CONFIDENTIAL COMPUTING SUMMIT 2023

Writing Digital Exams Secured by Remote Attestation and Cloud Computing

Thore Sommer

University of Applied Sciences and Arts Northwestern Switzerland (FHNW)

About Us


Niklaus Lang
(project manager)


Simon Kaspar
(CAMPLA developer)


Merima Hotic
(examinations)


Thore Sommer
(security, Lernstick)


Ronny Standtke
(Lernstick, BFH)


Martin Gwerder
(security expert)

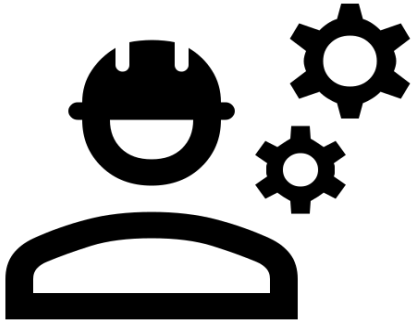

Norbert Hofmann
(staff, lecturer)


Marcel Steiner
(staff, lecturer)


Cinzia Garcia
(vice chair university development)

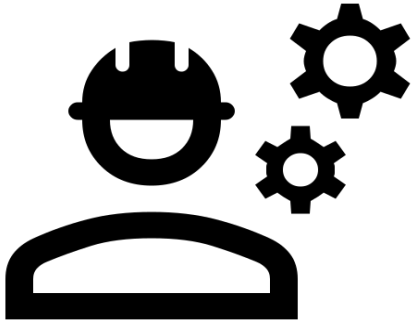

Stefan Walter
(vice chair university development)

Goals



competency-based
digital exams

Goals



competency-based
digital exams

School of Life Sciences
analysis of microscope images using Matlab

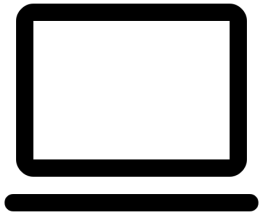
School of Education
reading and language comprehension
using recordings

Goals

fair

secure

robust and easy to use



bring your own device (BYOD)

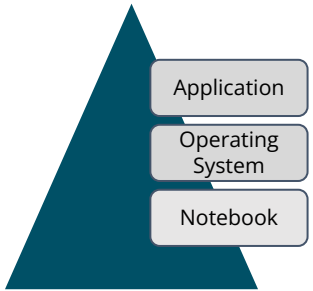
How?

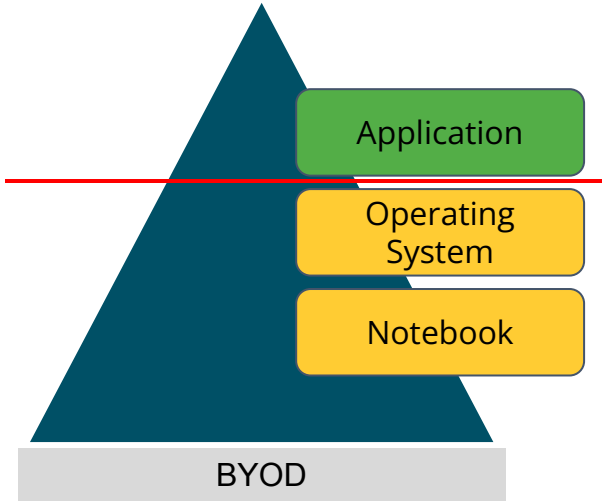
device lockdown and interface to exam environment

securing Lernstick using remote attestation

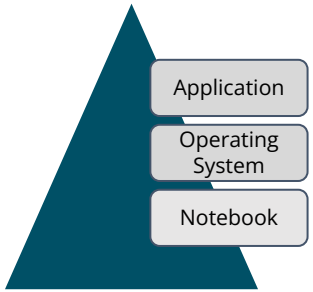
provisions and manages the exam environment

