STM32 security workshop

Tools installation – Prerequisites

Purpose

- Purpose :
  Guideline to **install tools and material** for the STM32 Security Workshop
  Check of the **prerequisite** (knowledge and homework)
- Materials provided :

  STM32SecuWS-material.exe

  -> STM32CubeProgrammer 2.4.0

  -> STM32CubeIDE 1.3.0

  -> STM32SecuWS material
- Environment supported : PC laptop with Windows 7 or newer, with Java JRE v8 (v1.80.0_191 or newer)

WARNING

material installation/homework could take from 2.30 hours up to more than 1 day !

prerequisite knowledge may require up to 10 hours

Agenda

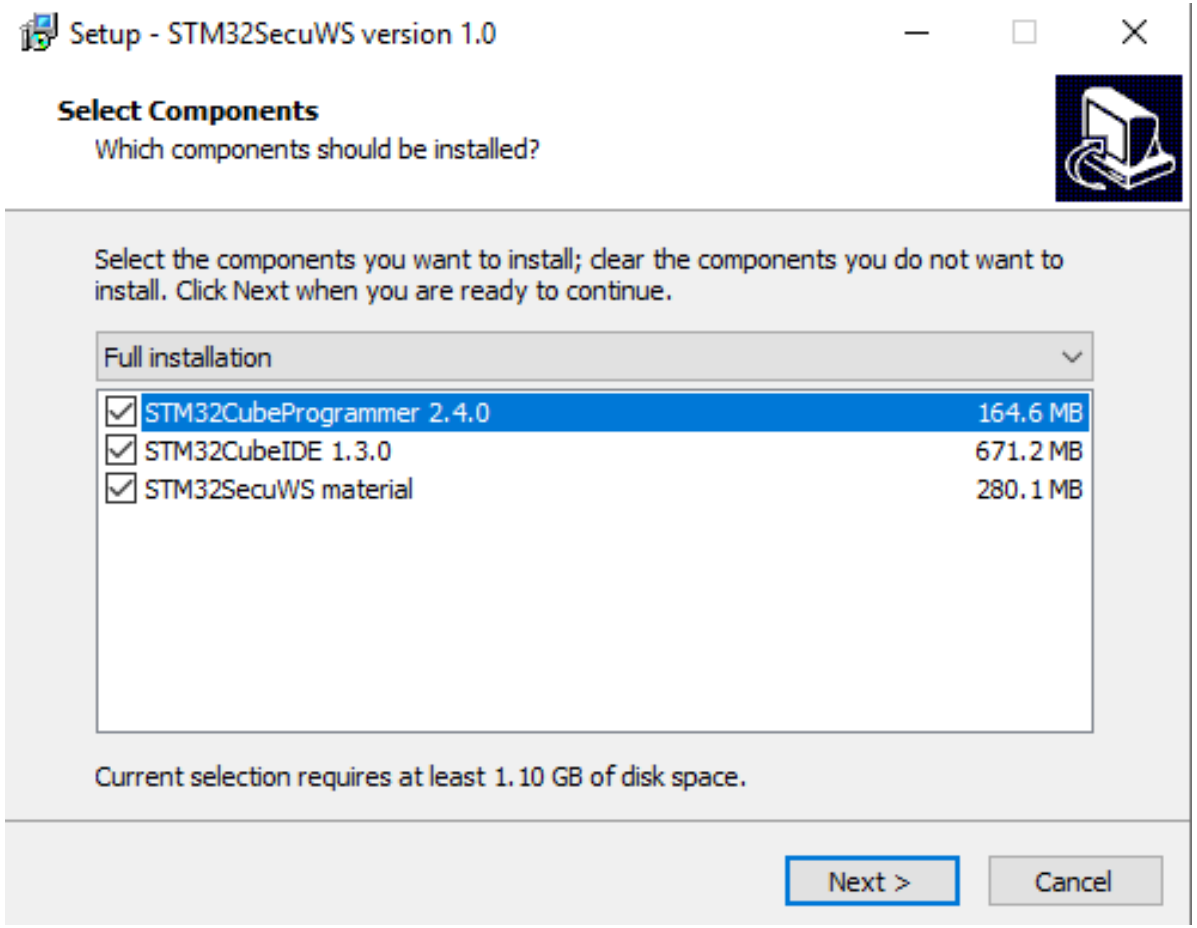
- Step 1 : Installation of standard tool and material (1 hour)
- Step 2 : Installation of SBSFU
  - 2-1 : Getting X-CUBE-SBSFU package **(WARNING : this step can take more than 1 day !)**
  - 2-2 : X-CUBE-SBSFU package installation (5 minutes)
- Step 3 : Installation setting check (5 minutes)
- Step 4 : Auto-test on your security skills (10 minutes)
- Step 5 : Homework before the Security workshop (1 hour)

Please do not skip any of those steps !

