Formal Foundations for Intel SGX Data Center Attestation Primitives

Muhammad Usama Sardar and Christof Fetzer

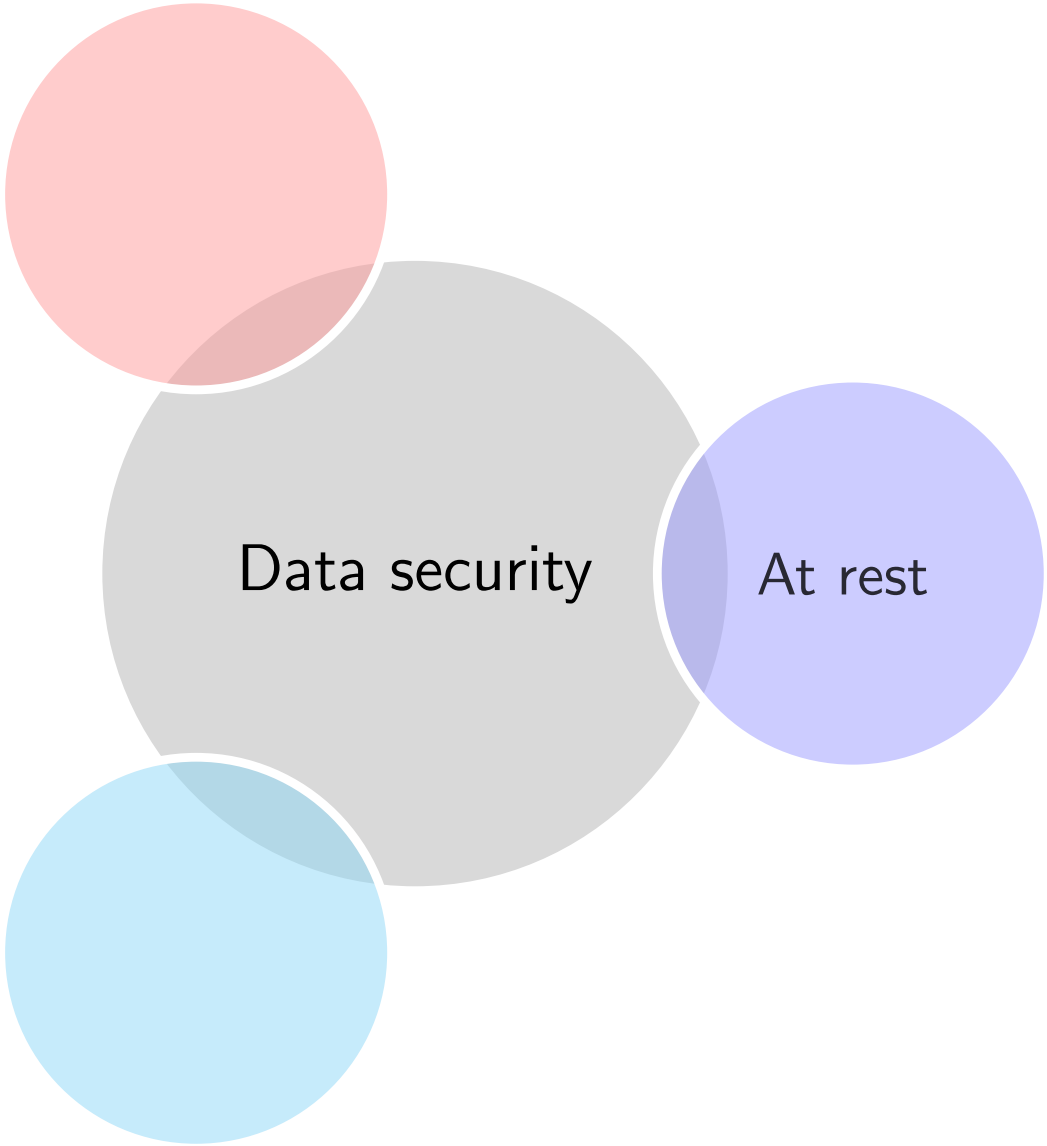
Thanks to: Rasha Faqeh, Do Le Quoc, Franz Gregor

Chair of Systems Engineering
Institute of Systems Architecture
Technische Universität Dresden
Dresden, Germany

