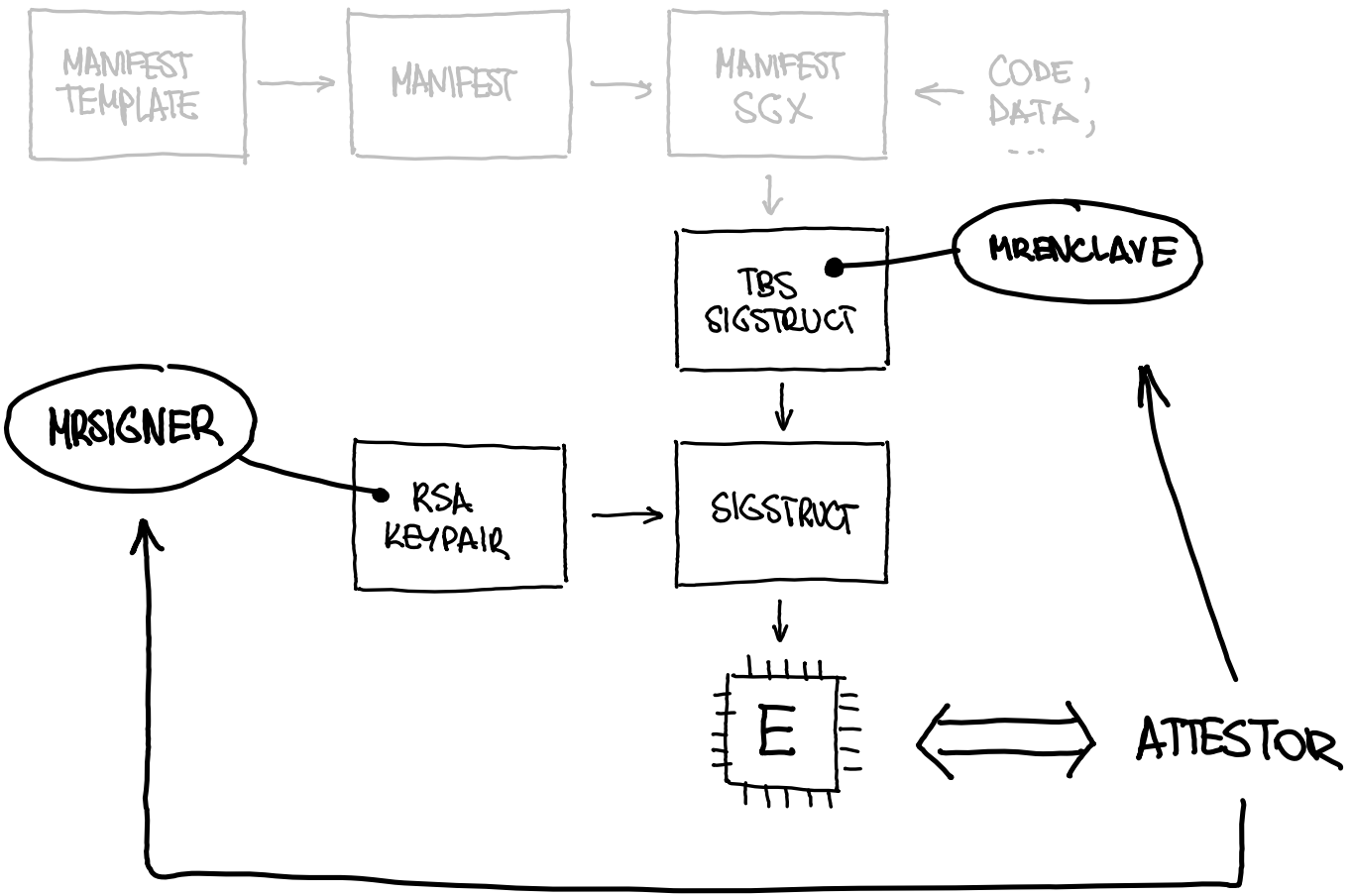
SGX ONE-TIME-KEY SIGNING

AND AN EXCURSION INTO PACKAGING

Wojtek Porczyk <woju@invisiblethingslab.com>

7.03.2023

GRAMINE SGX SIGNING AND ATTESTATION



PROBLEMS WITH RELYING ON MRSIGNER

→ KEY PROTECTION
(HSM, cloud APIs?, controls, audits, ...)

→ YOU NEED TO MAKE SURE YOU DON'T SIGN ANYTHING WRONG,
because if you do, then

→ KEY ROTATION?
re-sign everything

→ DATA COMPARTMENTALISATION (NONEXISTENT) ← IMPORTANT

→ IT'S A RELIC FROM THE PAST
when you needed Intel® Permission™
to run SGX® ENCLAVE !! 1

IT'S NOT ACTUALLY NEEDED

IF YOU ALSO CHECK MRENCLAVE

BUT

→ RSA SIGNATURE IS REQUIRED BY FORMAT(s)

→ PRIVATE KEY STILL NEEDS PROTECTION!