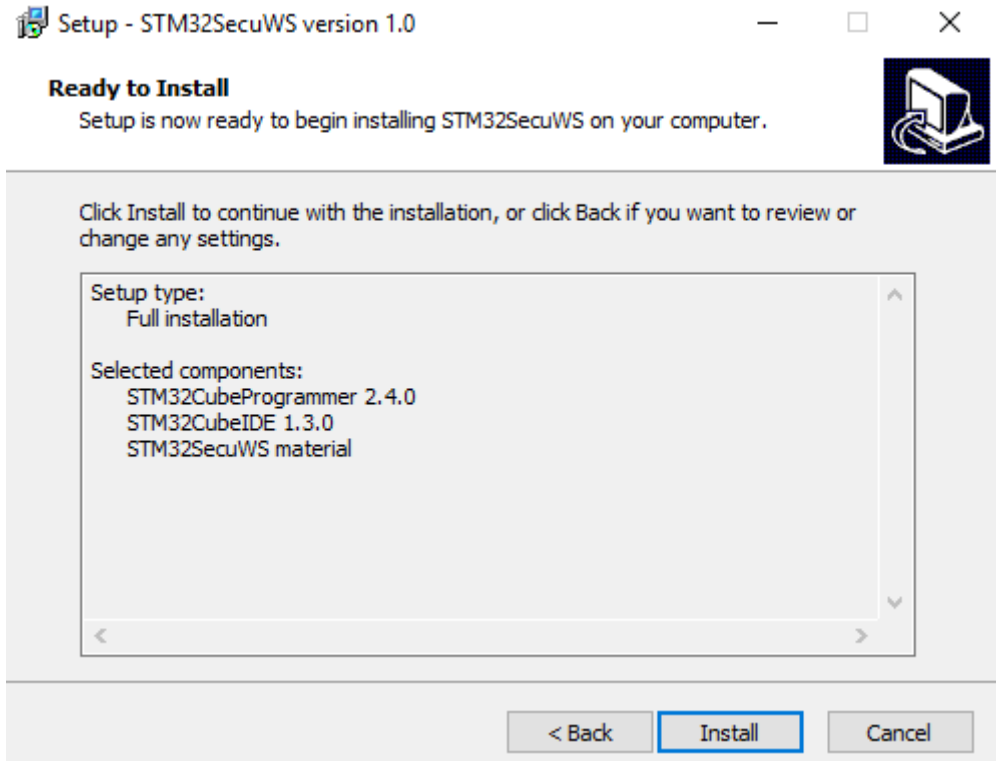
Step 1 : Installation of standard tool and material

Step 1 : STM32SecuWS-material.exe

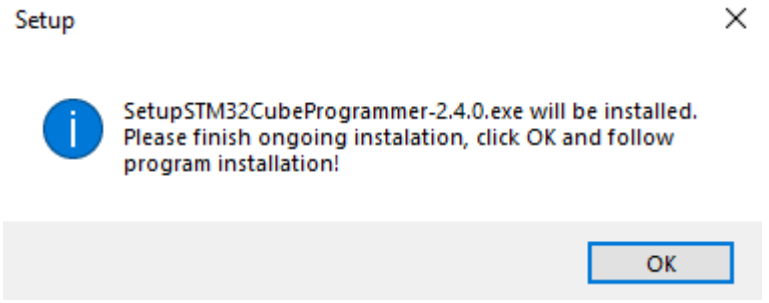
- On your PC, launch : STM32SecuWS-material.exe
- You can unselect components, if already installed some on you PC. But please, insure to have the correct software version installed.



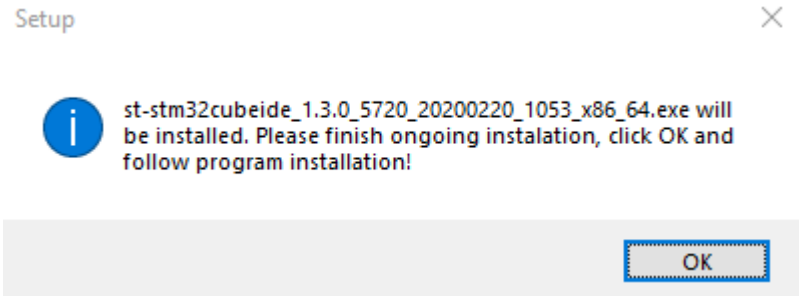
Step 1 : STM32SecuWS-material.exe



- WARNING : Please press OK only when CubeProgrammer installation is finished !



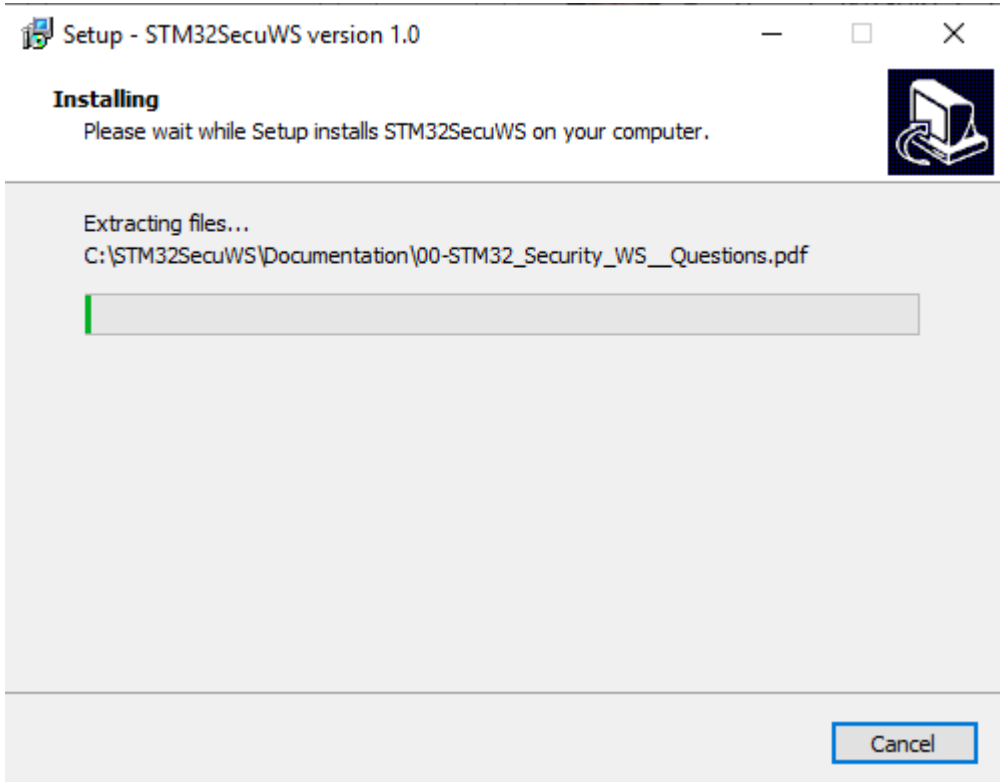
- WARNING : Please press OK only when STM32CubeIDE installation is finished !



