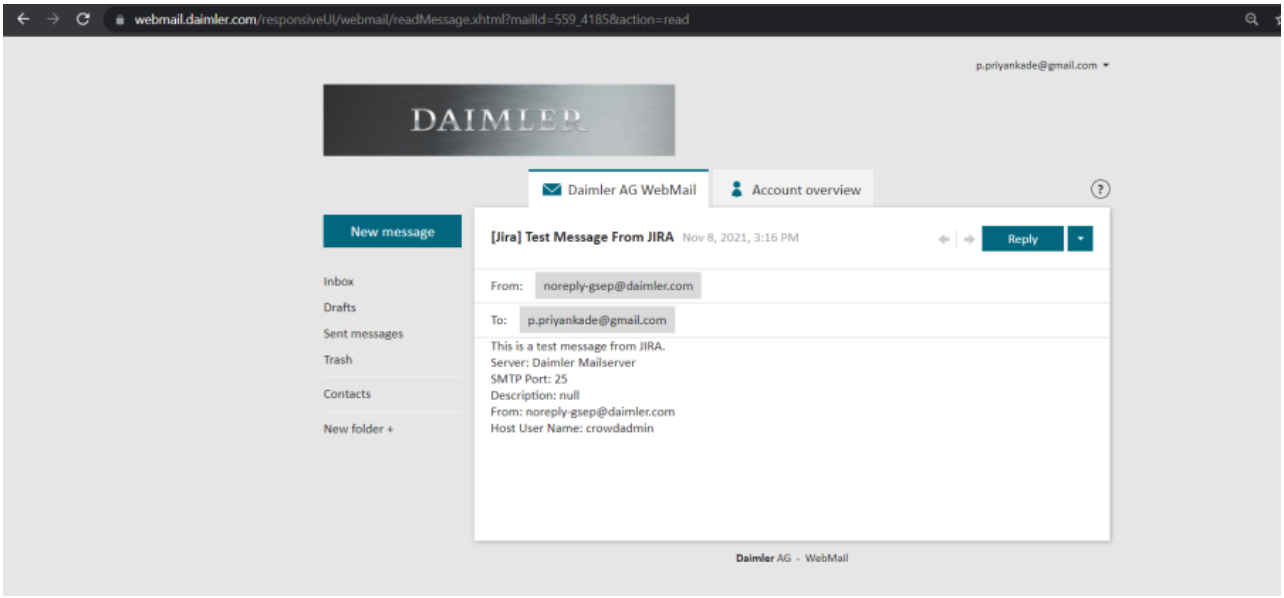

webmail.daimler.com/responsiveUI/registration/personal.xhtml
Incognito
DAIMLER
English
Registration for: p.priyankade@gmail.com
Personal Information
2 Channel
Daimler WebMail
Select
Select this option to read and write secure emails directly in your Web browser.
More information
After you complete the registration, you can open the secure message here directly in the Daimler WebMail portal.
Back
Cancel
Daimler AG - WebMail
webmail.daimler.com/responsiveUI/registration/finishedEnrollment.xhtml
Incognito
DAIMLER
Successfully completed
You have successfully registered. Click the button below to use your access data to log into Daimler WebMail and read your secure message in the Web portal.
Log in

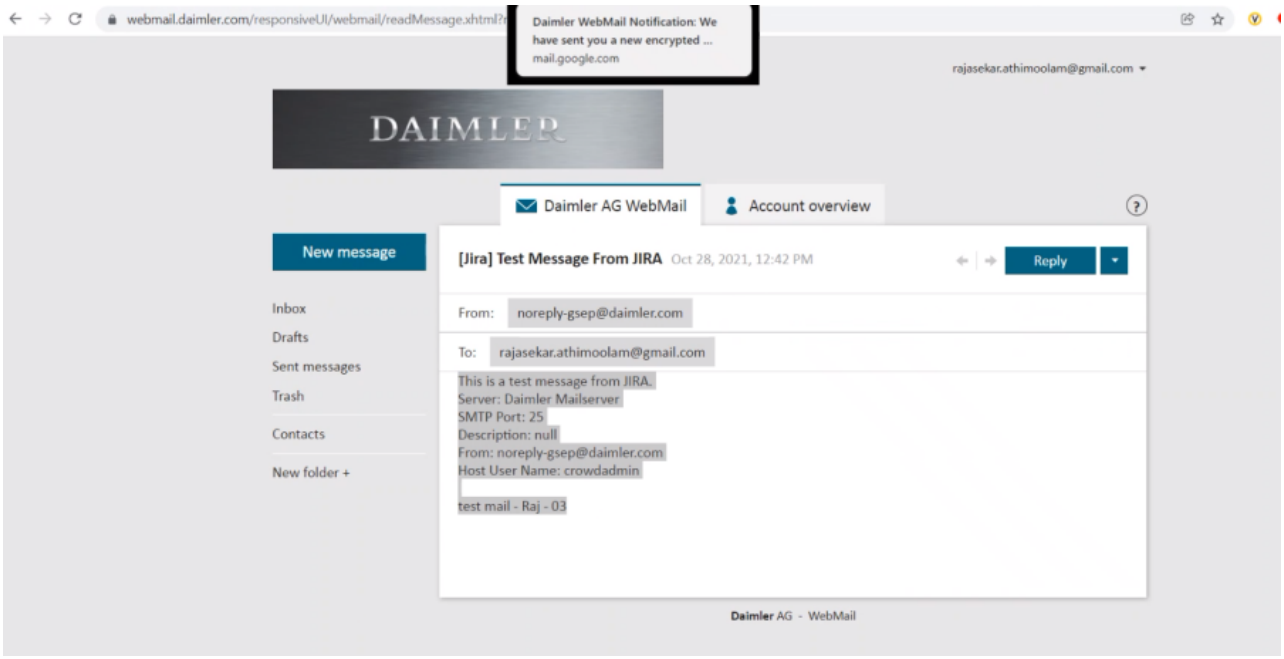


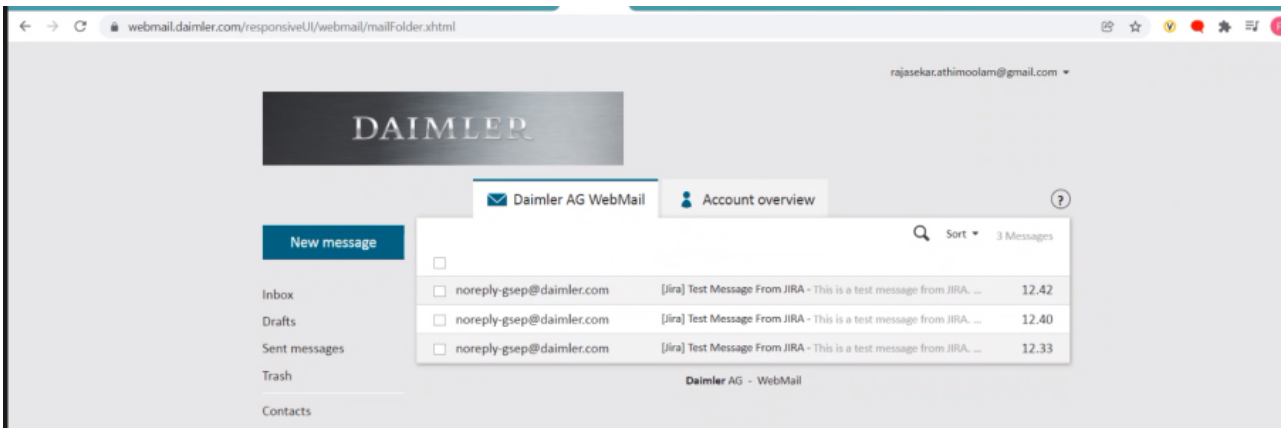
- After Registering and logging in to the Daimler Webmail with external mail ID, the mails are present in the Daimler Webmail inbox.

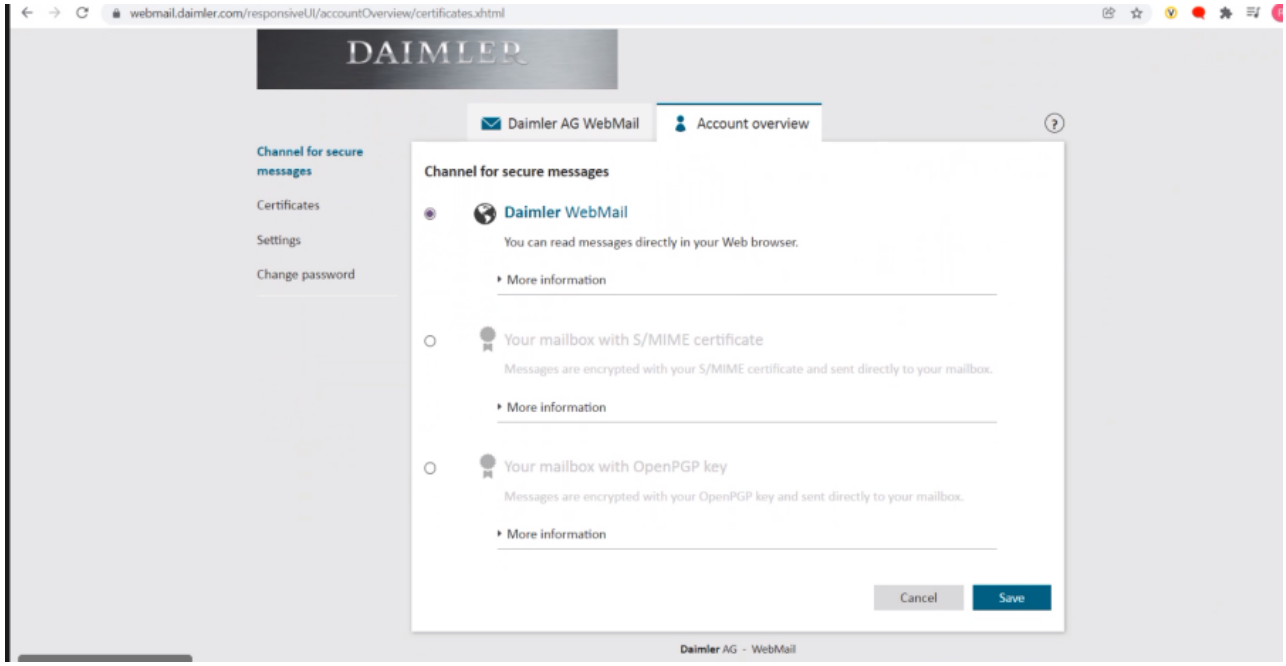


All encrypted emails sent to you by Daimler employees can now be accessed via your WebMail user account.


webmail.daimler.com/responsiveUI/webmail/readMessage.xhtml?mailId=559_4185&action=read
p.priyankade@gmail.com
DAIMLER
Daimler AG WebMail
Account overview
New message
[Jira] Test Message From JIRA Nov 8, 2021, 3:16 PM
Reply
Inbox
Drafts
Sent messages
Trash
Contacts
New folder +
From: noreply-gsep@daimler.com
To: p.priyankade@gmail.com
This is a test message from JIRA.
Server: Daimler Mailserver
SMTP Port: 25
Description: null
From: noreply-gsep@daimler.com
Host User Name: crowdadmin
Daimler AG - WebMail

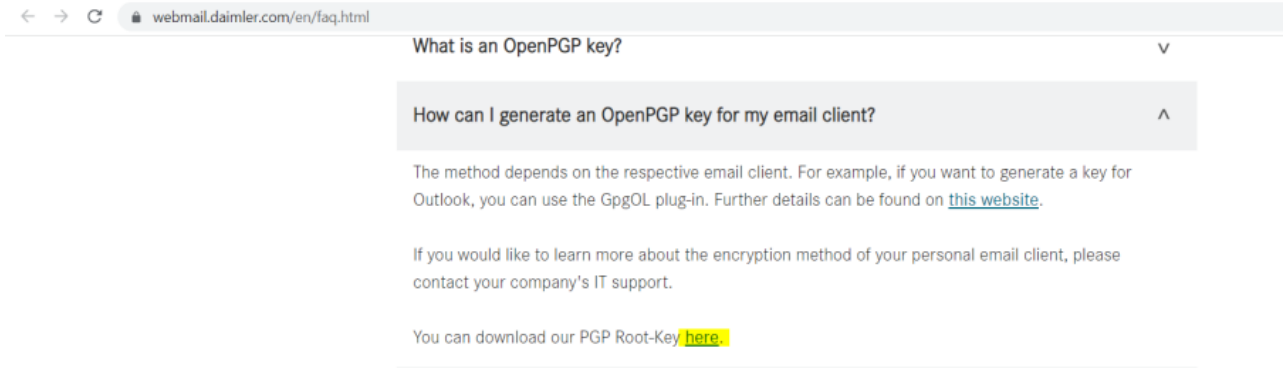

webmail.daimler.com/responsiveUI/webmail/readMessage.xhtml?
Daimler WebMail Notification: We have sent you a new encrypted ...
mail.google.com
rajasekar.athimoolam@gmail.com
DAIMLER
Daimler AG WebMail
Account overview
New message
[Jira] Test Message From JIRA Oct 28, 2021, 12:42 PM
Reply
Inbox
Drafts
Sent messages
Trash
Contacts
New folder +
From: noreply-gsep@daimler.com
To: rajasekar.athimoolam@gmail.com
This is a test message from JIRA.
Server: Daimler Mailserver
SMTP Port: 25
Description: null
From: noreply-gsep@daimler.com
Host User Name: crowdadmin
test mail - Raj - 03
Daimler AG - WebMail


webmail.daimler.com/responsiveUI/webmail/mailFolder.xhtml
rajasekar.athimoolam@gmail.com
DAIMLER
Daimler AG WebMail
Account overview
New message
Sort
3 Messages
Inbox
Drafts
Sent messages
Trash
Contacts
noreply-gsep@daimler.com [Jira] Test Message From JIRA - This is a test message from JIRA. ... 12.42
noreply-gsep@daimler.com [Jira] Test Message From JIRA - This is a test message from JIRA. ... 12.40
noreply-gsep@daimler.com [Jira] Test Message From JIRA - This is a test message from JIRA. ... 12.33
Daimler AG - WebMail



If you have an OpenPGP key or an S/MIME certificate, you can also access encrypted emails via your usual email account, e.g., in Outlook. To do this, you can answer the first message received by WebMail with an email, in which you can attach your OpenPGP key or sign with your S/MIME certificate. If you already registered on WebMail, you can adjust the settings accordingly: on the "Account Overview" tab under "Certificates" you can import your S/MIME certificate or PGP key. After successful import, all encrypted messages are sent directly to your inbox.

