SPECIFICATION DOCUMENT

CYSEC

ARCA TRUSTED OS

Hardware compatibility

Hardware recommendations summary

The following table summarizes the hardware specification requirements to deploy ARCA Trusted OS

Mandatory hardware requirement			
CPU	x86-64 - Intel	x86-64 - AMD	ARM
MINIMUM RESOURCES	CPU: 2vCPUs; Memory 8GB with ECC memory; DISK:SSD32GB		
UEFI/OVMF	Enable to upload CYSEC Secure boot public keys		
(v)TPM 2.0	To load and seal CYSEC FDE keys created at the installation phase in CPU (key rotation mechanism included) To save the hash value and verify those value during secure booth process to insure integrity		

Detailed product prerequisites for hardware/environment qualifications

This section lists the requirements on the hardware/environment to allow the deployment of ARCA Trusted OS on x86 (also called x86-64 or AMD64). The check of these requirements is the first step of a hardware/environment qualification.

1.Hardware component requirements in the case of a deployment on bare metal

Prerequisites for bare metal installation

REQUIREMENT	NECESSITY	NEEDS	NOTES
CPU Architecture	**Mandatory** without a match of this requirement ARCA Trusted OS cannot work at all	ARCA Trusted OS is deployed on CPUs with an x86 architecture (Intel or AMD, also known as x86-64 or amd64).	A version of ARCA Trusted OS for ARM is planed in 2023
UEFI	**Mandatory** without a match of this requirement ARCA Trusted OS cannot work at all	The hardware includes a BIOS capable of booting in UEFI mode with the ability to provision CYSEC's own Secure boot keys (PK, KEK and db).	

REQUIREMENT	NECESSITY	NEEDS	NOTES
TPM	**Highly recommended** without a match of this requirement, ARCA Trusted OS can work but the encryption keys are not protected (the key are stored in clear to the side of the client's data)	The hardware includes a TPM2.0 that can be used by ARCA Trusted OS to store the keys, chosen by the end-users, for the encryption of the hard disk.	Running ARCA Trusted OS without TPM2.0 or compatible vTPM is not recommended by CYSEC

–

2. Hardware component requirements in the case of a deployment in a VM

Prerequisites for VM installation

REQUIREMENT	NECESSITY	NEEDS	NOTES
CPU Architecture	**Mandatory** without a match of this requirement ARCA Trusted OS cannot work at all	ARCA Trusted OS is deployed on CPUs with an x86 architecture (Intel or AMD, also known as x86-64 or amd64)..	A version of ARCA Trusted OS for ARM architecture is planed in 2023
OVMF	**Mandatory** without a match of this requirement ARCA Trusted OS cannot work at all	The CSP environment allows: 1 - the modification of the OVMF of the Virtual Machine with the ability to provision CYSEC's Secureboot keys (PK, KEK and db) 2 - the use of this modified OVMF to create an image of ARCA Trusted OS VM.	–
v-TPM	**Highly recommended** without a match of this requirement ARCA Trusted OS can work but the encryption keys are not protected (the key are stored in clear to the side of the client's data)	The hardware includes a v-TPM that can be used by ARCA Trusted OS to store the keys for the encryption of the hard disk.	Running ARCA Trusted OS without TPM2.0 or compatible vTPM is not recommended by CYSEC

REQUIREMENT	NECESSITY	NEEDS	NOTES
CONFIDENTIAL COMPUTING (CC) (protection of data in-use)	**Recommended** without a match of this requirement ARCA Trusted OS can work but the end-users containers cannot benefit from the protection of data in-use, i.e. the protection against hypervisor, CSP administrator, etc…	The node provided by the CSP includes AMD Epyc (Gen 2, Gen 3 and Gen 4) CPUs and the CSP hypervisor support the creation of confidential VMs.	–
ATTESTED CONFIDENTIAL COMPUTING (protection of data in-use + remote attestation)	**Ideal case** with a match of this requirement ARCA Trusted OS can run in a confidential context and this confidential context can be attested.	The hardware includes AMD Epyc (Gen 3 and Gen 4) CPUs, the CSP hypervisor supports the creation of confidential VMs and the CSP hypervisor exposes the remote attestation process provided by AMD Epyc CPUs to guess VMs	CYSEC is currently evaluating the remote attestation on AMD-SEV-SNP

Qualified x86-64 servers

Cysec has already qualified the servers that are presented in the following table

Qualify hardware

NAME	DL385	DL345	DL325	TB116	113MFAC 2-605CB	SYS-1019SWR
Provider	HPE	HPE	HPE	AIC	Supermicro	Supermicro
Realsec HSM	Yes	Yes	No	Yes	Yes	Yes
Ultimaco HSM	Yes	Yes	Yes	Yes	Yes	Yes
CPU	2xAMD	1xAMD	1xAMD	1xINTEL	1xAMD	1xINTEL

Qualified VMs

CYSEC has already qualified the public cloud CPUs that are presented in the following table.

Cloud deployment

			aws
Confidential VM on AMD-SEV	Yes	Yes	Yes
ARCA Trusted OS	Yes	Yes	Yes

CYSEC has qualified the hypervisors that are presented in the following table.

VM deployment

	ORACLE		vmware
Hypervisor	Virtualbox	QEMU/KVM	VMware ESXi v7 or later(workstation Pro 16.2 in test)
ARCA Trusted OS	Yes	Yes	Yes

ABOUT CYSEC

CYSEC SA is a data security company based at the EPFL Innovation Park in Lausanne, Switzerland.
CYSEC brings 360° security in one click for container-based workloads and platforms through its ARCA trusted OS software.

CYSEC partners with leading cybersecurity research centers to develop technological innovations in the area of Confidential Computing and delivers its cybersecurity solutions for any vertical sector. For more information, please visit www.cysec.com.

CYSEC SA
EPFL Innovation Park, Building D
CH- 1015 Lausanne, Switzerland

info@cysec.com

www.cysec.com

www.linkedin.com/company/cysecsystems