

This is the startpage of TRUEman

TRUEman stands for =>
True Remote User Enrollment manager

The start page should give some info on how to login.

The whole App should support multi language depnding on the browser locale. First phase is ok to start with english

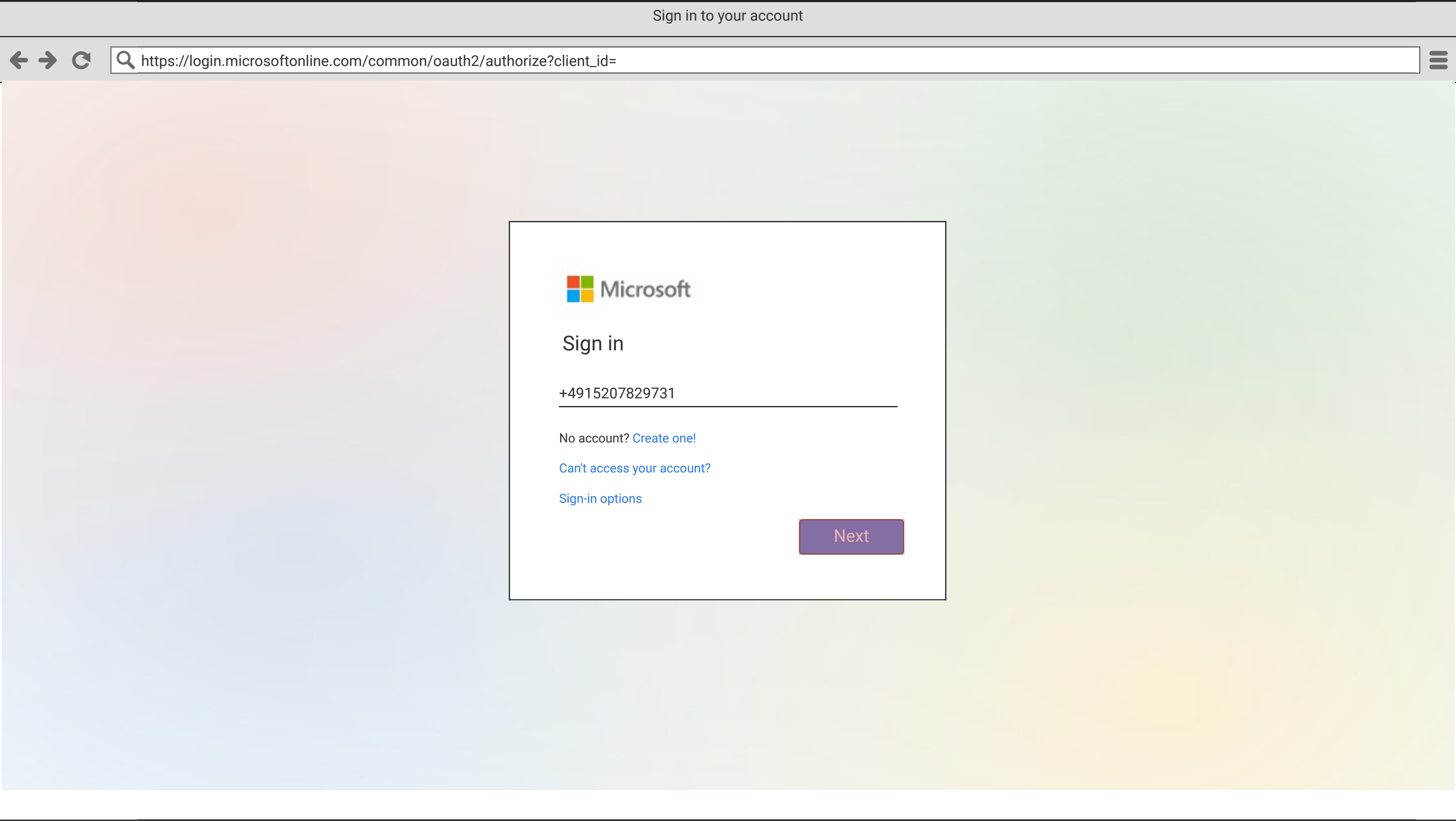
Progress of the user should be stored in a backend system. So it is possible to jump to the previous position in case of an interruption or an error.

