



Dasharo User Group #11 🎉 and Developers vPub 0x10 🍺

👋 DUG#11 Shameless Plug 👋





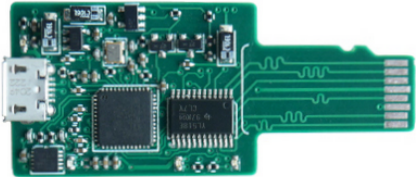
- 🌱 Growth & Transparency: Showcasing our evolution and commitment to open-source.
- 📖 Historical Record: A resource for 3mdeb, future customers, and the privacy/security community.
- 📈 Explore Business Model: Learn from our open-source firmware journey, including potential pitfalls.

What we will talk about

- Hardware,
- Services,
- Pace Enterprise Training,
- Dasharo Pro/Enterprise Package
- Accessories
- Everything available in 3mdeb shop: <https://shop.3mdeb.com>

The image features a dark gray background with the word "Hardware" centered in a bright green, sans-serif font. In the corners, there are decorative elements resembling circuit board traces. The top-left corner shows several parallel lines extending from the edge and ending in small circular nodes. The top-right corner features a more complex arrangement of lines, some parallel and some branching, also ending in circular nodes. The bottom-right corner has a few more lines and nodes, while the bottom-left corner is mostly empty except for the edge of the circuit lines.

Hardware



SDWire

89,00 €
(ex. VAT)

Overview

SDWire allows to flash SD card connected to the DUT (Device Under Test), without physical contact with the device. It serves as a SD card reader and SD card mux in one device. The PCB board is designed in such a way that it fits into micro SD card slots. Thanks to this, there is no need for special cables with a micro SD adapter, like in the muxPi product.

Documentation:

- [Getting started](#)
- [Specification](#)
- [Usage](#)
- [FAQ Section](#)

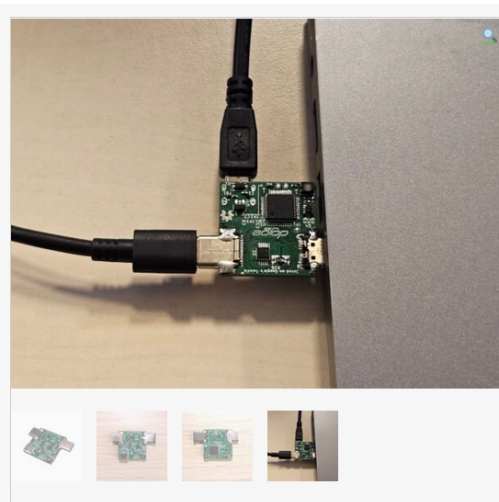
28 in stock

1

ADD TO CART

Enquiry for this product

<https://shop.3mdeb.com/shop/open-source-hardware/sdwire/>



Twonkie – USB-C sniffer

112,00 €

(ex. VAT)

Overview

An exclusive USB-PD sniffer/injector/sink inspired by the renowned Google project, Twinkie. It has been reimagined to be accessible to all enthusiasts. Twonkie is an excellent open-source solution for:

- Sniffing USB Power Delivery traffic on both Control Channel lines (CC1/CC2)
- Transparent interposer on a USB Type-C connection
- Monitoring VBUS and VCONN voltages and currents (Supports USB PD 3.1 EPR voltages up to 48V)
- Injecting PD packets on CC1 or CC2
- Putting Rd/Rp/Ra resistors on CC1 or CC2

The hardware design of [Twonkie](#) by [Joachim "dojoe" Fenkes](#) is licensed under CC BY 4.0.