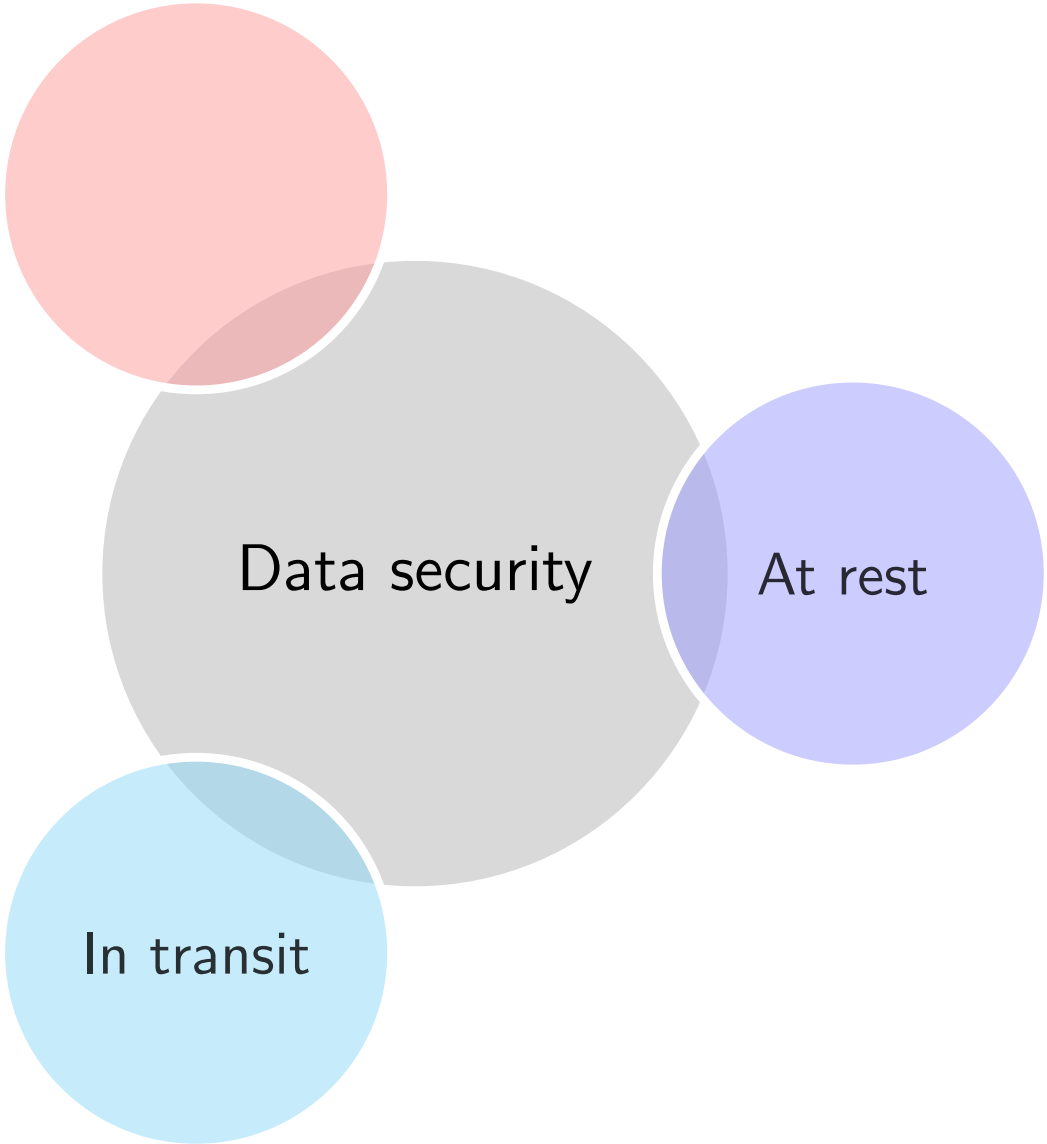
Arm Research Summit 2020

August 12, 2020

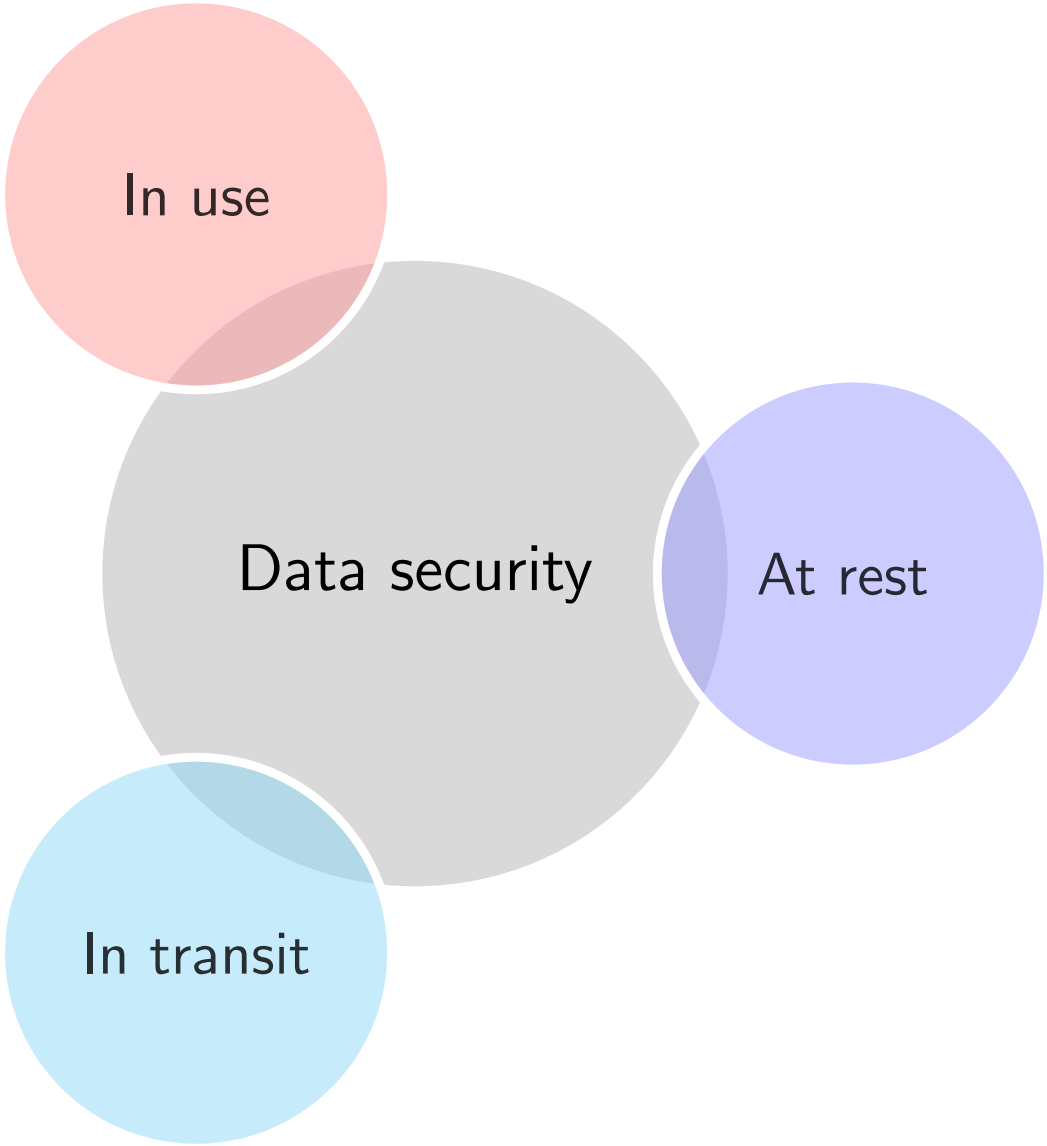
Data Security Paradigms



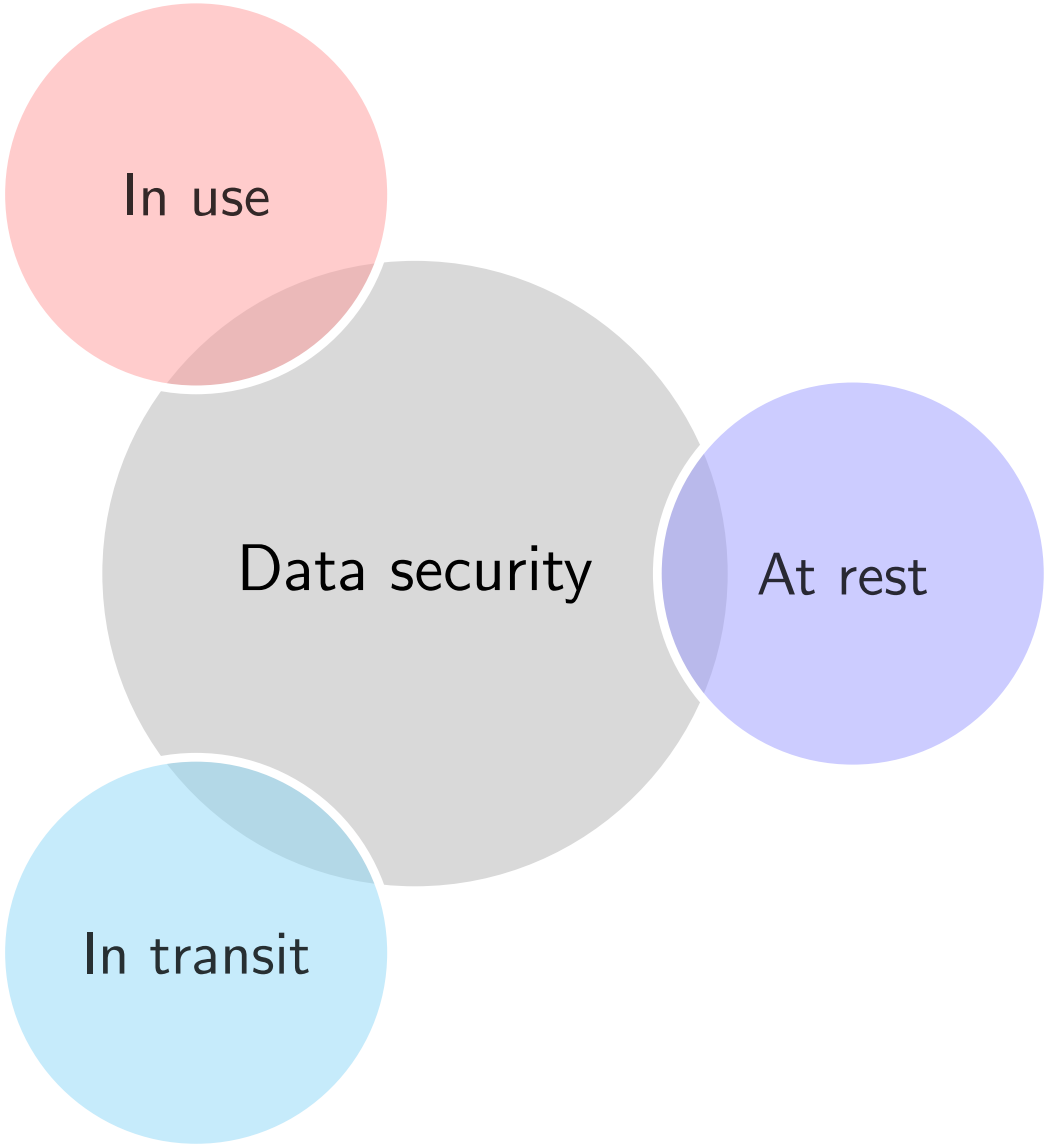
Data Security Paradigms



Data Security Paradigms



Data Security Paradigms



- Formal methods (e.g., for Needham–Schröder protocol)

Introduction

- HW-based Trusted Execution Environments (TEEs)

