Welcome to the Attestation Devroom!

Muhammad Usama Sardar[1] and Thomas Fossati[2]

[1]TU Dresden, Germany

[2]Linaro, Lausanne, Switzerland

February 2, 2025

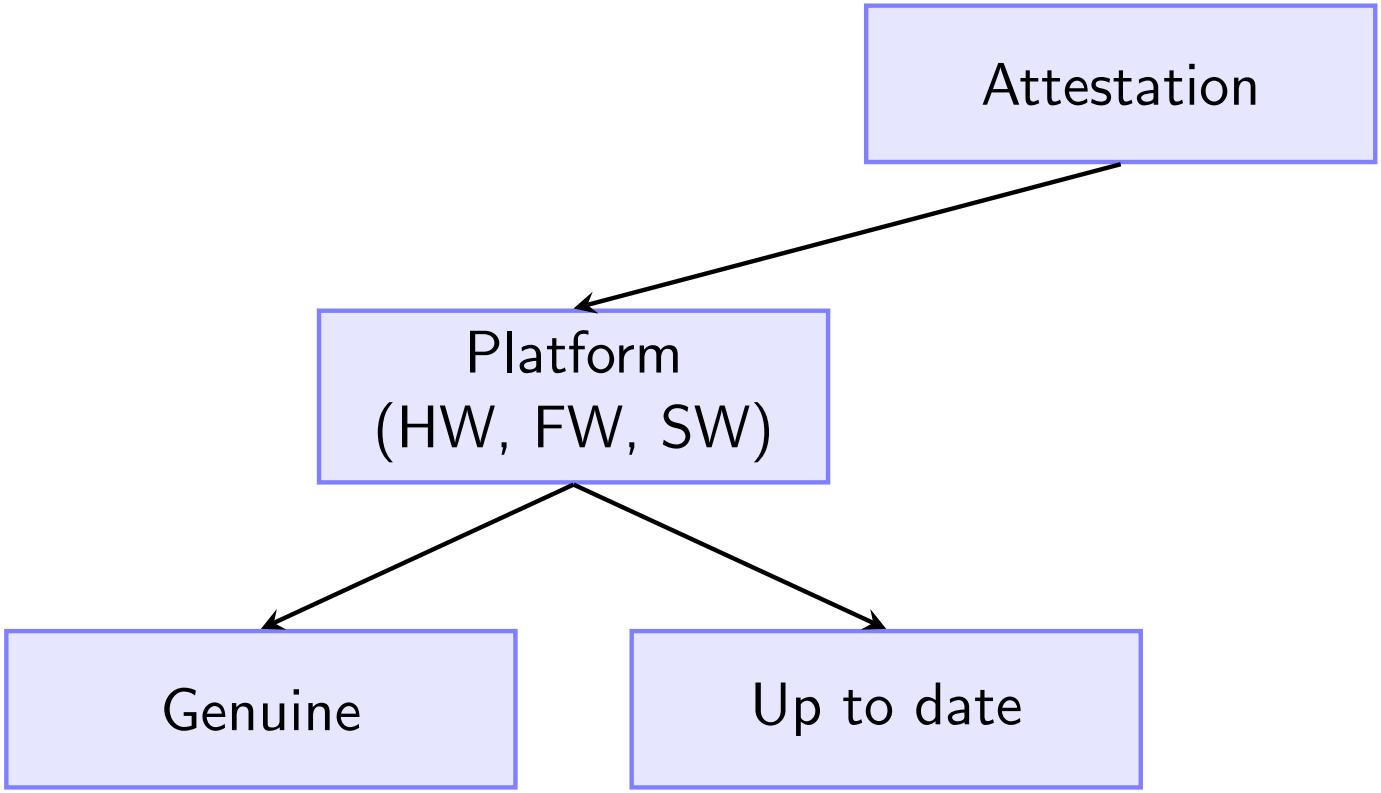
Usama would like to thank his sponsor!

Outline

Disclaimer

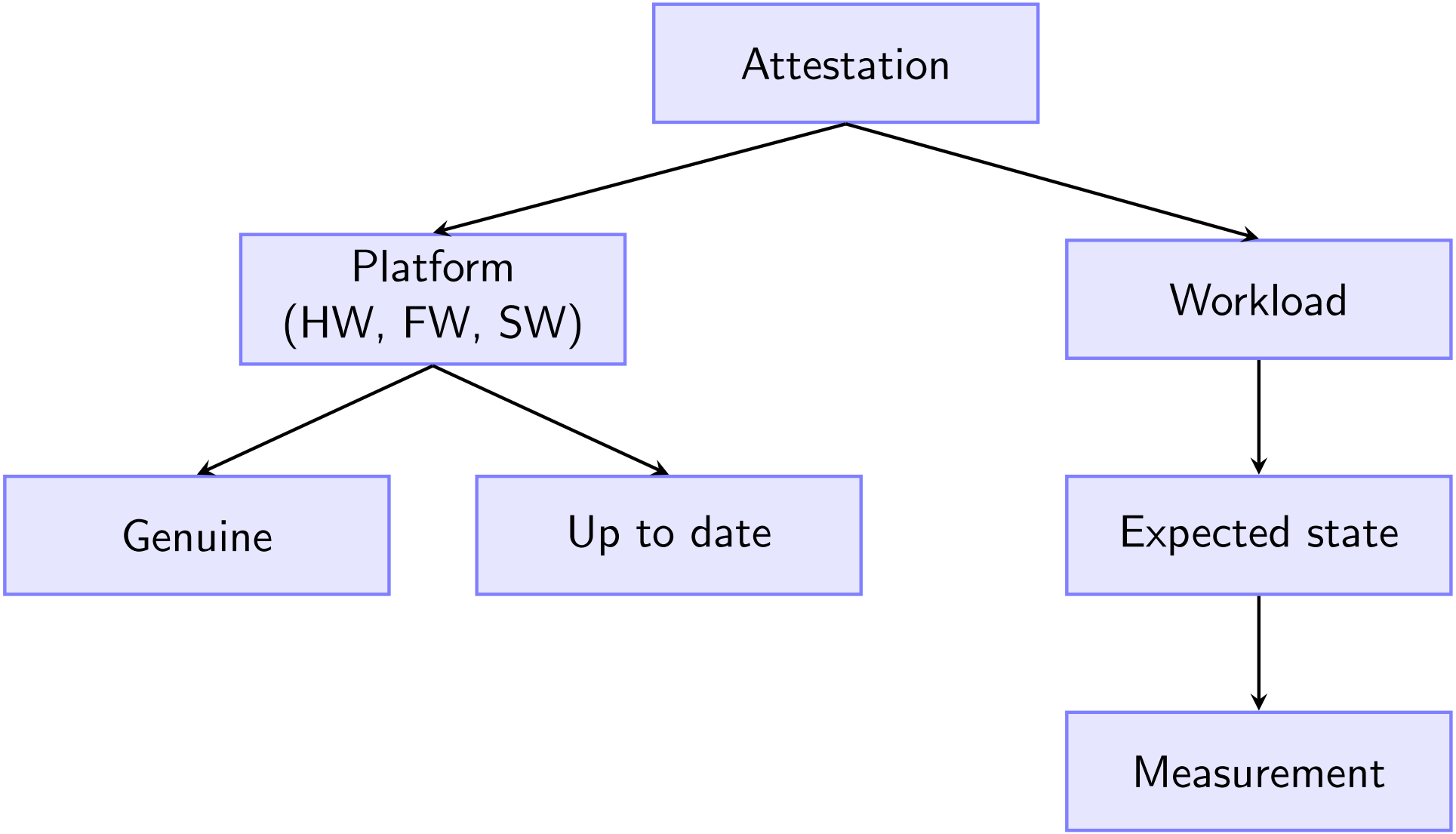
Many ambiguous and even contradicting definitions exist!

(Architecturally-defined) Attestation[1]



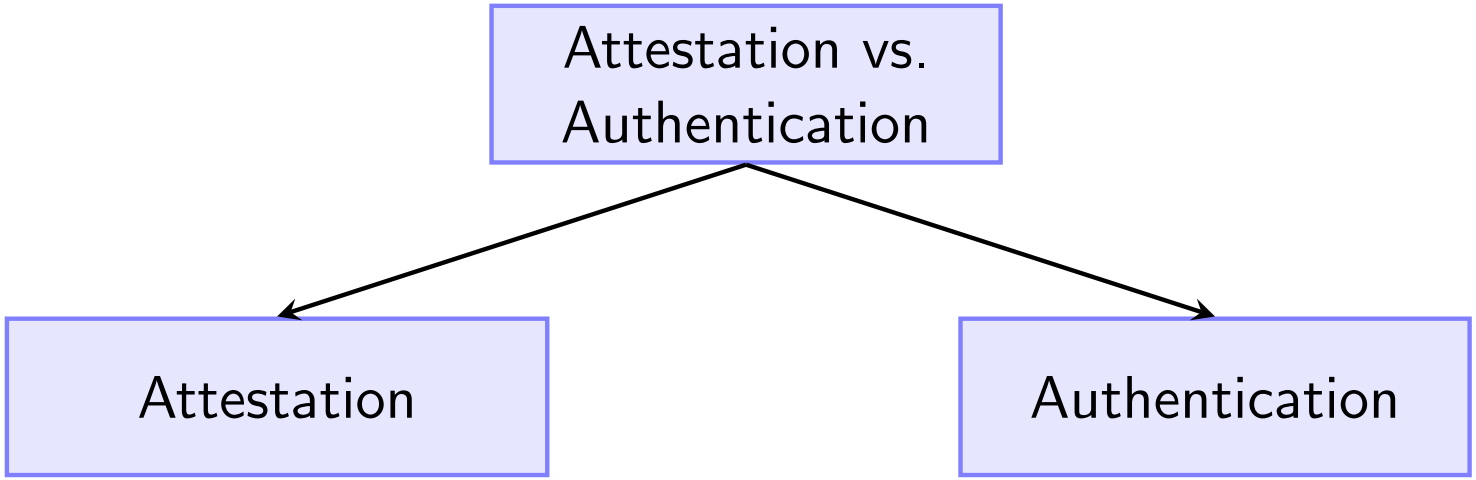
[1] Sardar, Fossati, Frost, and Xiong, "Formal Specification and Verification of Architecturally-defined Attestation Mechanisms in Arm CCA and Intel TDX", 2024.