Documentation:

- [Twonkie Introduction at Dasharo Universe](#)
- [GitHub documentation](#)

12 In stock

1

ADD TO CART

Enquiry for this
product

<https://shop.3mdeb.com/shop/open-source-hardware/twonkie-usb-c-sniffer/>



Dasharo Supported Hardware



ASRock SPC741D8-2L2T/BCM with
Dasharo (coreboot+UEFI) Pro
Package for Servers

BUY NOW



Full Build ASRock SPC741D8-2L2T/
BCM with Dasharo
(coreboot+UEFI) Pro Package for
Servers

BUY NOW

<https://shop.3mdeb.com/product-category/dasharo-supported-hardware/>



Gigabyte MZ33-AR1 with Dasharo
(coreboot+UEFI) Pro Package for
Servers

BUY NOW



Full Build Gigabyte MZ33-AR1 with
Dasharo (coreboot+UEFI) Pro
Package for Servers

BUY NOW

<https://shop.3mdeb.com/product-category/dasharo-supported-hardware/>



Dell OptiPlex 7010 SFF with Dasharo
(coreboot+UEFI) Pro Package for
Desktop

165,00 € – 435,99 €
(ex. VAT)

BUY NOW



Dell OptiPlex 9010 SFF with Dasharo
(coreboot+UEFI) Pro Package for
Desktop

210,00 € – 480,99 €
(ex. VAT)

BUY NOW

<https://shop.3mdeb.com/product-category/dasharo-supported-hardware/>



Hardkernel Odroid H4+ with
Dasharo (coreboot+UEFI) Pro
Package for Network Appliance

290,00 € – 529,50 €

(ex. VAT)

[BUY NOW](#)



Hardkernel Odroid H4+ for Pace
Enterprise Training (PET) –
DS09SBL

381,00 € – 498,00 €

(ex. VAT)

[BUY NOW](#)



OST2 Hardkernel Odroid H4+ with
Dasharo (coreboot+UEFI) Pro
Package for Network Appliance

335,50 € – 452,50 €

(ex. VAT)

[BUY NOW](#)

<https://shop.3mdeb.com/product-category/dasharo-supported-hardware/>



**NS70 Series 17.3" Dasharo laptop by
NovaCustom**

BUY NOW



**V54 Series 14" Dasharo laptop by
NovaCustom**

BUY NOW



**V56 Series 16" Dasharo laptop by
NovaCustom**

BUY NOW

<https://shop.3mdeb.com/product-category/laptops/>



Refurbished PC Engines APU with
TPM & Dasharo Pro Package

323,00 € – 502,00 €

(ex. VAT)

BUY NOW

<https://shop.3mdeb.com/product-category/system-boards/>

 Protectli Vault FW2B 239,42 € – 374,76 € (ex. VAT) BUY NOW	 Protectli Vault FW4B 313,36 € – 448,70 € (ex. VAT) BUY NOW	 Protectli Vault FW6A 350,34 € – 518,95 € (ex. VAT) BUY NOW	 Protectli Vault FW6B 461,26 € – 629,87 € (ex. VAT) BUY NOW	 Protectli Vault FW6C 553,70 € – 722,31 € (ex. VAT) BUY NOW
 Protectli Vault FW6D 636,89 € – 805,50 € (ex. VAT) BUY NOW	 Protectli Vault FW6E 738,57 € – 907,18 € (ex. VAT) BUY NOW	 Protectli Vault VP2410 – 4 port 424,28 € – 541,13 € (ex. VAT) BUY NOW	 Protectli WiFi Kit Wireless B/G/N at 2.4Ghz 42,90 € (ex. VAT) ADD TO CART	

<https://shop.3mdeb.com/product-category/vaults/>

The background features a dark gray field with light gray circuit-like lines. These lines are composed of straight segments and right-angle turns, some ending in small circular nodes. The lines are primarily located along the left and right edges, with a few extending towards the center.