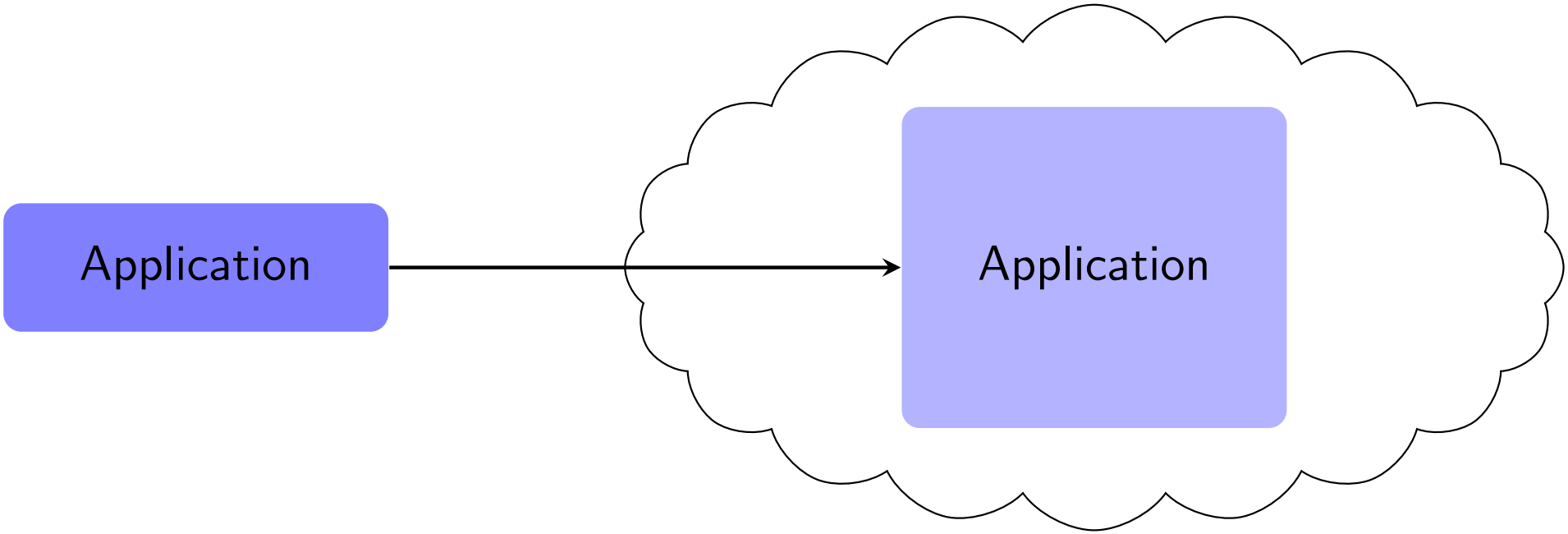
Introduction

- HW-based Trusted Execution Environments (TEEs)

Application

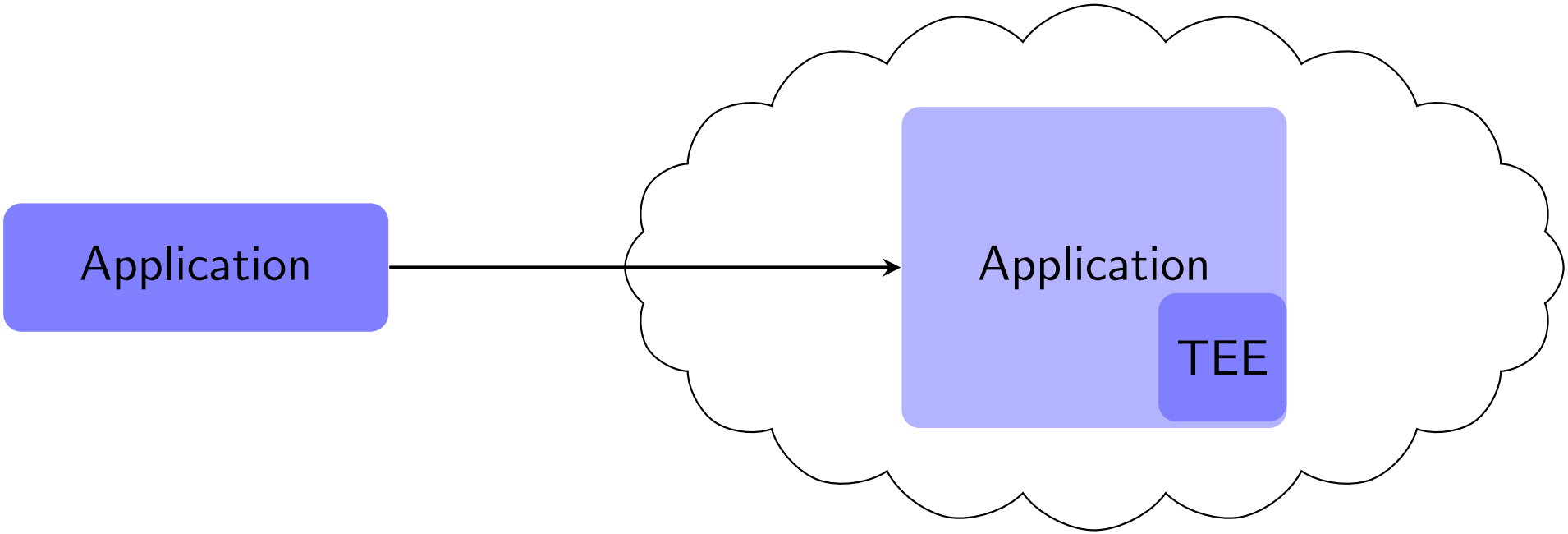
Introduction

- HW-based Trusted Execution Environments (TEEs)



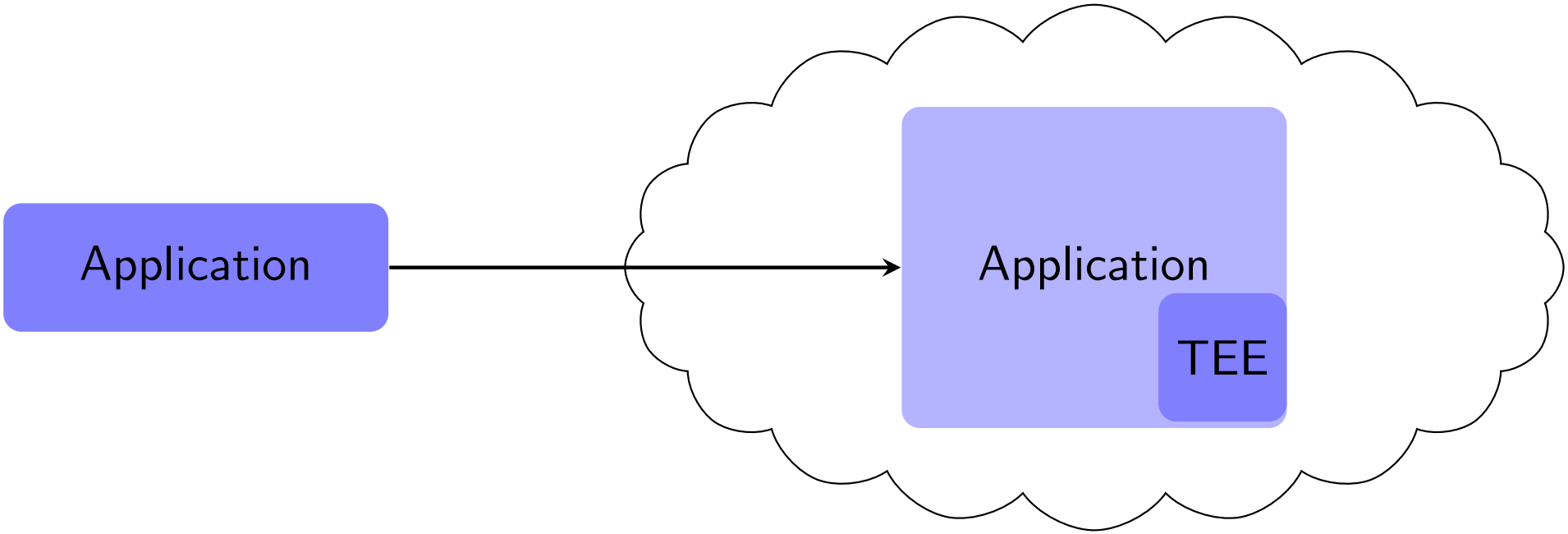
Introduction

- HW-based Trusted Execution Environments (TEEs)



Introduction

- HW-based Trusted Execution Environments (TEEs)