(Architecturally-defined) Attestation[1]

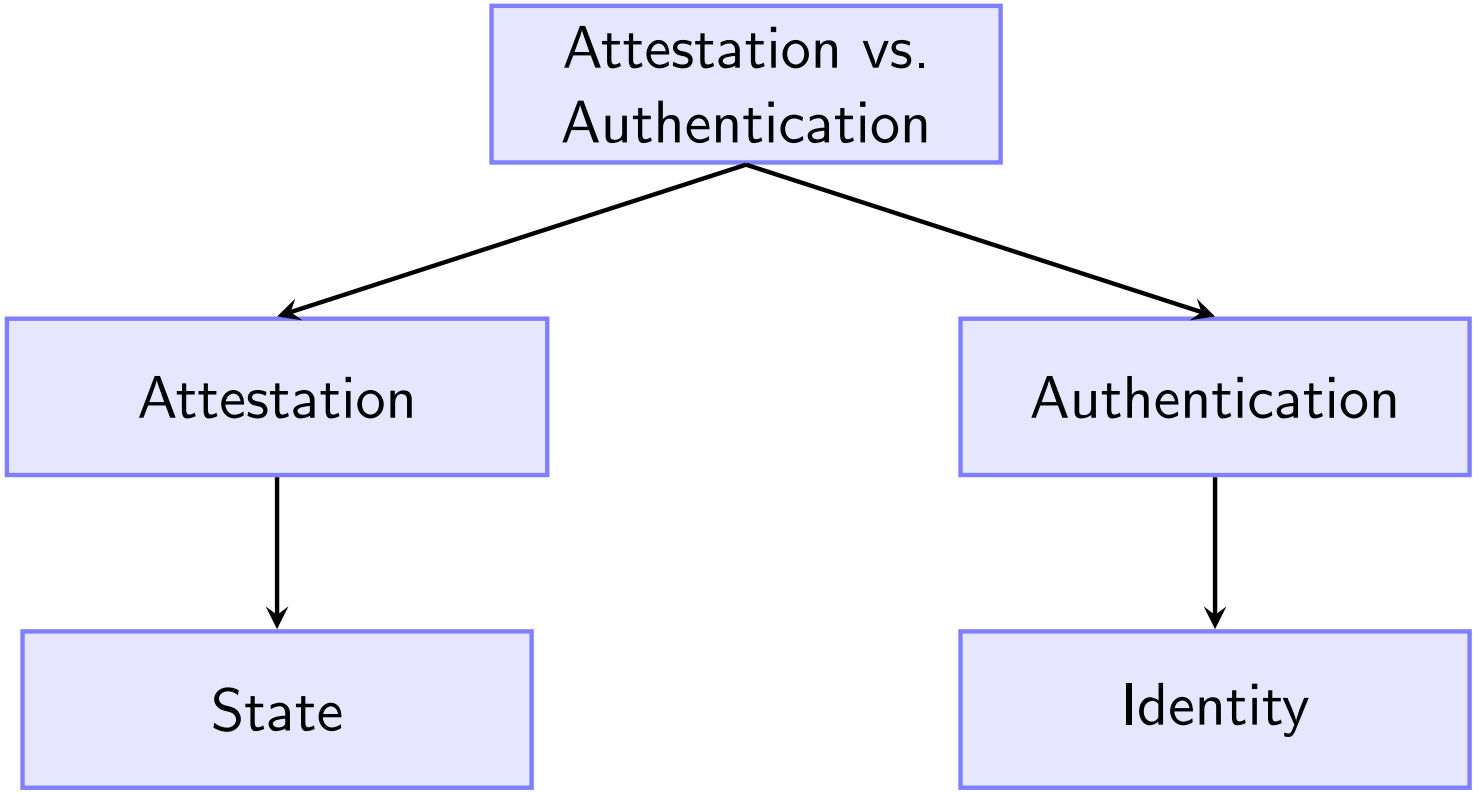


[1] Sardar, Fossati, Frost, and Xiong, "Formal Specification and Verification of Architecturally-defined Attestation Mechanisms in Arm CCA and Intel TDX", 2024.

