

Confidential Computing with Secure Execution (IBM Z)

—

Jakob Naucke

Cloud Development for Linux and OpenShift
on IBM Z & LinuxONE

IBM Secure Execution for Linux

IBM Z & LinuxONE/
s390x/“mainframe”
used for Red Hat
OpenShift workloads

Hardware confidential
computing support
since z15 (September
2019) & LinuxONE III

Necessarily based on
Linux KVM
virtualization

Other virtualized
confidential computing
technologies include
IBM Power’s PEF, AMD
SEV, and Intel TDX

How do you know your workload runs in a secured context?

```
$ ssh my-secure-domain  
Hi, this is the motd from your  
cloud provider! I am totally  
running this inside Secure  
Execution!
```

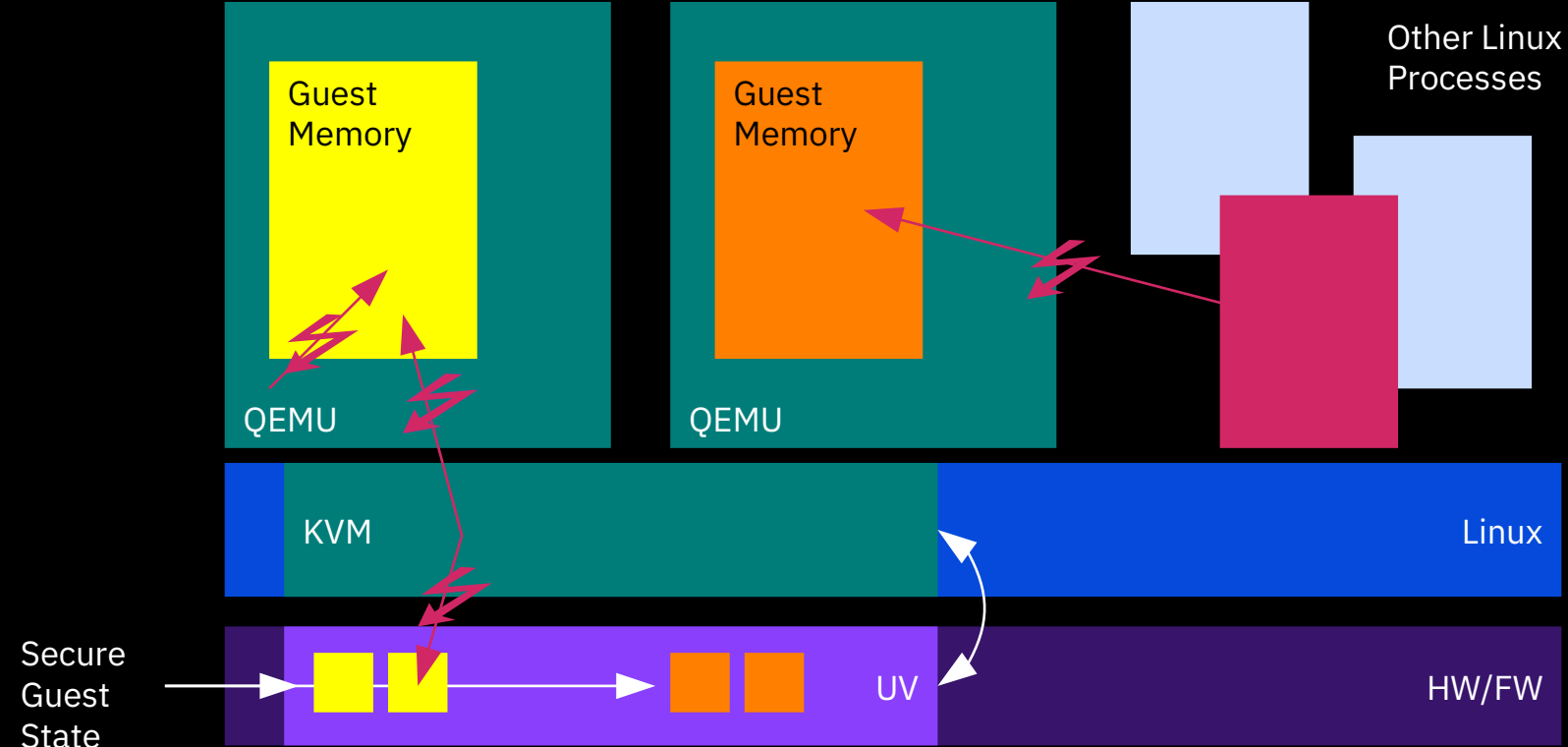
This can be achieved through attestation and smaller encrypted key containers.

Secure Execution (like PEF) relies on a fully **encrypted boot image** that can house anything.