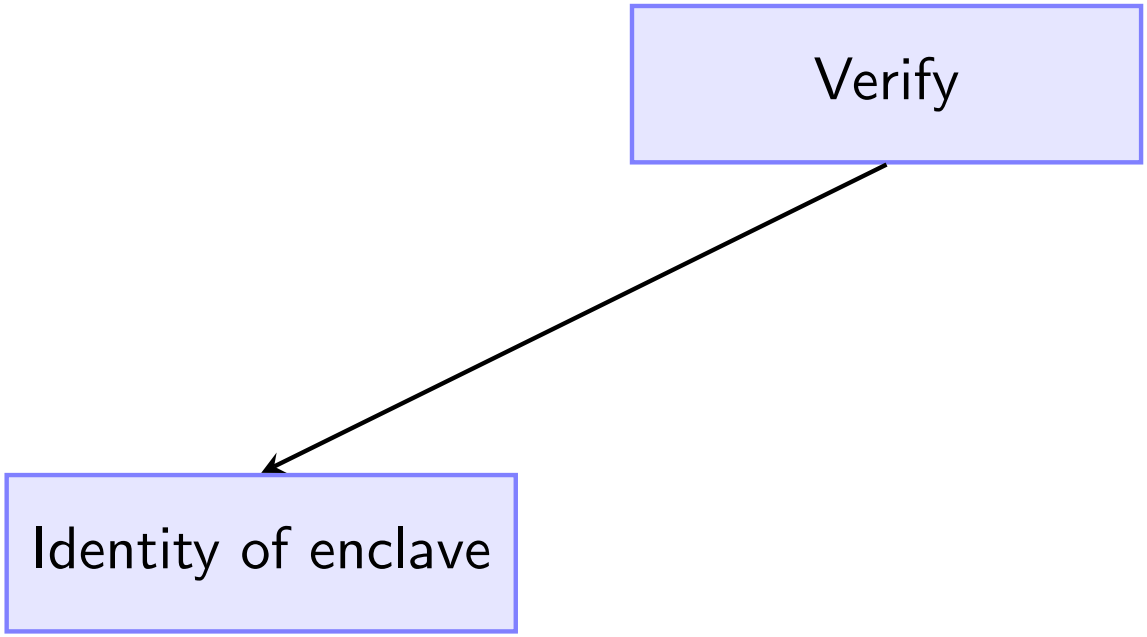
- Intel SGX, AMD SP, ARM TrustZone

Attestation

- Trust to challenger: right app in right platform

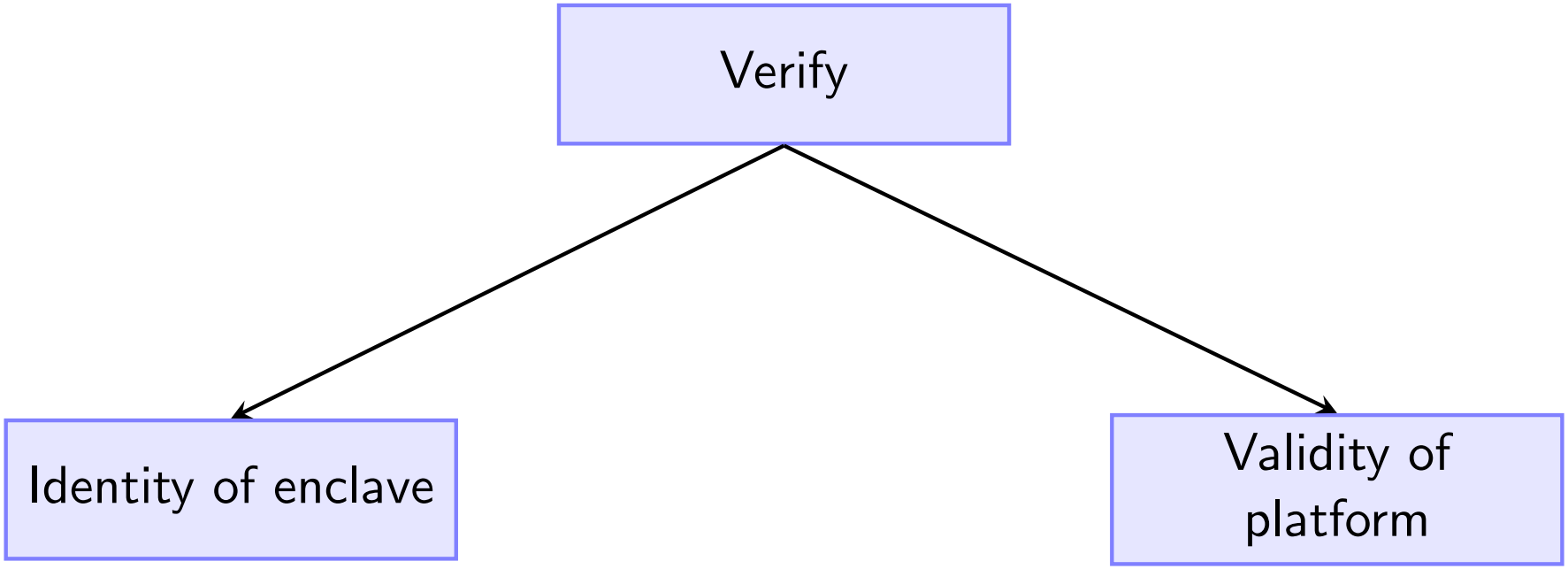
Attestation

- Trust to challenger: right app in right platform



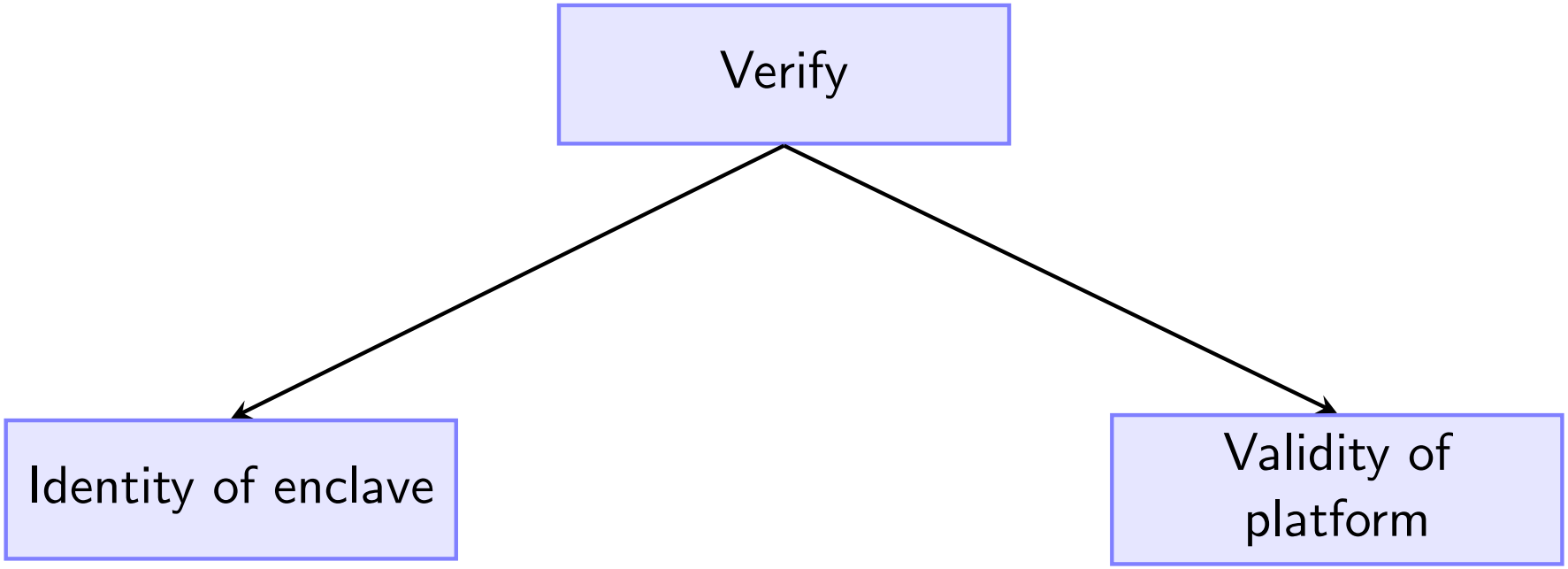
Attestation