Pace Enterprise Training

Client Type	Individuals		Business		
Cooperation Models	OST2	Public Security Conferences		Remote PET	PET Corporate Program
Target Audience	Community	Individual Clients	Business Clients	Corporate, NGO and Public Sector	Corporate**
Primary Use	Self-paced Education	Individual Employees Education		Teams Education	Division Education
Access to Materials	Open	Limited to Students		Limited to Students*	Limited to Division
Support Level	Community Support and Occasional Support from Instructor	Direct Support from Instructor		Extended Direct Support from Instructor	Direct Support from Team of Instructors
Customization	-	Limited		High	High
Pricing Model	Free	Pre-Paid to Conference Organizers		Pre-Paid to 3mdeb	Annual Contract
Additional Features	-	Pace and Content Adjustment According to Audience Needs Access to Instructure during Breaks and Afterhours		Material Adjustment According to Organization Needs Analysis of Individual Needs of Organization	Custom Curriculum for Whole Division

* - Unless direct agreement available, including recording, speaker notes etc.

- x86, Arm and POWER9/10
- All open-source firmware topics for each available framework (coreboot, EDKII, U-Boot, TrustedFirmware, OpenBMC, Yocto etc.)
- Closed source firmware components: ME/CSME/TXE/SPS, PSP/ASP, microcode, Intel ACMs
 - based on publicly available materials
- Low-level security mechanisms with example CVE exploitation (UEFI Secure Boot, Intel Boot Guard, closed source firmware etc.)
 - vulnerability class analysis
- Trusted Computing Technologies
 - BitLocker/LUKS/Heads
 - Measured Boot
 - SRTM/DRTM and other Root of Trust for Measurement
- Firmware development life-cycle from considerations at hardware design stage to long term maintenance.
- Your topic not on the list? Feel free to contact us: `contact<at>dasharo<dot>com`

DS01CBI: coreboot for embedded linux developers

Overview

- modern x86 architecture
- firmware design principles by examples
- boot flow from power on to system take off
- Coreboot walk through
- firmware build process based on Coreboot
- coreboot developer workflow
- remote testing environment
- SPI flash theory of operation
- flashing and debugging tools
- writing payloads hands-on workshop
- FSP – from theory to integration
- firmware security basics in Coreboot ecosystem
- MinnowBoard – hands-on workshop using previously
- gained knowledge



Duration

5 days

40 hours (8h/day)

70% lectures

30% hands-on workshop

<https://paceenterprisetraining.com/>

DS02RTA: Intel Root of Trust training

Overview

- Based on OST2 Arch4001, Arch4021, TC3001, TC3011 and TC3211
- UEFI introduction
- Modern x86 architecture
- Where is firmware and why blobs
- Intel x86 feature set and boot process
- Intel Root of Trust Technologies
- Other Root of Trust technologies overview
- Intel Management Engines features, vPRO, me_cleaner
- Workshops using Intel Skylake-based COMe module showing the process of enabling Boot Guard and practical examples of its features



Duration

4 days

17 hours (8h/day)

100% lectures

Materials

All training materials presentations and source code will be available for the client's internal usage.

<https://paceenterprisetraining.com/>

Overview

- Based on OST2 Arch2001, Arch4001 and Arch4021
- x86 assembly
- x86 operating system internals
- x86 boot process
- PCI and PCI Express
- Modern Intel system architecture
- DMA and IOMMU
- ISA and Plug and Play
- Debugging with GDB and core dumps
- System emulation with QEMU
- UEFI introduction
- UEFI Secure Boot
- Introduction to Roots of Trust and Trusted Computing Technologies



Duration

9 days

37 hours (4h/day usually, except for once 5h/day)

of lectures with hands-on labs

Materials

All training materials presentations and source code will be available for the client's internal usage.

Language

English

<https://paceenterprisetraining.com/>

ZH01ELI: Building and Development of Embedded Linux Systems

Overview

- Open source development overview
- Brief history of Linux
- Linux kernel introduction
- Using Git for source code management
- Introduction to Embedded Linux
- Getting kernel source code
- Linux kernel configuration and compilation
- Cross development
- Linux kernel modules
- Character device drivers
- Linux kernel debugging
- Device Tree files
- Typical Embedded Linux bootloaders
- Introduction to Build Systems
- Building custom Embedded Linux system for typical hardware target
- Embedded Linux tools
- Embedded Linux application development and debugging



Duration

4 days

32 hours (8h/day)

50% lectures

50% hands-on workshop

Materials

All training materials presentations and source code will be available for customer internal usage.