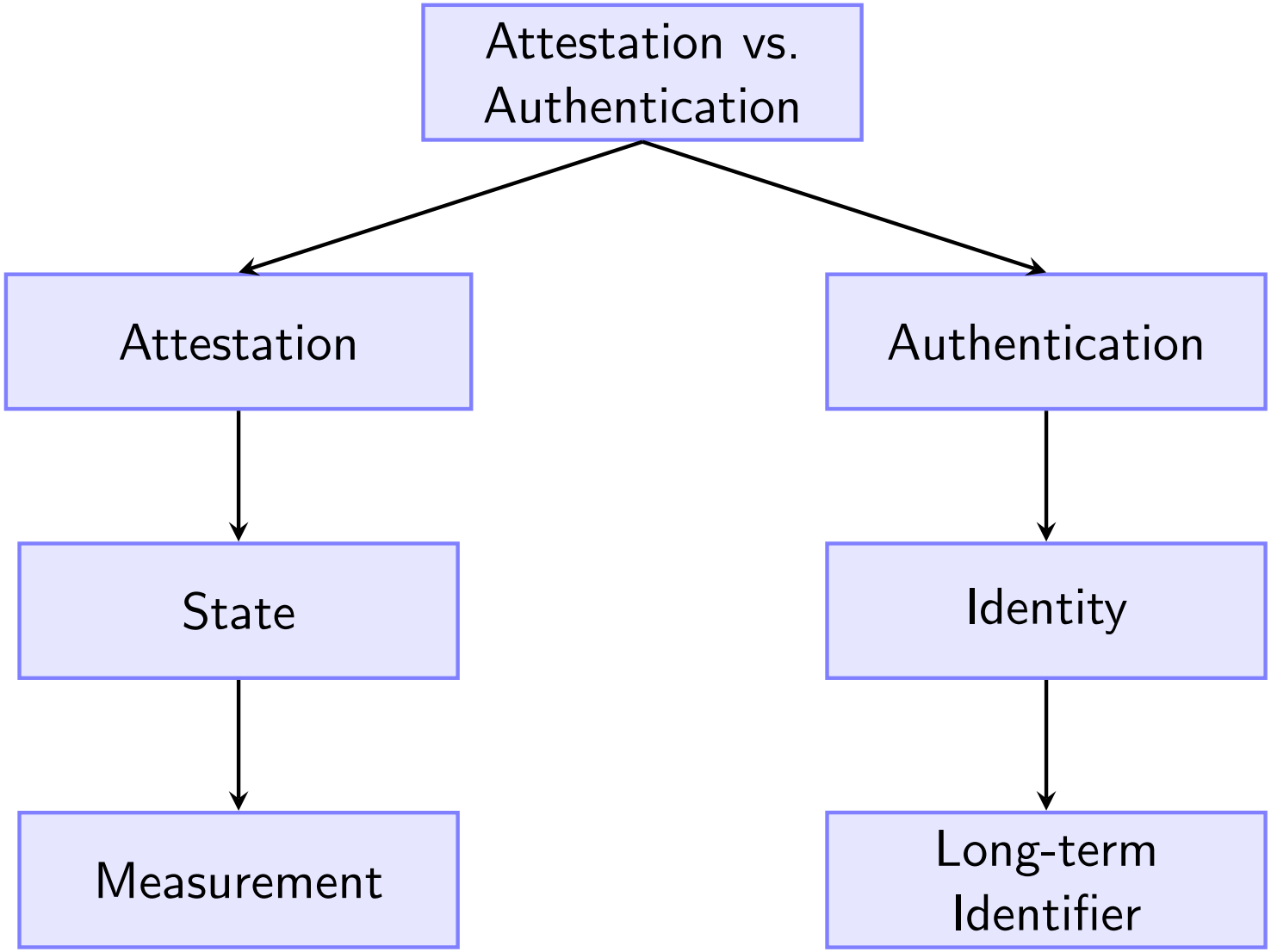
Attestation vs. Authentication



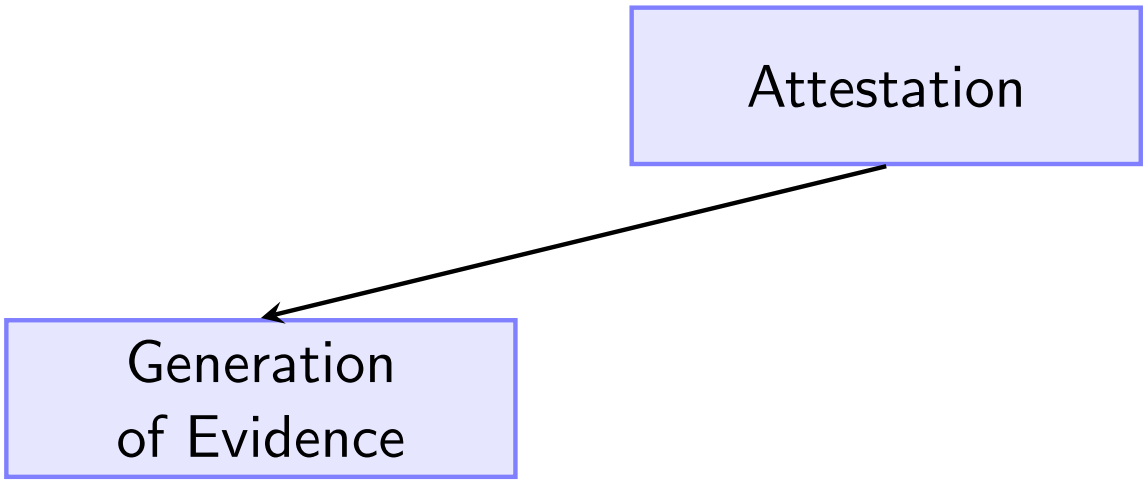
Attestation vs. Authentication

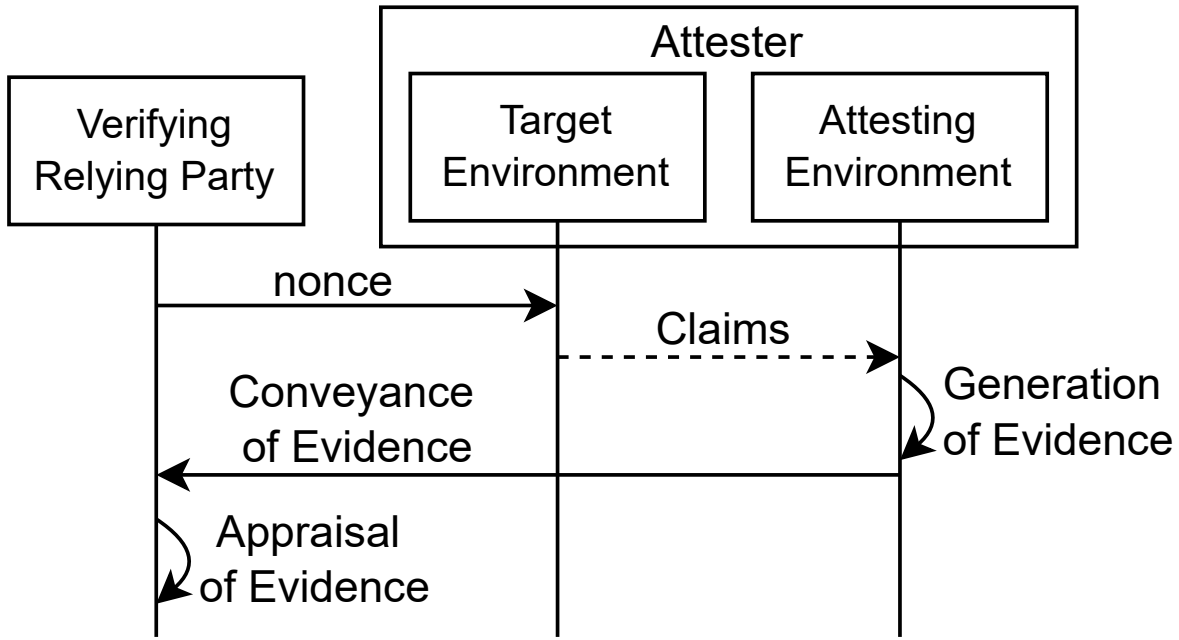


Attestation vs. Authentication

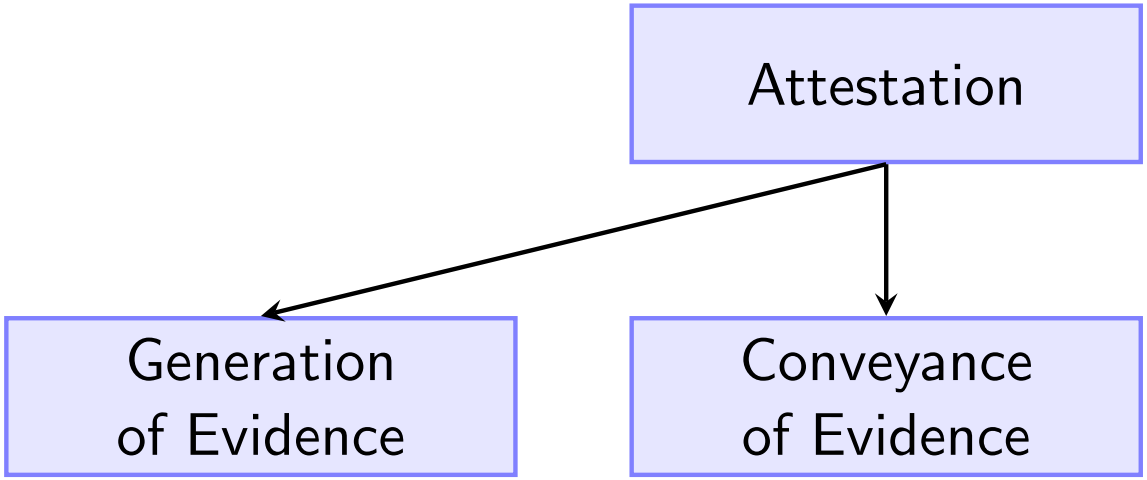


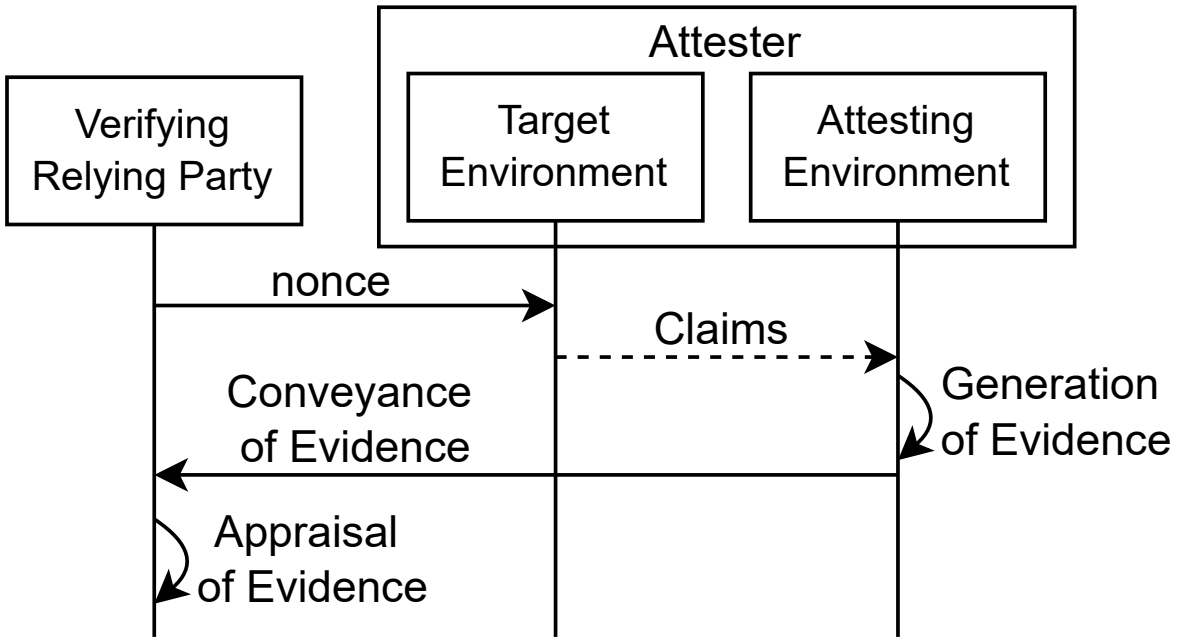
Protocol Perspective (Simplified)



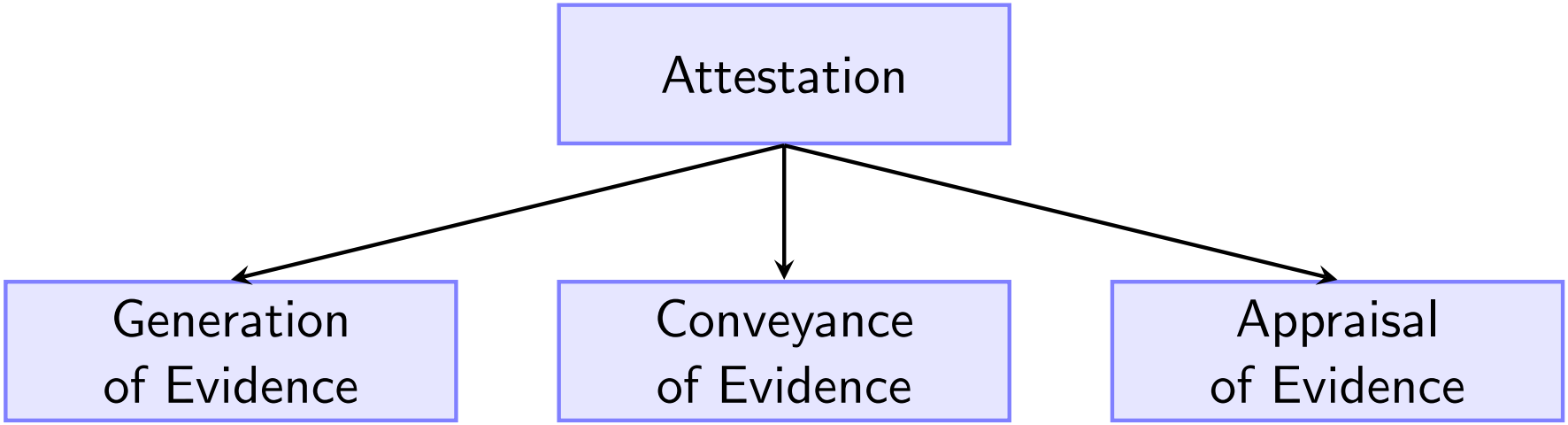


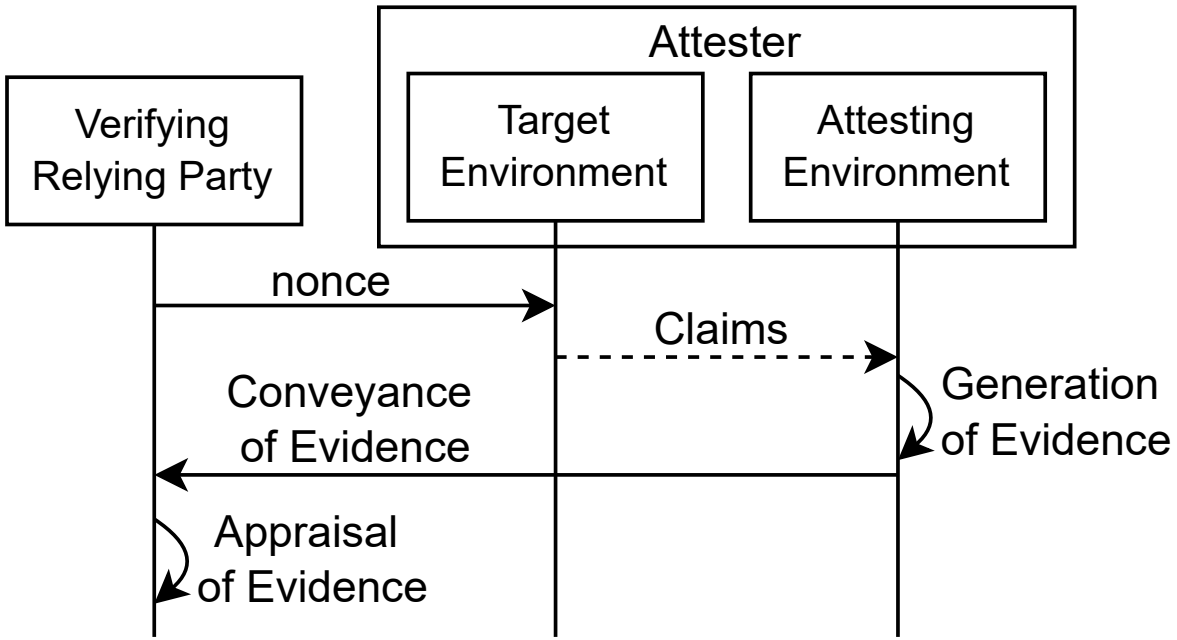
Protocol Perspective (Simplified)