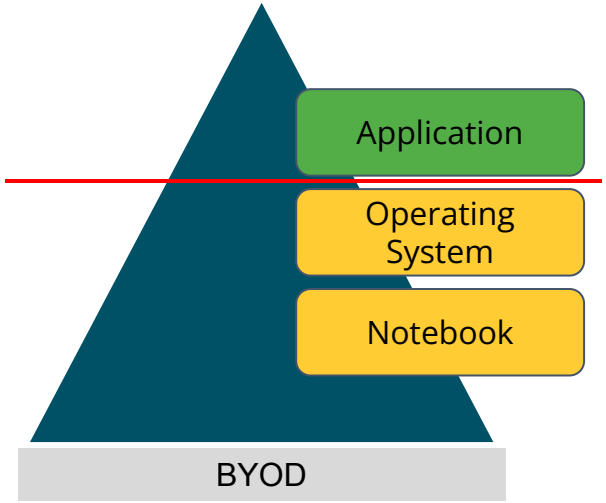
Bring Your Own Hardware (BYOH)

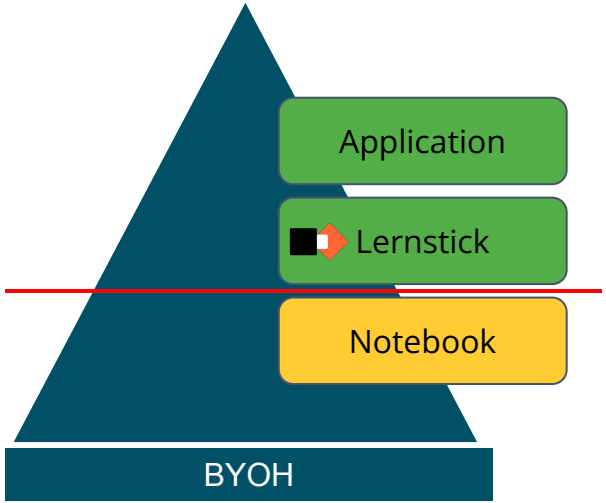




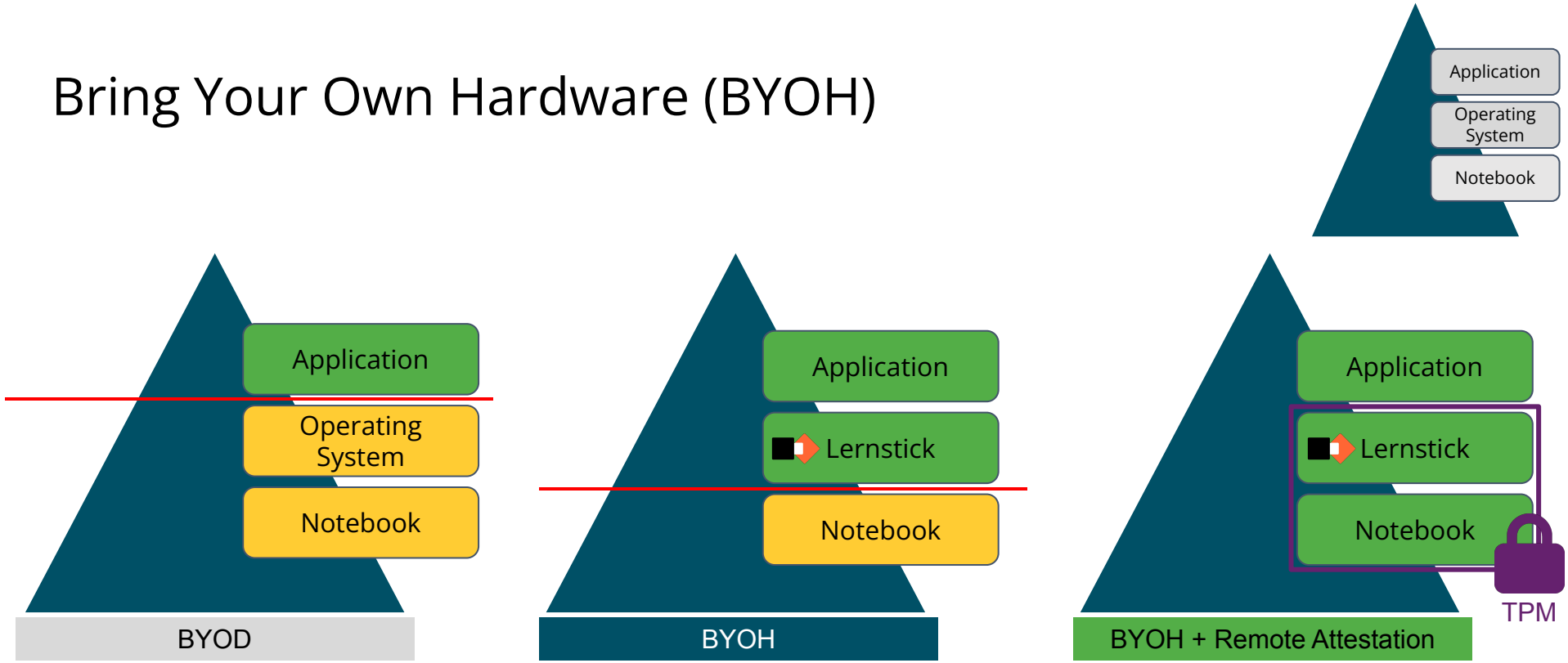
Bring Your Own Hardware (BYOH)



