ELASTIC Project
Secure Systems Group, Aalto University

Ionuț Groza, Xuan-Huy Ngo, Lachlan J. Gunn

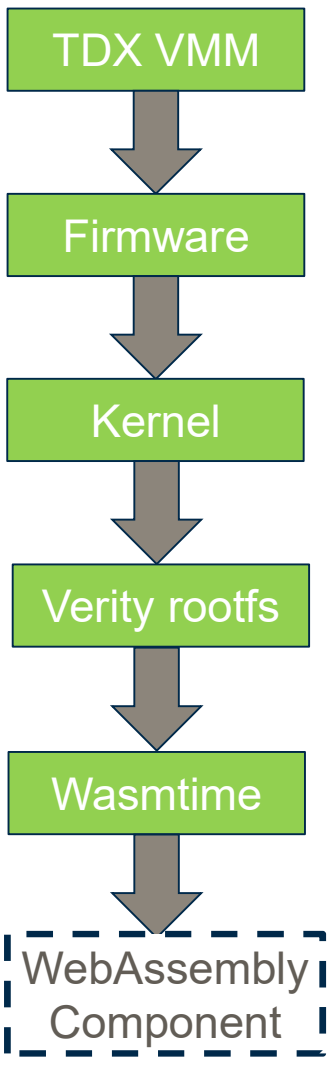
Building Trust in WebAssembly Components

Chains of Trust
Utilizing roots of trust to build trust in a protection mechanism and its underlying blocks.

Remote Attestation
Given a definition of good, a remote party can verify if it is satisfied by the system at hand.

WebAssembly Components
Compute workloads with improved performance, portability and sandboxing features.

Confidential Virtual Machines (CVMs)
VMs that offer hardware level memory protection mechanisms and remote attestation capabilities.



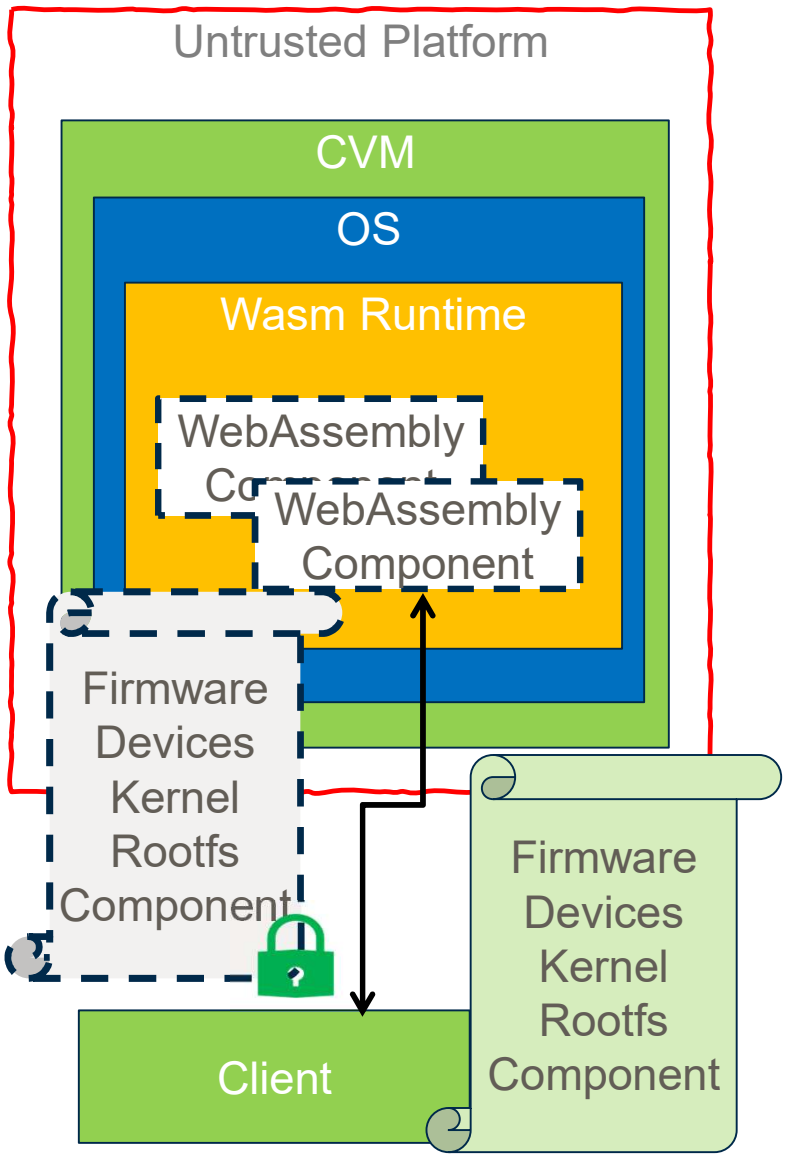
Intel TDX
Represents the root of trust which can be traced all the way to the manufacturer. It loads and measures the firmware.