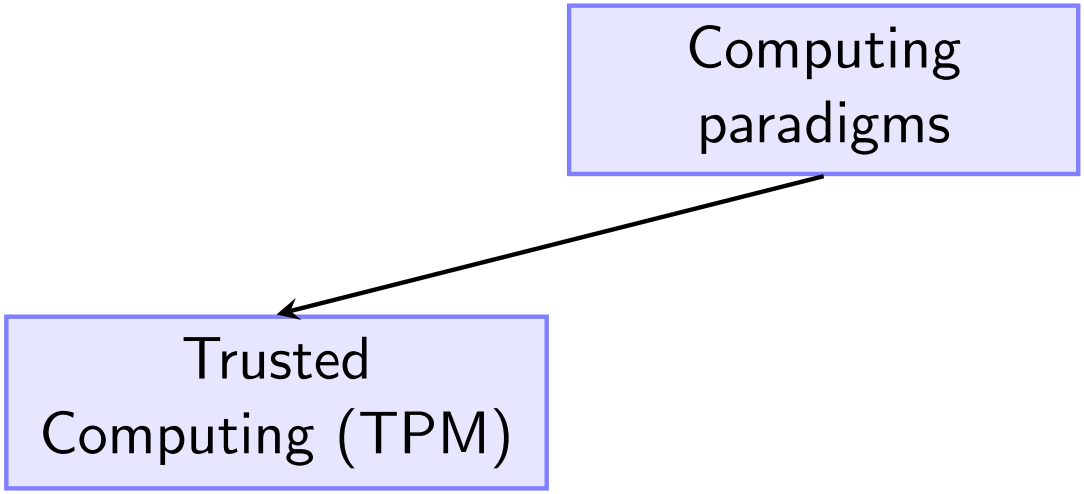


Protocol Perspective (Simplified)

