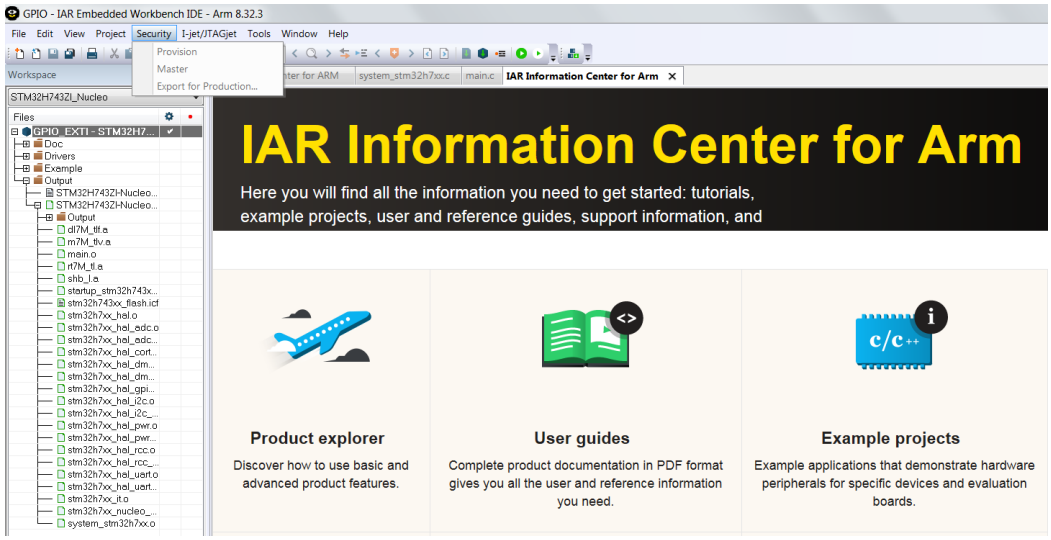
Enabling security in your application

C-Trust is designed to work as an extension to the IAR Embedded Workbench. The solution is totally integrated and straightforward to make use. C-Trust is the security enabler for any application. Installing C-Trust adds a **Security** menu in the IAR Systems IDE:



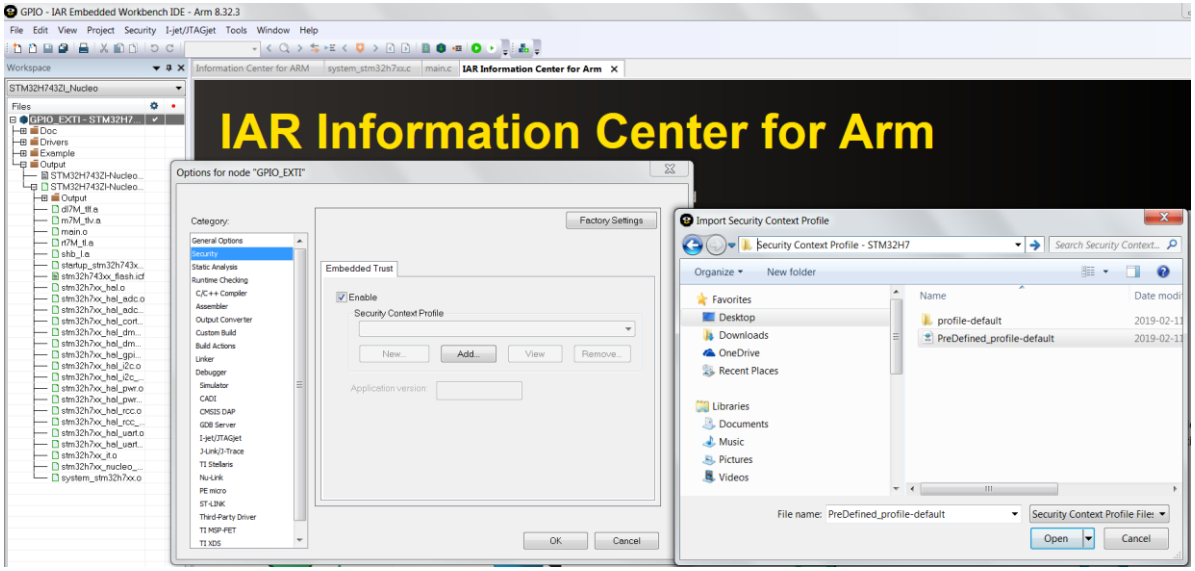
Notice that all options in the **Security** options category are grayed when security is not been enabled.