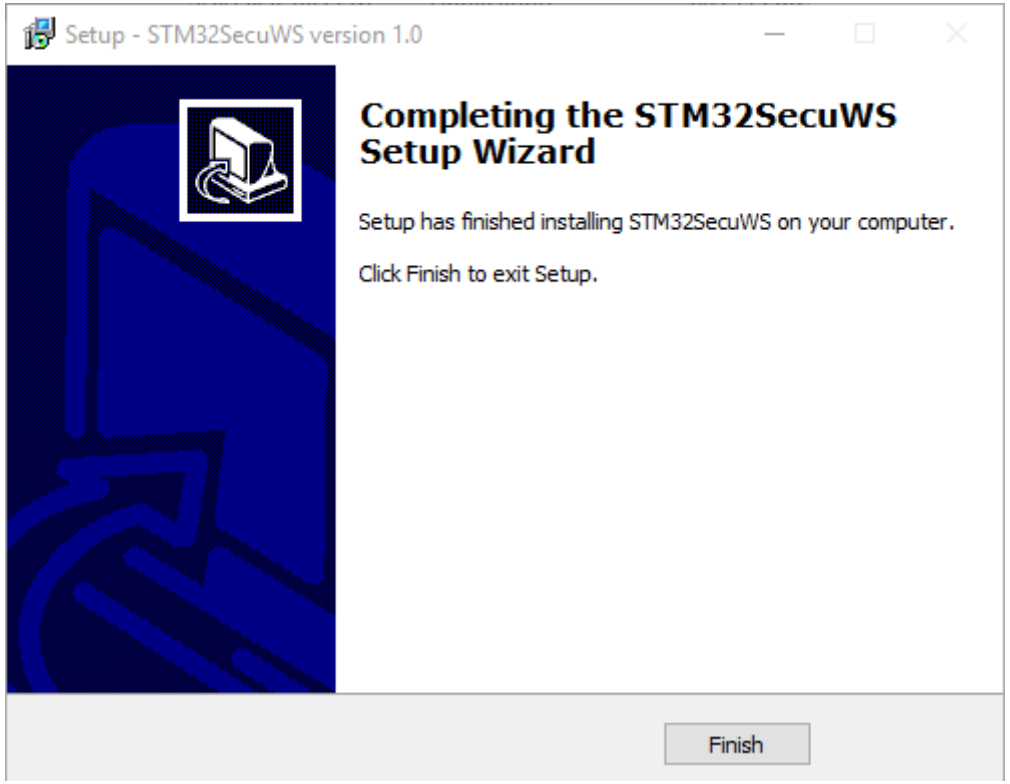
life.augmented

Step 1 : STM32SecuWS-material.exe

- At this step, the installation tool could take more than 1 minute before continuing….Please be patient.



