SPECIFICATION DOCUMENT

ARCA TRUSTED OS

Hardware compatibility

Basic hardware recommendations

The following table defines specifications requirements to deploy ARCA Trusted OS.

	MINIMAL	RECOMMENDED	MAXIMAL
CPU	2 vCPUs x86-64	8 vCPUs x86-64	64 vCPUs x86-64
MEMORY	8GB with ECC memory	64GB with ECC memory	2TB with ECC memory
DISK	SSD 32GB	SSD 1TB	SSD 4TB

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

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).	The overwhelming majority of today's DC servers, be it bare-metal or VMs, satisfy this requirement. *A version of ARCA Trusted OS for ARM architecture will be released in Q4 2022.*
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 Secureboot 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 with any hardware components.	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.	The present ARCA Trusted OS release (1.6.0) and the preceding ones CANNOT run on hardware without a TPM. The possibility to run ARCA without a TPM might be implemented later.
CONFIDENTIAL COMPUTING (protection of data in-use)	**Recommended** If ARCA Trusted OS runs on AMD CPU, and if the end-users use Kata-containers runtime, the end-user workloads benefit from the protection of data in-use	The server's CPU is AMD Epyc (Gen 2 and Gen 3) CPUs.	–

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

REQUIREMENT	NECESSITY	NEEDS	NOTES
vCPU Architecture	**Mandatory** without a match of this requirement ARCA Trusted OS cannot work at all	ARCA Trusted OS is deployed on vCPUs with an x86 architecture (Intel or AMD, also known as x86-64 or amd64)..	The overwhelming majority of today's DC servers, be it bare-metal or VMs, satisfy this requirement. *A version of ARCA Trusted OS for ARM architecture will be released in Q4 2022.*
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) and (2) the use of this modified OVMF to create an image of ARCA Trusted OS VM.	–
TPM	**Highly recommended** without a match of this requirement ARCA Trusted OS can work but the encryption keys are not protected with any hardware components	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.	The present ARCA Trusted OS release (1.6.0) and the preceding ones CANNOT run on hardware without a TPM. *The possibility to run ARCA without a TPM might be implemented later.*

REQUIREMENT	NECESSITY	NEEDS	NOTES
CONFIDENTIAL COMPUTING (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 and Gen 3) CPUs and the CSP hypervisor support the creation of confidential VMs (i.e. VMs running in the Trusted Execution Environment (TEE) provided by AMD Epyc CPUs).	–
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 2 and Gen 3) CPUs, the CSP hypervisor supports the creation of confidential VMs (i.e. VMs running in the Trusted Execution Environment (TEE) provided by AMD Epyc CPUs) and the CSP hypervisor supports the remote attestation of OVMF bundle provided by AMD Epyc CPUs..	–

Qualified servers up to now

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

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 CSP confidential VMs up to now

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

NAME	N2D	C2D
Provider	GCP	GCP
CPU	1xAMD	1xAMD

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