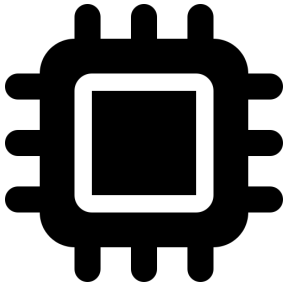




Bring Your Own Hardware (BYOH)



Trusted Platform Module (TPM)

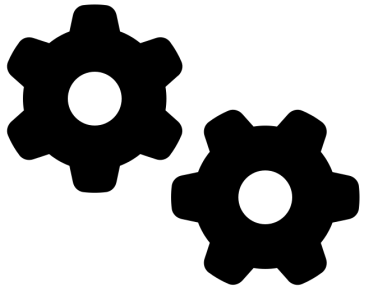


- root of trust
- cryptographic functions
- key generation and storage
- Platform Configuration Registers (PCRs)

- endorsement key and certificate
- device identity
- PCRs used for measured boot and runtime attestation

Cloud Assessment Management Platform (CAMPLA)

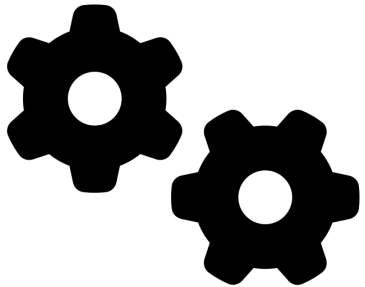
Backend



- provision VMs in cloud
- set security policies
- provide exam templates
- user management
- data integrity

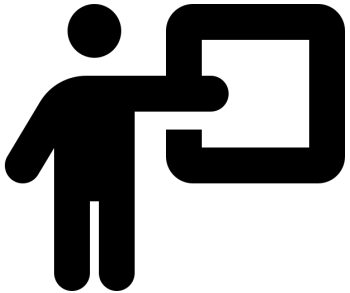
Cloud Assessment Management Platform (CAMPLA)

Backend



- provision VMs in cloud
- set security policies
- provide exam templates
- user management
- data integrity

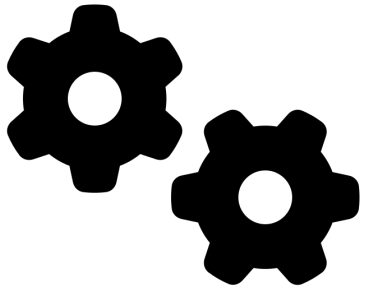
Lecturer



- create new exams
- upload materials
- start, examine and stop
- download written exams

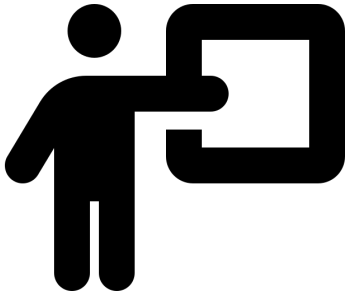
Cloud Assessment Management Platform (CAMPLA)