Step 1 : STM32SecuWS-material.exe

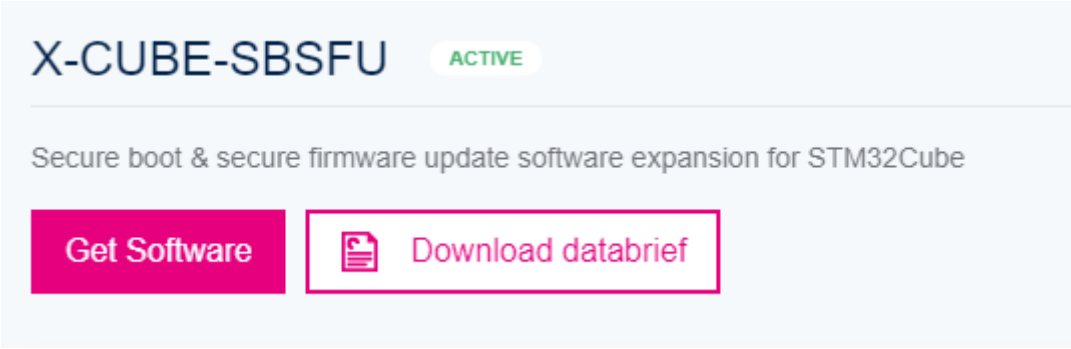


life.augmented

Step 2 : Installation of SBSFU

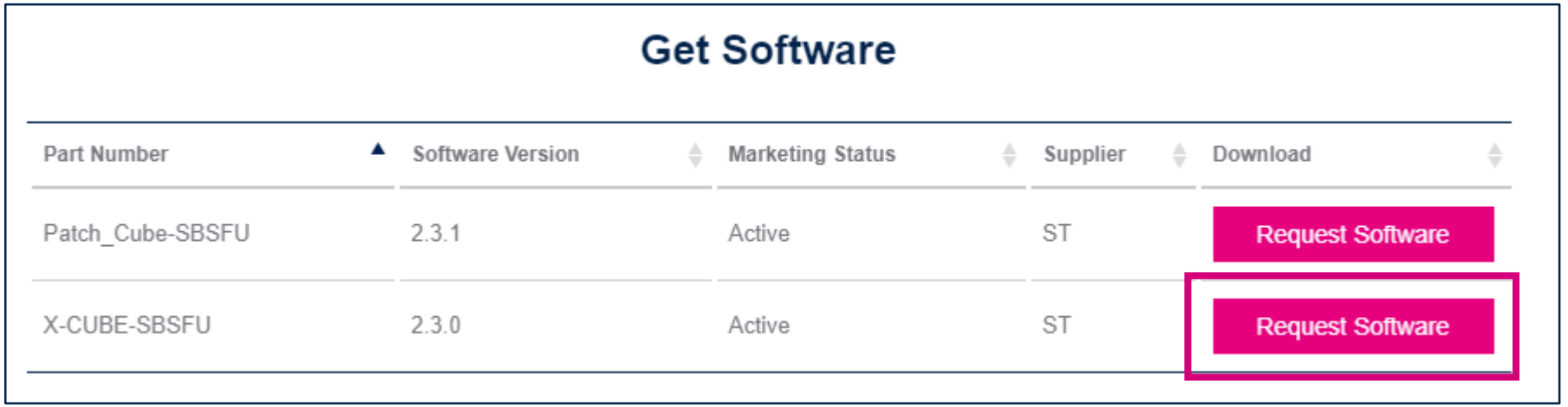
Step 2-1 :Getting X-CUBE-SBSFU package

- Request the XSBSFU package on this page :
  https://www.st.com/en/embedded-software/x-cube-sbsfu.html
- When displaying this web page, please login with your myST account or create one if necessary.
- So, at this step you are here and logged in



Step 2-1 : Getting X-CUBE-SBSFU package

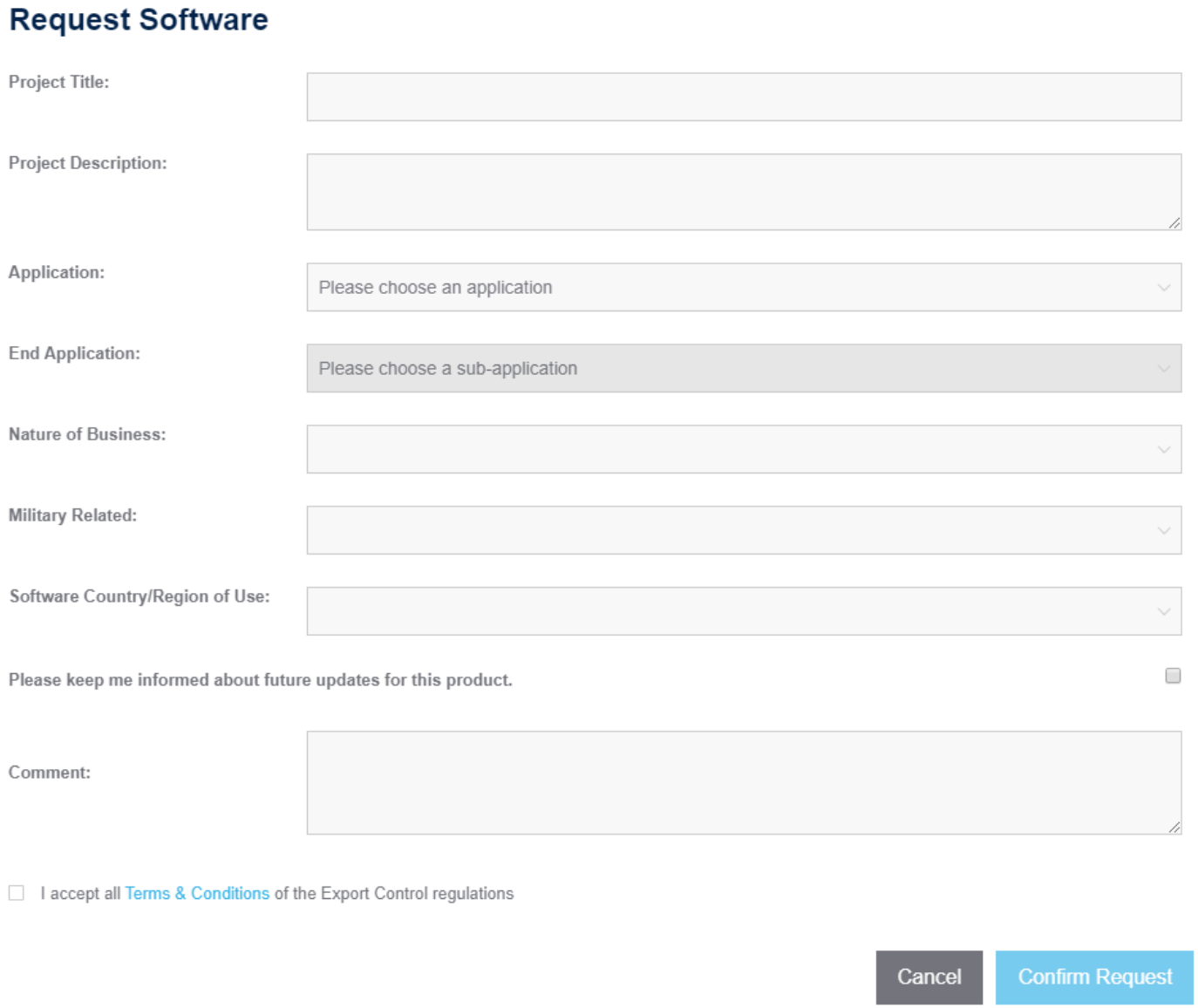
- Click on Get Software
- Select X-CUBE-SBSFU (version 2.3.0), click on Request Software
- (Patch is not useful for our workshop)



