# CUC8 Firmware Security

The unlock key to Device as a Service

# Real security. Real tough.

CUCO ANTI-THEFT REMOTE LOCK

## Self-compliance check, rules based

- Device protection
- Theft deterrence
- Non-destructive pre-boot lock
- Preventing operating system from booting
- Customizable interface
- Unlock recovery via web portal or phone

## Device lock down survives

- Operating system reinstallation
- Hard disk replacement
- ROM vulnerability attacks
- BIOS re-flash

**CUCo** is activated through subscriptions from licensed service providers and partners on pre-provisioned x86 compatible hardware (1). CUCo ready devices are fully tested and debugged by an engineering team before market introduction. Service providers can deliver the service through cloud based secure web access or by installing the authorization servers on the client's premises (usually government or telecom operators).

## Features check list

- Firmware UEFI based
- Trusted UEFI security model
- Full UEFI firmware run, software independent
- Software agnostic, compatible with Windows, Linux, Android, Chrome, etc
- Self-compliance UEFI firmware checks, operating systems independent
- Rules based on remote lock, independent of connectivity status
- Nondestructive pre-boot lock
- Protection against rogue CUCo BIOS re-flash when CUCo in active status
- Prevents operating system from booting when in lock status
- Unlock recovery via web portal, phone or remote API call
- Firmware detects software agent failures (self-healing) and notifies the user
- Resilient assurance. Compatible with TPM and optionally uses TPM key generation for server communication

## Cloud control platform (backoffice)

- Computing technology management
- Lock and unlock commands
- Device localization check (optional)
- Statistics

## Integration

- Server cloud based and optionally compatible with Microsoft Azure
- Open API to integrate with third party device management platforms
- Microsoft Intune MDM integration (2)
- Open-source MDM integration (2)
- Compatible and certified with most computer brands (3)

(1) Some restrictions apply. AMI and Intel BIOS are compatible. Phoenix, Award, Insyde and Byosoft BIOS under development.
(2) Under development
(3) Check online list

# CUCo – Central Unit Control

CUCo Firmware Security is a unique security technology for computers, tablets and smartphones (1), leveraging hardware, UEFI firmware and software agents to enable a device to self-compliance check, automatic or manual remote lock, remote unlock and locate, even before the operating system is running.

## Hardware protection

CUCo Firmware Security enables an intelligent protection of lost and stolen devices, intended to prevent unauthorized use of a computer, running on all modern x86 devices (1), from the lowest end tablet to the highest speck laptop, workstation or server. CUCo does not require traditional proprietary CPU or chipset security features, leveraging the UEFI firmware security model and is software agnostic.

## Contract compliance

CUCo Firmware Security dramatically improves the odds of hardware recovery and contract compliance, allowing inclusive and non-discriminatory projects that would otherwise face economically insurmountable obstacles. It's a truly unlock key to Device as a Service (DaaS) projects, as it solves the main obstacle of DaaS: the device control by the project owner while under a service contract. Telecom operator x86 device handout when subscribing an Internet service, can finally happen at the same time of the traditional smartphone handout on service subscription. Leasing companies can finally tap the vast SMB, SoHo and consumer market strongly limiting the default risk associated to the installment payments.

## Child protection

CUCo Firmware Security is a theft deterrement software because it nullifies the economic value of a locked device, making it uninteresting to transact on the black market.

## Theft deterrement

Now, large projects on education, where inclusivity and non-discrimination are paramount priorities, are finally possible. Students are protected from abuses when carrying a device with a security lock that fully prevents any thief or fencer from profiting from a stolen device that is blocked and unusable.

## Vulnerability attack proof

This unique security technology has been verified and guaranteed against vulnerability attacks. Through the implementation of dozens of projects in more than 1.2 million devices.

Device autonomous rules enforcement CUCo's internal rules engine has thresholds timer intervals and actions to take, independently of device network connectivity status. CUCo Firmware Security provides local, tamper-resistant, policy-based protection that works even if the operating system is reimaged or a new hard drive is installed.

Developed and patented (2) by Softi9 within an European consortium including research engineers specialized in security. Latest version is optimized for CometLake, AlderLake, GeminiLake and JasperLake Intel families and leverages the UEFI standard security model for future development.