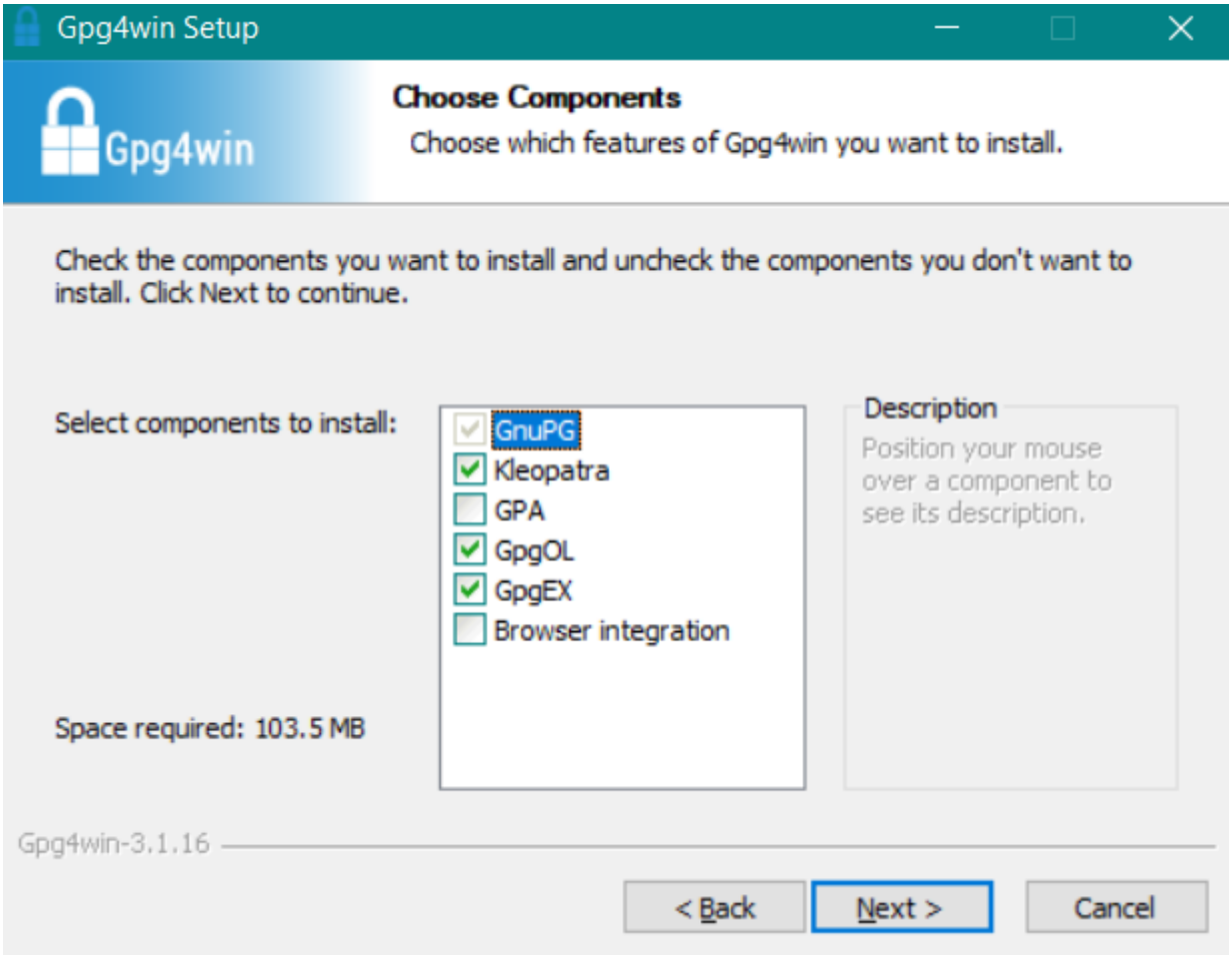
Step 2: Receiving encrypted emails directly without WebMail:
OpenPGP Key/SMIME certificate can be used depending on which external mail client you're using. Below documentation shows the steps on how to use OpenPGP key with Gmail:

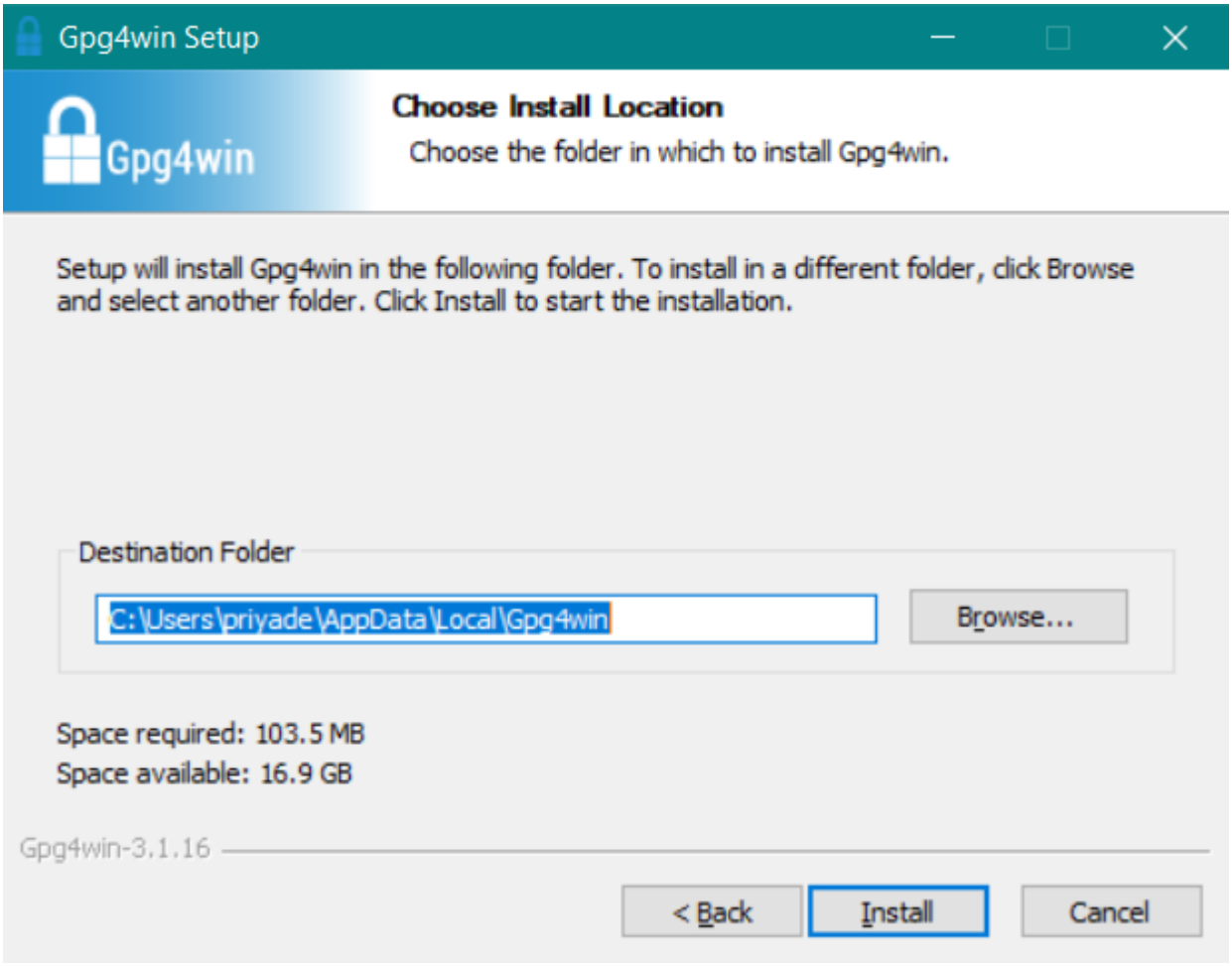


1. Download the Gpg4win tool for generating PGP key pair and use for encryption/decryption, as suggested in Daimler webmail document –

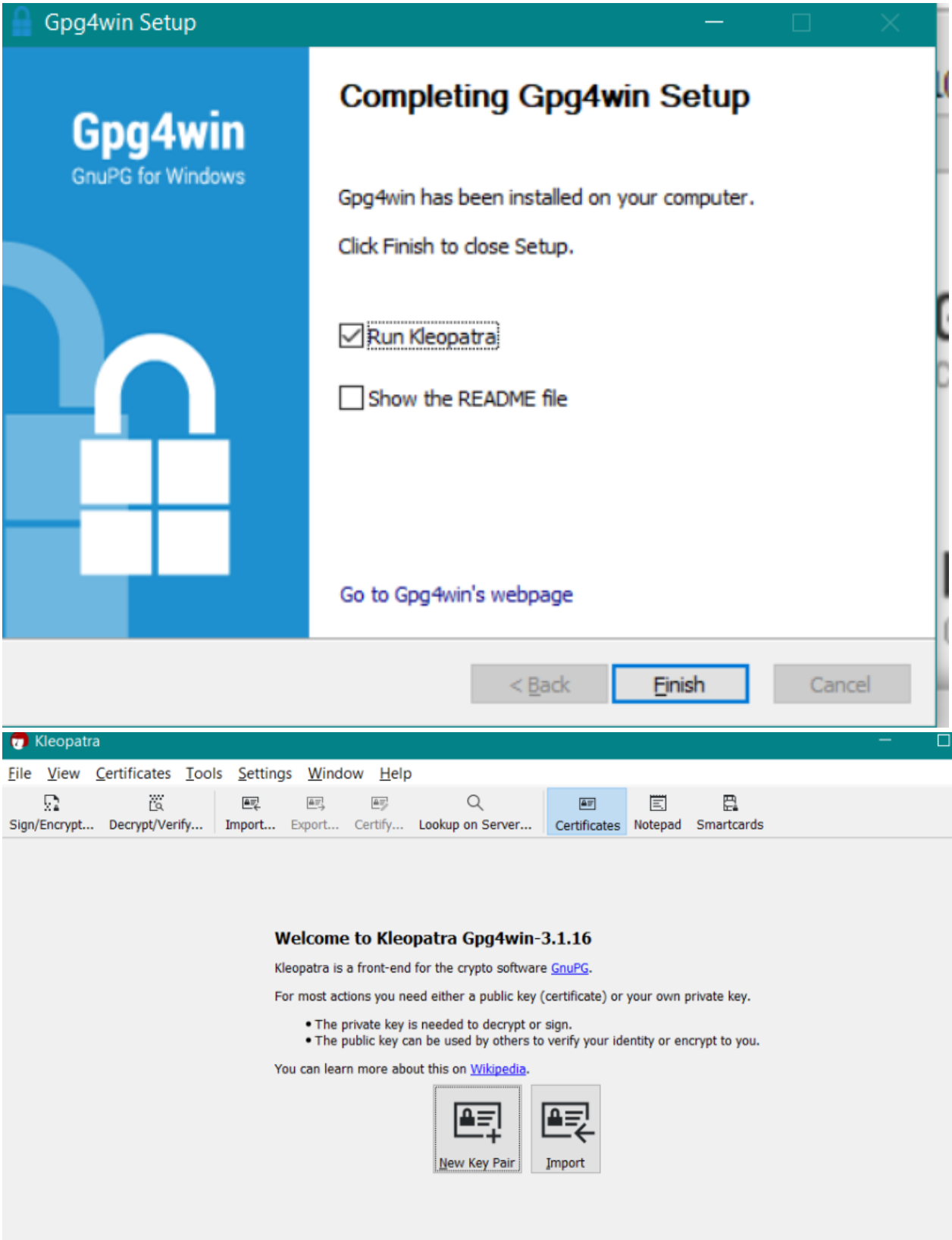
https://webmail.daimler.com/en/faq.html#:~:text=The%20method%20depends%20on%20the%20respective%20email%20client.%20For%20example%2C%20if%20you%20want%20to%20generate%20a%20key%20for%20Outlook%2C%20you%20can%20use%20the%20GpgOL%20plug%2Din.%20Further%20details%20can%20be%20found%20on%20this%20website.
Link to download: https://files.gpg4win.org/gpg4win-3.1.16.exe
Proceed with installation:


Gpg4win Setup
Gpg4win
GnuPG for Windows
Welcome to the installation of Gpg4win
Gpg4win is an installer package for Windows for EMail and file encryption using the core component GnuPG for Windows. Both relevant cryptography standards are supported, OpenPGP and S/MIME. Gpg4win and the software included with Gpg4win is Free Software.
Click Next to continue.
This is Gpg4win version 3.1.16
Release date 2021-06-11
Next >
Cancel

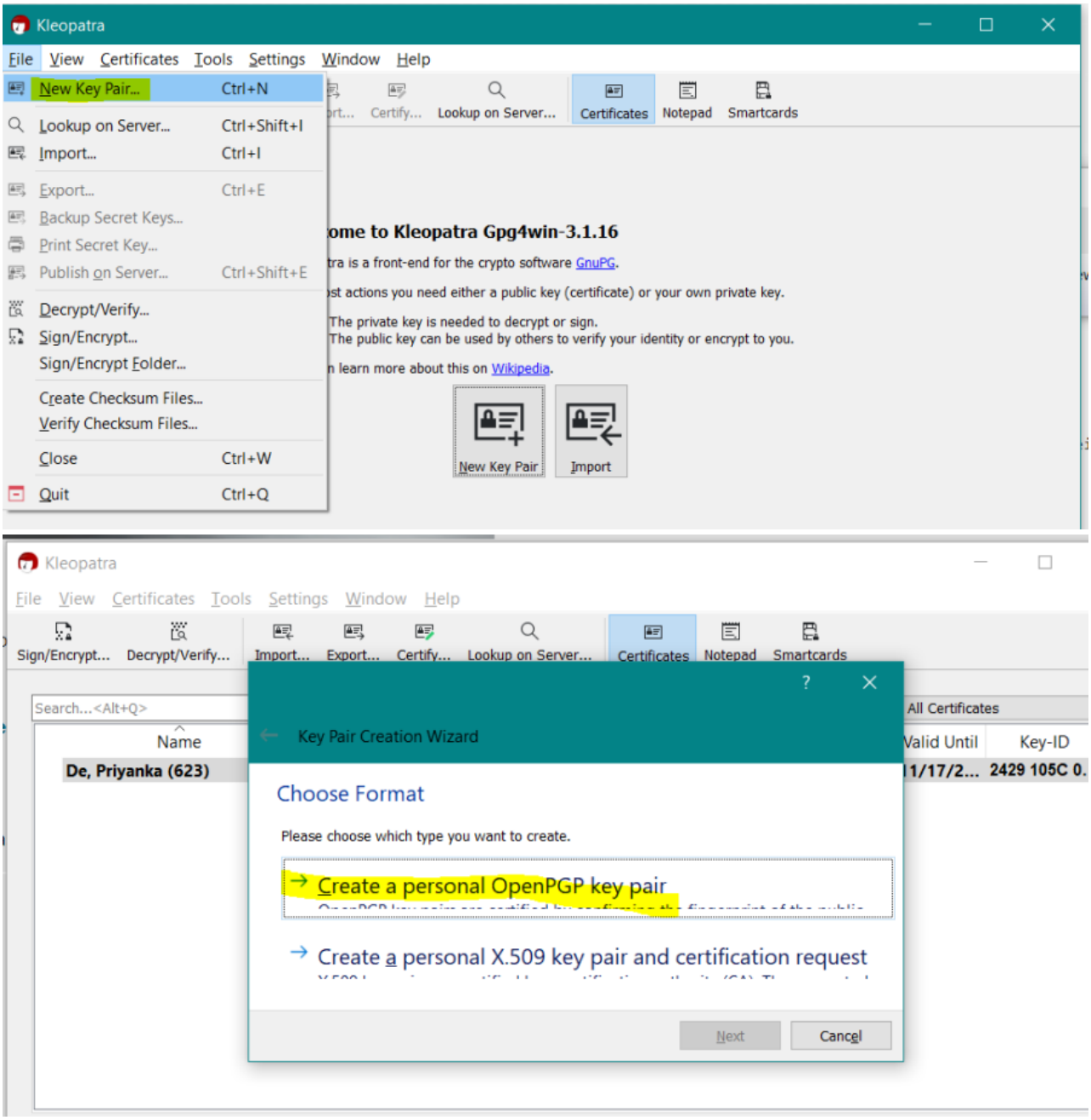

Gpg4win Setup
Gpg4win
Choose Components
Choose which features of Gpg4win you want to install.
Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.
Select components to install:
GnuPG
Kleopatra
GPA
GpgOL
GpgEX
Browser integration
Description
Position your mouse over a component to see its description.
Space required: 103.5 MB
Gpg4win-3.1.16
< Back
Next >
Cancel


Gpg4win Setup
Gpg4win
Choose Install Location
Choose the folder in which to install Gpg4win.
Setup will install Gpg4win in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.
Destination Folder
C:\Users\priyade\AppData\Local\Gpg4win
Browse...
Space required: 103.5 MB
Space available: 16.9 GB
Gpg4win-3.1.16
< Back
Install
Cancel

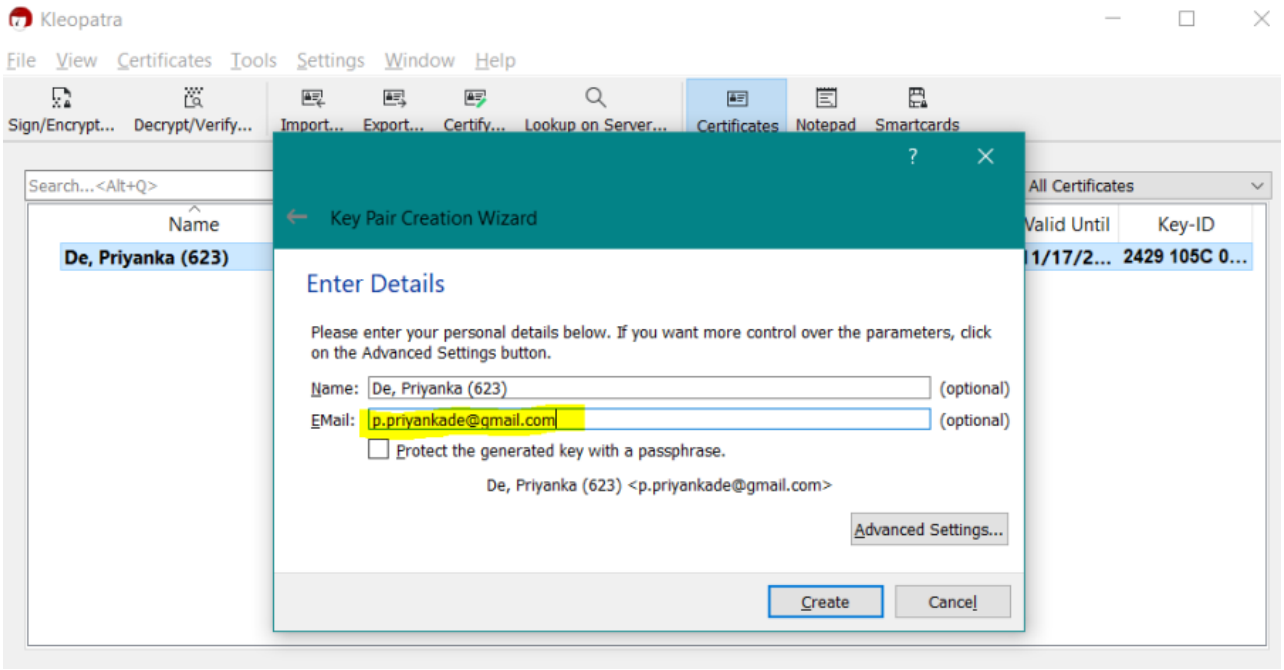

Gpg4win Setup
Gpg4win
Installing
Please wait while Gpg4win is being installed.
Execute: "C:\Users\priyade\AppData\Local\Temp\gnupg-w32-2.2.28-20210610-bin.exe" /S /C
Gpg4win
GnuPG for Windows
GpgOL
Crypto Mails
GpgEX
Crypto Files
GnuPG
Crypto Backend
Kleopatra
Crypto Manager
Gpg4win brings crypto to your desktop!
Gpg4win-3.1.16
< Back
Next >
Cancel



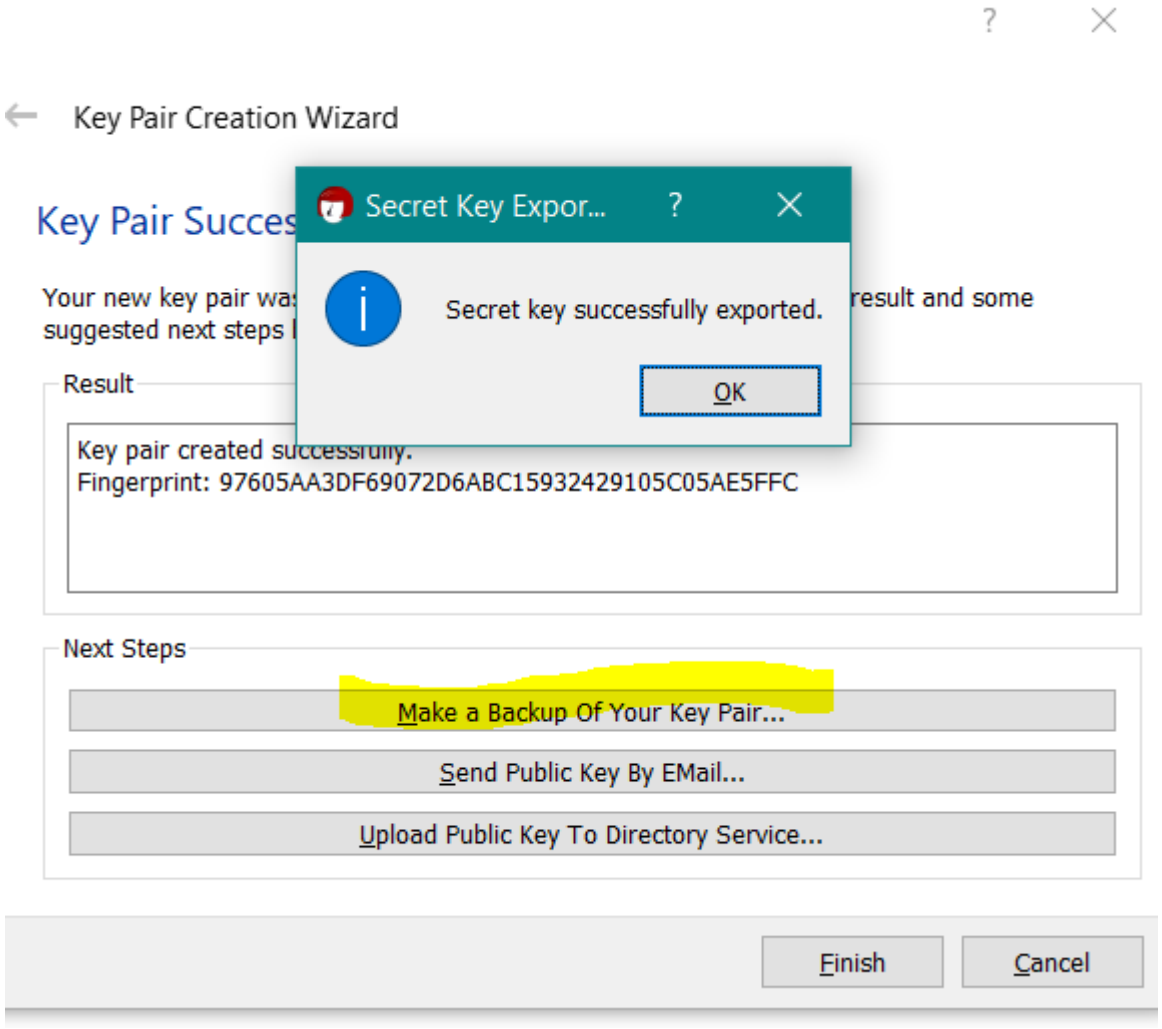
1. Generate New PGP Key pair:

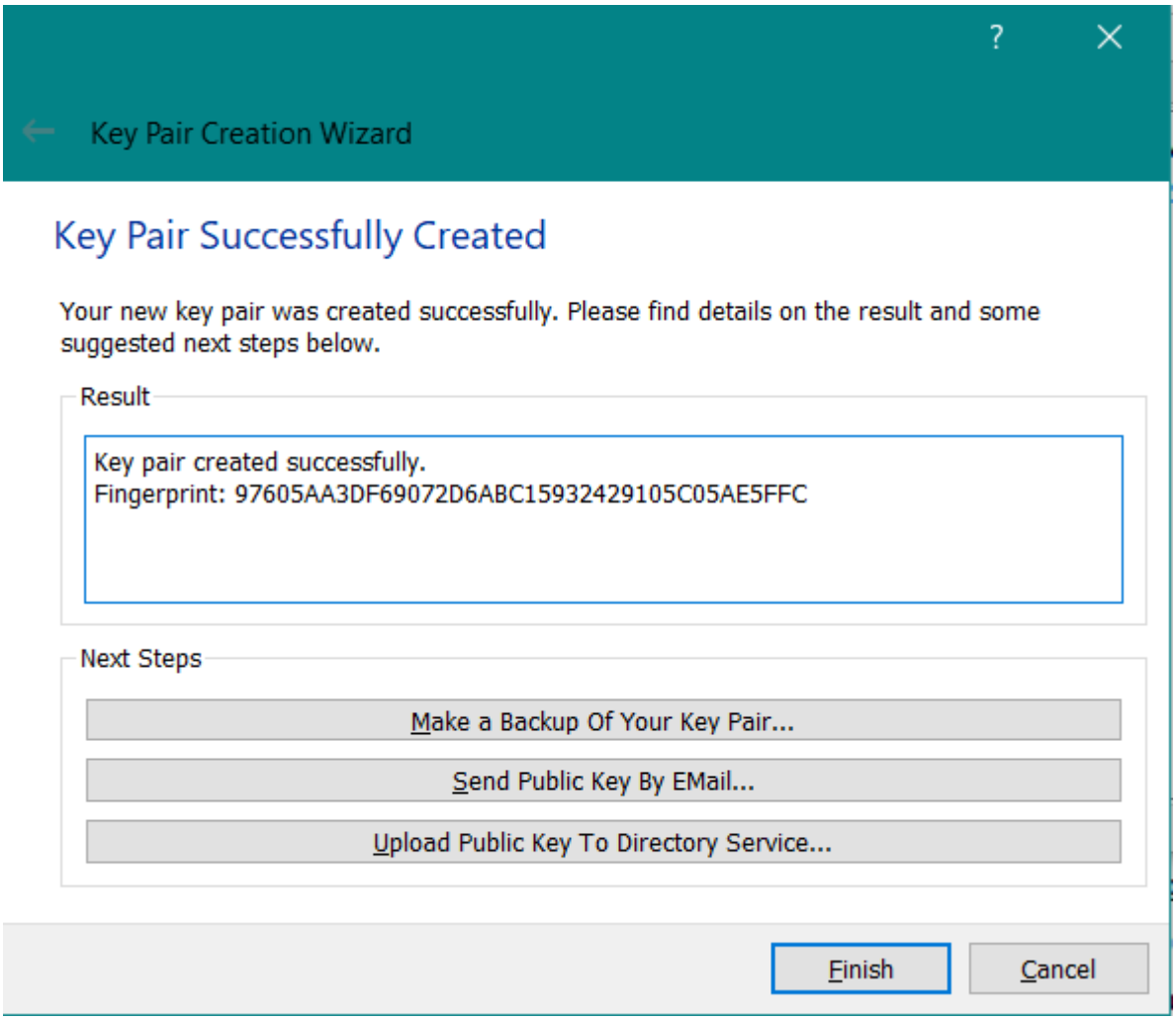

Kleopatra
File View Certificates Tools Settings Window Help
New Key Pair... Ctrl+N
Lookup on Server... Ctrl+Shift+I
Import... Ctrl+I
Export... Ctrl+E
Backup Secret Keys...
Print Secret Key...
Publish on Server... Ctrl+Shift+E
Decrypt/Verify...
Sign/Encrypt...
Sign/Encrypt Folder...
Create Checksum Files...
Verify Checksum Files...
Close Ctrl+W
Quit Ctrl+Q
Certify... Lookup on Server... Certificates Notepad Smartcards
ome to Kleopatra Gpg4win-3.1.16
tra is a front-end for the crypto software GnuPG.
st actions you need either a public key (certificate) or your own private key.
The private key is needed to decrypt or sign.
The public key can be used by others to verify your identity or encrypt to you.
n learn more about this on Wikipedia.
New Key Pair
Import

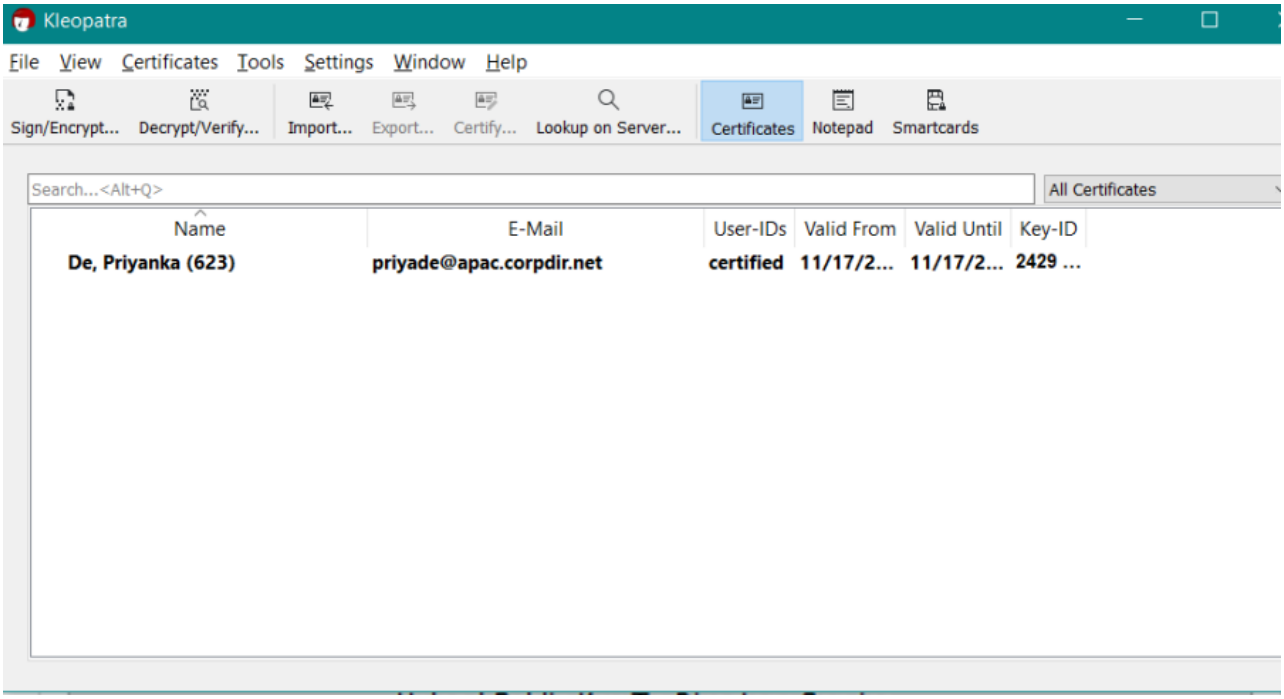
Kleopatra
File View Certificates Tools Settings Window Help
Sign/Encrypt... Decrypt/Verify... Import... Export... Certify... Lookup on Server... Certificates Notepad Smartcards
Search...<Alt+Q>
All Certificates
Name
Valid Until
Key-ID
De, Priyanka (623)
11/17/2... 2429 105C 0.
Key Pair Creation Wizard
Choose Format
Please choose which type you want to create.
Create a personal OpenPGP key pair
Create a personal X.509 key pair and certification request
Next
Cancel



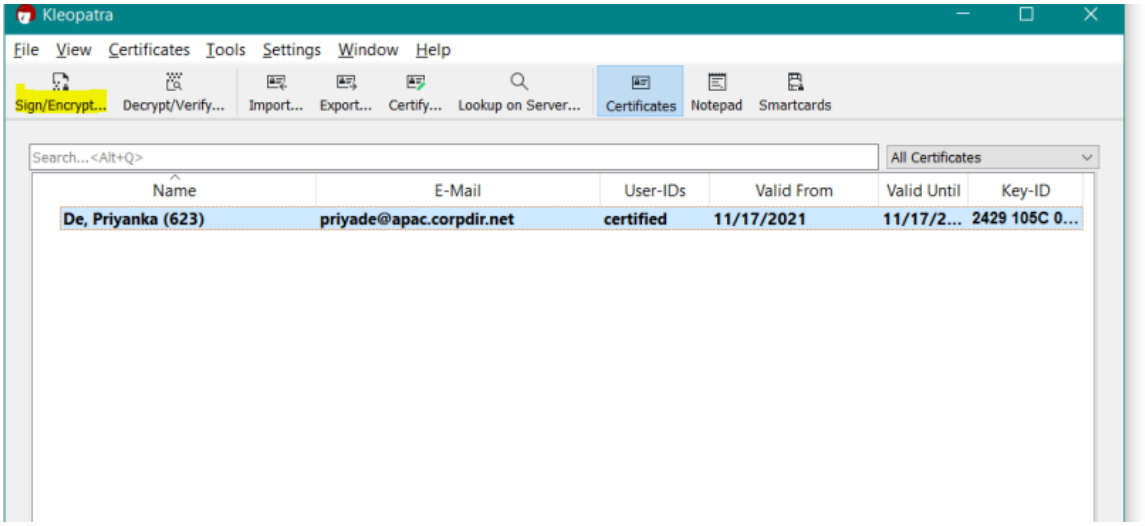
(Use external mail id here, where you will use this PGP key).


Key Pair Creation Wizard
Key Pair Succes
Your new key pair wa
suggested next steps
result and some
Result
Key pair created successfully.
Fingerprint: 97605AA3DF69072D6ABC15932429105C05AE5FFC
Next Steps
Make a Backup Of Your Key Pair...
Send Public Key By EMail...
Upload Public Key To Directory Service...
Finish
Cancel
Secret Key Expor...
Secret key successfully exported.
OK


Key Pair Creation Wizard
Key Pair Successfully Created
Your new key pair was created successfully. Please find details on the result and some suggested next steps below.
Result
Key pair created successfully.
Fingerprint: 97605AA3DF69072D6ABC15932429105C05AE5FFC
Next Steps
Make a Backup Of Your Key Pair...
Send Public Key By EMail...
Upload Public Key To Directory Service...
Finish
Cancel