Backend



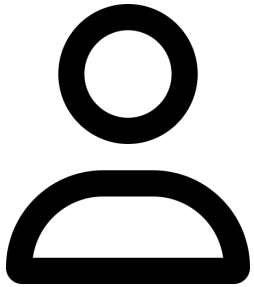
- provision VMs in cloud
- set security policies
- provide exam templates
- user management
- data integrity

Lecturer



- create new exams
- upload materials
- start, examine and stop
- download written exams

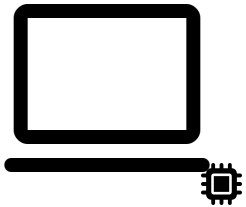
Student



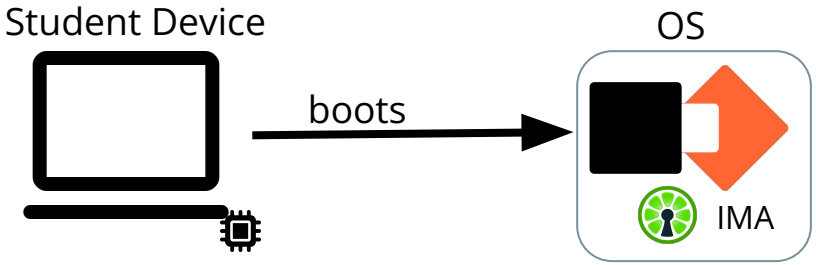
- upload materials (open book)
- log in to exam
- hand in written exam

