



ZAYA Secure Kernel Demonstrations

ZAYA is User Friendly

Image Separation

In ZAYA, Kernel and user applications images are separate images/binaries.

- Design & Develop
 - Download (OTA)
 - Certify
- each application individually.



Pure User Applications

OS and platform initialisations are hidden from the user application, and ZAYA Applications are ready to run in their main() functions like Rich OSes.

```
/* @brief User app main function */
void main(void)
{
    /* No OS, Driver Initialisation */

    /* Just implement your custom app */

    LOG("Hello World!");
}
```

ZAYA is Certification/Regulation Friendly

Security Evaluation Friendly

ZAYA Secure Kernel is designed to meet Security Regulations and abstracts all certification/regulation details from user applications.

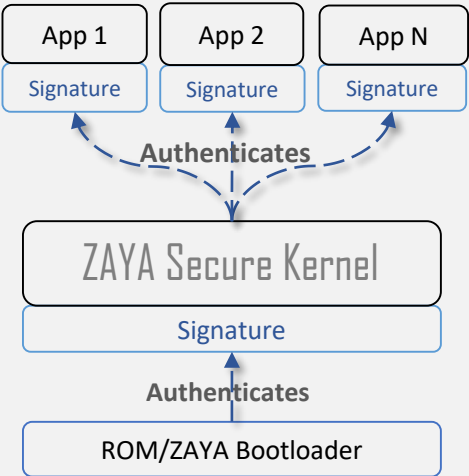
With ZAYA modular structure, ZAYA user applications are .certification free which is manufacturing an cost effective for OEMs.



ZAYA is Secure (*Compliant with security regulations/certifications)

Image Authentication (Chain of Trust)

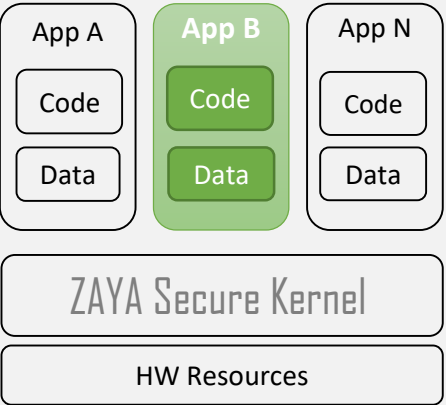
Each image authenticates the next level images.



Process Isolation

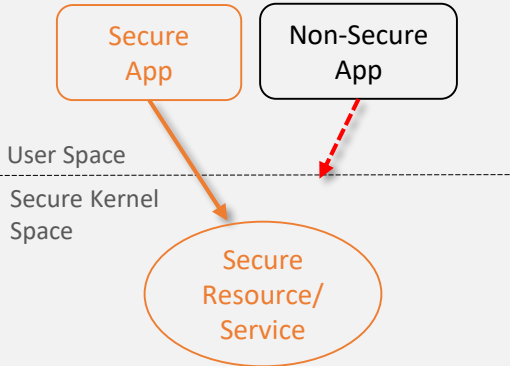
The user application can directly access only its Code and Data address range.
(*Principle of least privilege)

- No interference, No Security Violation.



Access Control

Only a "Secure Applications" can access a "Secure Resources".



ZAYA Secure Kernel Versions

Feature	Trial Version	Full Version
Secure Boot		
Disabled Debug Interface		
Encrypted Image		
Multi-Thread		
Thread Sync Primitives (e.g. Mutex, Semaphore)		
Timer, IPC (Message Box)		
Multiple User Applications		
Image Separation		
User Image Authentication		
Process Isolation		
Access Control		
Dynamic Addressing		
Security Evaluation Friendly		
Kernel Source Code		

* In this demonstration, ZAYA Trial Version is used.



ZAYA Secure Kernel Demonstrations for STM32F429I-Discovery

What Do You Need?

1. STM32F429I-Discovery Evaluation Board
2. Keil uVision 5 IDE
3. Terminal Application for UART Log Output.

Preparation

1. Connect STM32F429I-Discovery Board
2. Open Terminal Program with 460800 Baud Rate.

✓ Now, you are ready to run ZAYA Secure Kernel Demonstrations now.