The TRUEman framework should be easily customizable to adapt logo and css to the particular tenant.
Each "page" in TRUEman should be a kind of template that does a certain task.
Which "pages" appear in which order should be writable in a YAML/JSON job file, so that a customization per client can be done regarding the order and number of page flows.

The URI in the example shows that a client may be mapped via a hostname (in the example Contoso) and then one of n flows follows - where a /d/ stands for the default flow. That with several flows per mandant would be optional in the phase 1 however also.

Assests etc. should come best from a (public) storage. Public would have the advantage to work with CDN from e.g. Azure.
Assets we need are static content on the page and also videos.

Overall we should have a very fast "page impression".




The login against Azure AD should currently use the v1.0 token endpoint. Background is that only here we get an AMR claim back to check how the user authenticated himself.

This info can help us to see if we can skip the password part later in the process, since the user may already arrive at the portal with a user name and password instead of the phone sign in.


Nevertheless the actual sign in is handled by Azure AD and does not need any special treatments from TRUEman. We should go for OIDC as our auth provider

Values for AMR

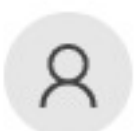
- OTP = SMS SignIn
- PWD = Password Signin
- RSA = E.g. with Hello for Business or Cert Based
- MFA = MultiFactor



It looks like this email is used with more than one account from Microsoft. Which one do you want to use?



Work or school account
Created by your IT department
+49 1520 7829731



Personal account
Created by you
+49 1520 7829731

Tired of seeing this? [Rename your personal Microsoft account.](#)

Back

Sign in to your account

←


→

↺

🔍

https://login.microsoftonline.com/common/oauth2/authorize?client_id=

☰



←

+49 1520 7829731

Enter Code

We just sent a code to +49 1520 7829731

Enter Code

Didn't receive it? Please wait for a few minutes and [try again](#).

Sign In

Government	Percentage
Current government	85%
Previous government	15%

Next

glueckkanja-gab.com



Since we only want to map new users (new hires) in the first step, the logical next step is the onboarding of their devices. In the future, however, a check against the backend could also take place here (data sources still to be defined) whether, for example, new hardware is currently flagged for enrollment for the user or whether the user is given the opportunity to manage existing hardware here (e.g. integration of RJ /me etc.).



Translated with www.DeepL.com/Translator (free version)

True Remote User Enrollment - Assign device

← → ↺ 🔍 https://gkgab.trueman.io/d/device/assign?\$assetId=c800d2cf-d734-4e35-8441-715fba1200b2

glueckkanja

gab

Christian Baumgartner  

Hello **Christian**,


we could not find any device for you yet. If you have the device in front of you, you can tell us the serial number so we can assign the device to you now.

If you need help to find the serial number look [here](#)

Serialnumber

Check

Copyright © 2020 Glück & Kanja Consulting AG. All rights reserved. [Privacy](#) | [Imprint](#)

[glueckkanja-gab.com](#) 

Here we check against the backend if we find a deivce with this serial number. In addition to Autopilot devices, we also check for mobile devices. In the first release of TRUEman we focus on Win10 devices. So a check against Intune Autopilot is sufficient here. As a condition we have to check if the device can be found at all, if it has no user assignment and if there is a user assignment, if it matches the current logged in user. If the serial number can be found and is assigned to the logged in user it must be checked if the device is already enrolled.

As a little extra we could search for devices that are assigned to the user but not yet enrolled BEFORE asking for the serial number and ask the user if the following device should be enrolled now (optional feature).

* Search for a matching AutoPilot device

If we find one
a) assign it to the currently logged in user

b) if we don't find one > display an appropriate message that there is a technical problem. Here you could very nicely bring a reference to Oliver Kieselbach's AutoPilot Manager Onboarding and dovetail it. (<https://oliverkieselbach.com/2020/12/08/autopilotmanager/>)

Optional / Phase 2
If there is more than one assignment to AP Devices from devices that are not yet enrolled and assigned to the user, we would still have to offer a selection to select the correct device (edge case - possibly also automatically selected via model).

