CONFIDENTIAL
REMOTE
COMPUTING

AN EDUCATION IN IMPERFECTION

TRAINING & CERTIFICATION

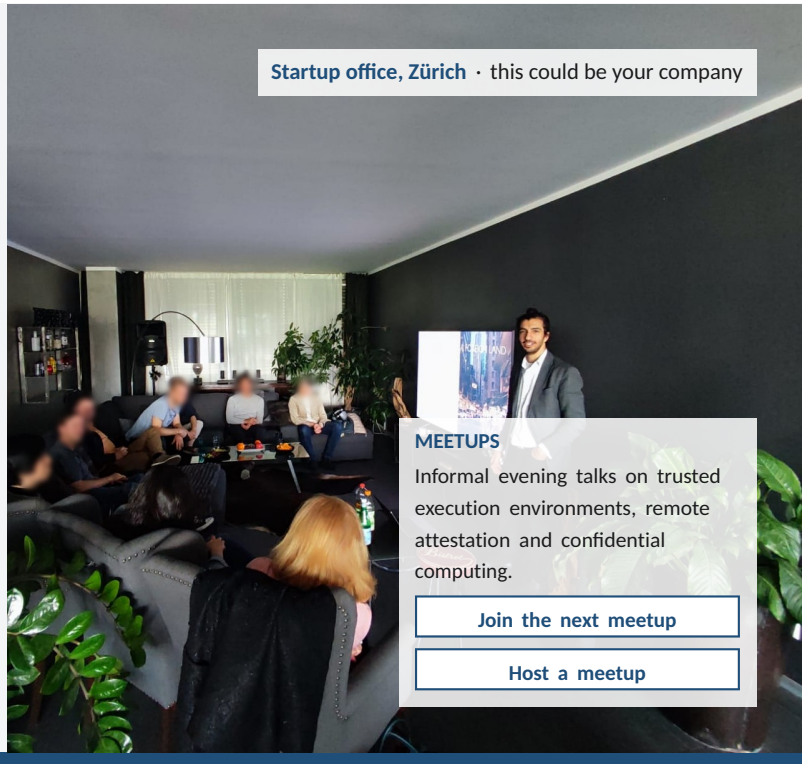
Hardware Roots of Trust, Remote Attestation and Trusted Execution

Two intensive days, 16 hours,
aligned with the Oxford course

Book a 30-minute call

or email hello@kuc.uk · https://trust.kuc.uk/

TPM 2.0 · SRTM/DRTM · MEASURED BOOT
REMOTE ATTESTATION · SEALING · TEE
SGX/TDX · TRUSTZONE · CONFIDENTIAL VMs
TCB MINIMISATION · SECURITY BY DESIGN



Build the skills to design, evaluate and ship systems that run on trusted hardware

Why this training?

Every modern platform ships a root of trust: a TPM, a CPU enclave, a secure monitor, a confidential virtual machine. Few engineers can say what those components actually guarantee, how to prove a remote machine is in a known state, and where the trust chain breaks. This course closes that gap. It is aligned with the Trusted Computing Infrastructures curriculum taught at the University of Oxford, condensed into two intensive days for practitioners, with worked examples from real platforms instead of vendor marketing:

- ✔ **Taught by the author of the paradigm:** Dr Küçük defined Confidential Remote Computing in his Oxford doctoral research, funded by Intel Corporation, and has taught trusted computing at Oxford.
- ✔ **Platform-level depth:** what the hardware does, instruction by instruction, from the first fetch after reset to a verified remote attestation. No slideware abstractions.
- ✔ **Immediately applicable:** security by design in practice: threat models, trust-chain diagrams, TCB minimisation and a practical guide to zero trust, for your next architecture review, product requirement or audit.
- ✔ **Interactive and certified:** worked examples and open discussion in a group of at most six, with a Certificate of Completion for every participant.

2 intensive days	Max. 6	In person	Certificate
09:00–17:00 16 hours	participants per course	in Zürich or at your premises	with individual credential ID

Course programme

One course, two full days (09:00–17:00, 16 hours), aligned with the thirteen lectures of the Oxford course:

- **Day 1, Foundations of Trusted Computing:** trust basics and definitions, chains and roots of trust, the trusted platform (elements, threats, use cases), TPM 2.0 (keys, seeds, sealing, binding, authorisation policies), static and dynamic roots of trust for measurement (SRTM, DRTM, Intel TXT), trusted, measured and verified boot, measurement logs and PCRs, local and remote attestation, attestation identity keys and privacy, provisioning.
- **Day 2, Trusted Execution and Confidential Computing:** trusted execution environments as reference monitors and TCB minimisation, hardware isolation and rings, malware and rootkit resistance, Intel SGX enclaves (memory protection, keys, attestation, TCB recovery, Boot Guard), Arm TrustZone, virtualisation and guest attestation, a brief look at confidential virtual machines (Intel TDX, AMD SEV-SNP, Arm CCA), device ownership, integrity measurement, applications (disk encryption), and the language of trust: what an attestation can and cannot tell you.

Content focus

As printed on the certificate, the course covers:

- Trust basics, chain of trust, roots of trust
- Trusted platform and trustworthy computing
- SRTM, DRTM, Intel TXT
- TPM 2.0: measuring, reporting, quoting
- Sealing, binding, sealed storage
- Trusted, measured and verified boot
- Local and remote attestation
- Provisioning and device identity
- TEE, SGX enclaves, Arm TrustZone
- Confidential VMs: TDX, SEV-SNP, CCA

Who is this training for?

Engineers and decision-makers who build on, buy or audit trusted hardware:

- Security and platform architects
- Firmware and embedded engineers
- Cloud, virtualisation and kernel engineers
- Product security and PSIRT teams
- Confidential AI and data-platform teams
- Security consultants and auditors
- CISOs, CTOs and technical product owners

Prerequisites: working knowledge of operating systems and computer architecture. No prior trusted-computing experience required.

Your instructor

Dr Küçük holds a DPhil in Computer Science from the University of Oxford, where he defined the Confidential Remote Computing paradigm (doi:10.5287/ora-2rovaxbjd) with PhD funding from Intel Corporation for SGX/TEE research, and has taught Trusted Computing Infrastructures. Software engineer and security architect; two Innosuisse projects at ETH Zürich (ETH D-INFK, ETH D-MAVT); published researcher, speaker at Black Hat Europe and DEF CON.

Course details

Participants	Max. 6 per course
Duration	2 intensive days, 09:00–17:00
Language	English
Level	Advanced
Location	In person, in Zürich or at your premises
Certificate	Certificate of Completion with an individual credential ID, per participant
Consulting	For certified participants: commercial products, architecture, and formal verification of products and protocols

Contact

Bring trusted computing and confidential computing into your team now and apply it in your next product.

Book a 30-minute call

Email hello@kuc.uk

Scan to visit
https://trust.kuc.uk/

Dr Küçük, Switzerland
hello@kuc.uk
cal.com/confidentialcomputing/30min
https://trust.kuc.uk/