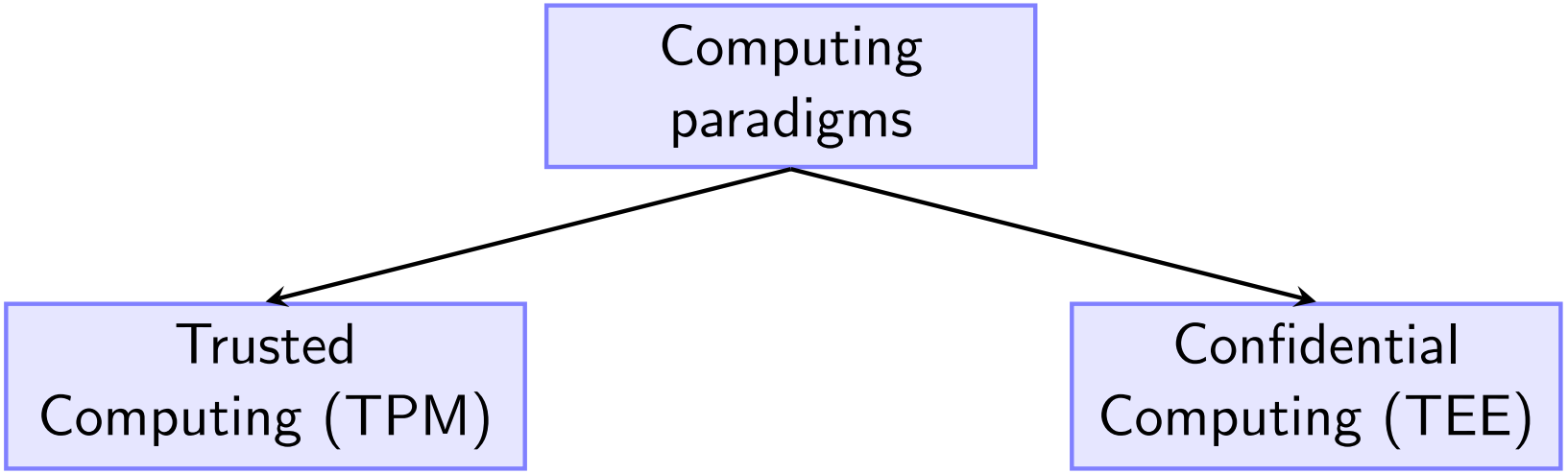




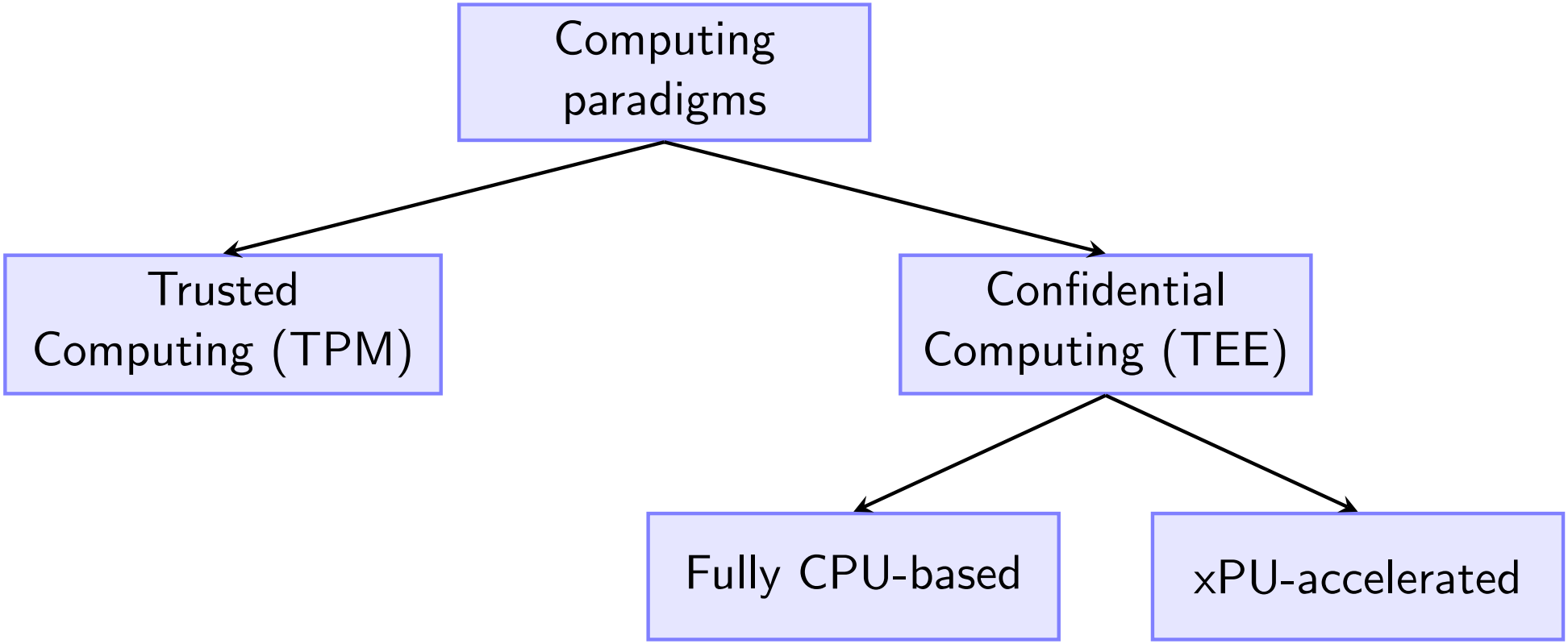
Computing Paradigms using Attestation



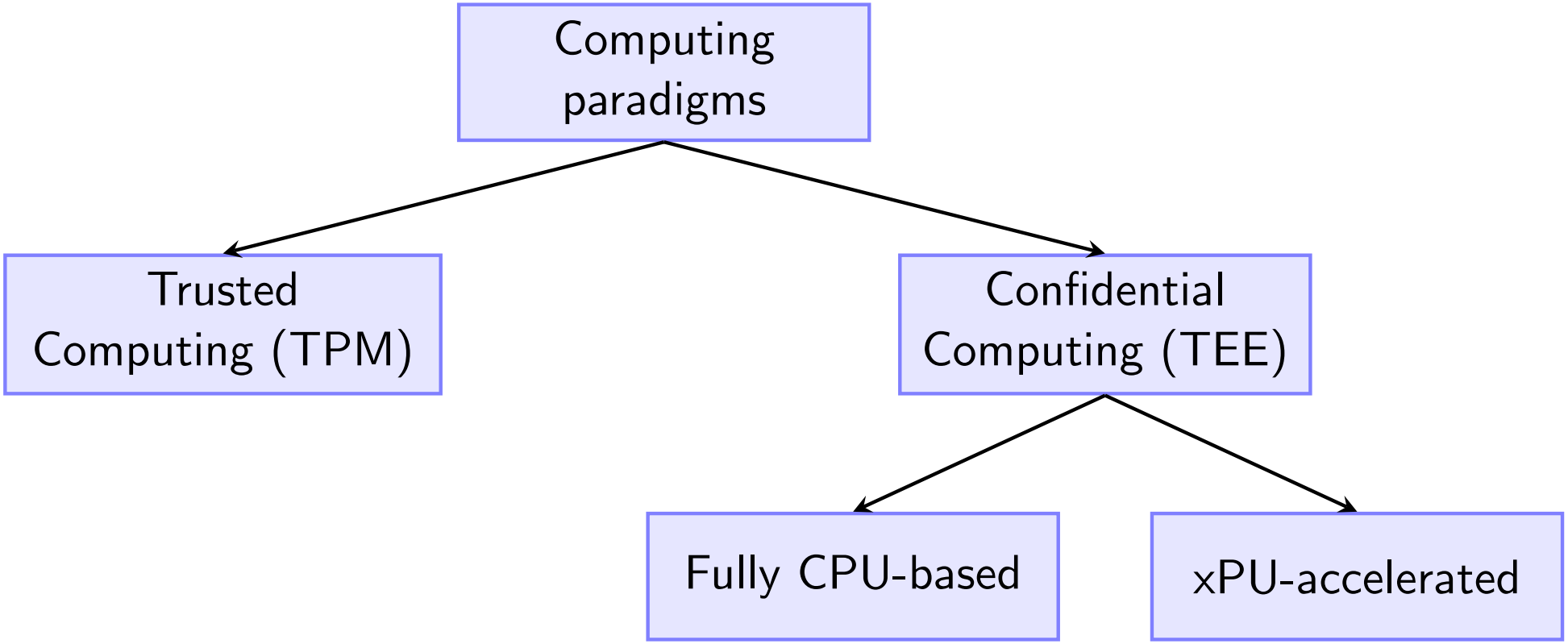
Computing Paradigms using Attestation



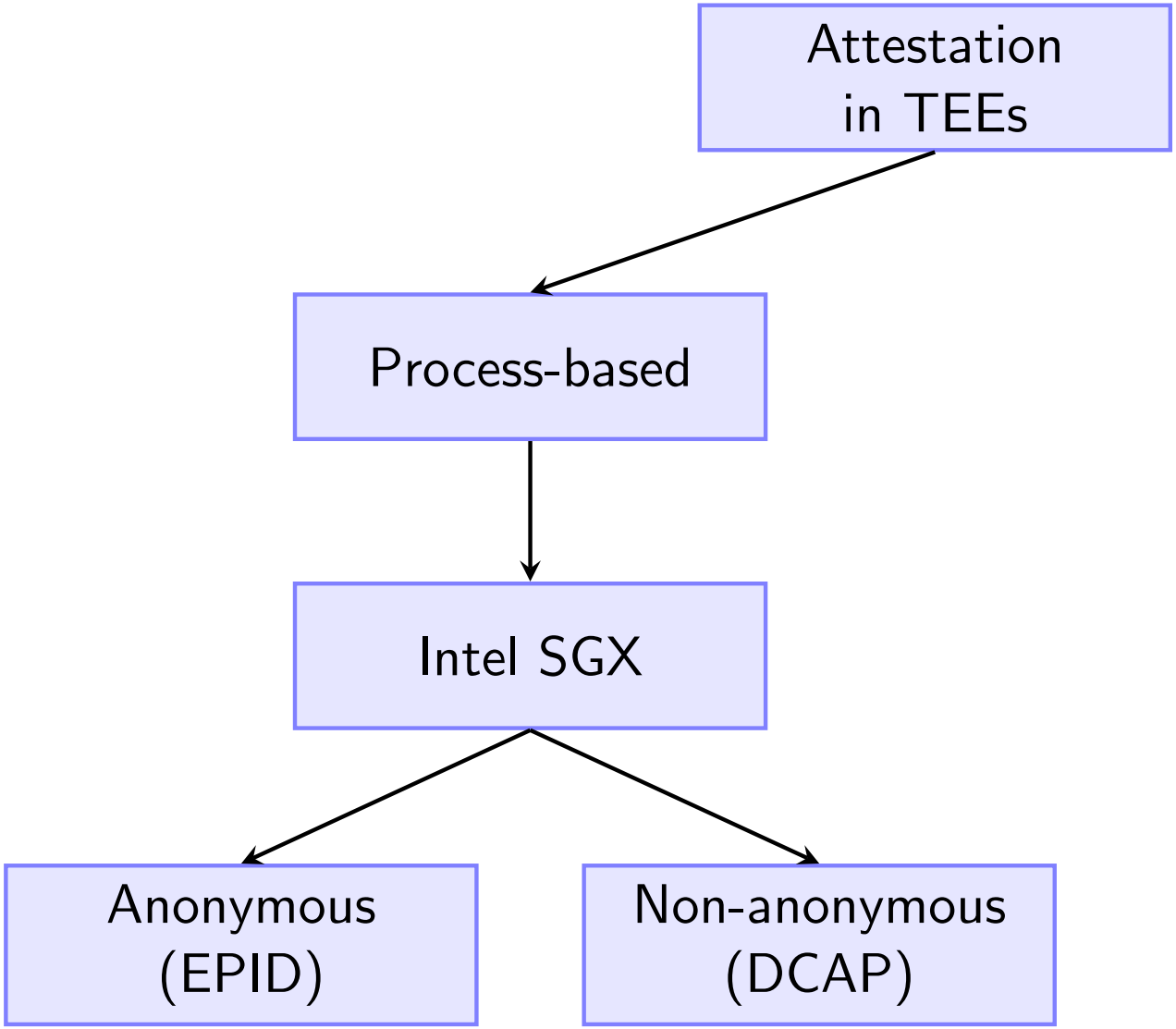
Computing Paradigms using Attestation



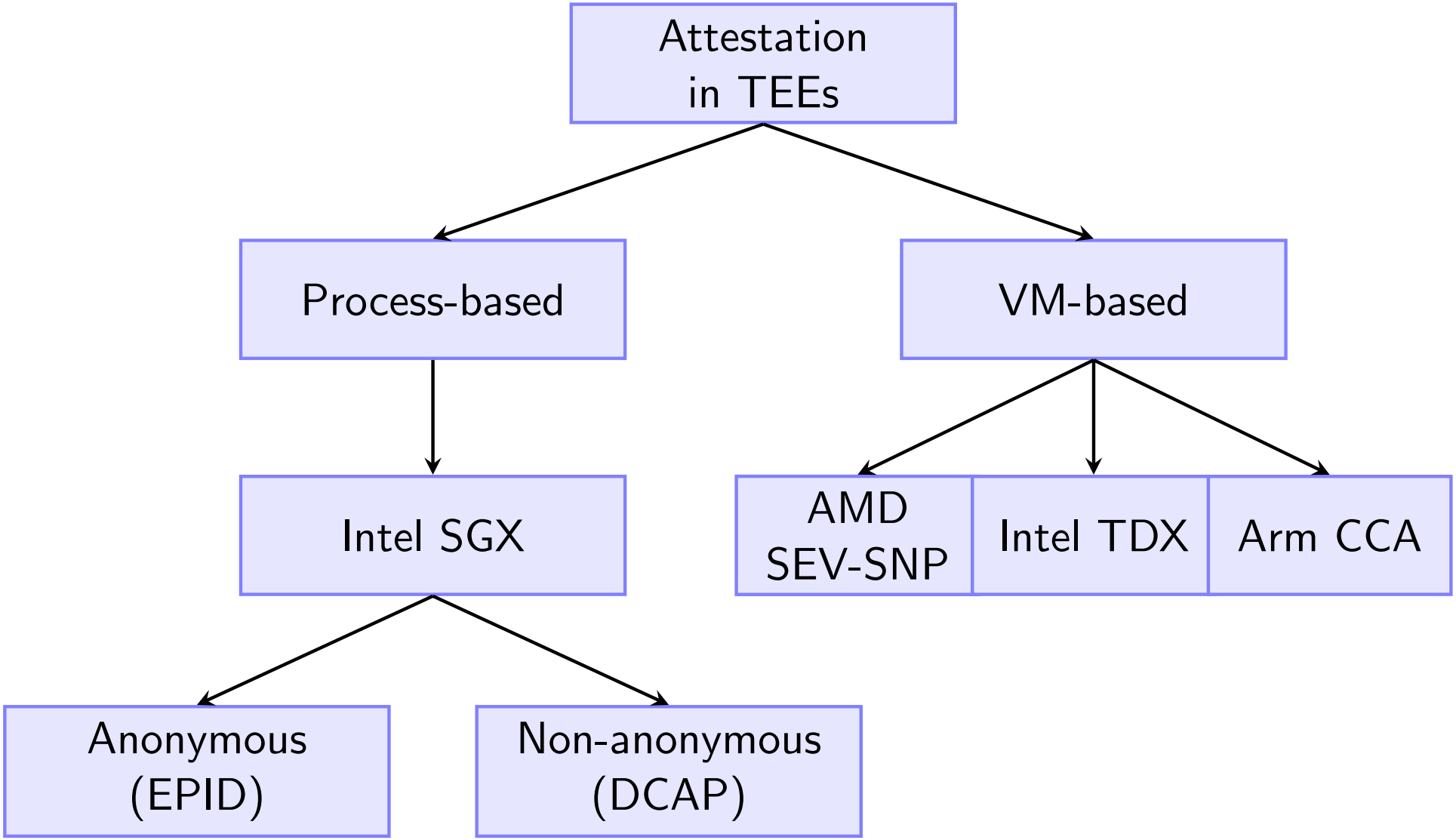