<https://www.st.com/en/evaluation-tools/32f429idiscovery.html>

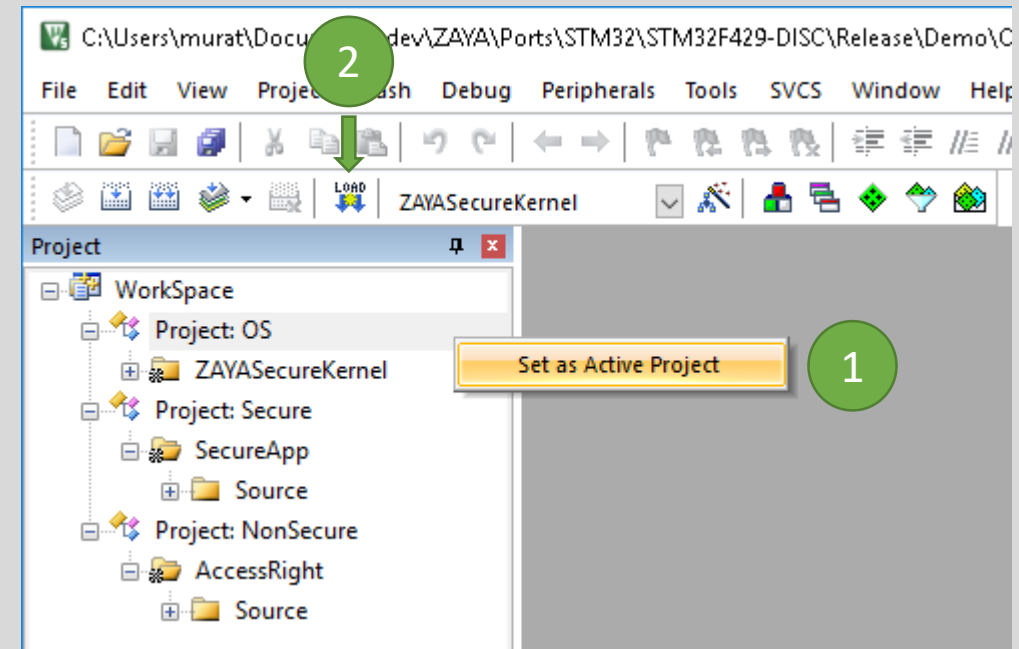
ZAYA Secure Kernel Demonstrations

Download the ZAYA Secure Kernel

1. Select OS Project in uVision using Context Menu.
2. Use the “LOAD” button (or F8) to download the OS.

OS Kernel Project

- There is no ZAYA Secure Kernel Source code in the OS project.
- Once you download the ZAYA Secure Kernel, it runs stand-alone and starts to protect the system.
- There is no need to download the Kernel again for each application modification.