- Trust to challenger: right app in right platform



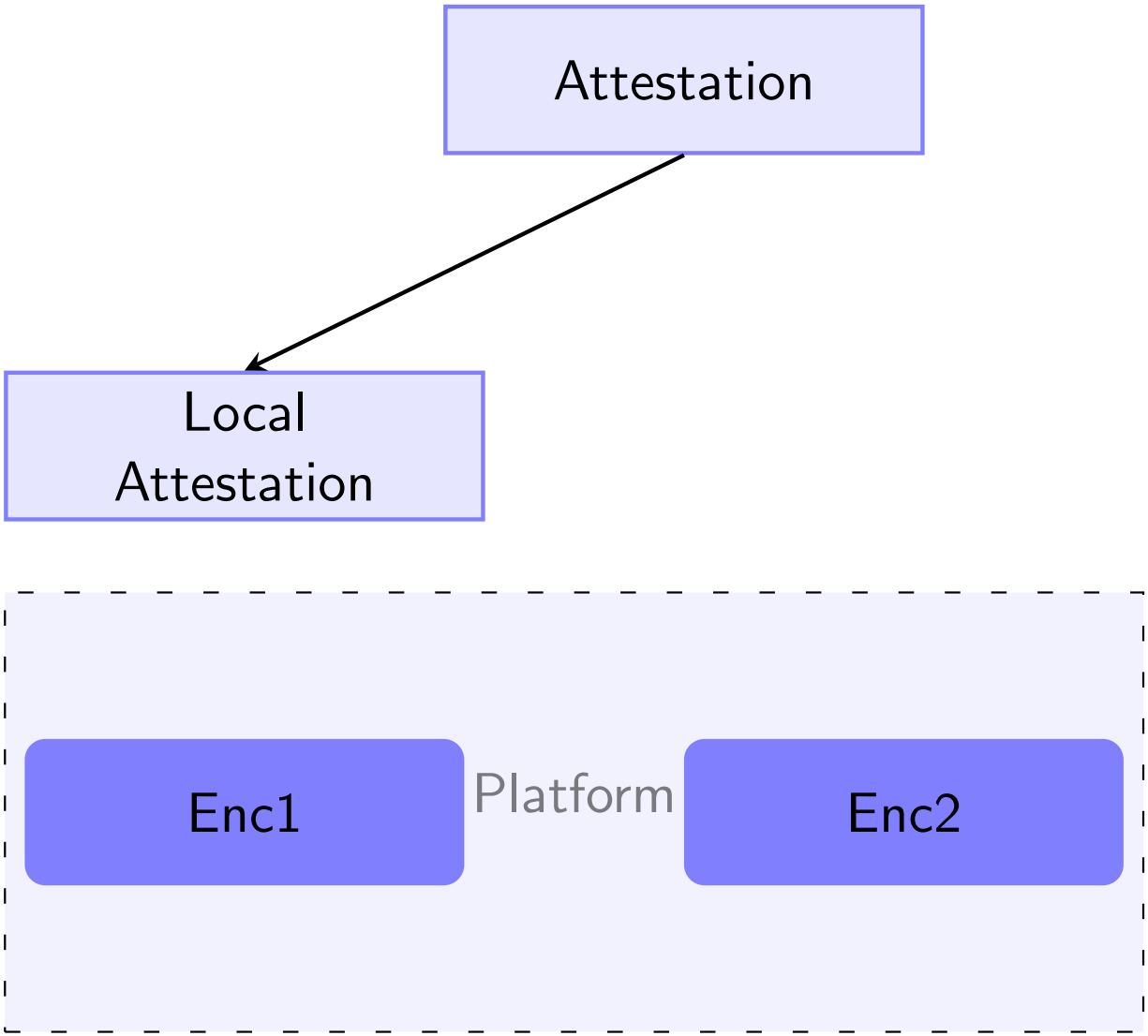
Attestation

- Trust to challenger: right app in right platform

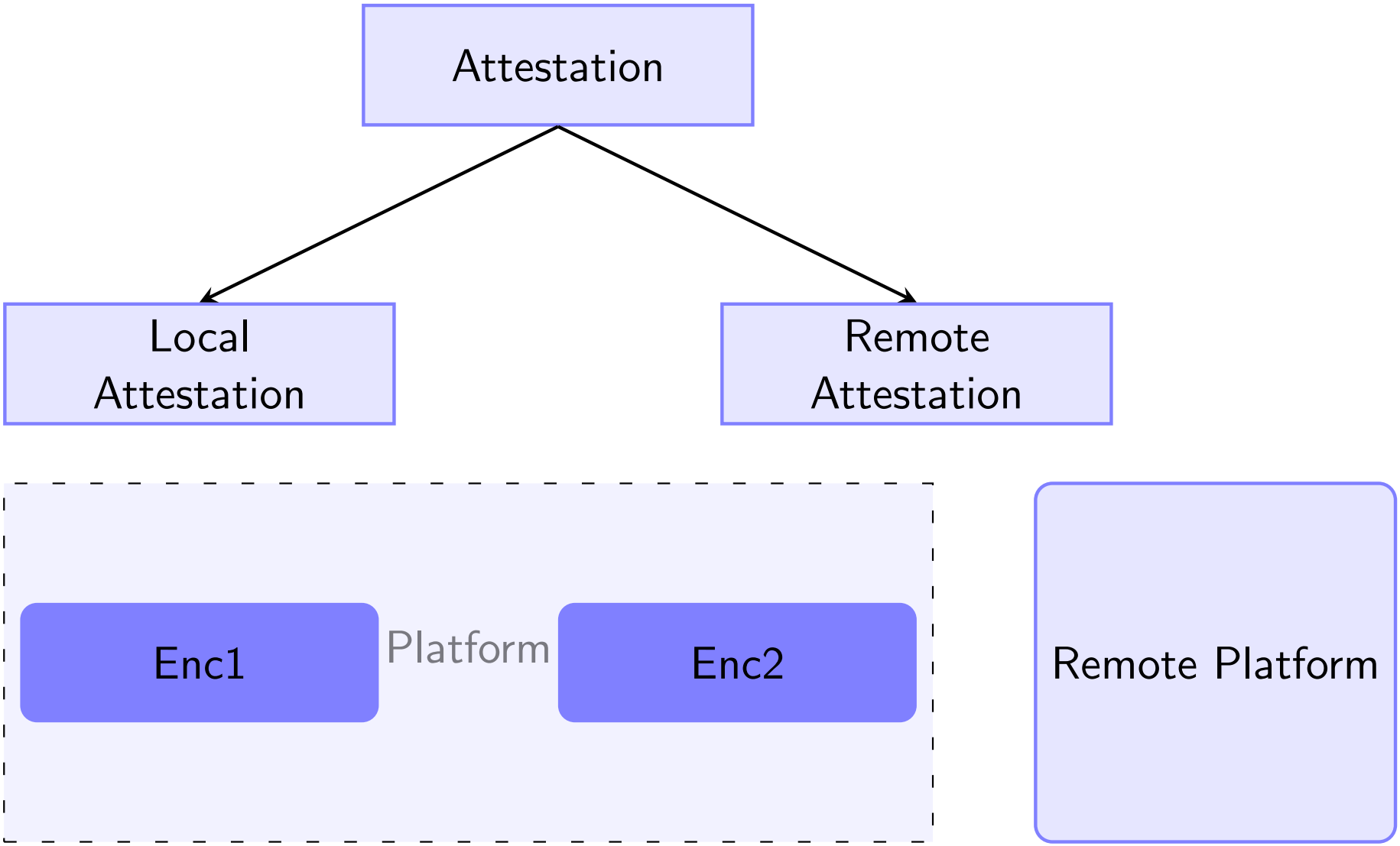


- Importance $\rightarrow$ Provisioning of secrets

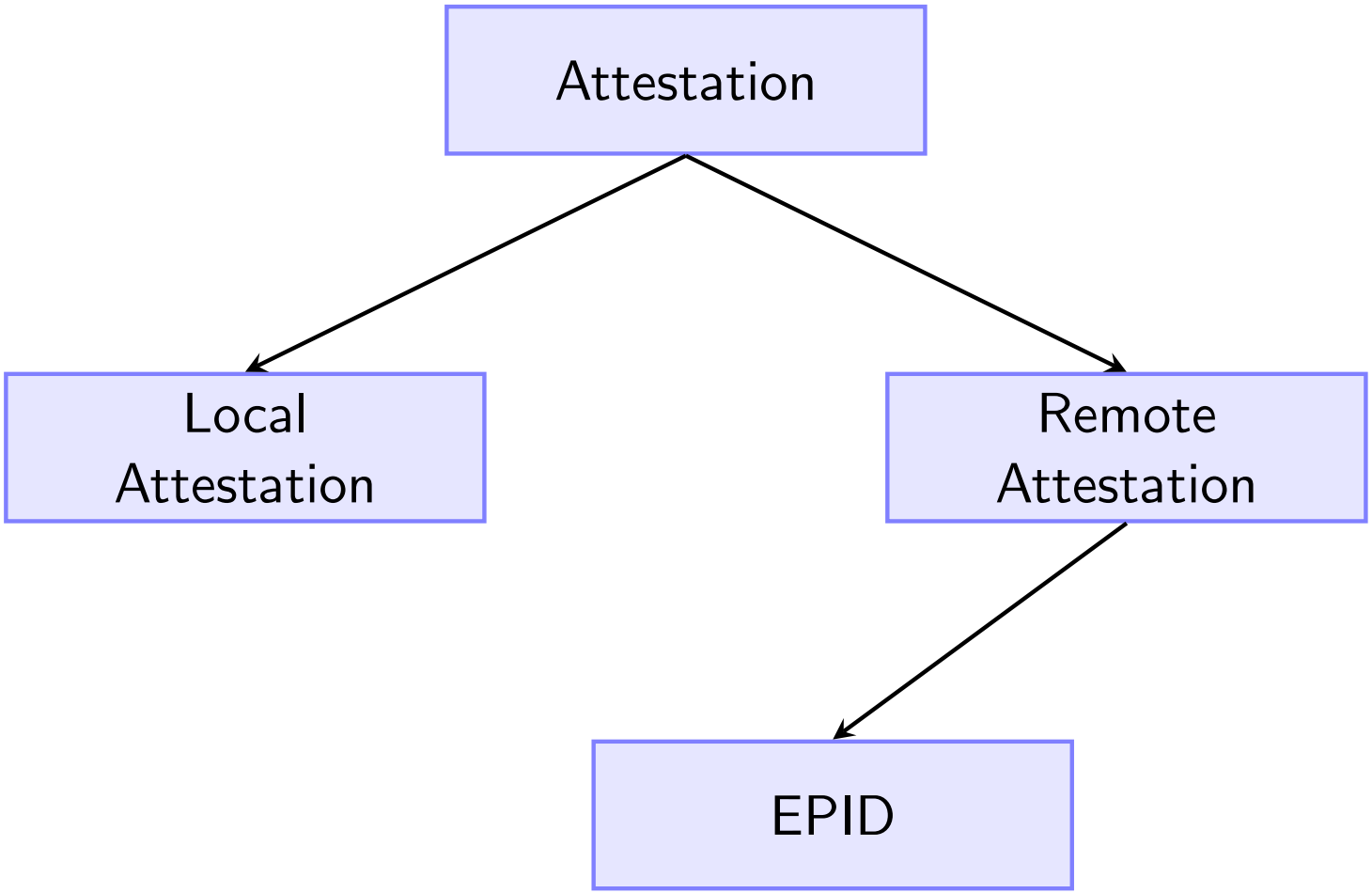