Computing Paradigms using Attestation



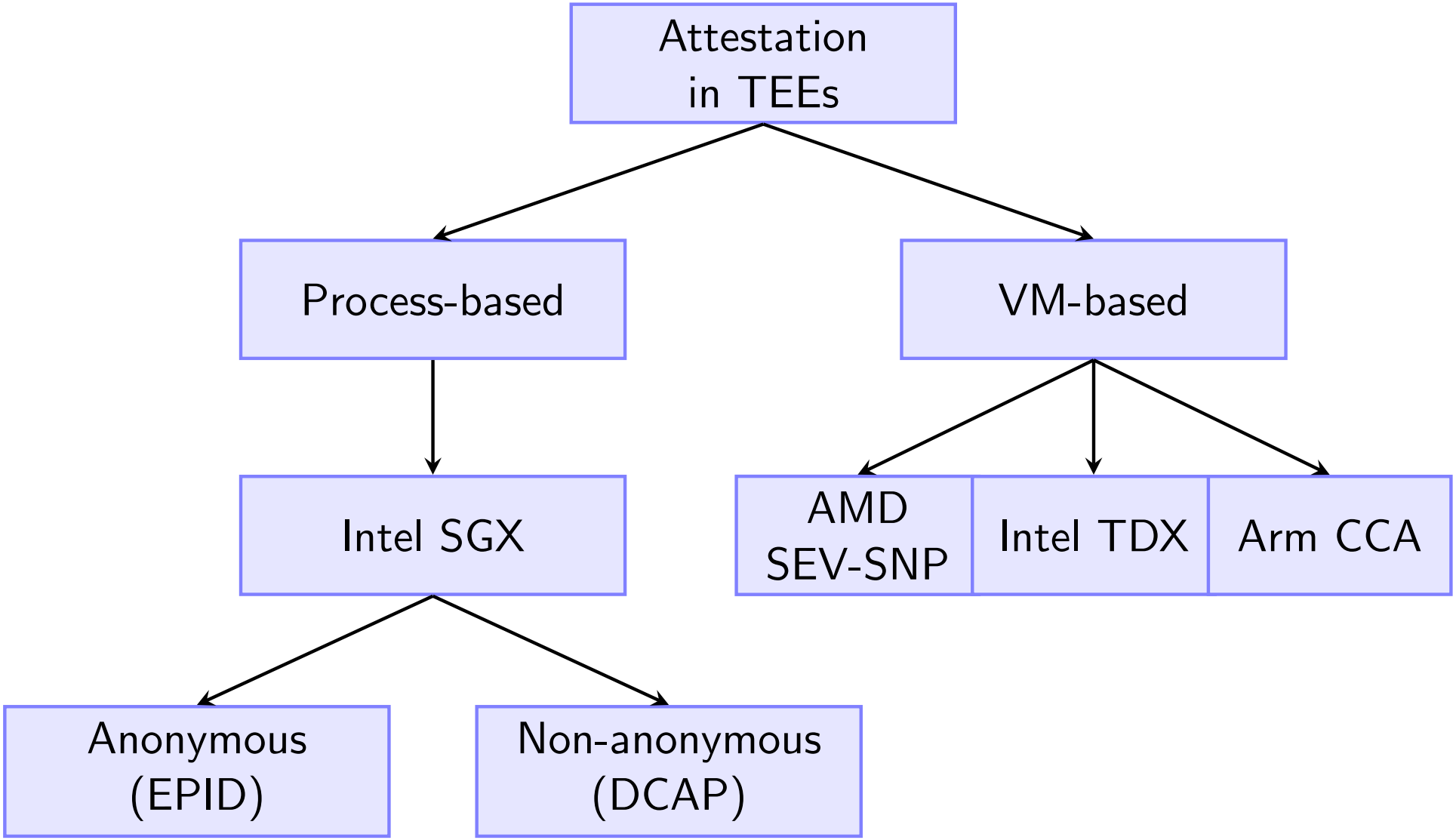
Attestation in Fully-CPU based CC



Attestation in Fully-CPU based CC

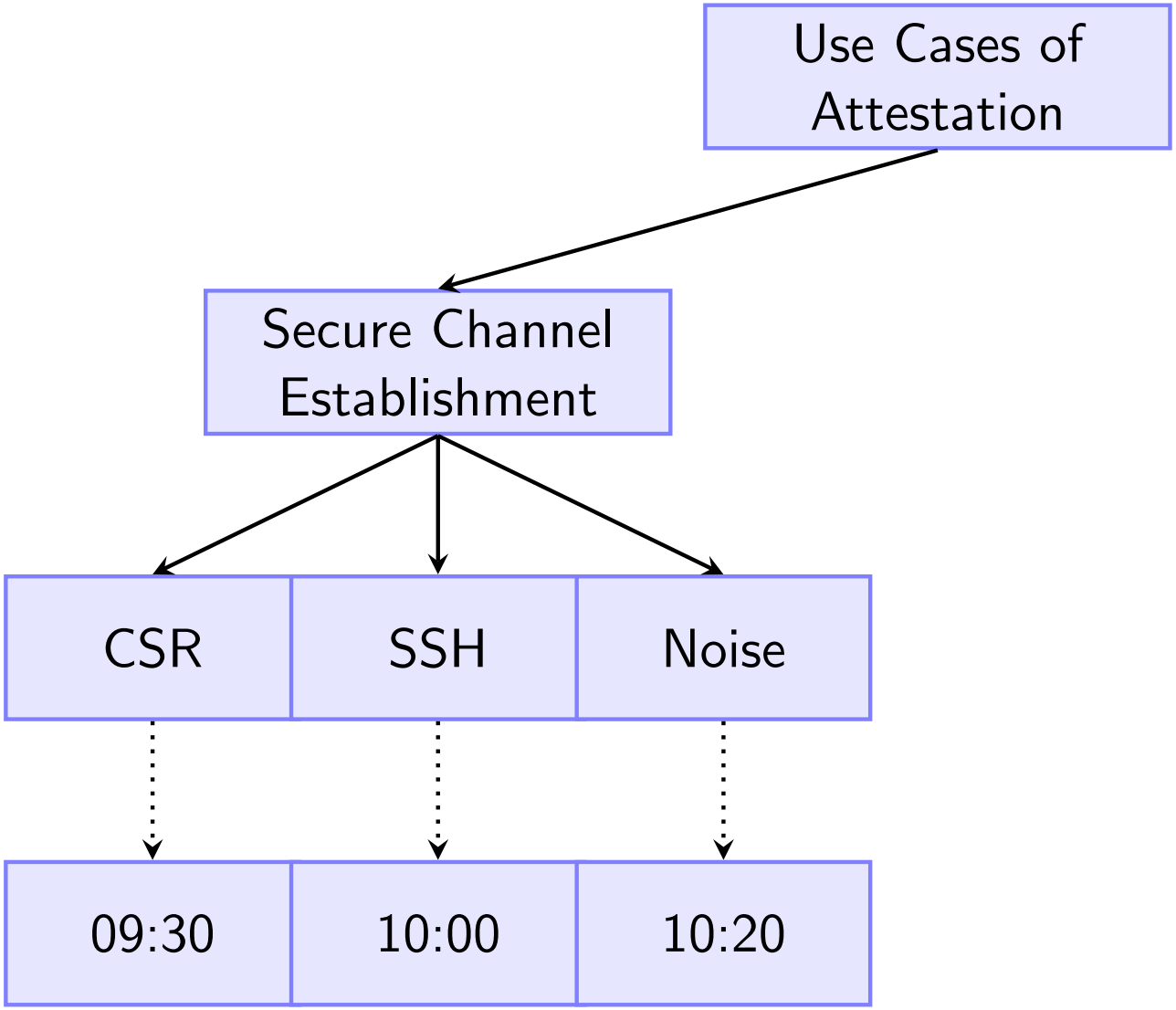


Attestation in Fully-CPU based CC

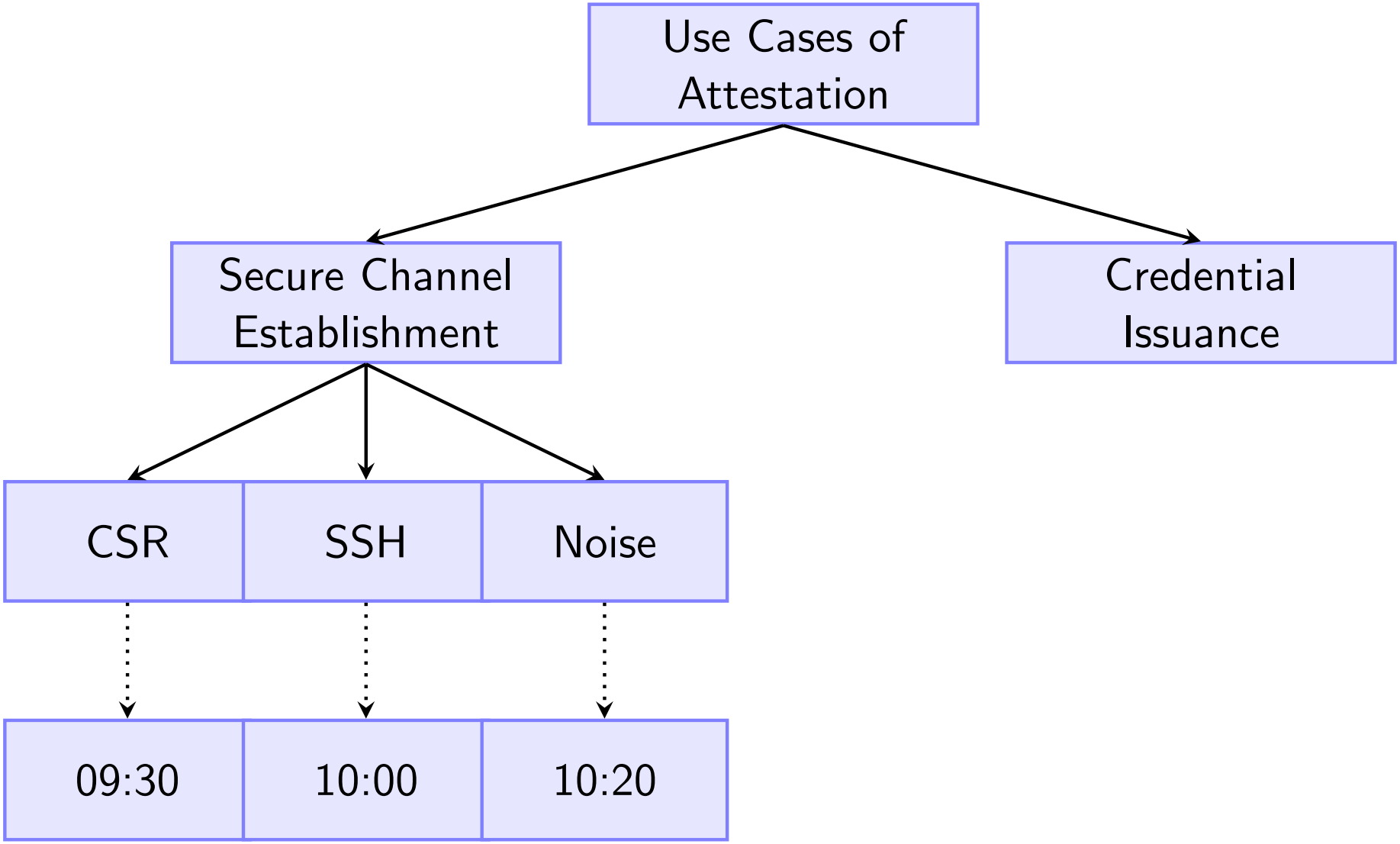


Planned EPID End Of Life (EOL): 2 April, 2025 (source)