Even more optional / Phase 3
Another option at this point would be that we know via an asset management/backend that the device has been shipped and we check the shipping status via appropriate APIs. If this is currently still in shipping, we could stop here at this point and display a shipping status.



🔍 [https://gkgab.trueman.io/d/device/assign?\\$assetId=c800d2cf-d734-4e35-8441-715fba1200b2](https://gkgab.trueman.io/d/device/assign?$assetId=c800d2cf-d734-4e35-8441-715fba1200b2)



Christian Baumgartner



Hello **Christian,**

we could not find a device for you yet. If you have the device in front of you, you can tell us the serial number now, so we can assign the device to you now.

If you need help to find the serial number please have a look [here](#).

Seriennummer

008127380157

Check

Copyright © 2020 Glück & Kanja Consulting AG. All rights reserved. Privacy | Imprint

glueckkanja-gab.com

When you click on "Check", the serial number entered is searched for in the Autopilot Devices in the backend. If a device is found which

- a) not yet enrolled &
- b) is not yet assigned to a user

this will now be assigned to the logged in user. It should also be checked whether the device has already been assigned a corresponding AP profile.

<https://docs.microsoft.com/en-us/graph/api/intune-enrollment-windowsautopilotdeviceidentity-list?view=graph-rest-beta>



Hallo **Christian**,

wir konnten für dich n
Gerät vor dir hast, kan
zuweisen können.

Wenn du Hilfe brauchst

Seriennummer

008127380157

Successfully assigned

We have found a Surface Book 3 with this serial number
and assigned it to your user. You can start setting it up
right away.

Next

e. Wenn du das
das Gerät jetzt




True Remote User Enrollment - Assign device

← → ↺ 🔍 https://gkgab.trueman.io/d/device/assign?\$assetId=c800d2cf-d734-4e35-8441-715fba1200b2

☰

glueckkanja gab

Christian Baumgartner  ☰

Hallo **Christian**,

wir konnten für dich noch kein Gerät vor dir hast, kann ich dir zuweisen können.

Wenn du Hilfe brauchst, dann schreibe mir eine E-Mail.

Seriennummer

008127380157

➔

A problem has occurred


We have not found a device with this serial number! Please check again that you have entered the serial number correctly.

If we still can't find the device you can contact us or try to register the [device yourself](#)(Win10 - Self register (optional)).

Back

e. Wenn du das Gerät jetzt

Copyright © 2020 Glück & Kanja Consulting AG. All rights reserved. Privacy | Imprint

[glueckkanja-gab.com](#) 

The errors must still distinguish a few cases here. Beside the SerialNotFound Error it could be e.g. also that the device has the status "Enrolled" or already another user was assigned. In this case the error should be corresponding.

True Remote User Enrollment - Network connection

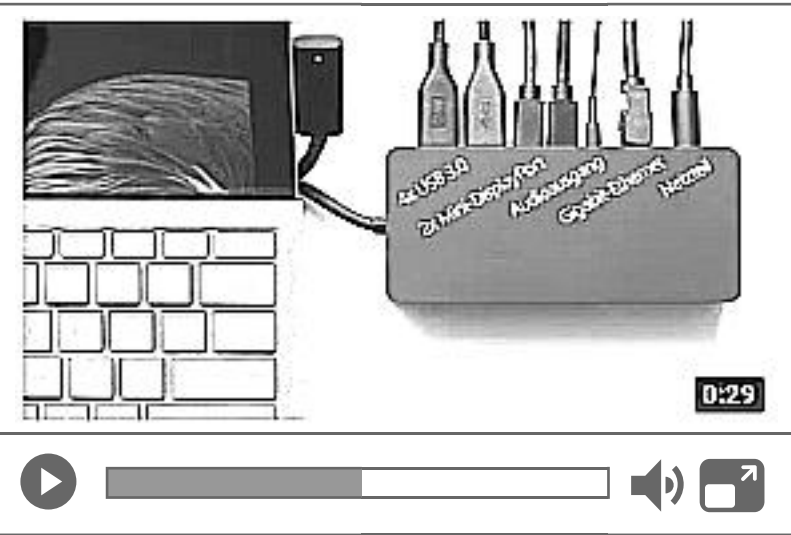
glueckkanja gab

Christian Baumgartner

In order to start setting up your Surface Book 3, you need to connect to the Internet. Here you can find a short guide on how to connect to the network with a cable or your Wi-Fi.