- Accept License Agreement

life.augmented

Step 2-1 : Fill the Export Control form



- This form is required because package contains crypto libraries.

Step 2-1 : X-CUBE-SBSFU package

- After export control form is filled you should receive an email with subject
  SOFTWARE DOWNLOAD - NOTIFICATION EMAIL
- **Then after validation delay (usually few hours)**, you will receive the download link by mail.
- Please follow the instructions to retrieve the package.
- The download link should provide a zip file with name:
  - STM32CubeExpansion_SBSFU_V2.3.0.zip

FAQ: Issue with download

This problem is generally associated with your web browser:

- ensure the web browser you’re using is up to date, Google Chrome and Internet Explorer work best.
- Also, please clear your entire browser's temporary internet files/cache.
- Turn off any ad blockers you may have.

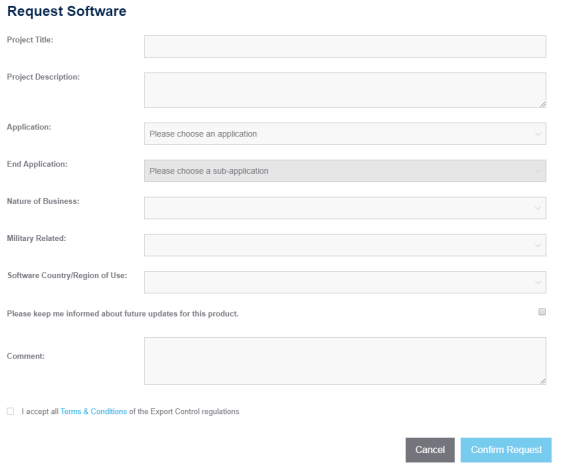
Once completed, close all web sessions down and open a new session and go to st.com.

Accept the cookie policy on st.com and again please ensure your pop up blocker is off.

Beware : the downloading link is valid only 48 hours.

life.augmented

FAQ : NOTIFICATION EMAIL/DOWNLOAD email not received



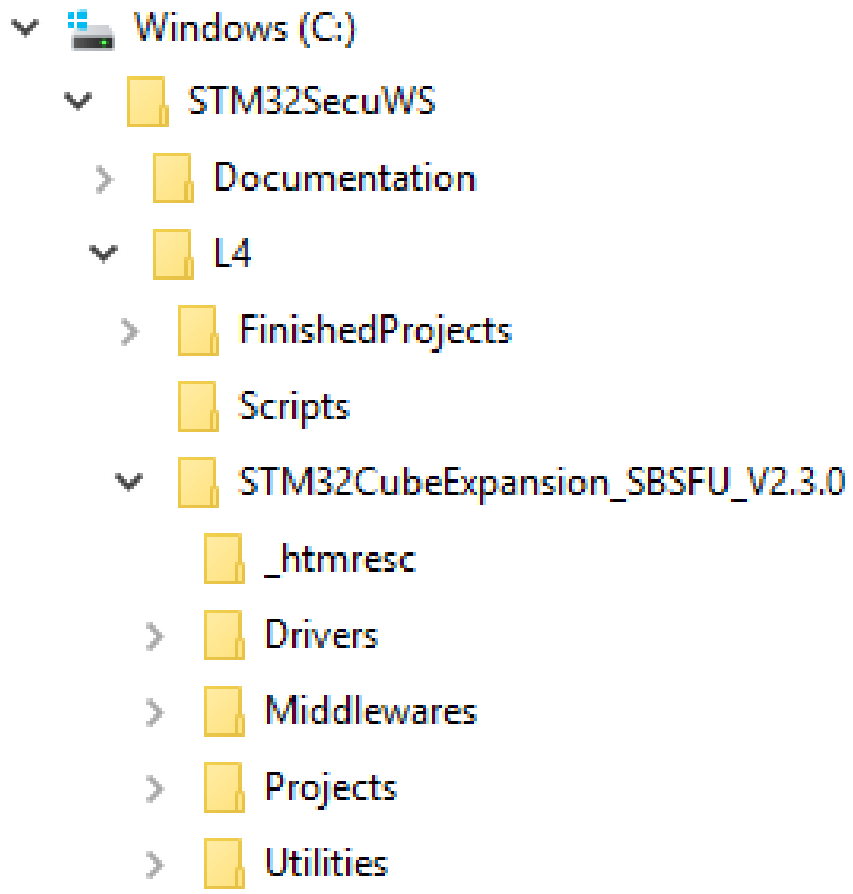
- Insure those mail are not in your spam
  - Title :SOFTWARE DOWNLOAD - NOTIFICATION EMAIL
    From : STMicroelectronics onlinesupport@notification.st.com
  - Title : Start your software download
    From : STMicroelectronics <onlinesupport@notification.st.com>
- Try the procedure again and please do a **screenshot** of the Export Control form **with your answers**
- After 48hours, if nothing received send a mail to microsupport.europe@st.com