Attestation in Intel SGX



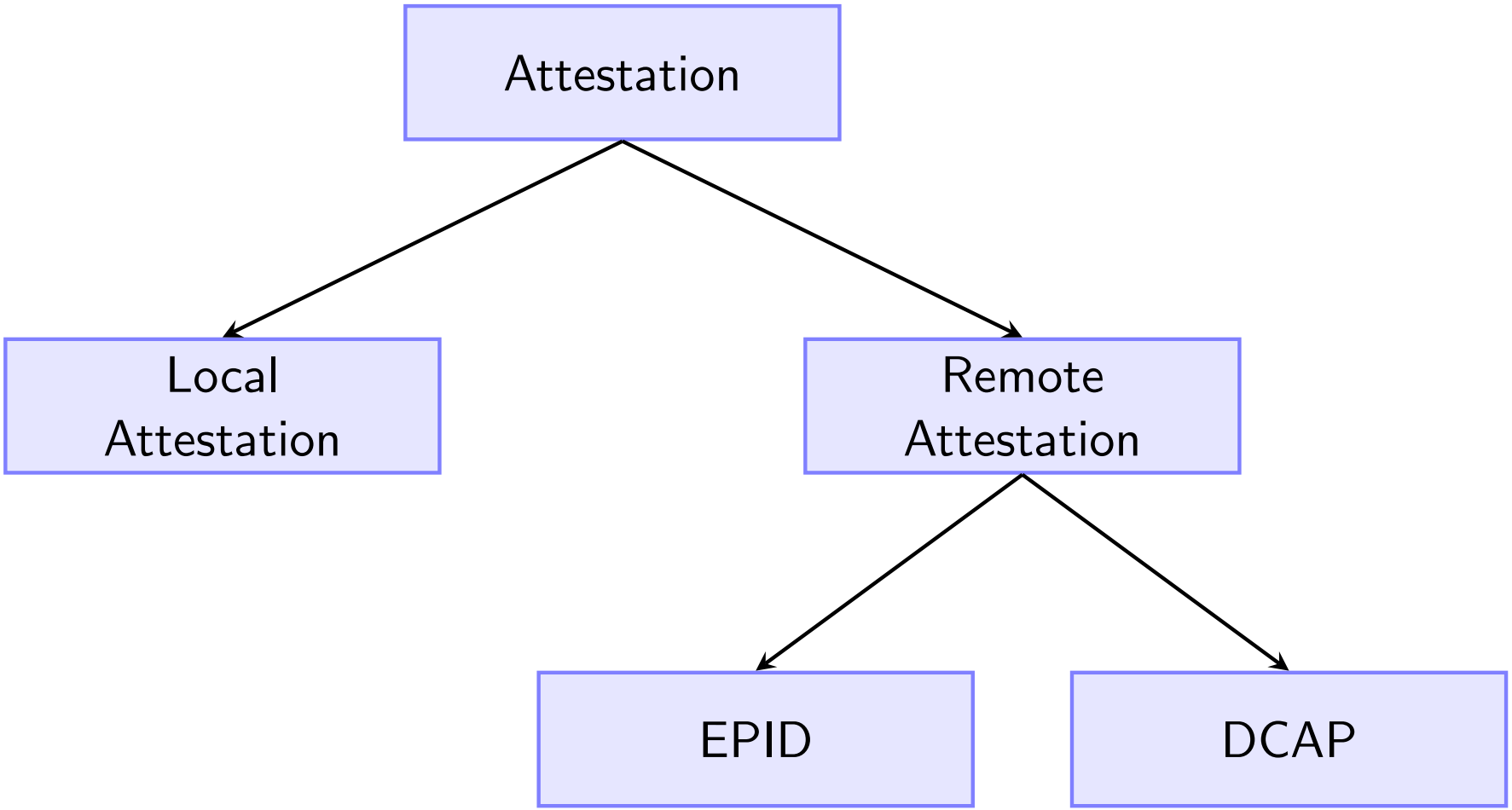
Attestation in Intel SGX



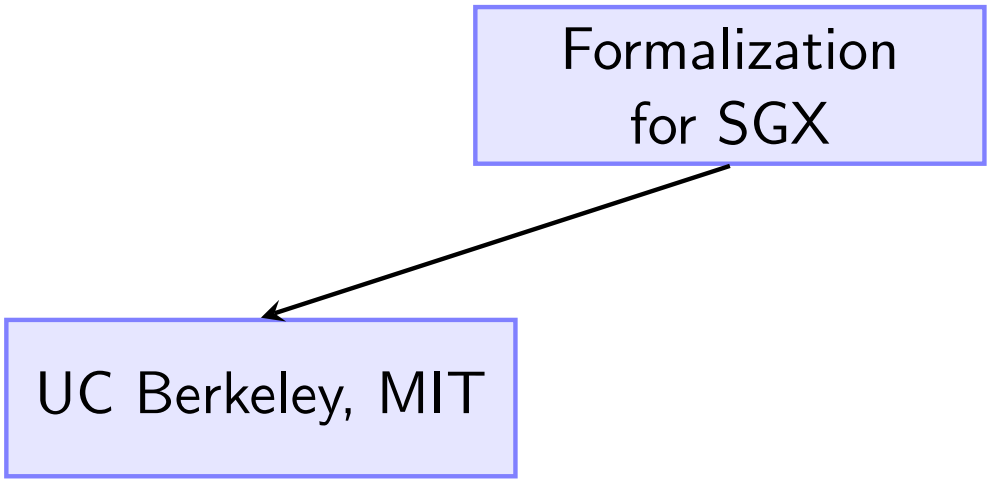
Attestation in Intel SGX



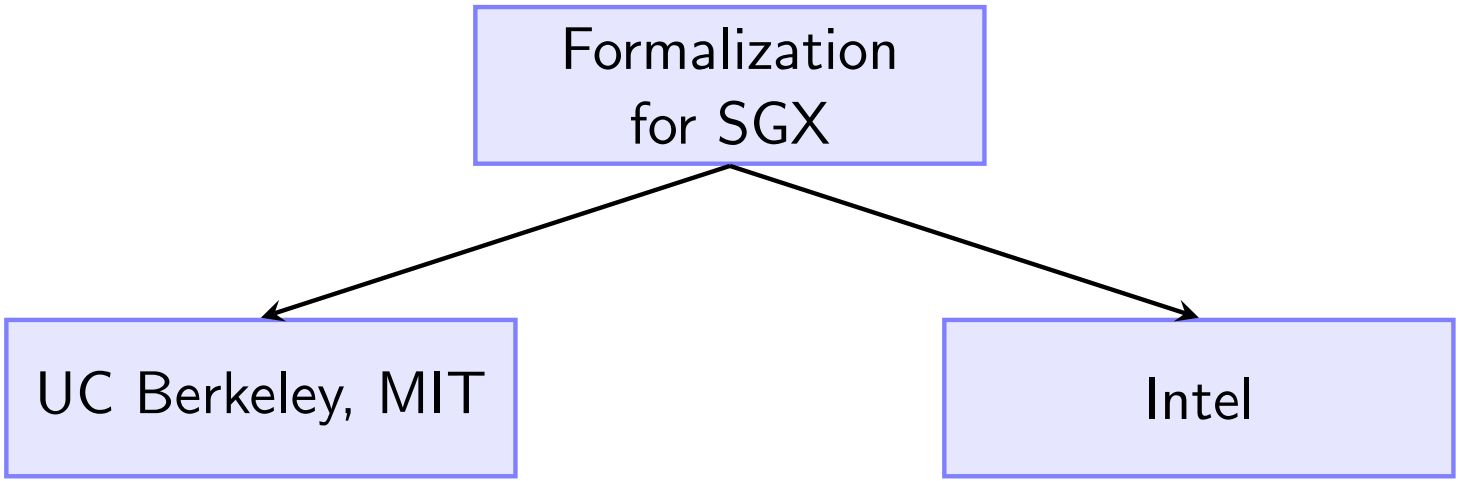
Attestation in Intel SGX



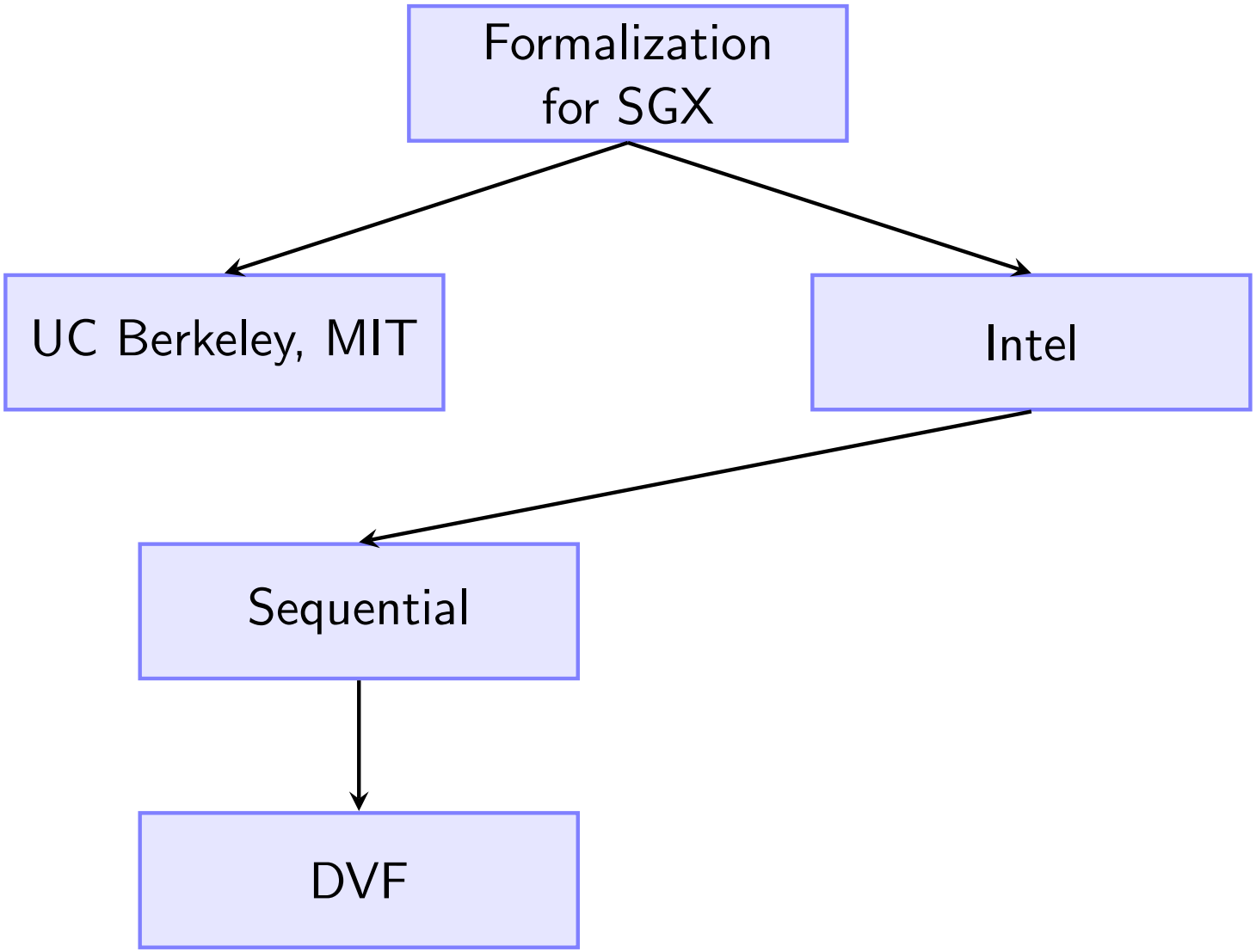
Related Work



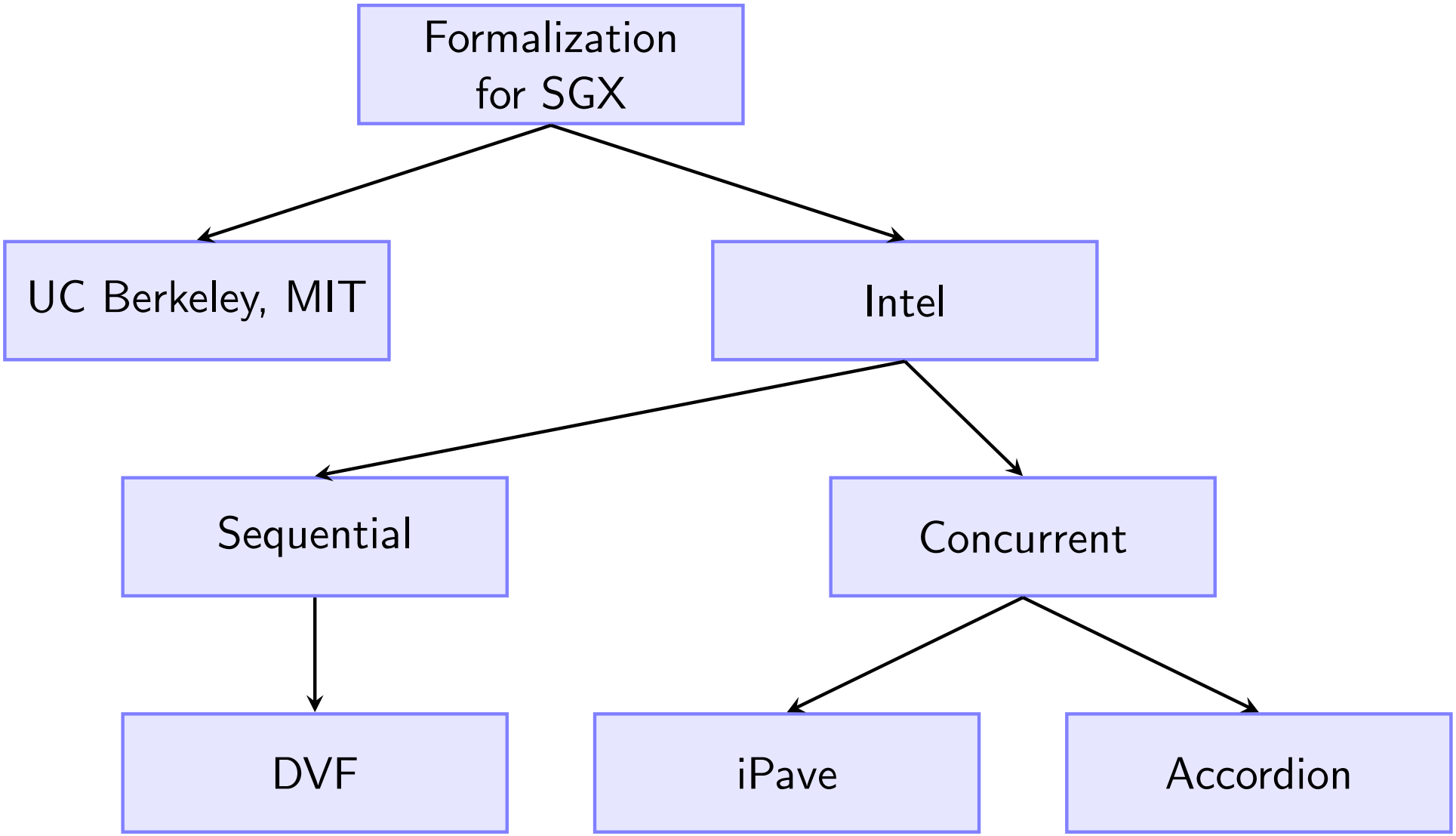
Related Work



Related Work



Related Work



Comparison with Intel's related work

Tool				
DVF[1]				
iPave[2]				
Accordion[3]				
Proposed				

[1] Amit Goel et al. "SMT-Based System Verification with DVF". In: *Satisfiability Modulo Theories*. Vol. 20. EasyChair, 2013, pp. 32–43.