<https://paceenterprisettraining.com/>

Overview

- Overview of an Embedded Linux system architecture
- Overview of the Yocto Project and OpenEmbedded ecosystem
- Using Yocto Project documentation
- Building emulation image
- Building image for the development board
- Board Support Packages and Yocto Project metadata
- Customizing the build with layers
- Image customization
- Extending existing recipes
- Overview of some of the existing build systems (Autotools, CMake, Meson)
- Creating a custom recipe
- Creating a custom image



Duration

4 days

28 hours (7h/day)

40% lectures

60% hands-on workshop

Materials

All training materials presentations and source code will be available for customer internal usage.

<https://paceenterprisettraining.com/>

DS08MSA: Mastering UEFI Secure Boot and Intel Root of Trust Technologies

Overview

- Understand the theoretical concepts behind UEFI Secure Boot, root of trust, and chain of trust technologies.
- Hands-on exploitation and defensive management of UEFI Variables and Authenticated Variables.
- Implement and validate UEFI Secure Boot through practical exercises.
- Identify, analyze, and exploit vulnerabilities, including BootHole and BitPixie (CVE-2023-21563).
- Dive into BootKitty, Hydrophobia, [Feb 2025 GRUB2 CVEs] and recent Gigabyte SMM vulnerabilities. (New)
- Implement and circumvent Intel Root of Trust, with a detailed case study on CVE-2017-5705 and a practical demonstration.



Audience

Embedded Developers, Firmware Developers, Platform and System Architects, Medical and Defense Product Owners, Hardware Hackers, Pen Testers, Operating Systems Security Researchers, Developers, and Maintainers.

Duration

3 days

21 hours (7h/day)

30% lectures

70% hands-on workshop

Materials

All training materials presentations and source code will be available for customer internal usage.

<https://paceenterprisetraining.com/>

DS09SBL: Dasharo TrustRoot Training

Overview

- Understand and explain the core concepts and functionalities of the Slim Bootloader boot flow and Intel Root of Trust.
- Apply practical skills in setting up, configuring, and troubleshooting Slim Bootloader boot flow and Intel Root of Trust technology.
- Integrate and provision advanced security technologies effectively in real-world scenarios.



Audience

Firmware / BIOS / Bootloader Developers, Platform Security Architects, Hardware and Embedded Engineers, Pen Testers & Security Researchers, open-source Firmware Community Contributors

Duration

4 days

21 hours (7h/day)

30% lectures

70% hands-on workshop

Materials

All training materials presentations and source code will be available for customer internal usage.

<https://paceenterprisetraining.com/>



<https://hardwear.io/netherlands-2025/training/mastering-uefi-secure-boot-and-intel-root-of-trust-technologies.php>

The background features a dark gray field with light gray circuit-like lines. These lines are composed of straight segments and right-angle turns, some ending in small circular nodes. The lines are primarily located along the left and right edges of the frame, with a few extending towards the center.

Dasharo Pro/Enterprise Package



Dasharo (coreboot+UEFI) Pro
Package for Desktop – 1 year

60,00 €
(ex. VAT)

ADD TO CART



Dasharo (coreboot+UEFI) Pro
Package for Network Appliance
– 1 year

46,00 €
(ex. VAT)

ADD TO CART



Dasharo (coreboot+SeaBIOS)
Pro Package for Network
Appliance – 1 year

99,00 €
(ex. VAT)

ADD TO CART

<https://shop.3mdeb.com/product-category/dasharo-pro-package>



Dasharo (Slim Bootloader+UEFI)
Pro Package for Network
Appliance

46,00 €
(ex. VAT)

ADD TO CART



Dasharo (coreboot+UEFI)
transition to (coreboot+Heads)
for Laptops

28,00 €
(ex. VAT)