- what if attestor forgets to check MRENCLAVE
- rogue employee signs an enclave to extract secret from attestor

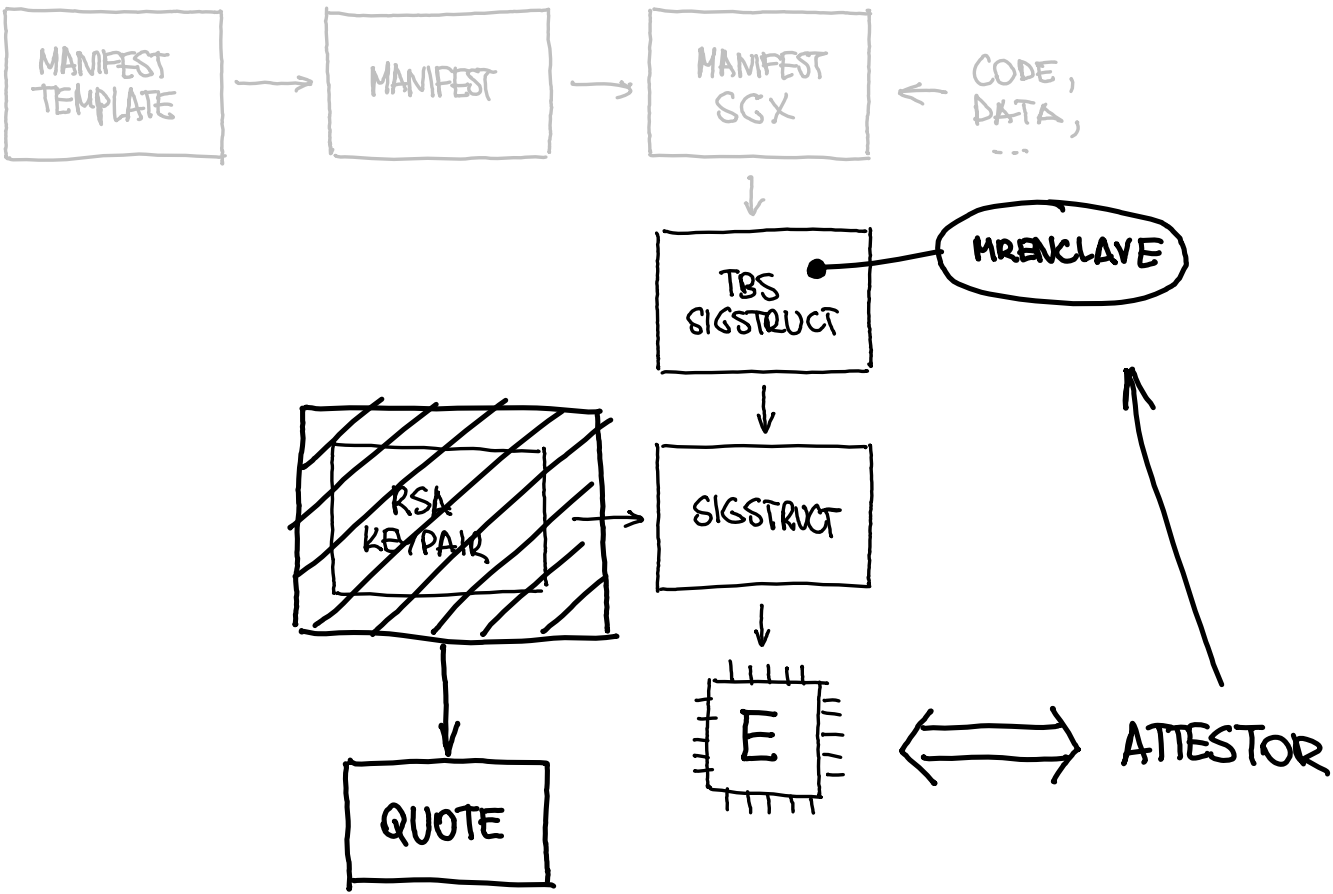
ONE TIME KEYS

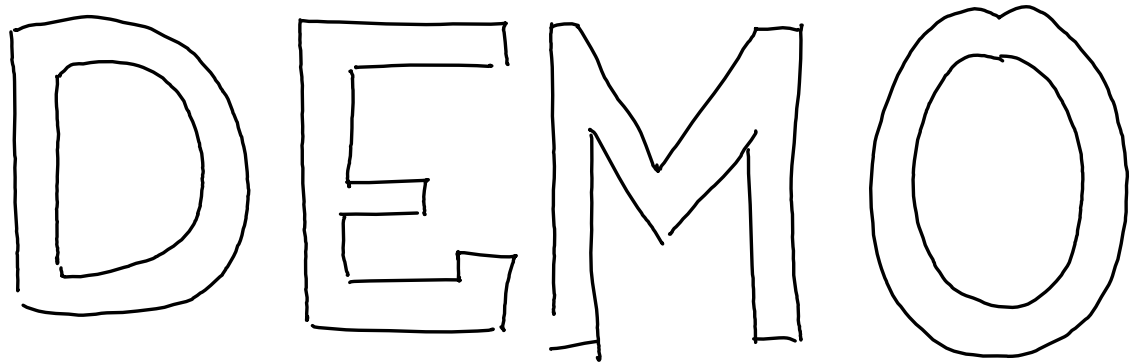
→ RANDOM

→ DISCARDED AFTER SINGLE OPERATION } INSIDE SGX ENCLAVE

→ PROOF: A QUOTE FROM THE SIGNING ENCLAVE
with MRSIGNER in user data

→ KEEPS ATTESTORS "WELL OILED"


MANIFEST TEMPLATE
MANIFEST
MANIFEST SGX
CODE, DATA, ...
TBS SIGSTRUCT
MRENCLAVE
RSA KEYPAIR
SIGSTRUCT
E
ATTESTOR
QUOTE


DEMO