TDVF and TD-Shim
Specialized firmware for Intel TDX. Extends the chain of trust to the OS via Secure Boot.

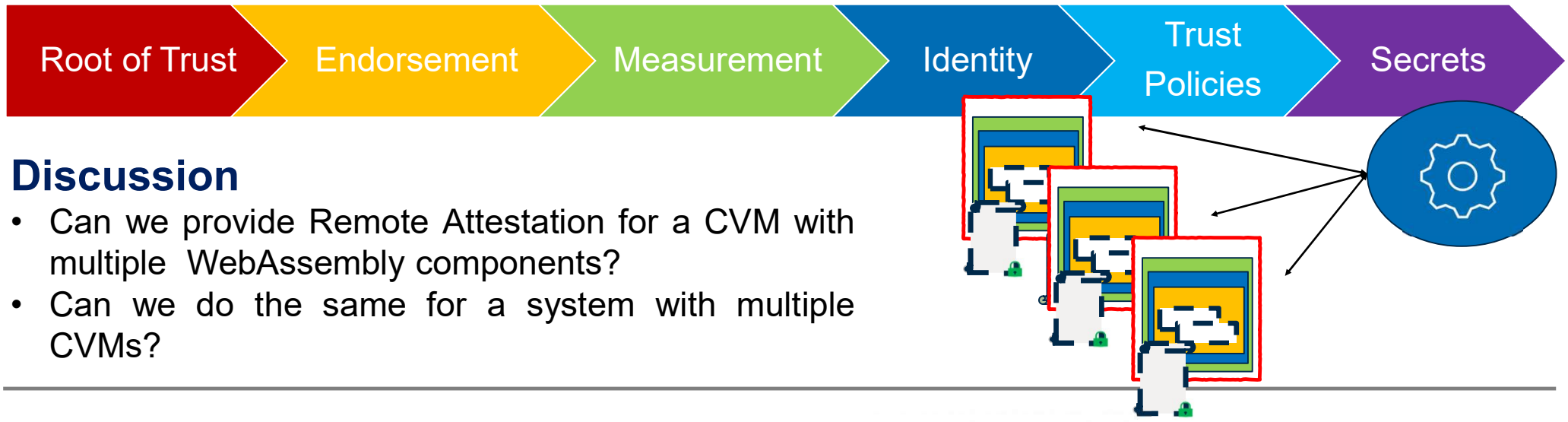
Unified kernel image (UKI)
A single executable containing the kernel image, kernel command line and *initrd*.

DM-Verity
Converts the *rootfs* to a *merkle* tree with the root hash embedded in the kernel command line, providing integrity and trust.

Wasmtime HTTP Embedding
Completes the chain of trust by measuring the component binary in the Remote Attestation evidence dynamically.



REMITS: A Model for Chains of Trust



Discussion
- Can we provide Remote Attestation for a CVM with multiple WebAssembly components?
- Can we do the same for a system with multiple CVMs?

Aalto University

Co-funded by the European Union

6GSNS

elastic

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or SNS-JU. Neither the European Union nor the granting authority can be held responsible for them.