ADD TO CART



Dasharo (coreboot+UEFI) Pro
Package for Servers

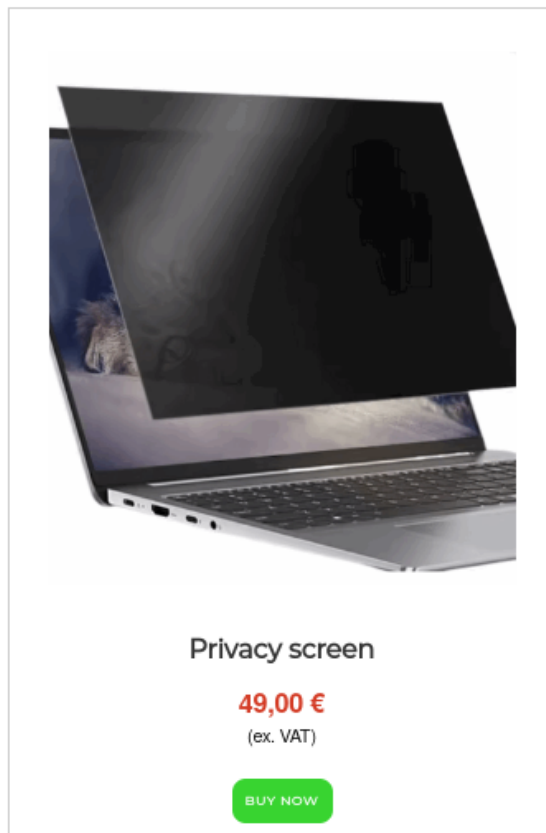
0,00 €
(ex. VAT)

READ MORE

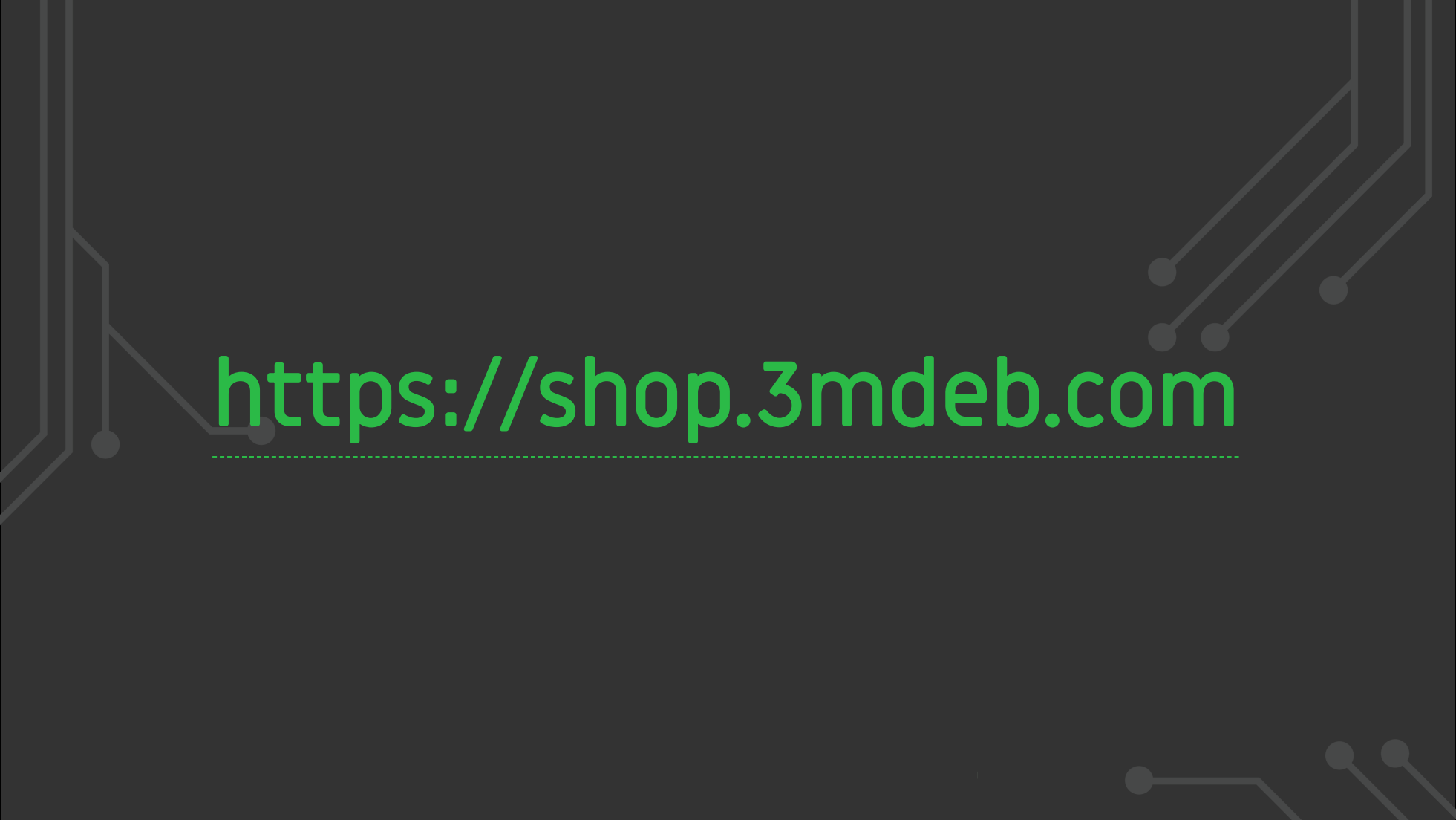
<https://shop.3mdeb.com/product-category/dasharo-pro-package>