Most major computer manufacturers have been already licensed and validated compatible devices with CUCo (3). CUCo is available for licensing by ODMs, MNCs, hardware SIs, IDHs under CUCo brand or white label scenarios and can be activated in many scenarios by governments, schools, universities, telecom operators, leasing companies and any DaaS project owners. The server component to control the device, can be cloud shared or on-premises installed by the DaaS project owner, depending on the size of the project. Server side can be deployed in Microsoft Azure and optionally hooks into Microsoft Intune MDM functions (4).

CUCo Firmware Security also provides secure low level hardware information for MDM functions that is critical for managing large networks of heterogenous devices and will also be the basis for CUCo Firmware MDM(5).

(1) Currently developed for x86, Intel architecture. ARM under development
(2) Patent pending
(3) Check online list
(4) Under development
(5) Details available under NDA

# Comparative analysis of CUCo against the 3 main competitors

| | CUCo | Competitor 01 | Competitor 02 | Competitor 03 |
|---|---|---|---|---|
| Open platform, UEFI standards based, copatible with multiple brands of end point devices (open license to ODM's) | ✓ | | ✗ | ✗ |
| Single purpose firmware level remote-lock, device auto-control, pre O.S. boot lock | ✓ | ✗ | ✓ | |
| No access to user data on device by platform manager (RGPD compliant) | ✓ | ✗ | ✓ | |
| Remotely reactivate device after locking event (non-dependency on software, but solely hardware/firmware lock) | ✓ | | ✗ | ✓ |
| Self-protection against hacking attempts to desactivate security on device | ✓ | ✓ | ✗ | |
| Low bandwidth and no-connectivity regular functioning for defined period | ✓ | ✗ | ✗ | |
| Multiple O.S. support, including Windows, Linux, Android, Chrome. Lock by firmware | ✓ | ✗ | ✗ | ✗ |
| Focus on "hardware only" security. Data and contente agnostic | ✓ | ✗ | ✓ | ✗ |
| Remote permanent "freedom" status to permanently deactivate security mechanism | ✓ | ✓ | ✗ | |
| Persistence across changes of O.S. | ✓ | ✗ | ✗ | ✗ |