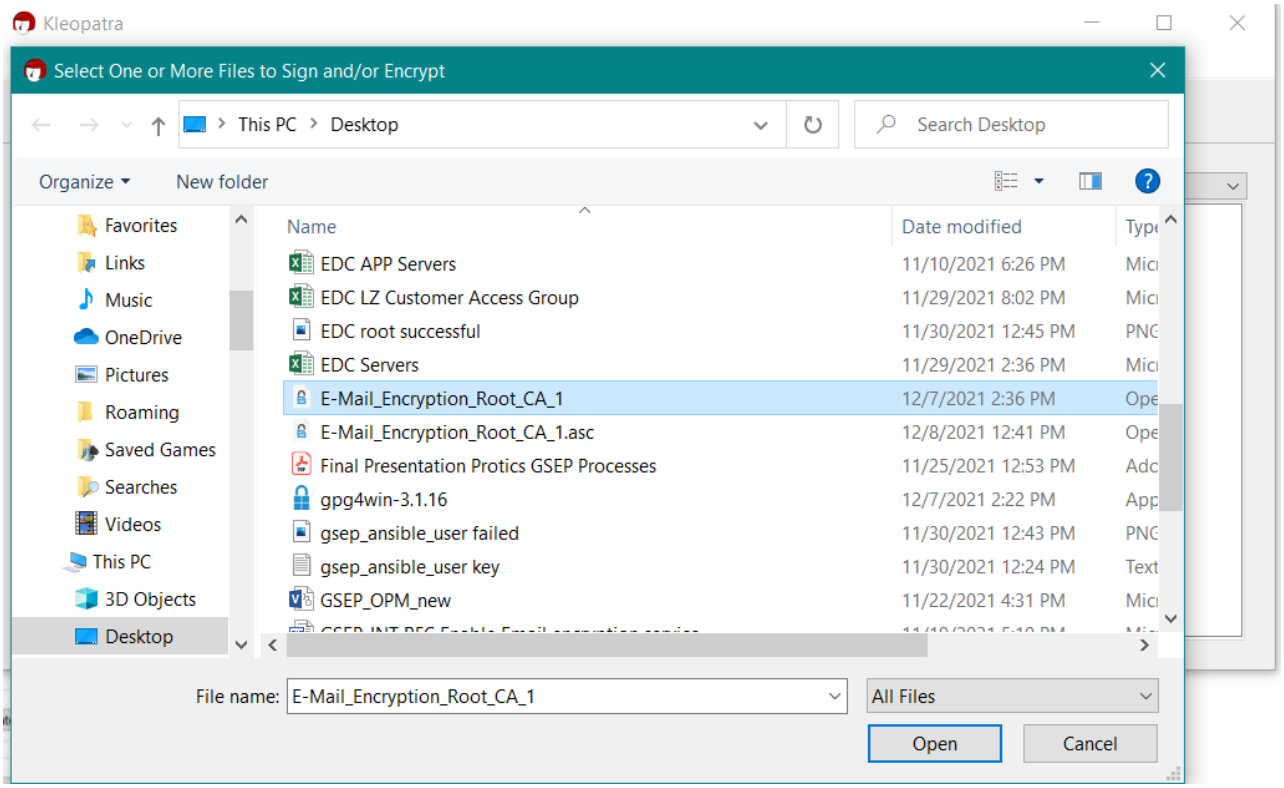


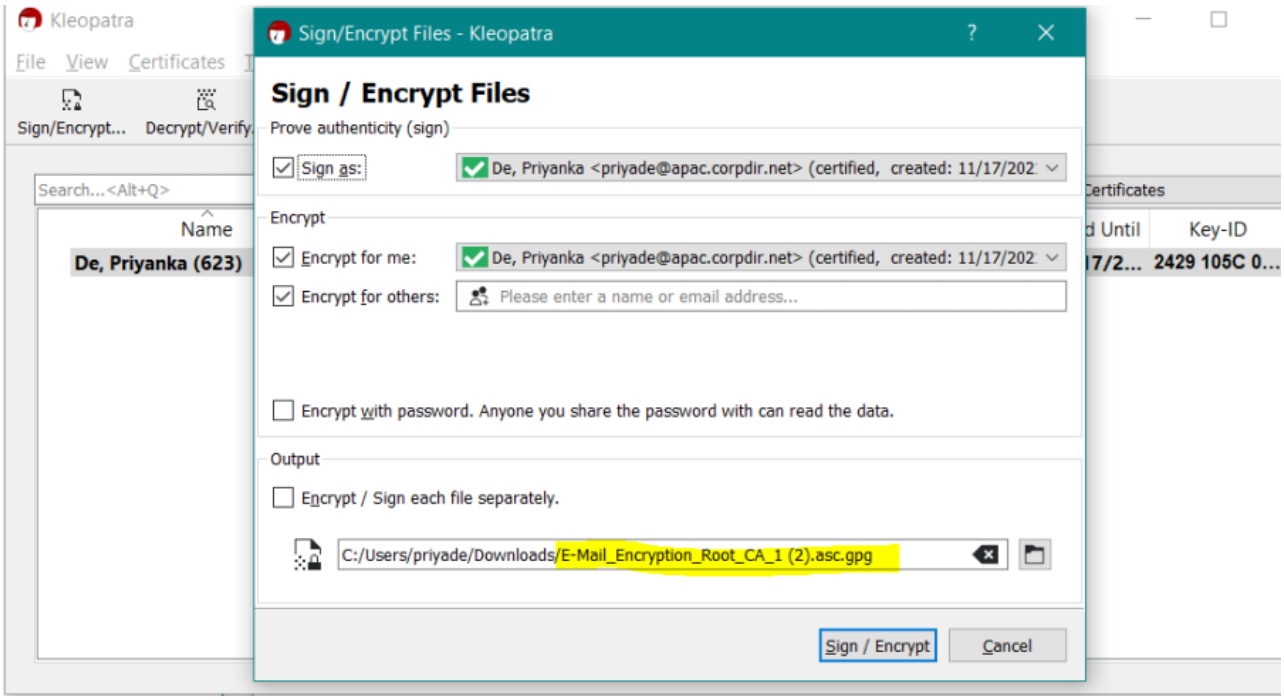
1. Sign it with Daimler Root PGP Key (https://webmail.daimler.com/en/faq.html)

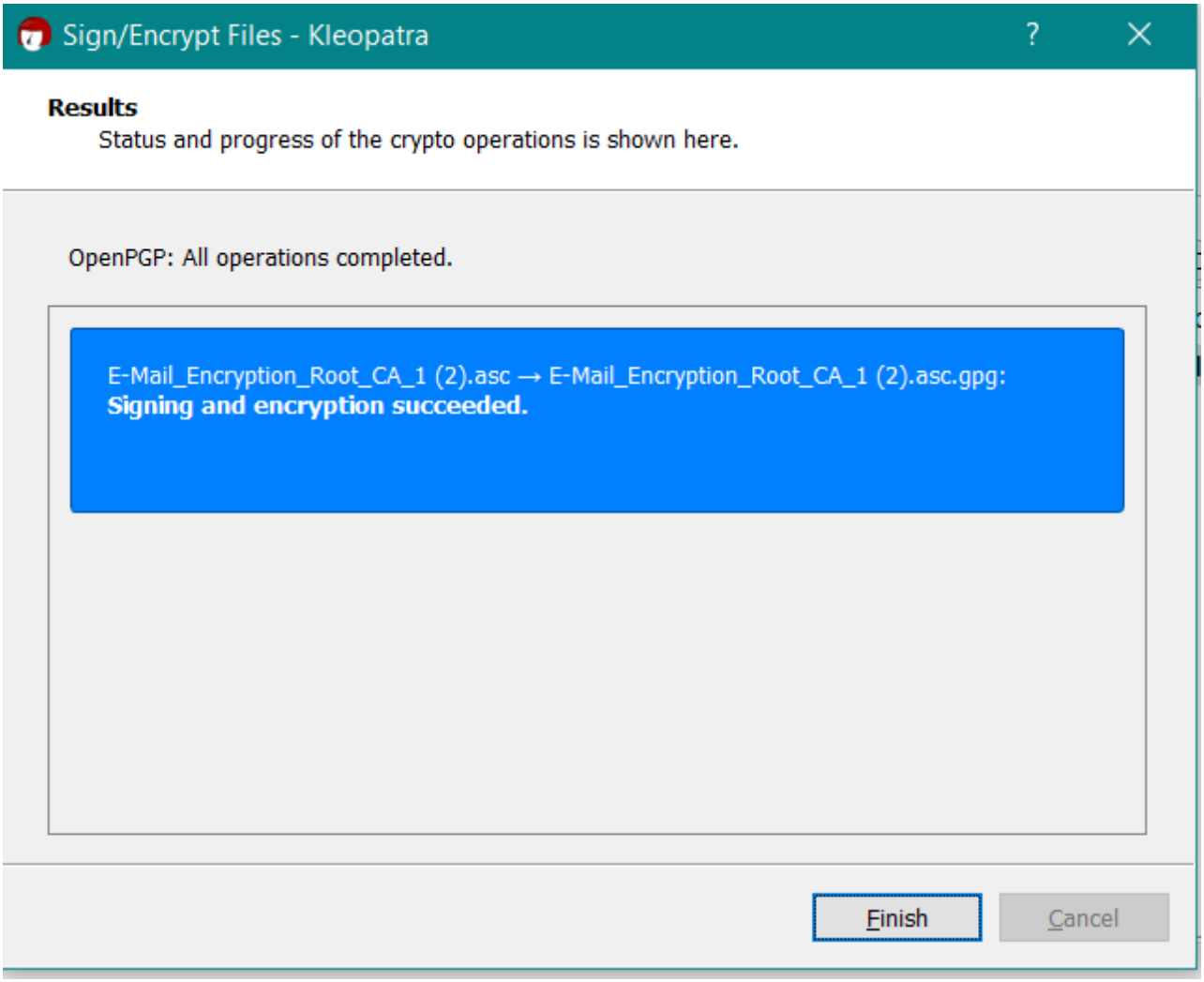


Download Daimler Root PGP Key from: https://webmail.daimler.com/E-Mail_Encryption_Root_CA_1.asc

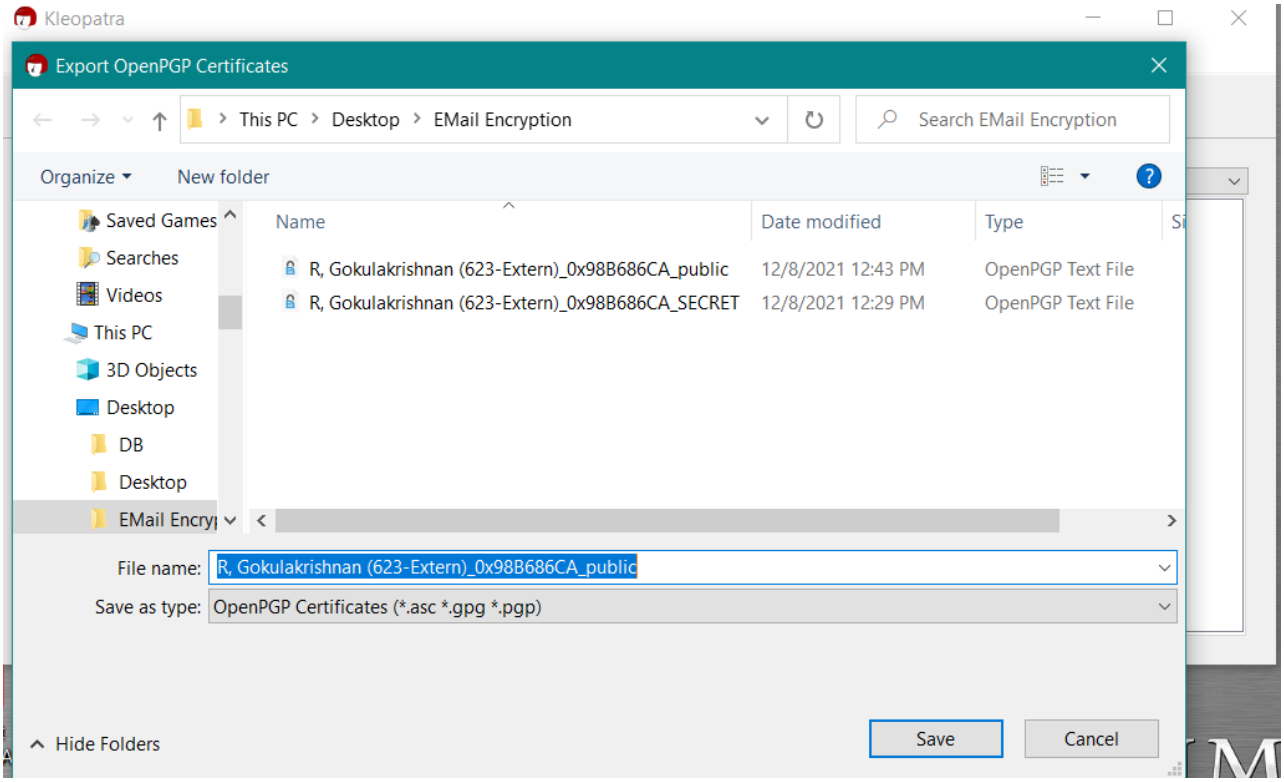
select the E-Mail_Encryption_Root_CA_1


Kleopatra
Select One or More Files to Sign and/or Encrypt
This PC › Desktop
Search Desktop
Organize
New folder
Favorites
Links
Music
OneDrive
Pictures
Roaming
Saved Games
Searches
Videos
This PC
3D Objects
Desktop
Name
Date modified
EDC APP Servers 11/10/2021 6:26 PM
EDC LZ Customer Access Group 11/29/2021 8:02 PM
EDC root successful 11/30/2021 12:45 PM
EDC Servers 11/29/2021 2:36 PM
E-Mail_Encryption_Root_CA_1 12/7/2021 2:36 PM
E-Mail_Encryption_Root_CA_1.asc 12/8/2021 12:41 PM
Final Presentation Protics GSEP Processes 11/25/2021 12:53 PM
gpg4win-3.1.16 12/7/2021 2:22 PM
gsep_ansible_user failed 11/30/2021 12:43 PM
gsep_ansible_user key 11/30/2021 12:24 PM
GSEP_OPM_new 11/22/2021 4:31 PM
File name: E-Mail_Encryption_Root_CA_1
All Files
Open
Cancel