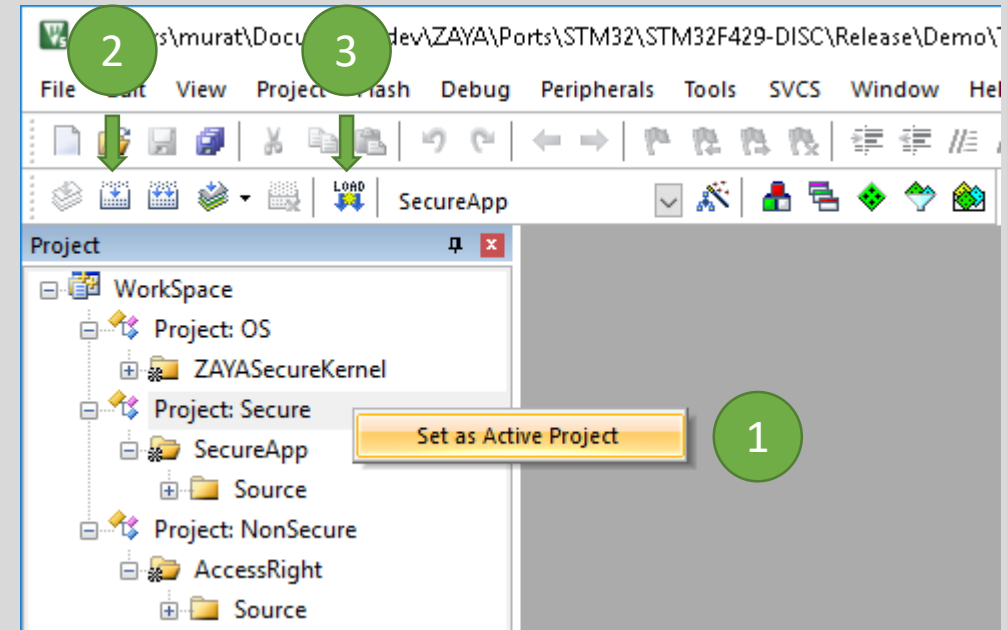
ZAYA Secure Kernel Demonstrations

Download the Example Secure ZAYA Application

1. Select “Secure” Project in uVision using context menu
2. Build(F7) the Secure Application.
3. Use the “LOAD” button to download the Secure Application.

Secure Application

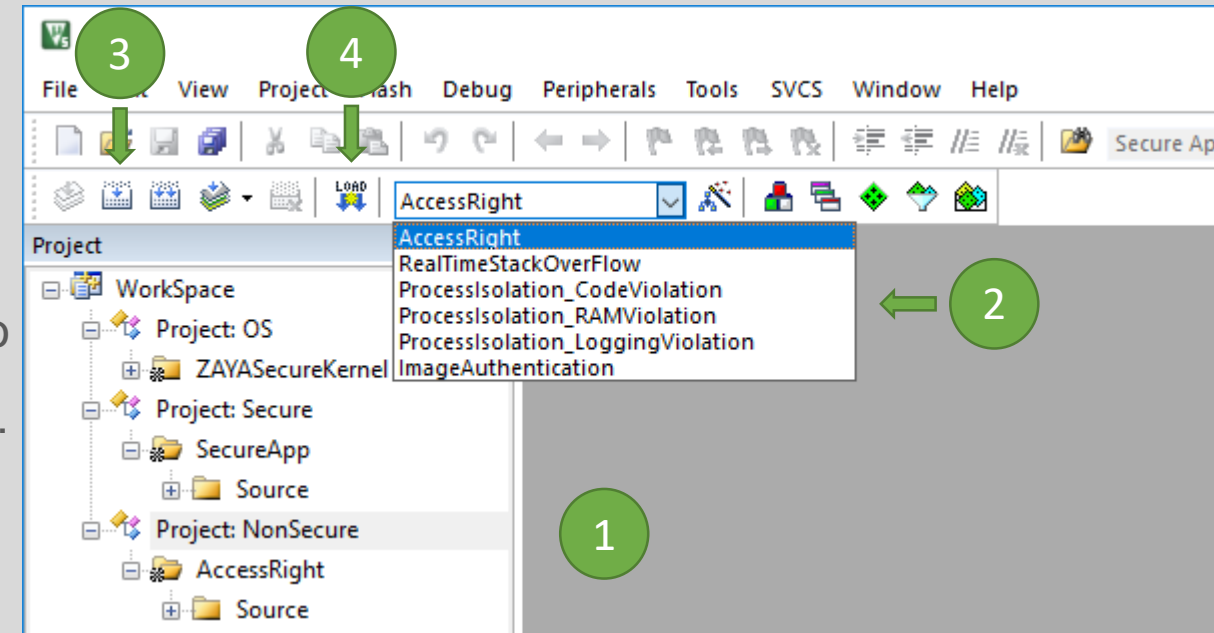
- Please see the main.c for example secure application implementation.
- You can play with secure application and re-install the app individually.



ZAYA Secure Kernel Demonstrations

Download the Example Non-Secure ZAYA Application

1. Select “NonSecure” Project in uVision.
2. Select “Demo Type” from the List
3. Build(F7) the Non-Secure Application for selected demo
4. Use “LOAD” button to download the Secure Application.
5. Repeat Step 2-4 for each demo type.



Non-Secure Application

- Please see the main.c for example non-secure application implementation.
- Non-Secure application is used to show demonstration cases so please select the build option to see test cases (Access Right, StackOverflow, Code/RAM Violation, Authentication)
- Each test case prints detailed information about the case.

Enjoy!

With Rich OS Features of ZAYA on small IoT devices.