Subject : Issue in with STM32 Security Workshop Tools Installation

life.augmented

Step 2-2 : X-CUBE-SBSFU package installation

- Please **unzip** the archive : STM32CubeExpansion_SBSFU_V2.3.0.zip at location **C:\STM32SecuWS\L4**
- Expected result :



life.augmented

Conclusion

- SBSFU installation is now done.

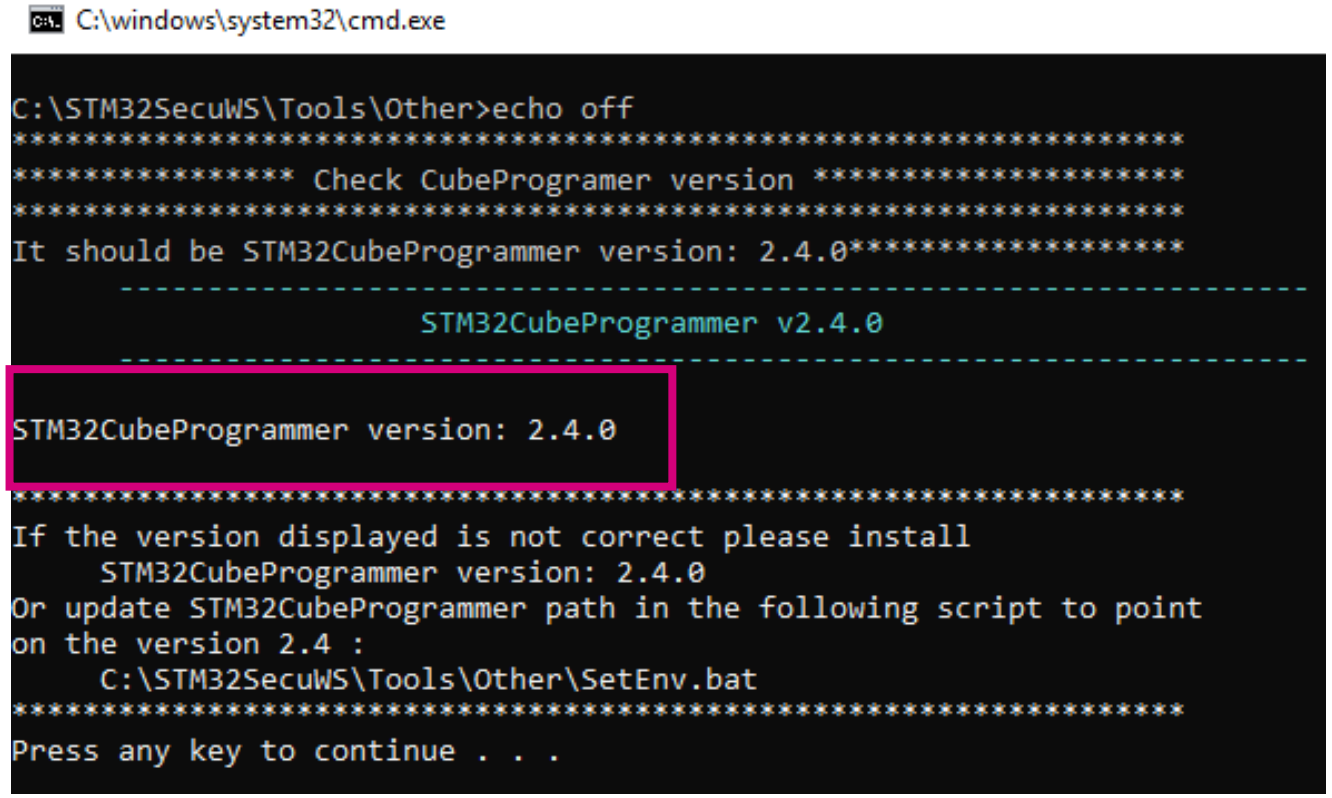
- If you face any issue during the setup, https://community.st.com/stm32-security-workshop

Step 3 : Installation setting check

Step 3 : Installation setting check

- Once all the installation done, please launch this script **C:\STM32SecuWS\Tools\Other\CheckEnv.bat**