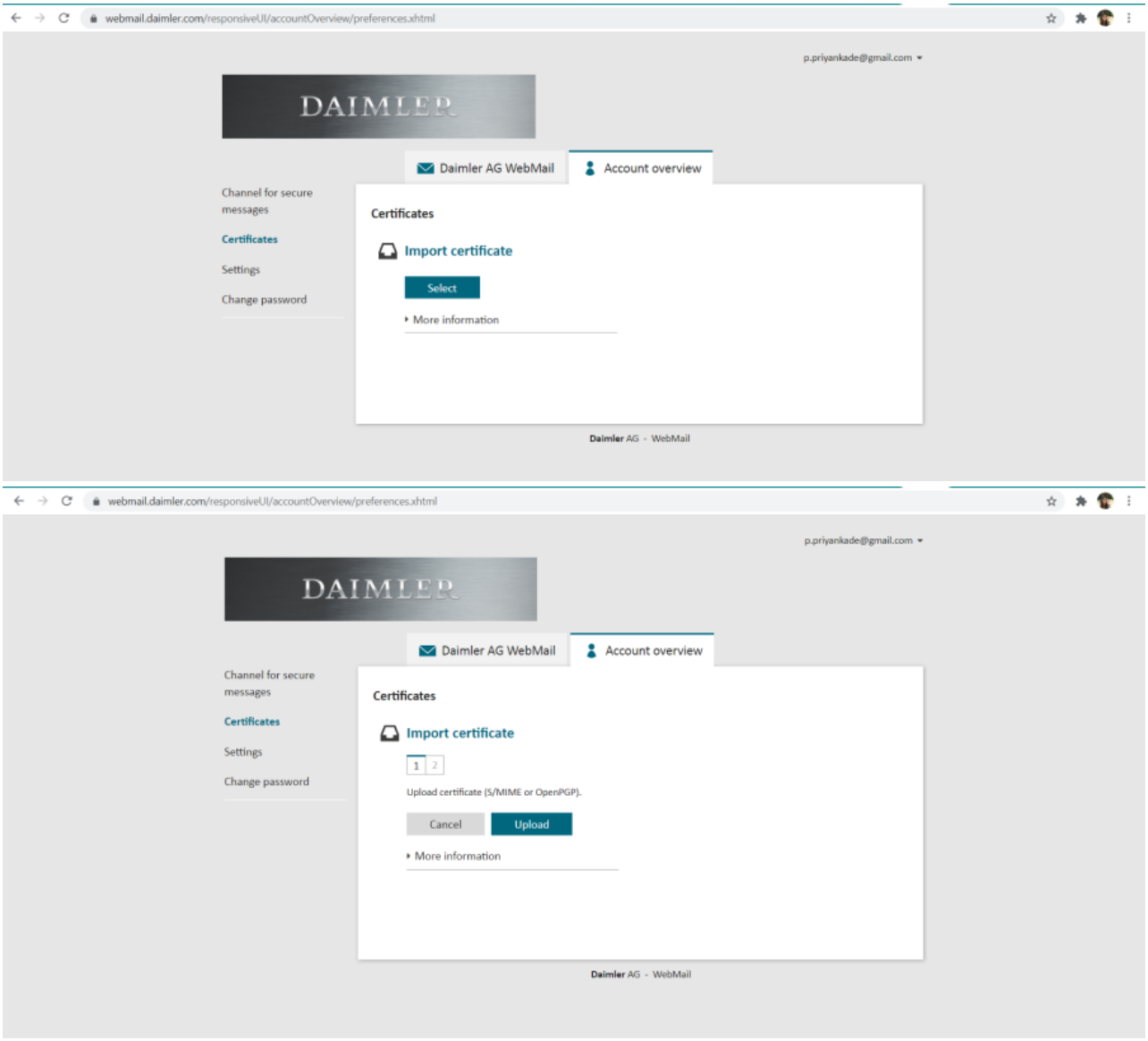

Kleopatra
File View Certificates
Sign/Encrypt...
Decrypt/Verify
Search...<Alt+Q>
Name
De, Priyanka (623)
Sign/Encrypt Files - Kleopatra
Sign / Encrypt Files
Prove authenticity (sign)
Sign as:
De, Priyanka <priyade@apac.corpdir.net> (certified, created: 11/17/202
Encrypt
Encrypt for me:
De, Priyanka <priyade@apac.corpdir.net> (certified, created: 11/17/202
Encrypt for others:
Please enter a name or email address...
Encrypt with password. Anyone you share the password with can read the data.
Output
Encrypt / Sign each file separately.
C:/Users/priyade/Downloads/E-Mail_Encryption_Root_CA_1 (2).asc.gpg
Sign / Encrypt
Cancel
Certificates
Until
Key-ID
2429 105C 0...



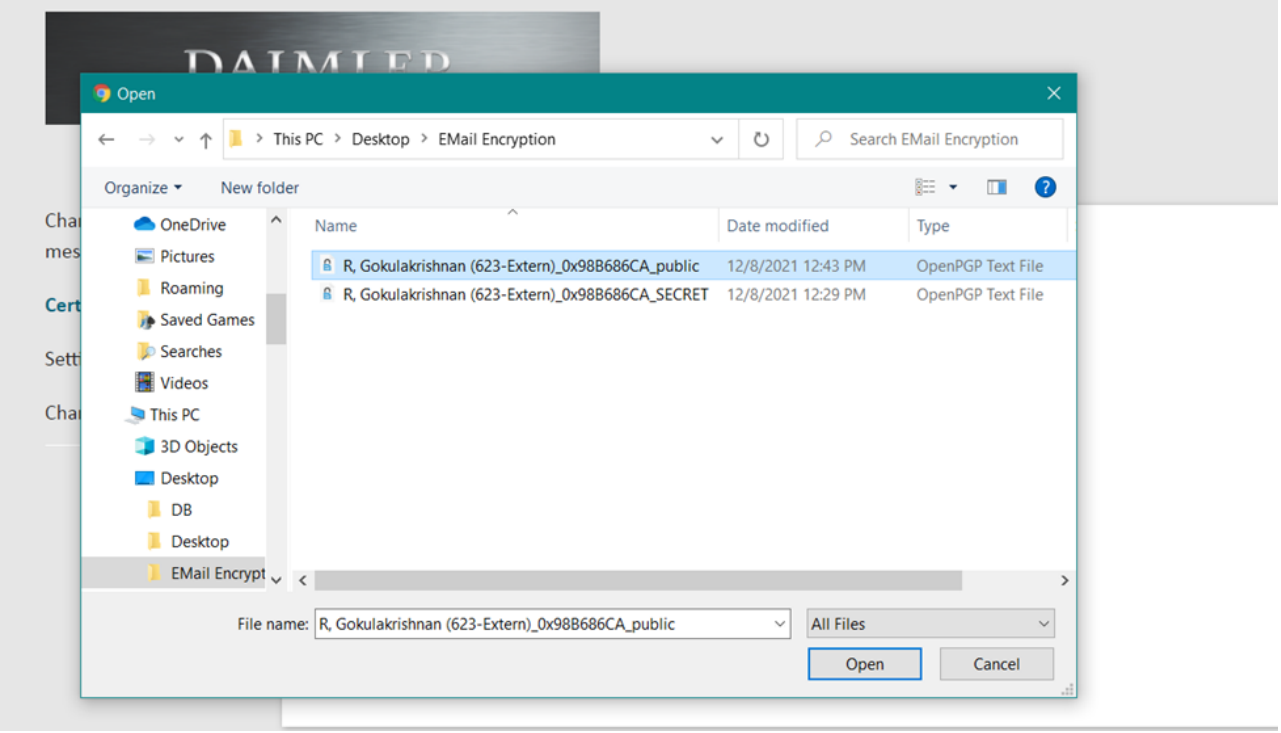
Export/save the public key

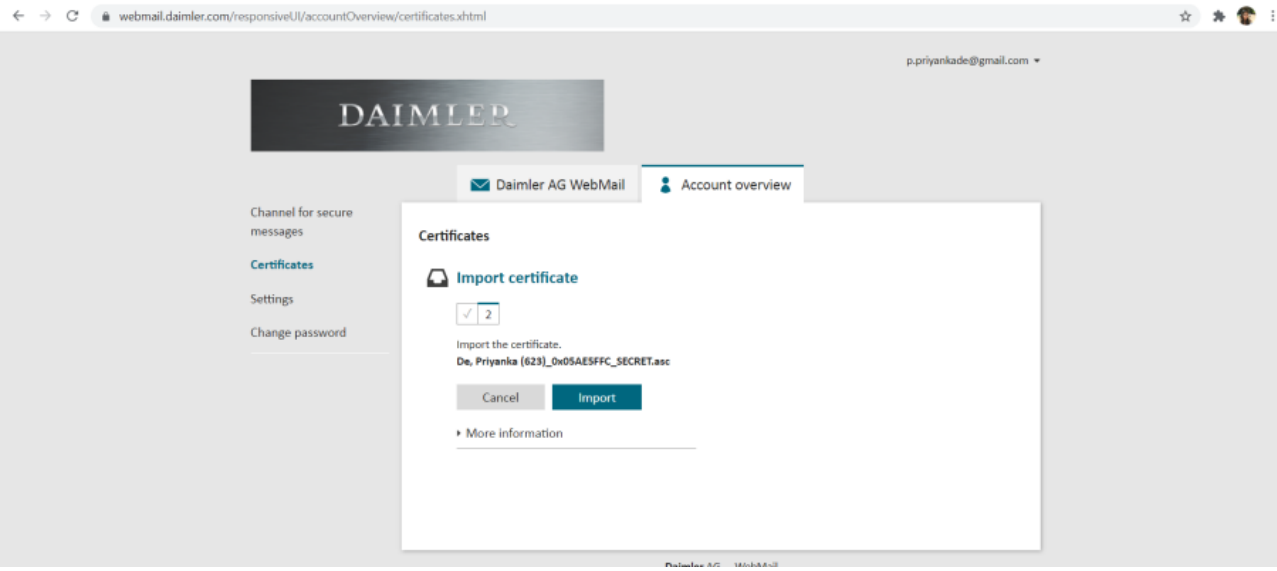


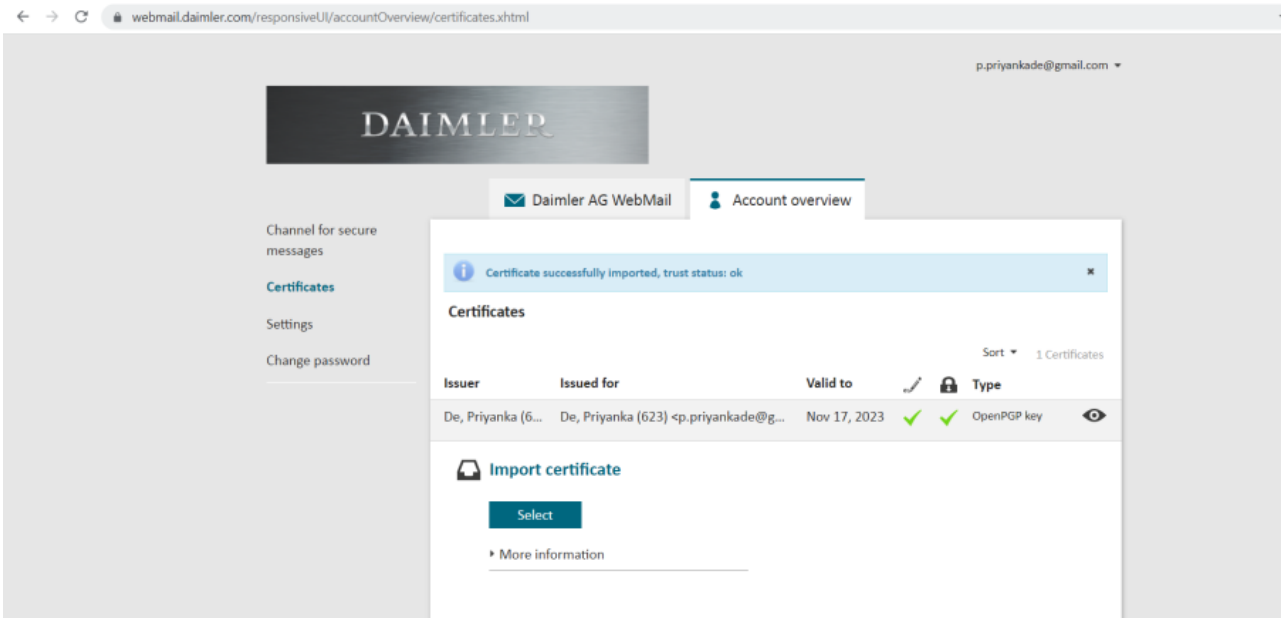
Import Daimler signed PGP key - under Certificates in WebMail portal:



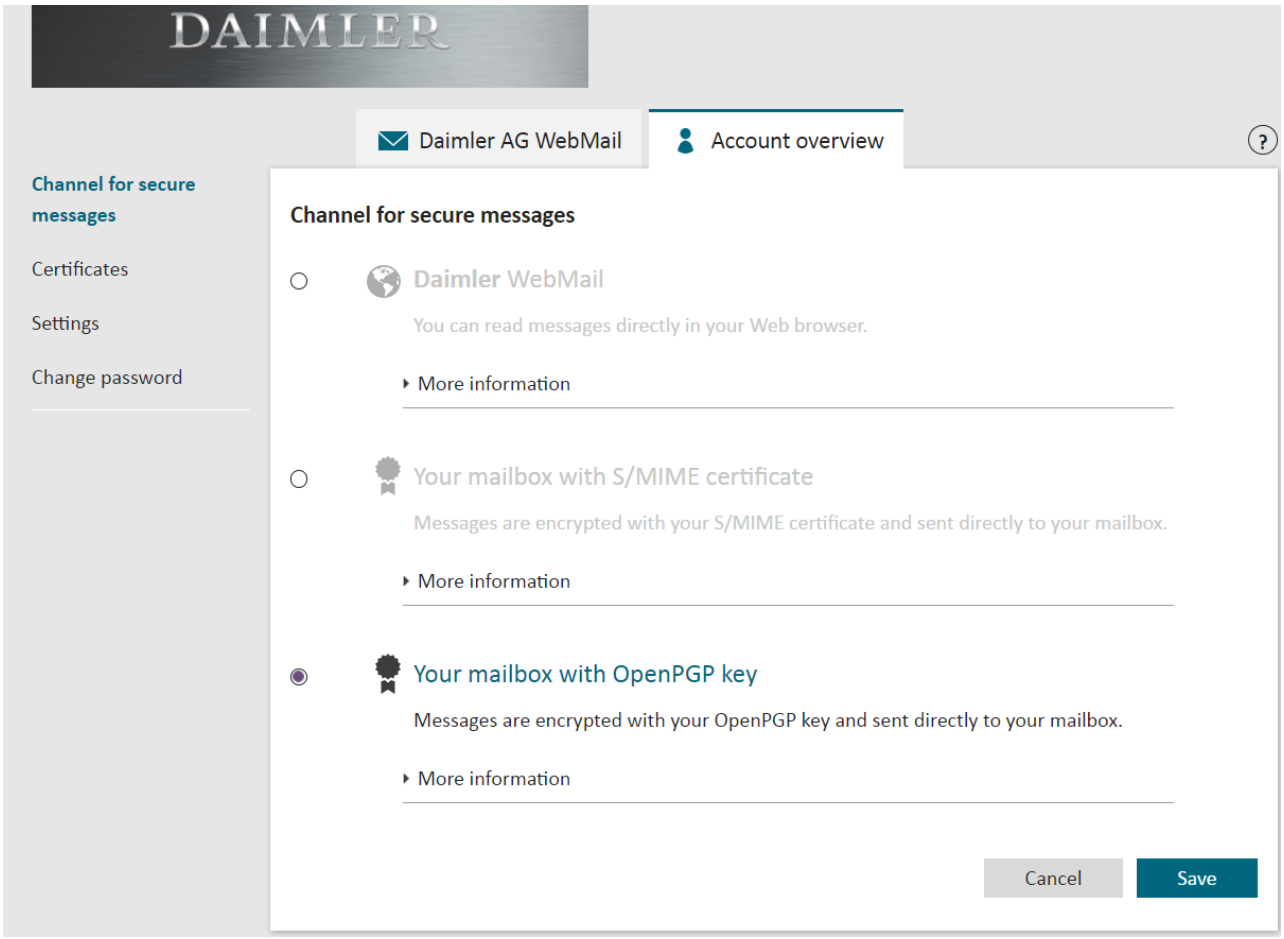
Import the public key

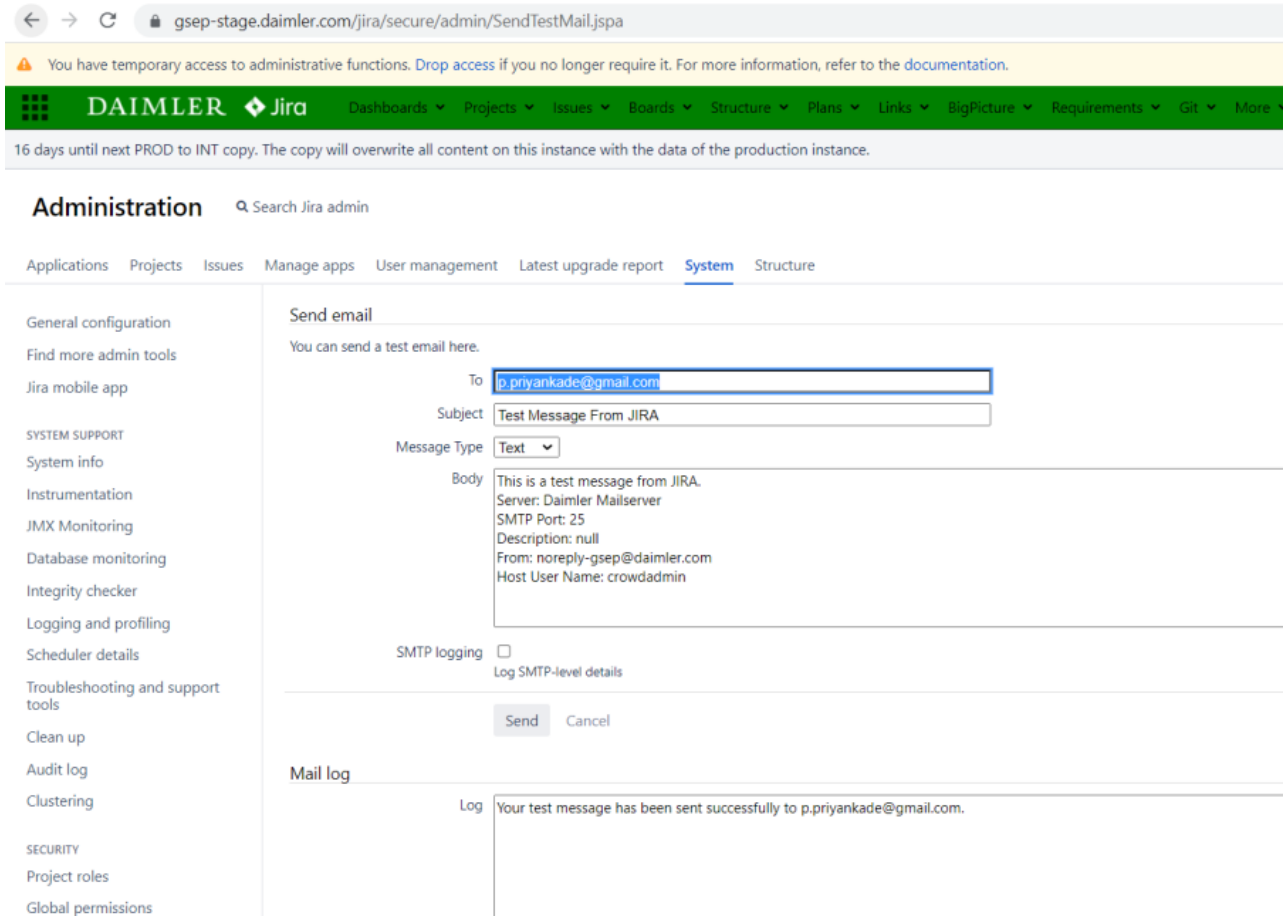

Open
This PC > Desktop > EMail Encryption
Search EMail Encryption
Organize
New folder
OneDrive
Pictures
Roaming
Saved Games
Searches
Videos
This PC
3D Objects
Desktop
DB
Desktop
EMail Encrypt
Name
Date modified
Type
R, Gokulakrishnan (623-Extern)_0x98B686CA_public
12/8/2021 12:43 PM
OpenPGP Text File
R, Gokulakrishnan (623-Extern)_0x98B686CA_SECRET
12/8/2021 12:29 PM
OpenPGP Text File
File name:
R, Gokulakrishnan (623-Extern)_0x98B686CA_public
All Files
Open
Cancel


webmail.daimler.com/responsiveUI/accountOverview/certificates.xhtml
p.priyankade@gmail.com
DAIMLER
Daimler AG WebMail
Account overview
Channel for secure messages
Certificates
Settings
Change password
Certificates
Import certificate
Import the certificate.
De, Priyanka (623)_0x05AE5FFC_SECRET.asc
Cancel
Import
More information



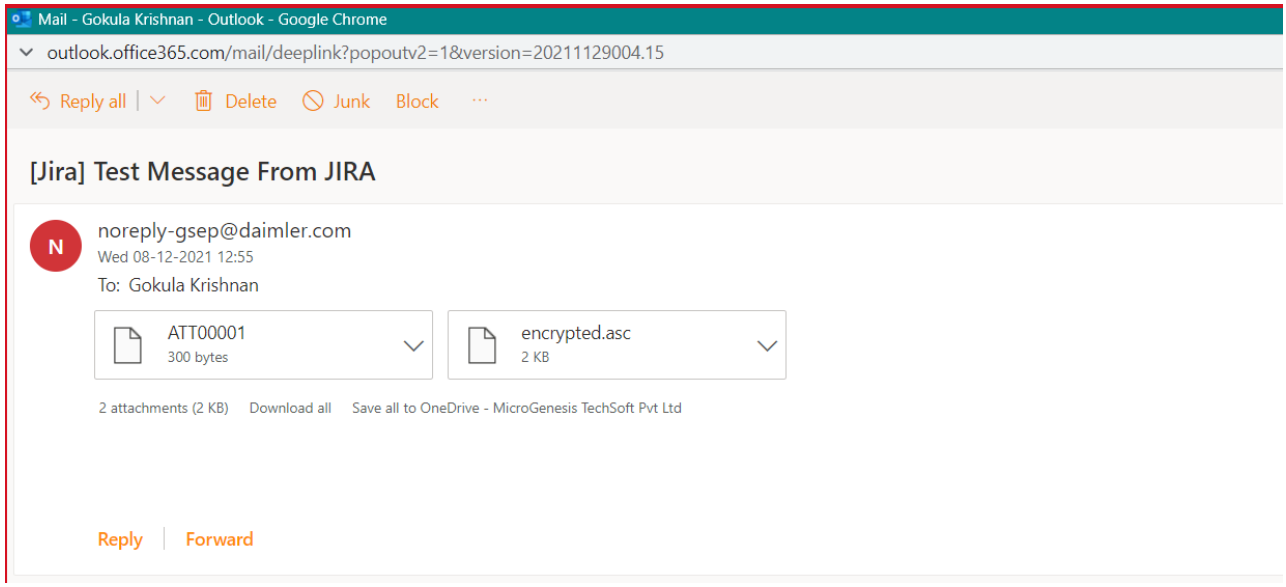
Change the channel for secure messages to Open PGP key and click on save



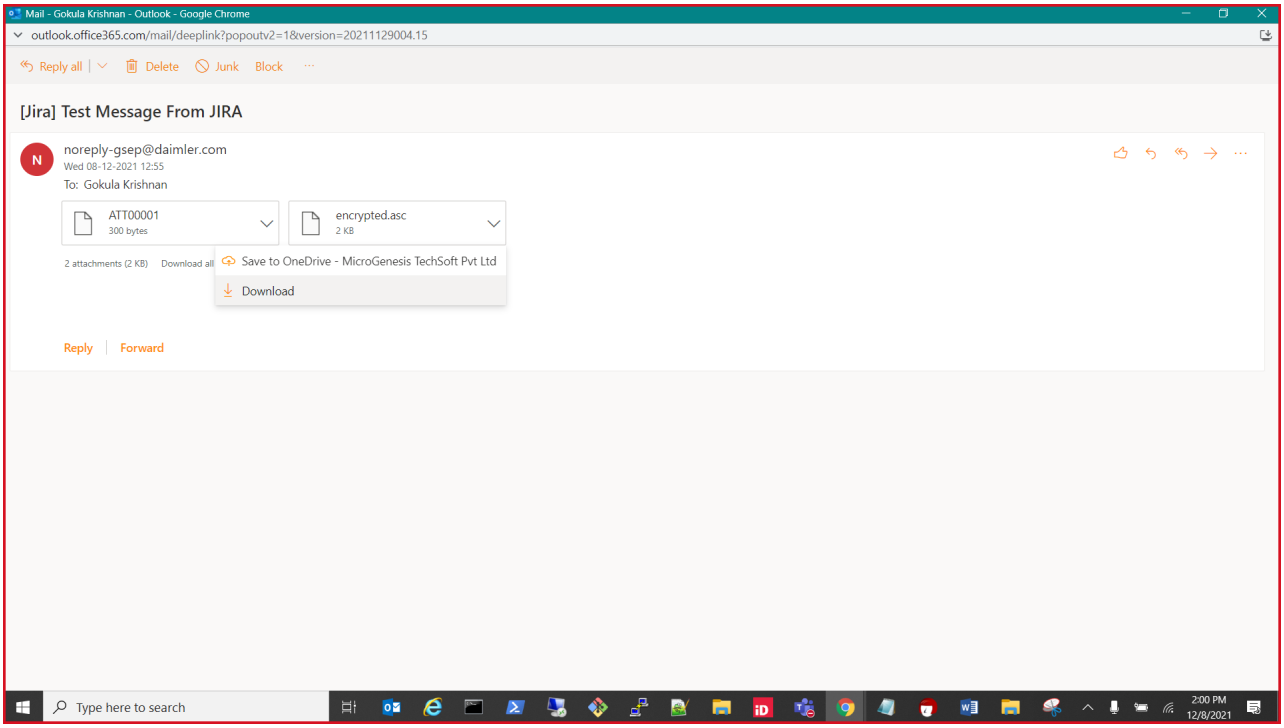


Decrypting the message:

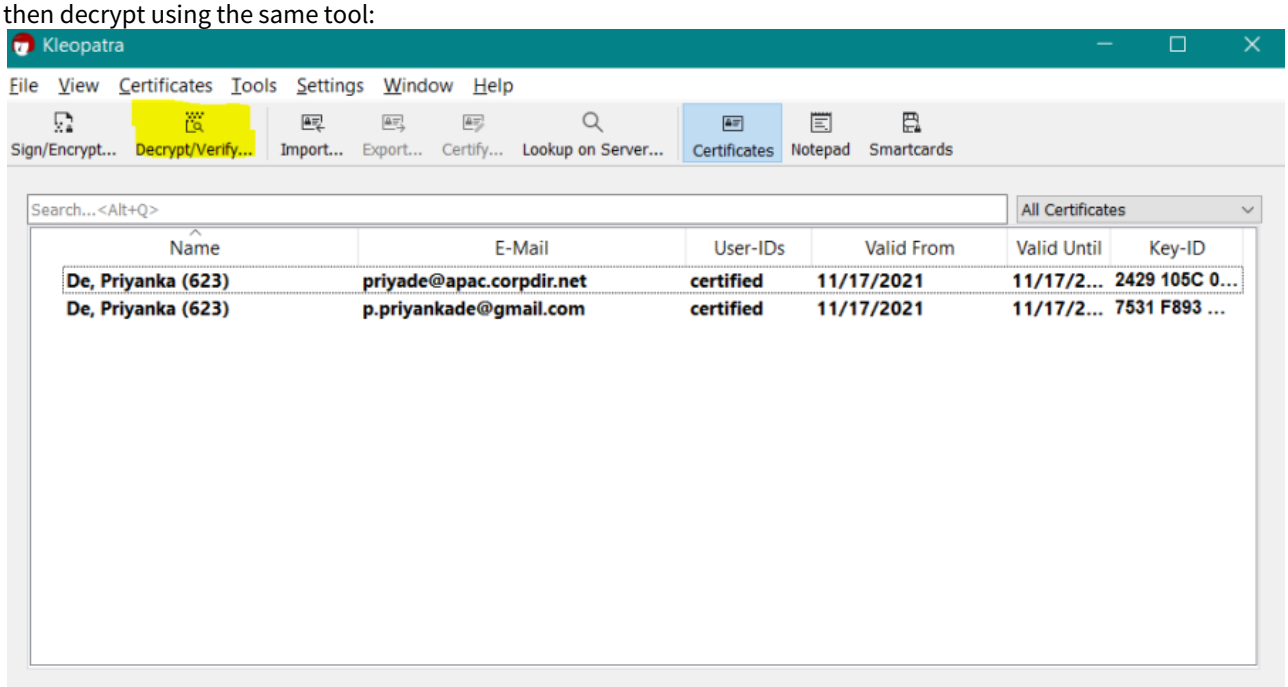
Go to your external mailbox (Outlook, Gmail etc)

