

3mdeb software services

SRTM Deployment



3MDEB

ul. Burgaska 9D/10
80-287 Gdańsk, Poland
TAX ID: PL2530164147

CONTACT

Piotr Król, 3mdeb CEO
+48 880 673 344
contact@3mdeb.com



[Website](#)



[About Us](#)



Table of Contents

1. [Service description](#)
2. [Key features](#)
3. [Service timeline](#)
4. [Service options](#)
5. [Requirements](#)
6. [Specification](#)
7. [Read-only recovery](#)
8. [Read-write main firmware](#)
9. [How to order](#)



Service description

SRTM (Static Root of Trust Measurement) is a technology which uses TPM (Trusted Platform Module) and cryptographic techniques to provide measurements of software and platform components so that system software as well as local and remote management applications may use those measurements to make trust decisions. It is used to protect BIOS, firmware and software from malicious attacks on a very low level. 3mdeb security engineers have enabled SRTM on numerous platforms as an open source implementation, and have a decent experience in its development.

Key features

Common challenges meet while enabling Static Root of Trust Measurement:

- proprietary firmware, closed-source tools.
- SPI chip, which can be an immutable root of trust.
- not-trivial recovery procedures.
- complex chain of trust.

Our solutions:

- open source firmware, open source tools. We leverage security with auditable code without back-doors.
- we can re-solder a board to make it have an SPI with proper protection mechanisms
- we are able to prepare recovery procedures matching the device environment (recovery using serial, through the network, etc.), we also have recovery dongle solution if it would turn out to be necessary.
- we are experienced in establishing a chain of trust, i.e.: coreboot, AGESA, FSP payloads(SeaBIOS, sortbootorder, memtest86+, iPXE), kernel, root file system, 2nd stage bootloader and eventually OS.



Service timeline

1. Customer is interested in 3mdeb Static Root of Trust Measurement implementation.
2. 3mdeb team prepare a microchip with a proper 3mdeb key.
3. After confirmation Customer receives a flashed chip, which can be soldered on a board. The chip contains 3mdeb master key, which can be proved to allow only the signed firmware to be used to flash the platform.
4. The Customer verifies, that the platform:
 - After trying to flash the firmware with unsigned or wrongly signed binary won't boot and fall into the recovery mode, in which all the media are unreachable.
 - After trying to flash the firmware with binary signed by 3mdeb the device will return from the recovery mode and shall boot without issues.
5. The Customer decides, if he/she wants to order flashed chips, devices with flashed chips or the procedure of building SRTM, and what maintainership option will be included. The Customer chooses what kind of key management option will be supported.
6. Customer invoicing and deployment phase sign-off.
7. Depending on the above, the customer receives deliverable as detailed in the scope.
8. Maintainership phase, depending on the scope.



Service options

Feature	Basic	Optimum	Premium
Flashed chip	✓	✓	✓
with 3mdeb master key			
Generating private key	✓	✓	✓
Customer key delivery	✓	✓	✓
Flash lockdown	✓	✓	✓
Full recovery enabled	✓	✓	✓
Signed release on demand	X	✓	✓
3mdeb keys maintainership	X	✓	✓
Mixed keys maintainership	X	✓	✓
Custom improvements	X	X	✓
Custom solutions	X	X	✓
Hardware development support	X	X	✓

Basic option

The Customer receives a validated microchip signed with a 3mdeb master key. The Client is invoiced for preparation and delivery. After proving that SRTM works as should be, one decides how many chips or devices He or She want to acquire. After invoicing there is a stage of signed image deployment and provisioning (flash lockdown) and the chips signed with client's keys are delivered.

Optimum option

After delivery of chips or devices, the Client has access to firmware updates, which are delivered on demand (usually monthly, for every release), and which are signed with His or Her keys. Keys are maintained by 3mdeb. There are also possible mixed solutions with 3mdeb partial keys maintainership.

Premium option

The Client may suggest own custom solutions or expected features. These can vary and it is considered a new project which requires new cost proposal. Client's device hardware development infrastructure may be integrated with 3mdeb infrastructure for hardware development purposes.



Requirements

Crucial is to determine the scope of work. SRTM deployment means that we deliver our clients a solution for the chosen board. The board has to have a chip, which has required protection mechanisms. If it doesn't, we can either use a dongle with the correct chip, or someone (a vendor, 3mdeb) has to replace it on the board. This service is based on deployment of Static Root of Trust Measurement for firmware. This technology can be obviously used in trusted booting of OS, if the OS contains support for TPM based passwordless encryption, but be aware, that enabling the secure boot for OS with coreboot firmware and SRTM changes the scope of the work dramatically.

We may generate and maintain keys for your firmware and provide updates whenever it is suitable for you.

Specification

SRTM in coreboot is based on the vboot module and TPM drivers which provide both cryptographical verification and measurements of the executed/used firmware components.

Typical vboot enabled firmware image consists of max 3 firmware volumes, each serving a different purpose. These particularly are:

- write protected read-only partition for recovery
- read-write firmware partition A for the main, normal, verified boot path
- read-write firmware partition B as a fallback, secondary, verified boot path



Read-only recovery

The write-protected read-only partition is the most crucial part of the whole image. It contains the vboot library/verstage, bootblock with reset vector and the public keys used for read-write firmware partitions verification. Thus it is marked as write-protected and read-only since it is the Core Root of Trust for Measurement. In order to provide the safety the read-only partition is being permanently locked with SPI flash block protection mechanism to avoid attacks on the vital part of SRTM implementation. The reset vector and vboot should be immutable to ensure the security of the implementation. The public part of the root key is also stored in the read-only partition. Root key was used to derive the recovery keys and firmware signing keys.

Among mentioned purposes, the read-only partition is also considered as a recovery partition. In case the read-write partitions contain invalid firmware the immutable read-only partition should be always bootable. Since it is trusted, because of flash protection in place. However, the recovery partition should boot only trusted recovery OS/application allowing to flash correctly signed read-write firmware. We offer the following solutions for recovery applications:

- minimal Linux kernel embedded into a read-only partition with gnupg, network, detachable storage drivers and flashing utility (without kexec or other possibilities to boot other OS)
- dedicated recovery payload (developed on demand at additional cost) embedded into a read-only partition



Read-write main firmware

Read-write partitions contain the main, updatable firmware that is verified by the vboot located in a trusted read-only partition. The whole firmware in the partition is signed with firmware signing key derived from root key. The signature, hash and the keyblock built from public parts of root keys and firmware signing key is packed into a structure called VBLOCK. VBLOCK is also a part of read-write firmware partition and is the first component verified during normal, verified boot path. If the hashes of VBLOCK are valid, then hashes and signatures of the bootable part of the partition are calculated and checked against those present in the VBLOCK. Only then the firmware is considered valid and executed. In case of failure, the partition is marked invalid and on next boot, the read-write partition B is tried as a fallback. If both partitions are invalid, the platform enters the recovery boot path.

In contrast to read-only firmware, the read-write firmware has typical storage drivers and boot capabilities from external and internal devices without restrictions. Most commonly used payload in such case is SeaBIOS.

How to order

Just [contact us](#) or [book a call](#).