The asymmetric key is tied to the machine and can be verified through a certificate authority.

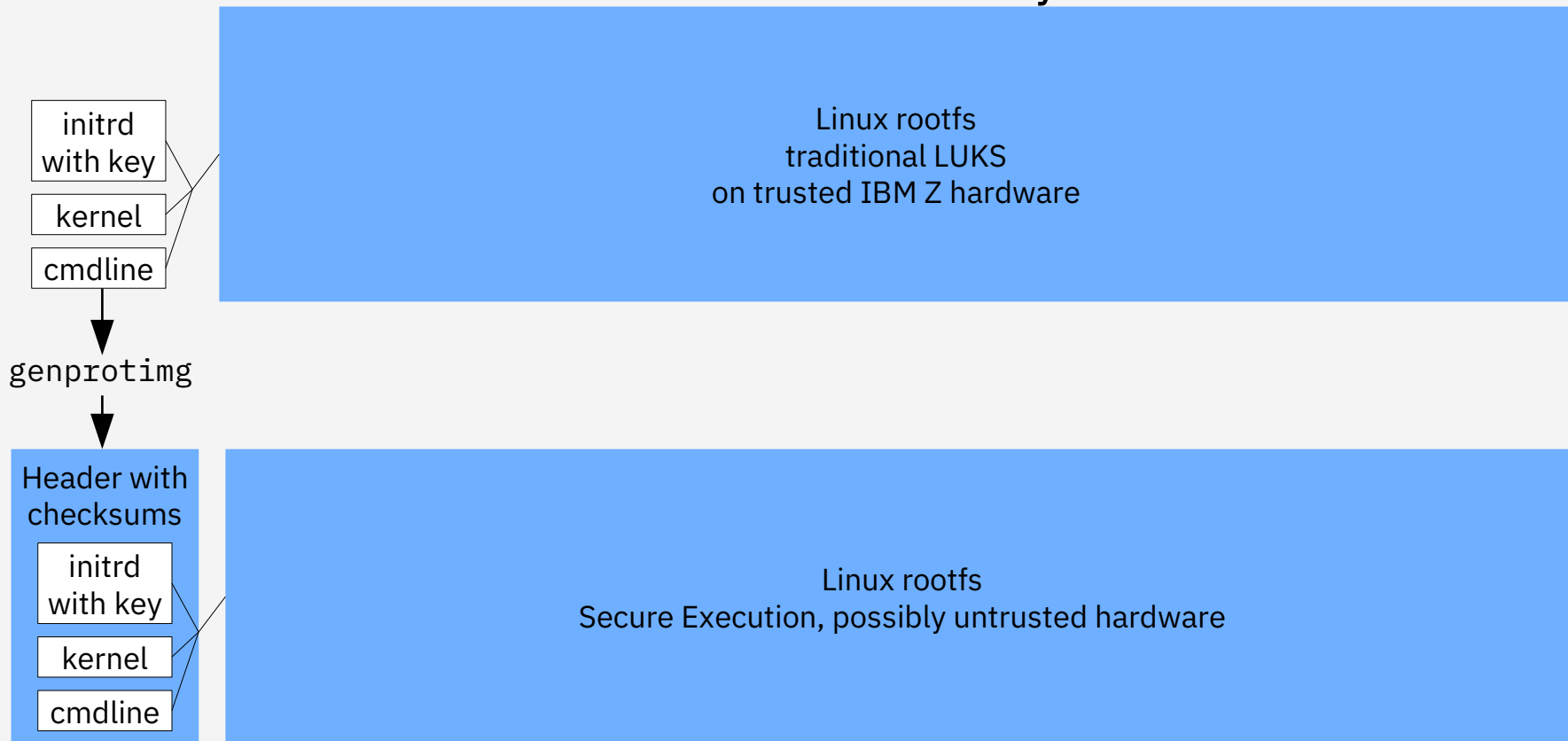
But how can the machine retrieve the private key for decryption? If the *hypervisor* could simply read it, you haven't gained anything.