The trusted execution environment is configured through a Security Context Profile. It is a description of the security environment that is required to protect your application. The security context provides:

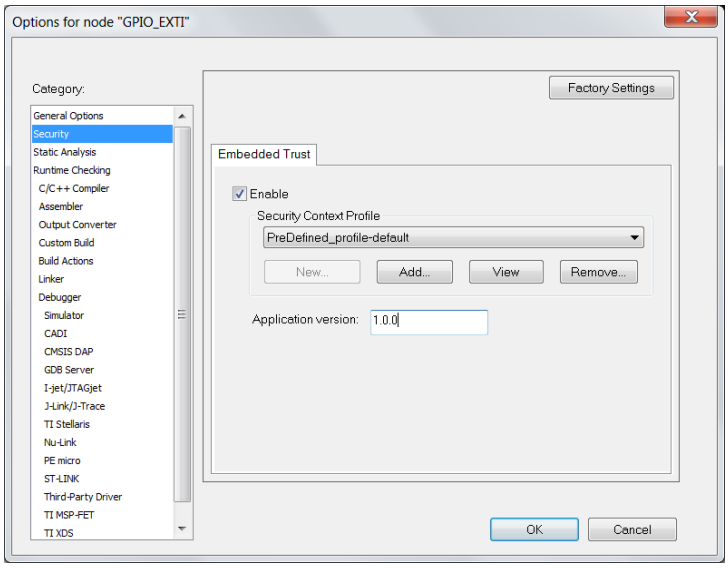
- Storage directory of keys, logging etc.
- Cryptographic keys and certificates
- Secure Boot configuration including:
    - Device security
    - Application update process
    - Update policy
    - Device memory layout

With C-Trust, you can import and add an existing or pre-defined security context to your project. This adds security into the workflow without any overhead or special actions.

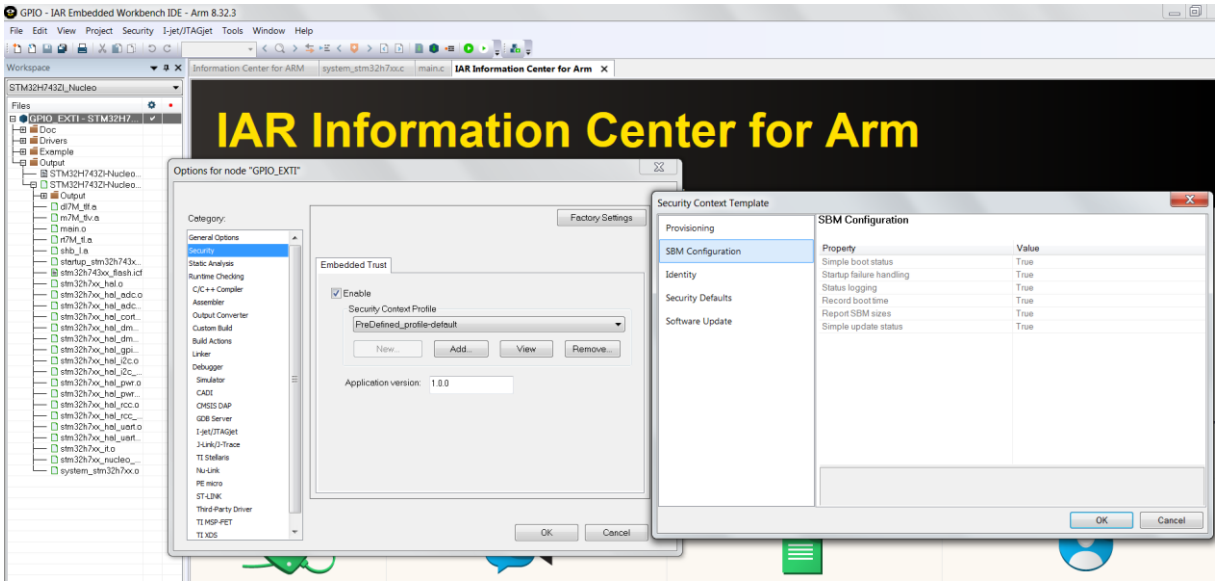
Adding an existing security profile becomes possible when the **Enable Security** option is selected in the project settings:



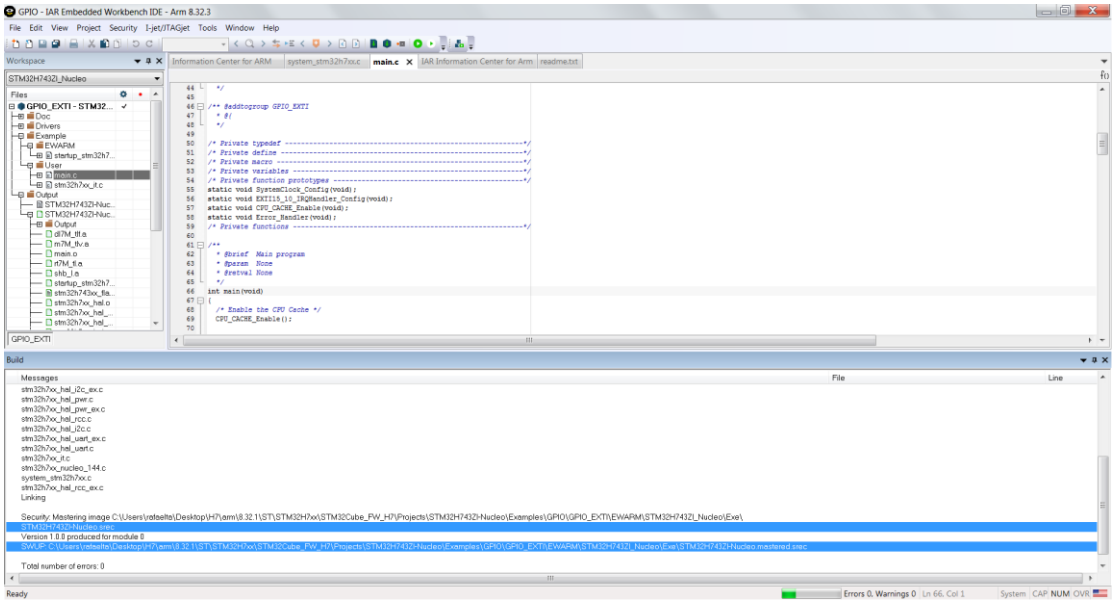
The final step after locating and adding the pre-defined security context framework, for example the Base or Advanced security context is to set the application version number. This is also the only option that can be edited using C-Trust:



All the other options in the profile can only be inspected, but not changed or edited.



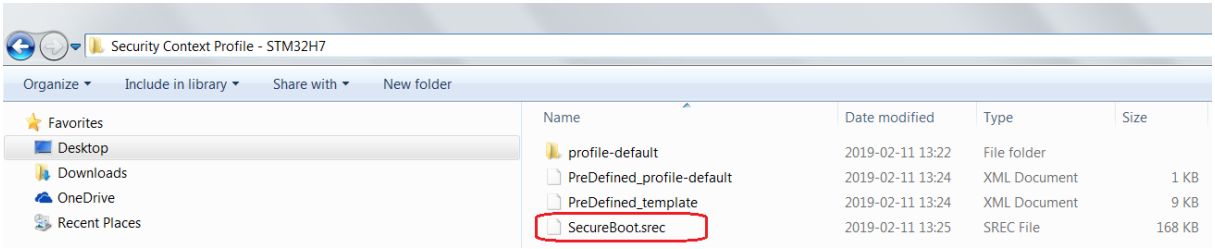
As a developer, it will be the exact same development workflow, but with the difference that now a secure development workflow is in place. The mastering step will be added at the end of the build process, which is executed automatically.