Use Cases of Attestation



Use Cases of Attestation



Outline

Example: Attested TLS

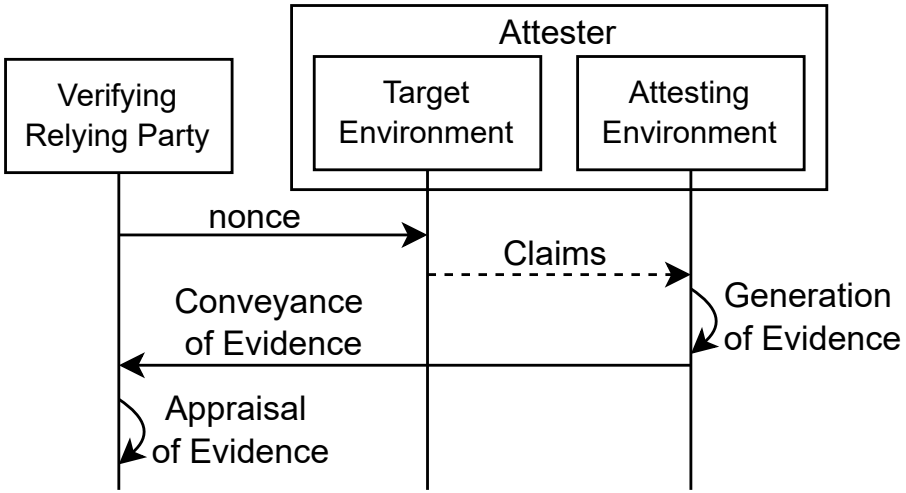


Figure: Remote Attestation

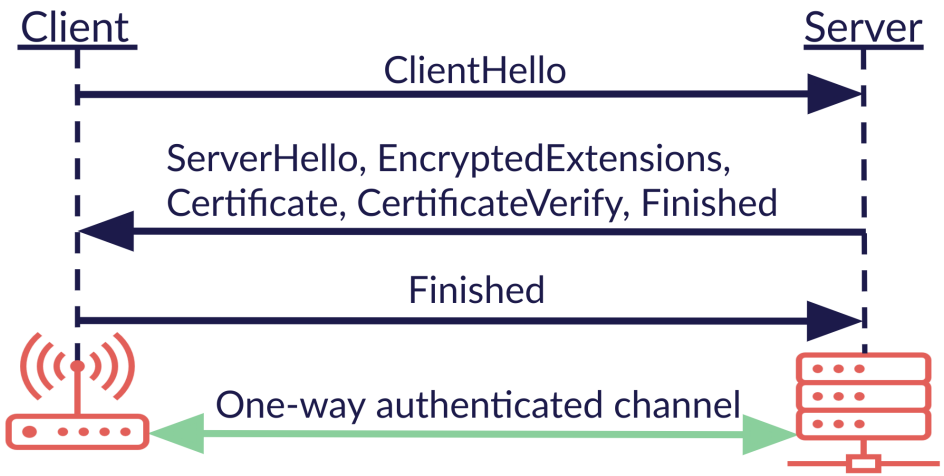
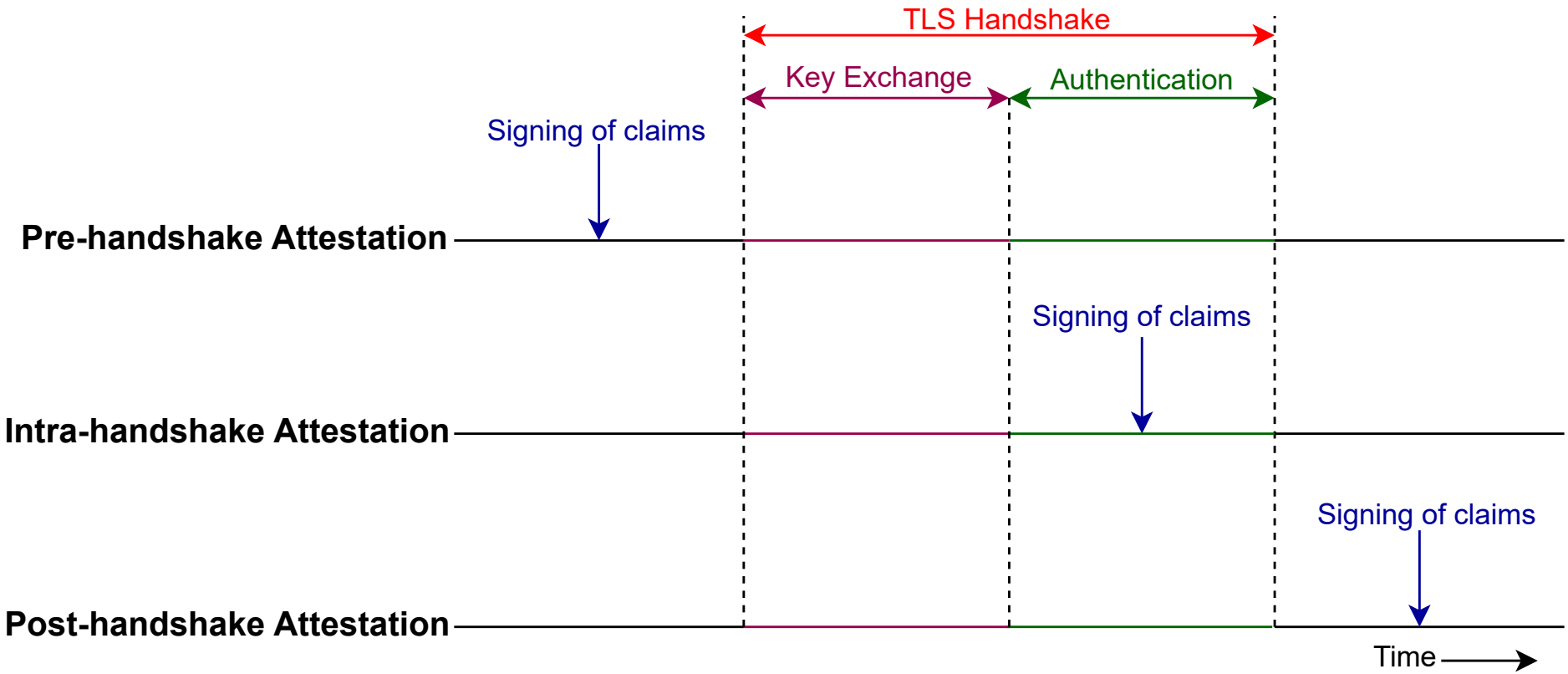