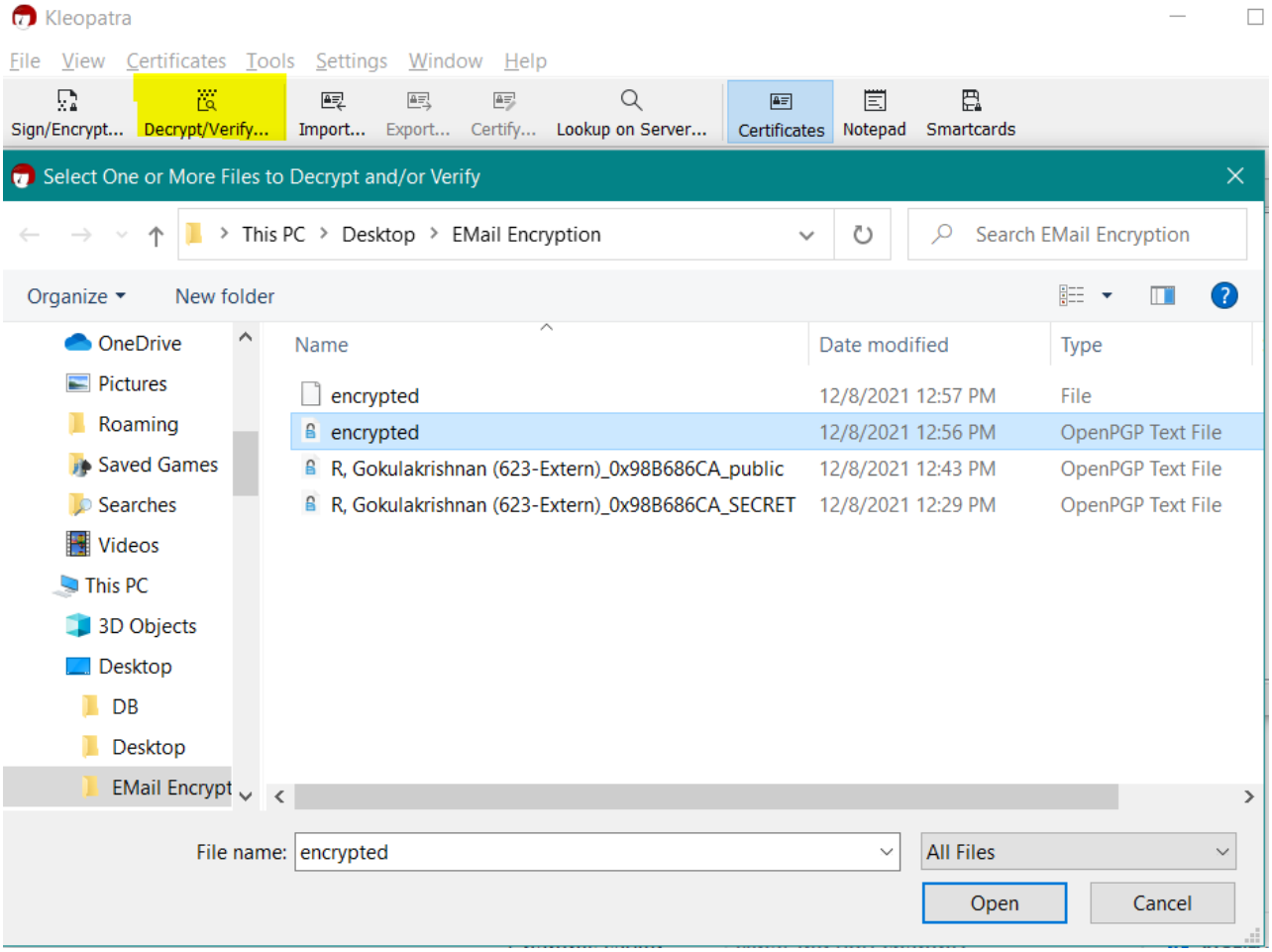


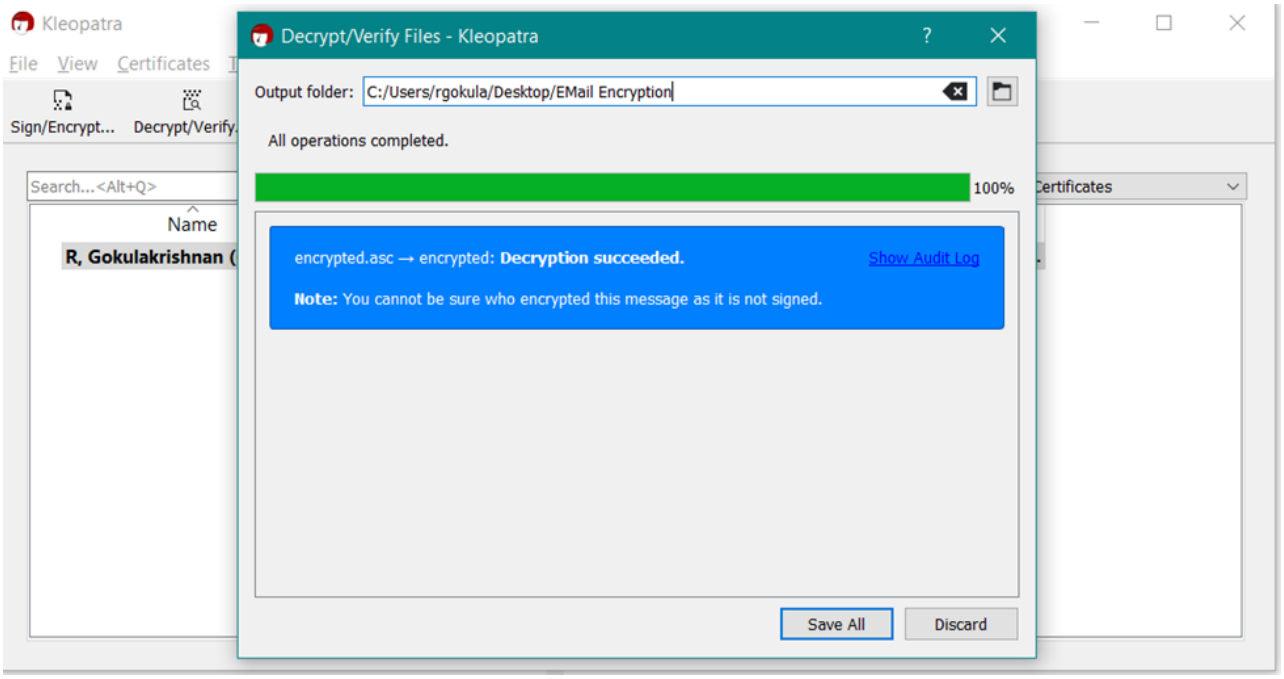
First, download the encrypted.asc message

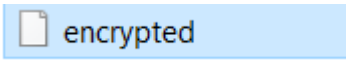


then decrypt using the same tool:




Kleopatra
File View Certificates Tools Settings Window Help
Sign/Encrypt...
Decrypt/Verify...
Import...
Export...
Certify...
Lookup on Server...
Certificates
Notepad
Smartcards
Select One or More Files to Decrypt and/or Verify
This PC › Desktop › EMail Encryption
Search EMail Encryption
Organize
New folder
OneDrive
Pictures
Roaming
Saved Games
Searches
Videos
This PC
3D Objects
Desktop
DB
Desktop
EMail Encrypt
Name
Date modified
Type
encrypted 12/8/2021 12:57 PM File
encrypted 12/8/2021 12:56 PM OpenPGP Text File
R, Gokulakrishnan (623-Extern)_0x98B686CA_public 12/8/2021 12:43 PM OpenPGP Text File
R, Gokulakrishnan (623-Extern)_0x98B686CA_SECRET 12/8/2021 12:29 PM OpenPGP Text File
File name: encrypted
All Files
Open
Cancel



Creates encrypted message file - 

, which can be opened in Notepad:

```
Content-Type: multipart/mixed;
    boundary="----=_Part_103738_941650507.1637219174155"

------=_Part_103738_941650507.1637219174155
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 7bit

This is a test message from JIRA.
Server: Daimler Mailserver
SMTP Port: 25
Description: null
From: noreply-gsep@daimler.com
Host User Name: crowdadmin

This is a test email
------=_Part_103738_941650507.1637219174155--

```

9 How to onboard suppliers to GSEP

Click here[81]to view the documented details steps to onboard Supplier user.

This guide shall assist Mercedes-Benz suppliers that requires access to GSEP Tools, GSEP user onboarding include prerequisites, and support contact details.

Steps to follow in Mercedes-Benz supplier portal:

1. Supplier user must register with valid user details (incl. phone number, email id) in Mercedes-Benz supplier portal[82]. Step by step info: GSEP supplier registration guide[83] in Mercedes-Benz supplier portal. Note: Follow supplier portal FAQ[84]s for more details.
2. Once the user id approved by the portal admin, validate your account, login with temporary password sent via email and set new password, check if login is successful. More info: E-mail verification & password reset[85].

Note: Login into supplier portal and GSEP at least once in 3 months to keep your account valid/active.

The continue with GSEP setup:

1. Please check: How to Login in GSEP(see page 6)
2. Once the registration is complete, reach out to the Mercedes-Benz project point of contact person to raise request in Zula[86]to grant access to projects in GSEP platform.
3. User onboarding to GSEP is complete, when the access request is approved. Approval process may take few days to complete.
4. Supplier user would receive a welcome email from GSEP that consists of:
   a. GSEP-ALM certificate along with installation guide (to access GSEP via internet, the user based ALM certificate must be installed in the users system e.g. in Web browser, GIT client, etc.) that connects to GSEP.
   b. Certificate password.
   c. GSEP password reset link.
5. After installing certificates, please try to access GSEP landing page: https://gsep.daimler.com/.
6. Try to access GSEP User Knowledge Base[87] as well available on the GSEP landing page.
7. Access your project in the desired application available on the landing page, check: How to Login in GSEP(see page 6)
   a. Jira and confluence-Please use your supplier portal id and supplier portal password as user name and password followed by ping id to login. More details related to MFA: multi-factor authentication.
   b. Other GSEP applications-Please use your supplier portal id and GSEP password from the welcome mail to login.

If you have problems, check this page: GSEP - How to get help[88].

For queries regarding Mercedes-Benz supplier portal registration for users/company or access issues, please reach supplier portal helpdesk via phone or email provided below.
Phone Numbers:

- Germany: +49 (0) 711 17 95120

81 https://team.sp.wp.corpintra.net/sites/03009/General%20Information/GSEP_Supplier_OnePager.pdf
82 https://supplier-portal.daimler.com/portal/en
8 https://team.sp.wp.corpintra.net/sites/03009/_layouts/15/WopiFrame.aspx?sourcedoc=%7BA7B1B88E-7984-42BB-A102-7C1218C820C3%7D&file=GSEP%20-%20Supplier%20Registration%20Guide%20in%20Mercedes-Benz%20Supplier%20Portal.docx&action=default&IsList=1&ListId=%7BCEBA1A57-3AC0-4DE8-B0D6-55A86320BD7F%7D&ListItemId=104
84 https://supplier-portal.daimler.com/portal/public-help
85 https://supplier-portal.daimler.com/docs/DOC-2278
86 https://zulaplus.e.corpintra.net/ZulaPlus/faces/pages/template/zula-home.xhtml
87 https://gsep.daimler.com/confluence/pages/viewpage.action?spaceKey=GSEPUKB&title=GSEP+User+Knowledge+Base+Home
88 https://gsep-int.daimler.com/confluence/display/GSEPUKB/GSEP+-+How+to+get+help

- Global Toll Free: + (00) 800 711 70372
- E-Mail: Support.Supplier-Portal@daimler.com[89]

Please note: If a phone number starts with +, then the country-specific area code must always be pre-dialed from a landline (e.g. 00 from Germany or 011 from the USA).

ServiceNow KB article- KB0349945[90]

89 mailto:Portal@daimler.com
90 https://servicenow.i.mercedes-benz.com/esc?id=kb_article&table=kb_knowledge&sys_kb_id=107b37af1b3499101d67a7953b4bcb06