If you get stuck, you can also contact our support team below.

Surface Dock und Netzwerk anschließen



0:29

Herstellen einer Verbindung mit meinem WLAN



7:23

Next

Copyright © 2020 Glück & Kanja Consulting AG. All rights reserved. Privacy | Imprint

glueckkanja-gab.com

Here we show professional help videos for establishing a network connection. Especially for Win10 / macOS devices this is now a critical step, especially in environments that are not managed (e.g. Home Router or FritzBox).

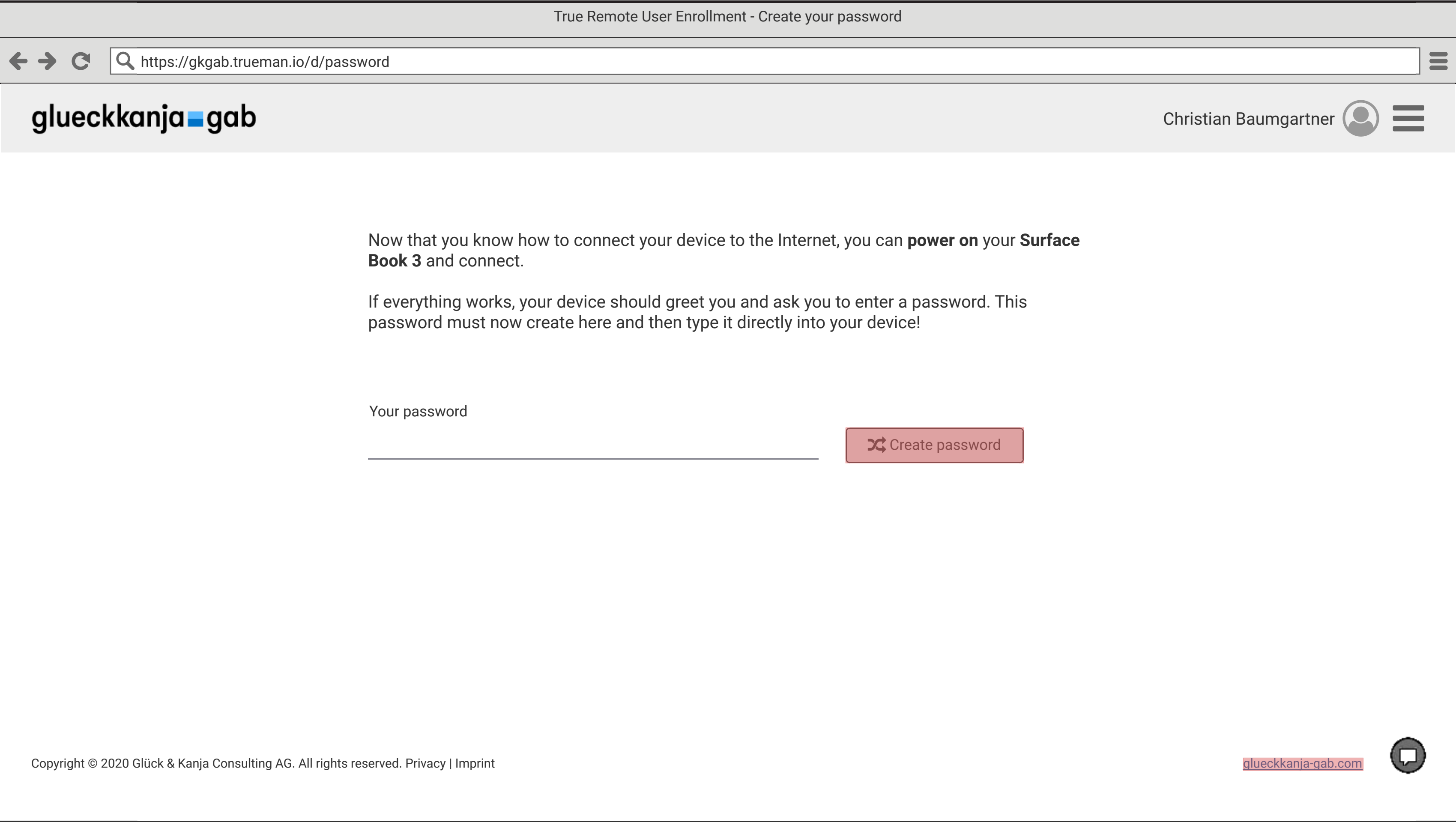
Here, only videos suitable for the device/manufacturer should be displayed for the model/type at hand.