Figure: TLS 1.3

Pre-/Intra-/Post-HS Attestation



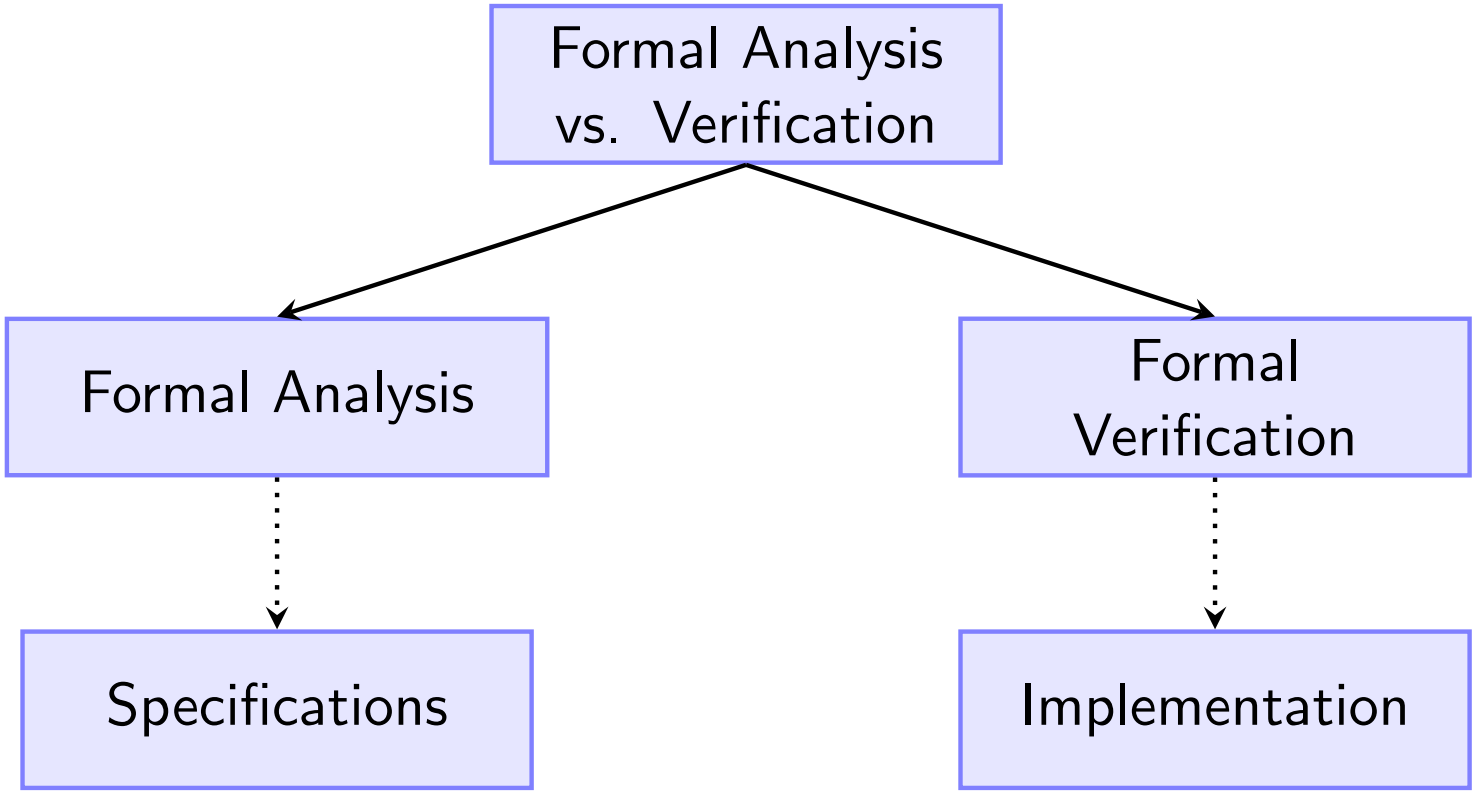
Talks Today: Attested Secure Channels

	Pre-/Intra-/Post-HS	TEE
Attested CSR	Pre-HS	Intel SGX
Attested SSH	Post-HS	Intel TDX
Attested Noise	Pre-HS?	Any

Core Idea

Open source and
precise specifications!

Formal Analysis vs. Verification



Levels of Assurance for Attested TLS Protocols

	RA-TLS[2] (Pre-HS)	TLS attest[3] (Intra-HS)	SCONE[4] (Post-HS)
(a) Open-source implementation	✓[5]	✓[6]	×
(b) Informal specifications available	×	✓[7]	×
(c) Formal specifications	✓[8]	×	×
(d) Formal analysis of specifications	✓[9]	×	×
(e) Formal verification of implementation	×	×	×

[2] Knauth, Steiner, Chakrabarti, Lei, Xing, and Vij, *Integrating Remote Attestation with Transport Layer Security*, 2018.

[3] Tschofenig, Sheffer, Howard, Mihalcea, Deshpande, Niemi, and Fossati, *Using Attestation in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)*, 2024.

[4] Arnautov et al., "SCONE: Secure Linux Containers with Intel SGX", 2016.

[5] *Gramine*, 2024.

[6] *Hardware-Backed Attestation in TLS*, 2024.

[7] Tschofenig, Sheffer, Howard, Mihalcea, Deshpande, Niemi, and Fossati, *Using Attestation in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)*, 2024.

[8] Sardar, Niemi, Tschofenig, and Fossati, "Towards Validation of TLS 1.3 Formal Model and Vulnerabilities in Intel's RA-TLS Protocol", 2024.

[9] Sardar, Niemi, Tschofenig, and Fossati, "Towards Validation of TLS 1.3 Formal Model and Vulnerabilities in Intel's RA-TLS Protocol", 2024.

Outline

Verifiers and friends

- Verification is a central concept in Attestation
- The act of appraising (making sense of) Evidence.
- Driven by a Policy provided by the *"Verifier Owner"*
- Informed by supply chain inputs: Reference Values (Attester's desired state) and Endorsements (Attester's actual state)
- Produces a (signed) appraisal statement called Attestation Result
- The AR is used by a Relying Party in a trust decision regarding the Attester
- The RATS architecture provides a dedicated role: Verifier
- Verifier can be a separate TTP, or co-located with RP

Verifiers and friends (cont.)

There are talks that directly or indirectly involve the most relevant OSS verifier [and Verifying RPs] projects:

- CoCo/Trustee AS (Magnus)
- Veraison (Jag and Suzaki-san)
- Oak (Katsiarina and Ivan)
- Keylime (Jean, but also Thore and Anderson at Friday's attestation workshop!)

Verifiers and friends (cont.)

- Lots of good stuff!
- Different use cases, different goals
- Cross-pollination is happening
- FOSDEM, CCC, IETF, Linaro Connect, is bringing us together

(More) Talks

Reference value providers

Jean-Philippe's "Virtual Machine attestation on Arm CCA"

(Highly dynamic) Attesters

Magnus's "Measurement and Attestation Schemes for Container Sandboxes"

Conveyance protocols

Jean's Secure Push Attestation with Extensible REST APIs

RATS end-to-end integrations

Jag's "Remote Attestation in the cloud"

Suzaki-san's "Remote Attestation on Arm TrustZone OP-TEE with Veraison Verifier"

Outline

Honorable Mentions (some presented in Friday workshop[10])

- Content Authenticity & its Provenance (Yogesh Deshpande)
- APIs for Endorsement Flows (Paul Howard)
- Expanding Keylime: Attestation for TEEs (Anderson Toshiyuki Sasaki)
- Remote Attestation for Confidential MPC and Collaborative AI (Drasko Draskovic, Danko Miladinovic)
- Attestation in Production (Jonathan McDowell)
- Trustless Attestation Verification with Zero-Knowledge Proofs (Dayeol Lee)
- TPM based Remote Attestation: Pitfalls and Lessons Learned (Thore Sommer)
- Secure Cloud-Native IoT (Anastassios Nanos)
- Lightweight Intra-handshake Attestation over EDHOC (Yuxuan)
- Attestation Servers and Protocols (Klaus Heinrich Kiwi, Yash Mankad)
- Privacy-Preserving Attestation (Oana Barbu)
- Attested TLS for Confidential Computing (Muhammad Usama Sardar)

[10] `https://github.com/muhammad-usama-sardar/attestation-workshop-fosdem25`

ACK

- Hannes Tschofenig (University of Applied Sciences Bonn-Rhein-Sieg and Siemens)
- Simon Frost (Arm)
- Ned Smith (Intel)
- Arto Niemi (Huawei)
- Tuomas Aura (Aalto University)
- Ionut Mihalcea (Arm)
- Carsten Weinhold (Barkhausen Institut)
- Michael Roitzsch (Barkhausen Institut)
- Yogesh Deshpande (Arm)
- Yaron Sheffer (Intuit)
- Cedric Fournet (Microsoft)
- Thore Sommer (Kiel University)
- Nikolaus Thümmel (Scontain)
- Giridhar Mandyam (Mediatek)
- Jonathan Hoyland (Cloudflare)
- Laurence Lundblade (Security Theory LLC)
- Gilang Mentari Hamidy (KU Leuven)
- Jo Van Bulck (KU Leuven)
- Dionna Amalie Glaze (Google)
- Kathleen Moriarty (Transforming Information Security LLC)

Special thanks for help in devroom organization!

- Ionut Mihalcea (Arm)
- Jo Van Bulck (KU Leuven)
- Fritz Alder (NVIDIA)

Key References

Arnautov, Sergei et al. "SCONE: Secure Linux Containers with Intel SGX". In: *USENIX Symposium on Operating Systems Design and Implementation*. 2016, pp. 689–703. URL: https://www.usenix.org/conference/osdi16/technical-sessions/presentation/arnautov.

Gramine. 2024. URL: https://github.com/gramineproject/gramine/tree/master/CI-Examples/ra-tls-mbedtls (visited on 10/10/2024).

Hardware-Backed Attestation in TLS. 2024. URL: https://github.com/CCC-Attestation/attested-tls-poc (visited on 11/30/2024).

Knauth, T., M. Steiner, S. Chakrabarti, L. Lei, C. Xing, and M. Vij. *Integrating Remote Attestation with Transport Layer Security*. Tech. rep. Intel Labs, 2018. URL: https://arxiv.org/abs/1801.05863.

Sardar, Muhammad Usama, Thomas Fossati, Simon Frost, and Shale Xiong. "Formal Specification and Verification of Architecturally-defined Attestation Mechanisms in Arm CCA and Intel TDX". In: *IEEE Access* 12 (2024), pp. 361–381. DOI: 10.1109/ACCESS.2023.3346501.

Sardar, Muhammad Usama, Arto Niemi, Hannes Tschofenig, and Thomas Fossati. "Towards Validation of TLS 1.3 Formal Model and Vulnerabilities in Intel's RA-TLS Protocol". In: *IEEE Access* 12 (2024), pp. 173670–173685. DOI: 10.1109/ACCESS.2024.3497184.

Tschofenig, Hannes, Yaron Sheffer, Paul Howard, Ionuț Mihalcea, Yogesh Deshpande, Arto Niemi, and Thomas Fossati. *Using Attestation in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)*. Internet-Draft. Work in Progress. Internet Engineering Task Force, Oct. 2024. 34 pp. URL: https://datatracker.ietf.org/doc/draft-fossati-tls-attestation/08/.

Exciting Talks!

Event	Speakers	Start	End
Sunday			
Welcome to attestation devroom!	Thomas Fossati, Muhammad Usama Sardar	09:00	09:25
Binding Intel SGX Root-of-Trust to PKI to Establish High-Performant Trusted Channel Between Enclaves	Gilang Mentari Hamidy	09:30	09:55
Integrating Intel TDX remote attestation into SSH	Fabian Wesemann	10:00	10:15
Attested Noise Protocol for Low-TCB Trusted Execution Environments	Ivan Petrov, Katsiaryna Naliuka	10:20	10:45
Secure Push Attestation with Extensible REST APIs	Jean Snyman	10:50	11:20
Measurement and Attestation Schemes for Container Sandboxes	Magnus Kulke	11:25	11:50
Virtual Machine attestation on Arm CCA	Jean-Philippe Brucker	11:55	12:10
Remote Attestation in the cloud	Jagannathan Raman	12:15	12:35
Remote Attestation on Arm TrustZone OP-TEE with VERAISON Verifier --- current status and future plan ---	Kuniyasu Suzaki	12:40	13:00