Step 3 : Installation setting check



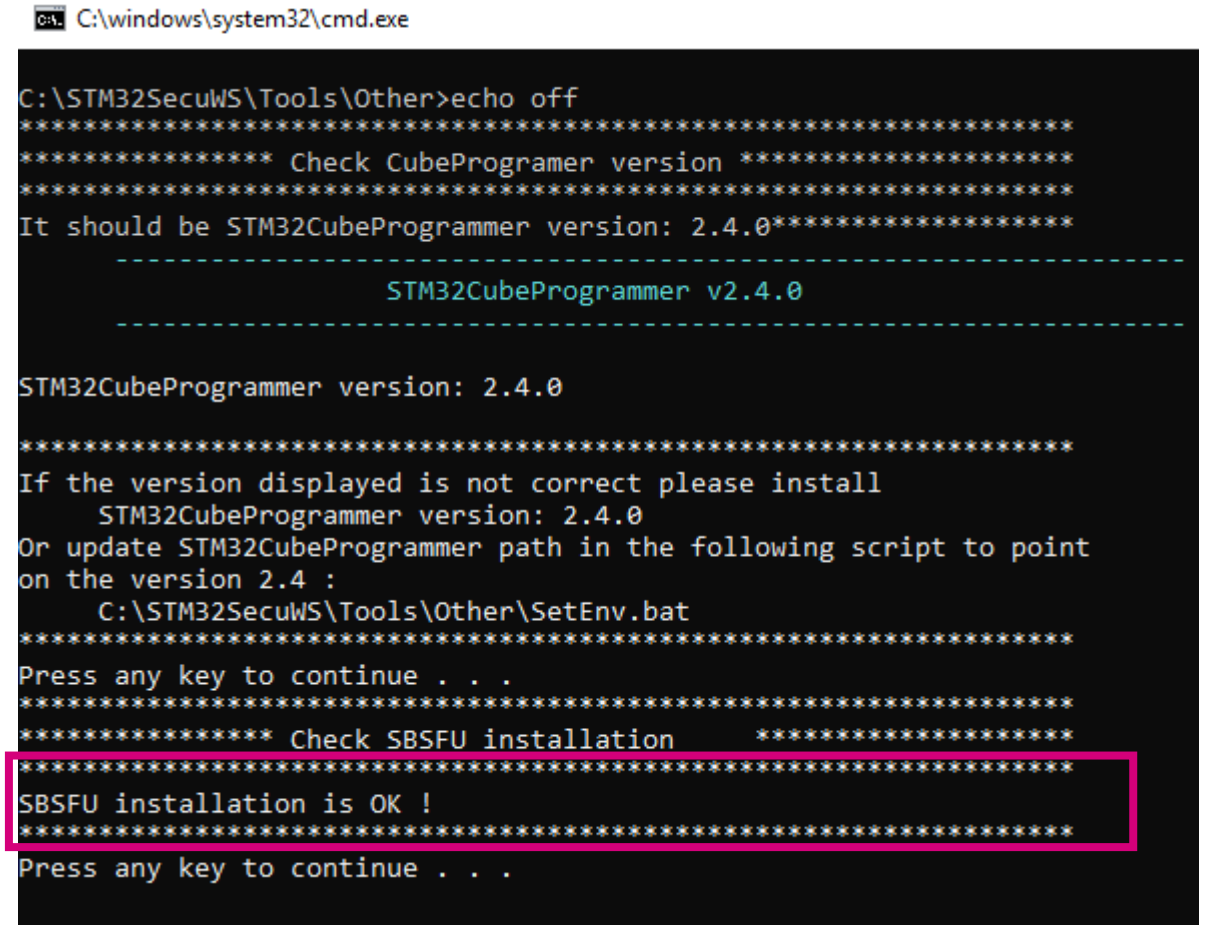
- **version displayed is 2.4.0 : installation is ok, please press any key**

- Remark : If you haven't use the default path for STM32CubeProgrammer install, you will need to update the variable Prog64 in this script **C:\STM32SecuWS\Tools\Other\SetEnv.bat**

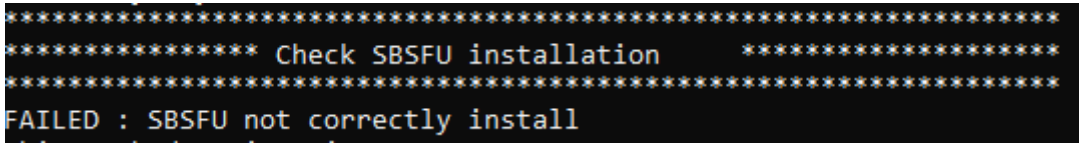
set Prog64="C:\Your_installation_path\STM32CubeProgrammer\bin\STM32_Programmer_CLI.exe"

life.augmented

Installation setting check



- If you seen this following message



please check location where you unzip X-SBSFU

Conclusion

- Tools installation is now done.

- If you face any issue during the setup, https://community.st.com/stm32-security-workshop

Step 4 : Auto-test

Purpose

- **Basic knowledge of security is required to attend the workshop.**

  It is well covered by various MOOC sessions

  MOOC Security part 1 : **Introduction to security (1/2 hour)**

  https://www.youtube.com/playlist?list=PLnMKNibPkDnH1iwS2UMs8v3VSj5ZCpNED

  MOOC Security part 2 : **Basics of crypto (2 hours)**

  https://www.youtube.com/playlist?list=PLnMKNibPkDnFSFh57UFTZLpy-7lZiwTHh

  MOOC Security part 3 : **STM32 security features (6 hours)**

  https://www.youtube.com/playlist?list=PLnMKNibPkDnFzux3PHKUEi14ftDn9Cbm7

  MOOC Security part 4 : **STM32 security in practice (2.30 hours)**

  https://www.youtube.com/playlist?list=PLnMKNibPkDnF0wt-ZI74SflnsBV4yKzkO

- Find following a **short test to evaluate yourself** and know which session to watch before the workshop.