INPUT:

Device type & model

API

Call against an API to get back matching videos that are embedded.



For the generation of the passwords we could plan different variants.

One idea would be to use a Diceware/EFF Word List procedure. Here, different words are appended to each other. The entropy of such a password is very high. With such a password you could also define that this is not initial but the final password.

In the backend, the password could be written to an Azure Keyvault to give the user a way to retrieve the password again during setup. Only after a time X (e.g. 2 days) the password is cleaned up in the vault.

The password generator could also offer different variants - depending on what the user prefers. A nice example for different secure variants can be found here:

<https://www.rempe.us/diceware/#eff> resp.
<https://password.blue/>

An alternative would be to set a password here, which the user has to change after the first use - still to be discussed.

IMPORTANT: The step should be skipped if the value in AMR is not OTP in the id_token of the login!


True Remote User Enrollment - Create your password


← → ↺

🔍

https://gkgab.trueman.io/d/password

☰

glueckkanja  gab

Christian Baumgartner  ☰

Now that you know how to connect your device to the Internet, you can **power on** your **Surface Book 3** and connect.

If everything works, your device should greet you and ask you to enter a password. This password must now create here and then type it directly into your device!

Dein Kennwort

client-metapher-maxime-bohnen-haber-bier


↻ Create password

Your new password is quite long, isn't it? But since it only consists of words, you can remember it well. After the first login you will rarely need your password because everything works with a PIN or fingerprint.

Next

Copyright © 2020 Glück & Kanja Consulting AG. All rights reserved. Privacy | Imprint

glueckkanja-gab.com





🔍 <https://gkgab.trueman.io/d/password>



Christian Baumgartner



Nachdem du nun weißt, man eine Internetverbindung mit deinem Gerät herstellen kann, kannst du nun dein **Surface Book 3 einschalten** und verbinden.

Wenn alles geklappt halt sollte dich dein Gerät begrüßen und dich zur Eingabe eines Kennworts auffordern. Diese K

Important Do not proceed until you have successfully entered and changed your password.

Continue?

No, back

Yes, next

Dein Kennwort

client-metapher-1

Dein neues Kennwort steht kannst du dir das gut merken. Na, wenn du es nicht merken brauchst du alles mit einer PIN



True Remote User Enrollment - Waiting for device

←

→

↺

🔍

https://gkgab.trueman.io/d/device/checkin

☰

glueckkanja

gab

Christian Baumgartner

☰

Wait until your device is ready

Approximate waiting time 4 minutes

Copyright © 2020 Glück & Kanja Consulting AG. All rights reserved. Privacy | Imprint

glueckkanja-gab.com

At this point, the following things have happened on theWin10 Workplace:

- 1. the device is switched on
- 2. the device has successfully connected to a network with Internet access
- 3. the device has connected via autopilot and
- 4. the user has entered his password

We now wait here and periodically check against the appropriate Graph API / Intune endpoint and poll the enrollment status of the device

INPUT
Device ID from the previous link in Azure AD/Intune.
Status for enrollment from Azure AD

True Remote User Enrollment - almost done

←

→

↺

🔍

https://gkgab.trueman.io/d/device/checkin

☰

glueckkanja

gab

Christian Baumgartner

☰

Your machine is now busy and does the main work. You can use the time to learn more about your first days and customize your workspace.

To the portal

Copyright © 2020 Glück & Kanja Consulting AG. All rights reserved. Privacy | Imprint

glueckkanja-gab.com

Here you could now start the wizard for the next device. (e.g. roll out another iOS device etc.).

If there are no more devices to be set up in the queue, the redirect to the portal can now take place.

The portal would not be in focus in the first step and the wizard would stop at this point. We could redirect to an individual URL (e.g. portal.office.com or intranet.contoso.com etc.).