Enter the Ultravisor



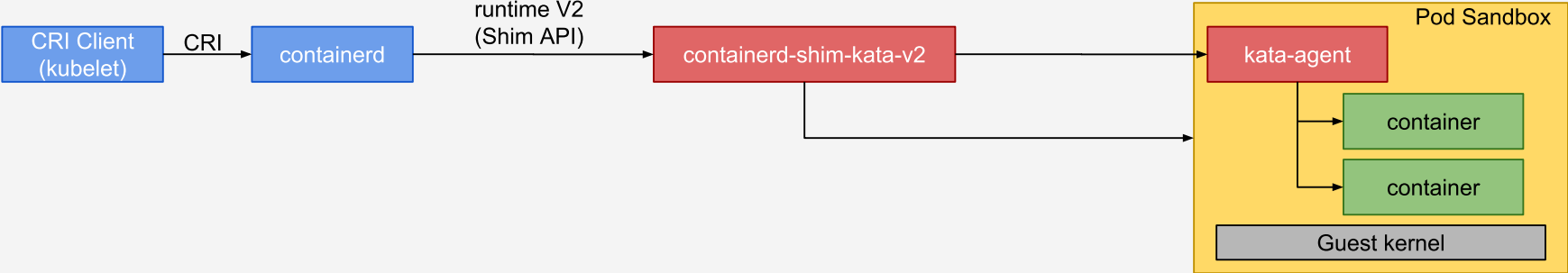
“Classical” Secure Execution

...but what if you want containers?



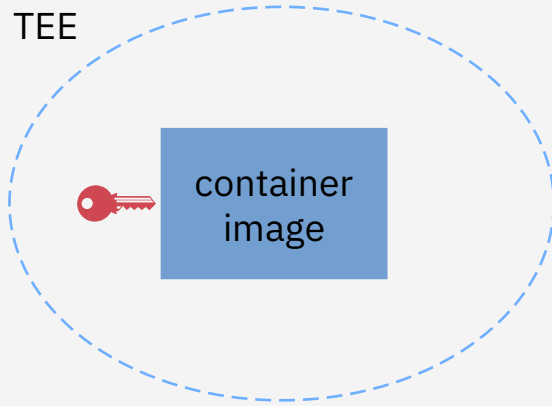
Enter Kata Containers

“The speed of containers, the security of VMs”



How do you achieve confidential computing with Kata Containers?

TEE



Utilize hardware. Lock the agent.

As a first, basic solution, we can put anything we might want to use into a custom, encrypted image.

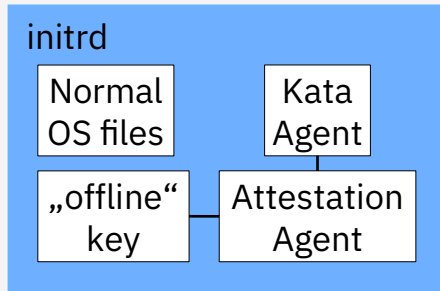
This image is pulled upon creating a container.

Where is the key to decrypt it?

Integrating the current Secure Execution workflow with the Attestation Agent

“Bake-in” approach

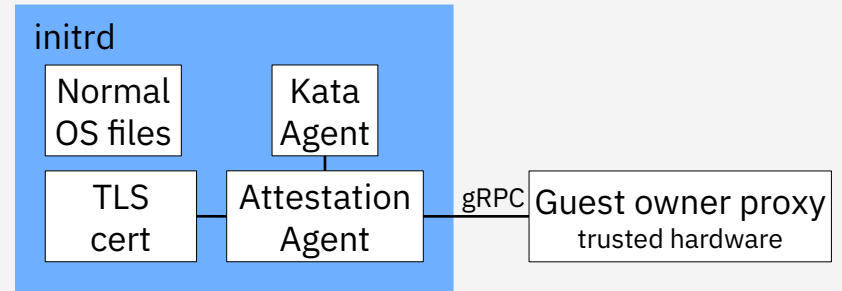
Integrate the keys to decrypt image layers



Simple, but inflexible

“Key fetch” approach

Classical authentication



(Somewhat) more flexible
TLS as substitute for runtime attestation

Thank you

Jakob Naucke
Cloud Development for Linux and OpenShift on IBM Z & LinuxONE

—
jakob.naucke@ibm.com
github.com/Jakob-Naucke
ibm.com

© Copyright IBM Corporation 2021. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and ibm.com are trademarks of IBM Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available at [Copyright and trademark information](#).

IBM, the IBM logo, IBM Z, IBM z15, IBM LinuxONE, Secure Execution, IBM Power, and PEF are trademarks of IBM Corporation in the United States and/or other countries. Red Hat and OpenShift are trademarks or registered trademarks of Red Hat Inc. in the United States and/or other countries. Intel and TDX are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and/or other countries. AMD and SEV are trademarks or registered trademarks of Advanced Micro Devices Inc. in the United States and/or other countries. UNIX is a registered trademark of The Open Group in the United States and/or other countries. Linux is a trademark of Linus Torvalds in the United States and/or other countries.

Any performance data contained in this document was determined in a controlled environment. Actual results may vary significantly and are dependent on many factors including system hardware configuration and software design and configuration. Some measurements quoted in this document may have been made on development-level systems. There is no guarantee these measurements will be the same on generally-available systems. Users of this document should verify the applicable data for their specific environment. IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

Information is provided "AS IS" without warranty of any kind. All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area. All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