Question 1

- What is the meaning of RDP ?
  - Real Dual Protection
  - Reinforced Dual Protection
  - ReaDout Protection

Answer 1

- What is the meaning of RDP ?
  - Real Dual Protection
  - Reinforced Dual Protection
  - **ReaDout Protection**

MOOC Security Part3 - STM32 Security features - 08 - Readout protection theory

https://www.youtube.com/watch?v=Il2QceXsbyE&list=PLnMKNibPkDnFzux3PHKUEi14ftDn9Cbm7&index=9&t=8s

Question 2

- What is the role of the firewall on STM32?
  - A software system that filters illegal memory accesses
  - A hardware mechanism to create a security enclave
  - A hardware mechanism used to protect against attack on the debug port

Answer 2

- What is the role of the firewall on STM32?
  - A software system that filters illegal memory accesses
  - **A hardware mechanism to create a security enclave**
  - A hardware mechanism used to protect against attack on the debug port

MOOC Security Part3 - STM32 Security features - 16 - Firewall theory

https://www.youtube.com/watch?v=c-RLSIon548&list=PLnMKNibPkDnFzux3PHKUEi14ftDn9Cbm7&index=17&t=125s

Question 3

- What is SHA256 ?
  - A signature algorithm
  - An encryption algorithm
  - A hash algorithm

Answer 3

- What is SHA256 ?
  - A signature algorithm
  - An encryption algorithm
  - **A hash algorithm**

MOOC Security Part 2 - Basics of cryptography - 3 Integrity

https://www.youtube.com/watch?v=0bODQQw0Dj8&list=PLnMKNibPkDnFSFh57UFTZLpy-7lZiwTHh&index=3

Question 4

- When using asymmetric cryptography, which key is used to check a signature
  - The public key
  - The private key

Answer 4

- When using asymmetric cryptography, which key is used to check a signature
  - **The public key**
  - The private key

MOOC Security Part 2 - Basics of cryptography - 3 Integrity

https://www.youtube.com/watch?v=0bODQQw0Dj8&list=PLnMKNibPkDnFSFh57UFTZLpy-7lZiwTHh&index=3

Question 5

- To encrypt a big datafile, it's better to use
  - Symmetric cryptography
  - Asymmetric cryptography
  - Symmetric or Asymmetric, it's just a different security scheme

life.augmented

Answer 5

- To encrypt a big datafile, it's better to use
  - **Symmetric cryptography**
  - Asymmetric cryptography
  - Symmetric or Asymmetric, it's just a different security scheme

MOOC Security Part 2 - Basics of cryptography - 1 Introduction, encryption-decryption principle

https://www.youtube.com/watch?v=sjje0UOLckg&list=PLnMKNibPkDnFSFh57UFTZLpy-7lZiwTHh&index=1

Question 6

- This information is present in a certificate :
  - An encrypted public key
  - A public key with its signature
  - A private key encrypted with its signature

Answer 6

- This information is present in a certificate :
  - An encrypted public key
  - **A public key with its signature**
  - A private key encrypted with its signature

MOOC Security Part 2 - Basics of cryptography - 4 Authentication

https://www.youtube.com/watch?v=PjmdZTyp5z0&list=PLnMKNibPkDnFSFh57UFTZLpy-7lZiwTHh&index=4

Question 7

- What is a secure boot purpose?
  - A mechanism that ensures your IOT device is registered to a server
  - A mechanism that ensures boot code never crash
  - A mechanism that ensures application code executed is genuine

Answer 7

- What is a secure boot purpose?
  - A mechanism that ensures your IOT device is registered to a server
  - A mechanism that ensures boot code never crash
  - **A mechanism that ensures application code executed is genuine**

MOOC Security part 4 : Security Part4 - STM32 security in practice - 08 Secure bootloader introduction
https://www.youtube.com/watch?v=BnnGvyg6fN4&list=PLnMKNibPkDnF0wt-ZI74SflnsBV4yKzkO&index=8

Question 8

- What is the link register in Cortex M ?
  - If is used to link 2 registers
  - It contains the return address of function call
  - It contains the address of current executed instruction

life.augmented

Answer 8

- What is the link register in Cortex M ?
  - If is used to link 2 registers
  - **It contains the return address of function call**
  - It contains the address of current executed instruction

http://infocenter.arm.com/help/index.jsp?topic=/com.arm.doc.ddi0439b/Chdedegj.html

Question 9

- Can a Non-Secure interrupt occur during execution of Secure service in TrustZone environment?
  - Yes
  - No

Question 9

- Can a Non-Secure interrupt occur during execution of Secure service in TrustZone environment?
  - **Yes**
  - No

Security Part3 - STM32 Security features - Appendix - Software security based on Isolation

https://www.youtube.com/watch?v=HfxzQK4bBqo&list=PLnMKNibPkDnFzux3PHKUEi14ftDn9Cbm7&index=32

Conclusion

- If you don’t feel comfortable with those questions, we advise you to come back to our Security MOOC offer.

Step 4 : homework

Homework

- Due to remote format of this workshop, you are require to do **two homeworks** before the session.
- Please follow instruction from this documents:

C:\STM32SecuWS\Documentation**SBSFU_Home_work.pdf**

HW board required : Nucleo-L476RG

C:\STM32SecuWS\Documentation**TFM_Home_work.pdf**

HW board required : Nucleo-L552ZE

Conclusion

- Once you finished, those two home work, you’re ready for the STM32 Security Workshop session

- If you face any issue during the setup, https://community.st.com/stm32-security-workshop

Thank you

life.augmented