# Usage benefits

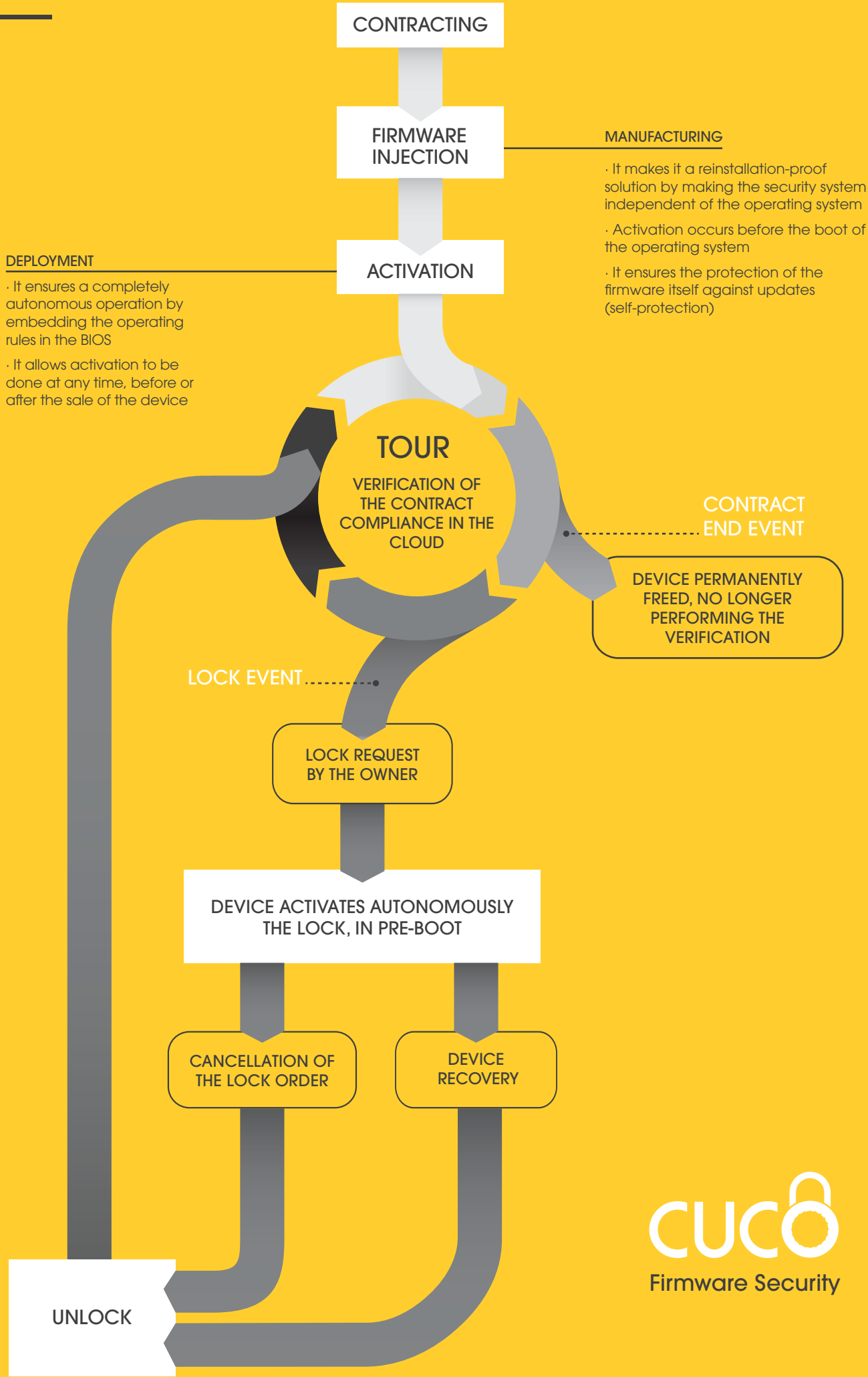
## Protecting users

- The theft deterrence nature of CUCo technology is the most effective protection against user´s abuse
- Devices with CUCo, being remotely locked, are not a target to be stolen, wrongly reported missing or traded in black markets and this creates a safer usage environment for the end user of the device

## Protection of property

- Device owner is fully protected since any event of lost, stolen or contract abuse (e.g.: device not returned at contractual date) allow the device owner to remotely lock and recover these devices
- Device owner can have multiple brands and diverse operating systems on its network, all protected with same security system
- In Device as a Service scenarios, the device owner can assure the return and recovery of the device in the event of any contractual breach and easily enforce the missing recurrent payments of the contract
- Theft deterrence is as black-market value nullity

# workflow




cuco
Firmware Security

# Case Study

## Education pilot

In the aftermath of E-escola project in Portugal, it was launched a pilot project to test CUCo validity as a contract enforcement and theft deterrement system.

Several thousand units of laptops worth 500€ each were made available to low-income students at 149€ each and a service contract of 14.9€ per month for 2 years' time. No credit check was required, just signing up for the contract and paying the initial amount through a debit in the bank account stated in the contract.

Statistical data showed, after running the program for more than 2 years, that 27.9% of users stopped paying the monthly installments at some point. CUCo Firmware Security on the laptops detected the noncompliance and automatically locked the device. Following the customized "lost-and-found/locked" message, 98.6% of users contacted the call-center, payed the overdue installments and got a one-time code to unlock the device and reactivate it. CUCo provided a massive reduction of default payments by locking uncompliant units.

It was also confirmed that 3% of the units have been offline for more than 2 months, and CUCo´s internal rules locked them even without network connectivity. During the period, 2% of the units have been reported by users as stolen or lost, but given their "digital footprint" when contacting the CUCo server, most were recovered and handed back to the user or reported to the authorities. At the end of the contract period all compliant units were freed from the CUCo control.

In this scenario, the majority of the installments in default would have been lost or the cost of recovering them through the traditional recovery agents or legal system would be too high and thus CUCo Firmware Security proved to save more than 20% of the sales price per unit. If not for the CUCo solution, large deployment projects based on future financial streams would not be viable. CUCo is a truly enabler for DaaS model in Education.

cuco
www.cuco-firmware.com
sales@cuco-firmware.com

Developed by:
softi9

Cofinanced by:
CENTRO 2020
PORTUGAL 2020
UNIÃO EUROPEIA
Fundo Europeu de Desenvolvimento Regional

201EN01C001