The background is a dark gray with decorative circuit-like lines in a lighter gray. These lines are located in the corners: top-left, top-right, and bottom-right. They consist of straight lines of varying lengths and angles, some ending in small circular nodes.

Accessories



<https://shop.3mdeb.com/product-category/accessories/>

The background is a dark gray with faint, light gray circuit-like lines. These lines are composed of straight segments and right-angle turns, with small circles at the junctions, resembling a printed circuit board (PCB) layout. The lines are distributed across the frame, with some entering from the left and others from the top right.

<https://shop.3mdeb.com>

The background is a dark gray with decorative circuit-like lines in the corners. The top-left corner features a vertical line that branches into two horizontal lines, each ending in a small circle. The top-right corner has several parallel diagonal lines, each ending in a small circle. The bottom-right corner shows a few more parallel diagonal lines, also ending in small circles. The word "Backlog" is centered in a bright green, sans-serif font.

Backlog

The image features a dark gray background with decorative circuit-like lines in the corners. These lines are light gray and form various geometric shapes, including rectangles and triangles, with small circles at the ends, resembling electronic components or connectors. The lines are positioned in the top-left, top-right, and bottom-right corners.

Services

Zarhus Services

[01Y] Base OS: Audio support and compatibility tests

Zarhus OS: Base OS – Audio support and compatibility tests

4200,00 €
(ex. VAT)

ADD TO CART

[02] Base OS: Bluetooth support and PTS-related Zarhus OS code changes

Zarhus OS: Base OS – Bluetooth support and PTS-related Zarhus OS code changes

5900,00 €
(ex. VAT)

ADD TO CART

Base OS: Buttons interface support (keyboard standard input)

Zarhus OS: Base OS – Buttons interface support (keyboard standard input)

2450,00 €
(ex. VAT)

ADD TO CART

S: Device controller server application for display management

Zarhus OS: Base OS – Device controller server application for display management (HTTP)

6300,00 €
(ex. VAT)

ADD TO CART

[032-OLED] Base OS: Display support

Zarhus OS: Base OS – Display support (3x OLED mono/color)

2450,00 €
(ex. VAT)

ADD TO CART

<https://shop.3mdeb.com/shop/zarhus-services/>