CAMPLA – Examination

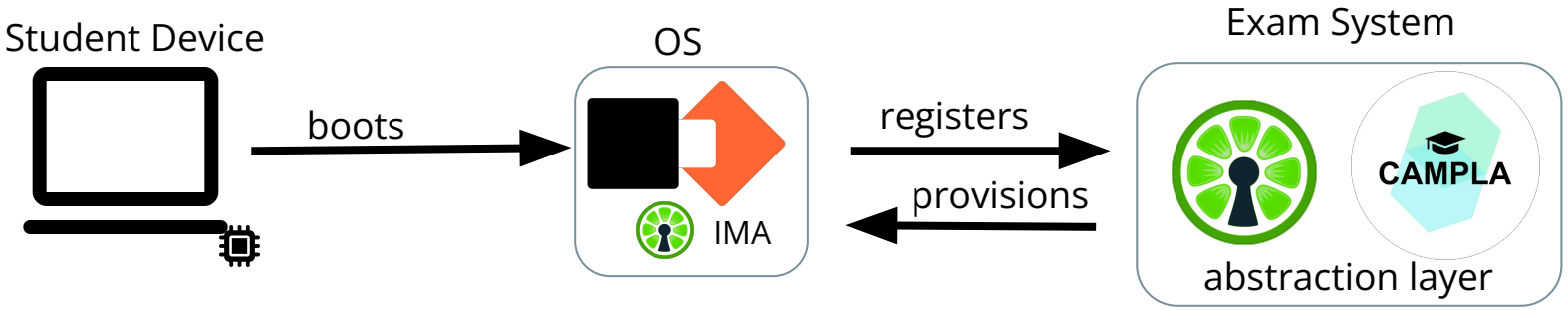
Student Device



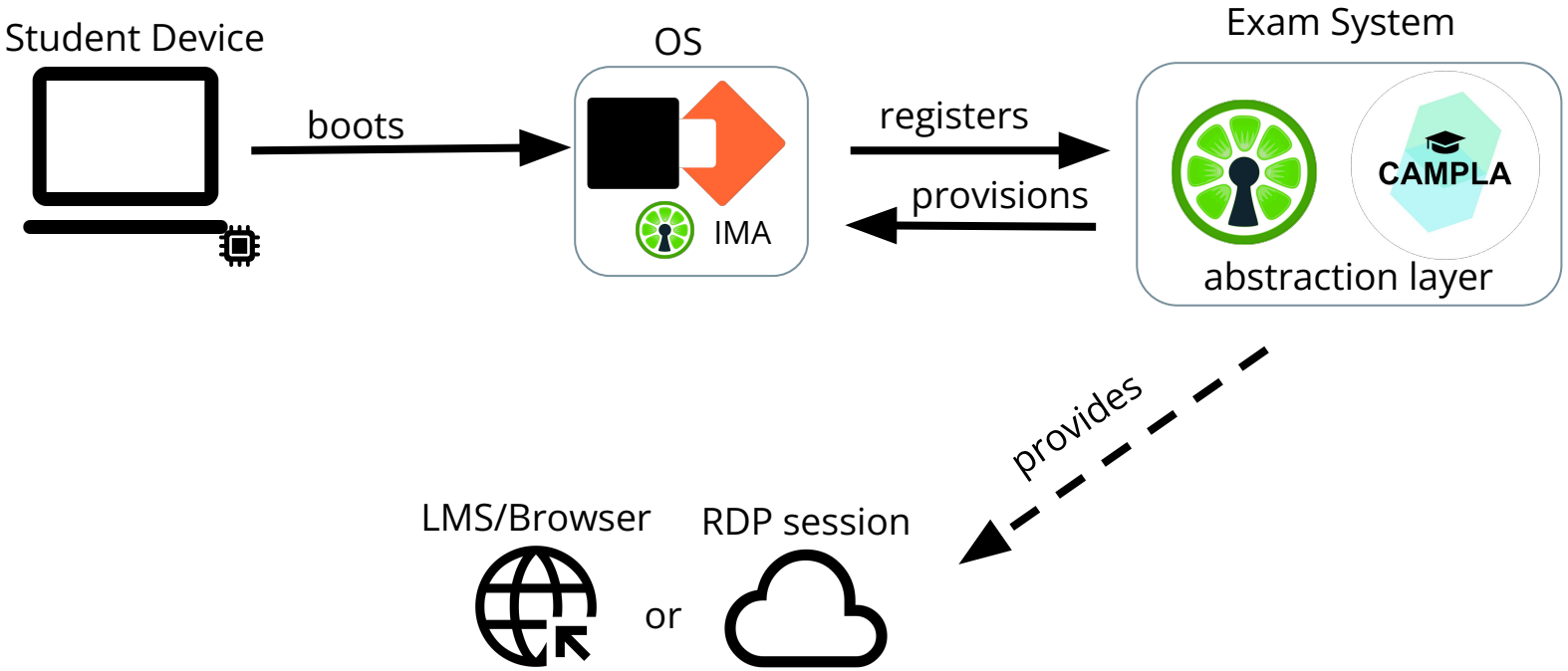
CAMPLA – Examination



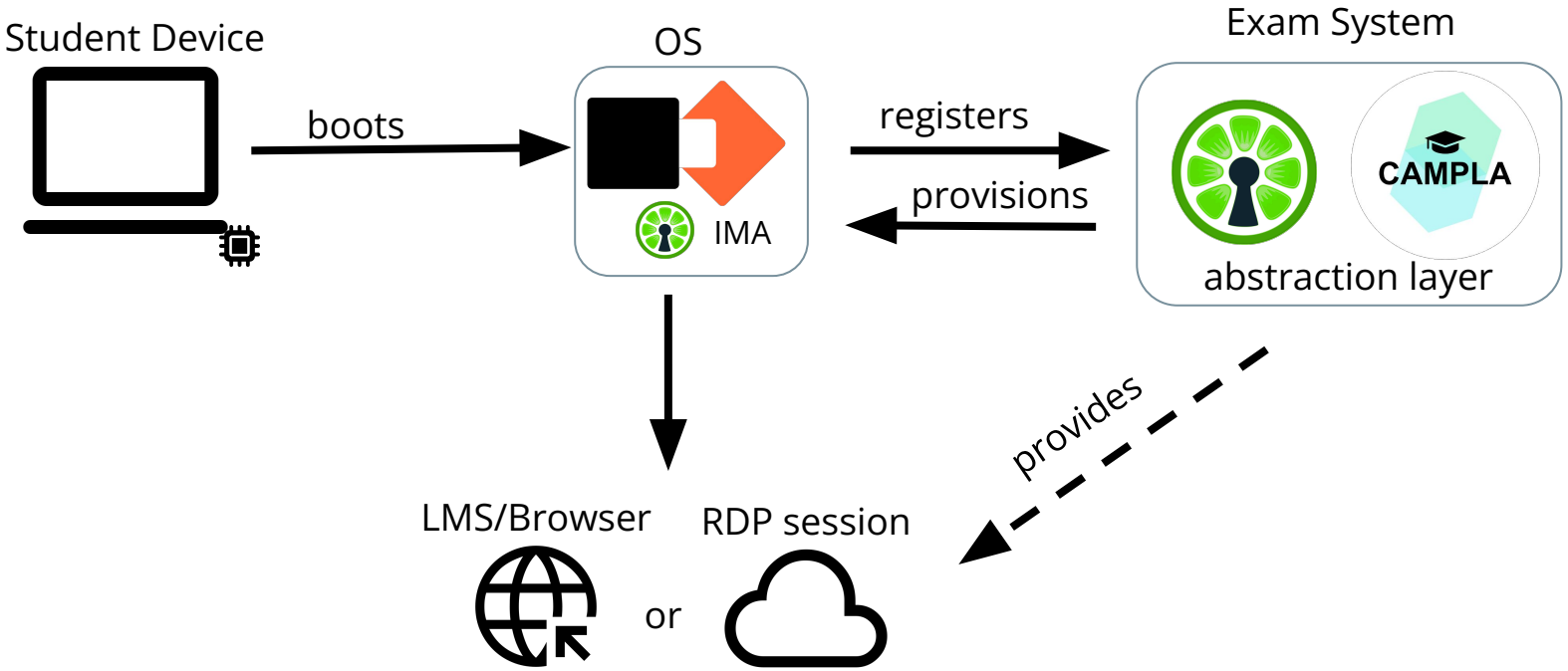
CAMPLA – Examination



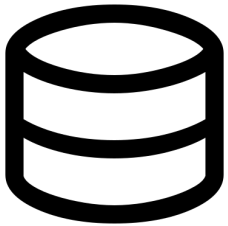
CAMPLA – Examination



CAMPLA – Examination

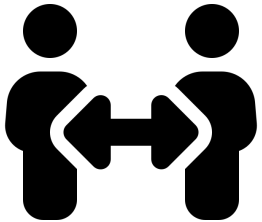


Challenges

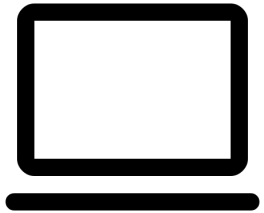


data required for remote attestation

threat model



abstraction and separation



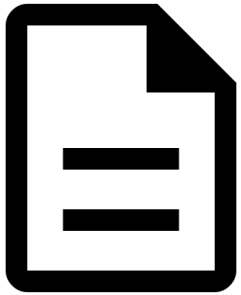
consumer hardware

Conclusion

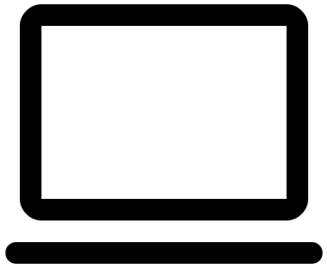
It works!

Conclusion

It works!



100+
exams

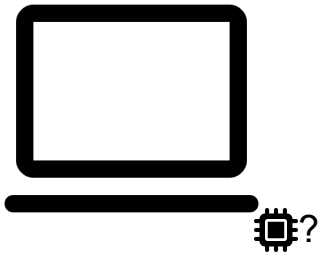


340+
different devices

high acceptance

Next Steps

- MAC (AppArmor)
- integrity enforcement
- confidential VMs



non-TPM devices

- more universities
- SaaS offering

More information at campla.github.io

More information at campla.github.io

Contact
thore.sommer@fhnw.ch
campla.services@fhnw.ch