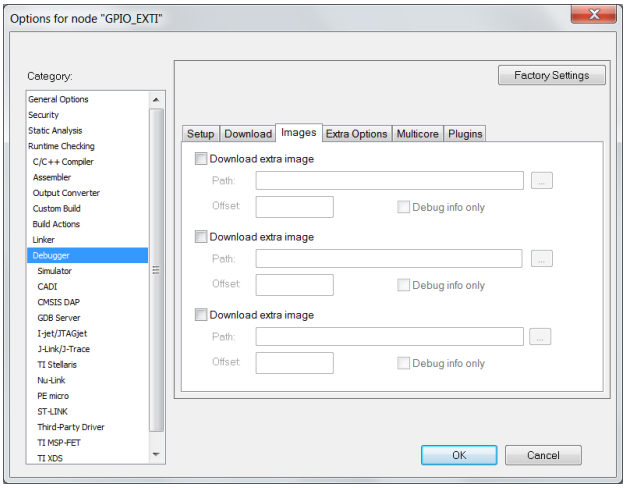
Mastering the application means that the IDE/C-Trust encrypts and signs the embedded application package to be accepted by the SBM (secure boot manager).

The encrypted application must be validated and decrypted to run on the target. This process is straightforward and transparent for the developer. The secure boot is provided with the basic and advanced security profile templates package.

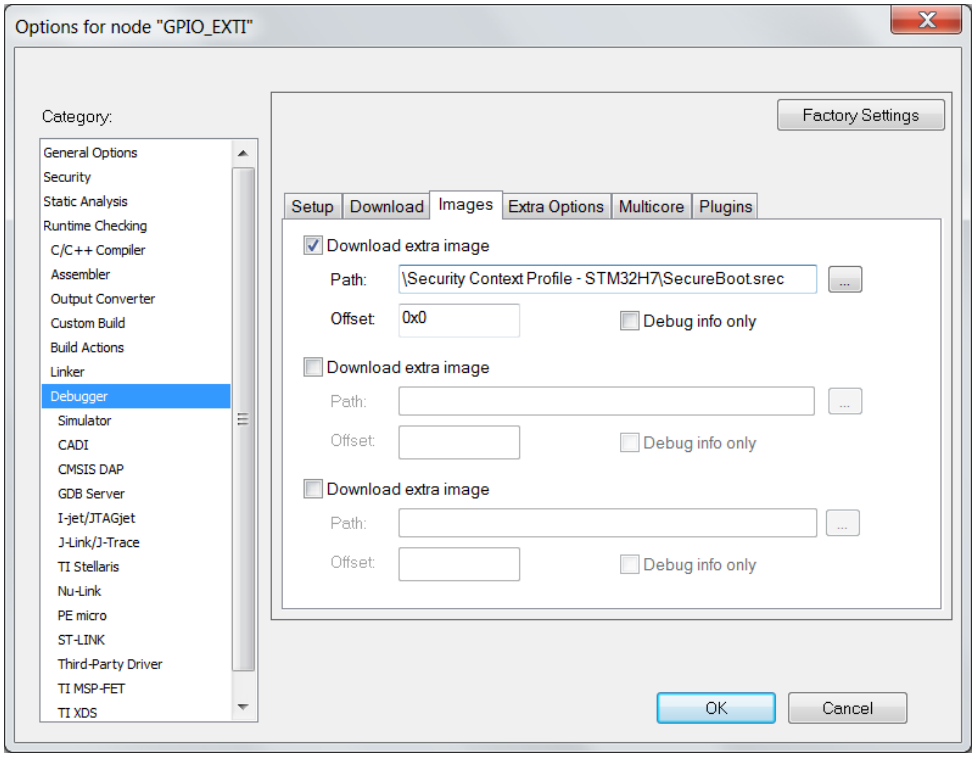
Having the secure booting process adds full security to the flow.



The secure boot is added to the process in the **Debugger** options category, on the **Images** page:



This ensures that the secure boot manager can be downloaded to the target and that the mastered application is accepted though the validation process.



From this point in the process, debugging is fully available and security is a natural part of the application development. Notice that the security context profile can be replaced any time.

Editing or creating a customized security profile requires a license for Embedded Trust. The secure boot provided with the security context template only has minimal functionality.

Notice that the security context is primarily the responsibility of the security expert/officer at the customer site. The security expert should be familiar with the terminology and technology used in security applications (such as cryptographic keys and digital certificates). This knowledge will enable the security expert to specify the properties of the security context.

The base and advanced security context frameworks are the fastest way to get started. C-Trust enables security in your application in just a few steps. Security just moved from a specialist capability into mainstream development thanks to C-Trust.

Please access https://www.iar.com/embedded_trust/ if you are interested in learning more about the security solution from IAR Systems.