[2] Ranan Fraer et al. "From visual to logical formalisms for SoC validation". In: *2014 Twelfth ACM/IEEE Conference on Formal Methods and Models for Codesign (MEMOCODE)*. ACM/IEEE. 2014, pp. 165–174.

[3] Rebekah Leslie-Hurd, Dror Caspi, and Matthew Fernandez. "Verifying linearizability of Intel® software guard extensions". In: *International Conference on Computer Aided Verification*. Springer. 2015, pp. 144–160.

Comparison with Intel's related work

Tool	Concurrency			
DVF[1]	No			
iPave[2]	Yes			
Accordion[3]	Yes			
Proposed	Yes			

[1] Goel et al., "SMT-Based System Verification with DVF".

[2] Fraer et al., "From visual to logical formalisms for SoC validation".

[3] Leslie-Hurd, Caspi, and Fernandez, "Verifying linearizability of Intel® software guard extensions".

Comparison with Intel's related work

Tool	Concurrency	Non-determinism		
DVF[1]	No	Yes		
iPave[2]	Yes	No		
Accordion[3]	Yes	No		
Proposed	Yes	Yes		

[1] Goel et al., "SMT-Based System Verification with DVF".

[2] Fraer et al., "From visual to logical formalisms for SoC validation".

[3] Leslie-Hurd, Caspi, and Fernandez, "Verifying linearizability of Intel® software guard extensions".

Comparison with Intel's related work

Tool	Concurrency	Non-determinism	Open-source	
DVF[1]	No	Yes	No	
iPave[2]	Yes	No	No	
Accordion[3]	Yes	No	No	
Proposed	Yes	Yes	Yes	

[1] Goel et al., "SMT-Based System Verification with DVF".

[2] Fraer et al., "From visual to logical formalisms for SoC validation".

[3] Leslie-Hurd, Caspi, and Fernandez, "Verifying linearizability of Intel® software guard extensions".

Comparison with Intel's related work

Tool	Concurrency	Non-determinism	Open-source	Implementation details
DVF[1]	No	Yes	No	High
iPave[2]	Yes	No	No	High
Accordion[3]	Yes	No	No	High
Proposed	Yes	Yes	Yes	Low

[1] Goel et al., "SMT-Based System Verification with DVF".

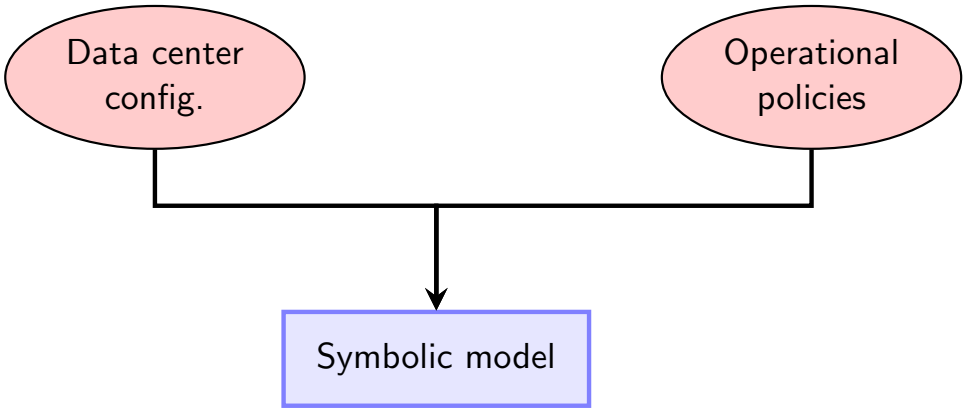
[2] Fraer et al., "From visual to logical formalisms for SoC validation".

[3] Leslie-Hurd, Caspi, and Fernandez, "Verifying linearizability of Intel® software guard extensions".

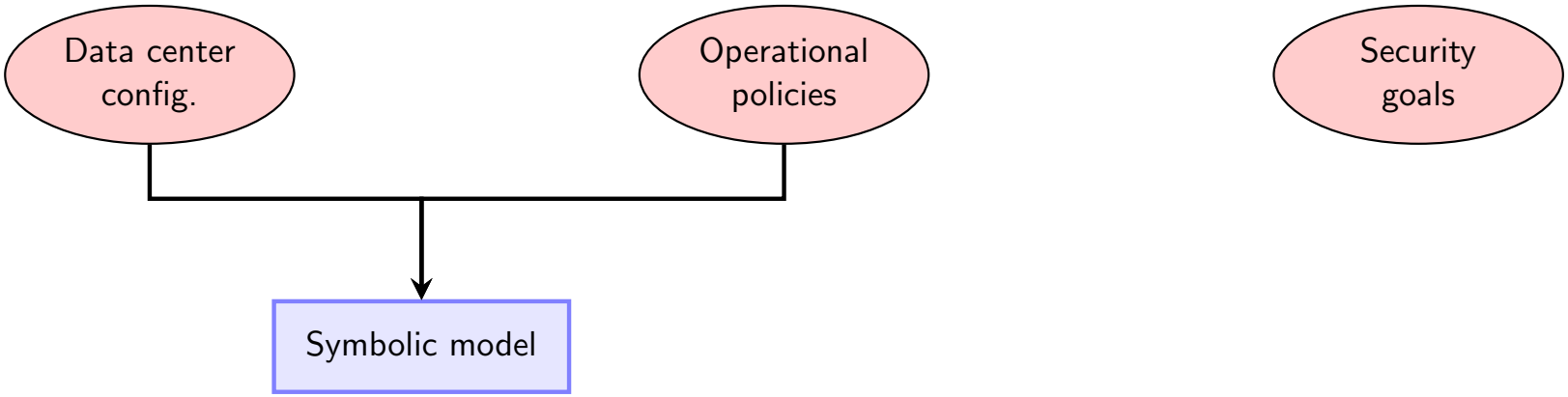
Workflow of the Proposed Approach

Workflow of the Proposed Approach

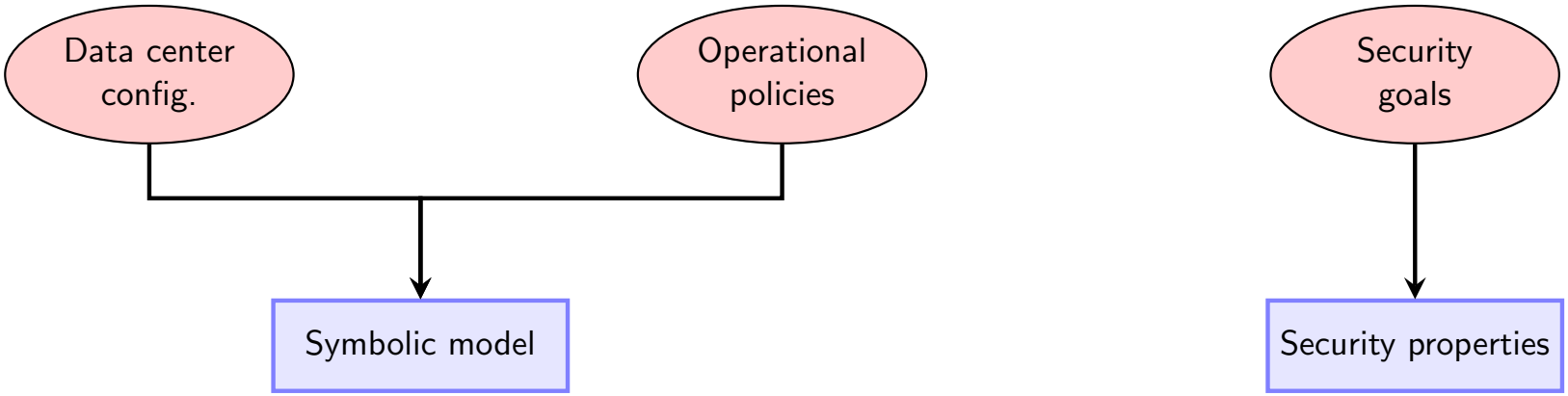
Workflow of the Proposed Approach



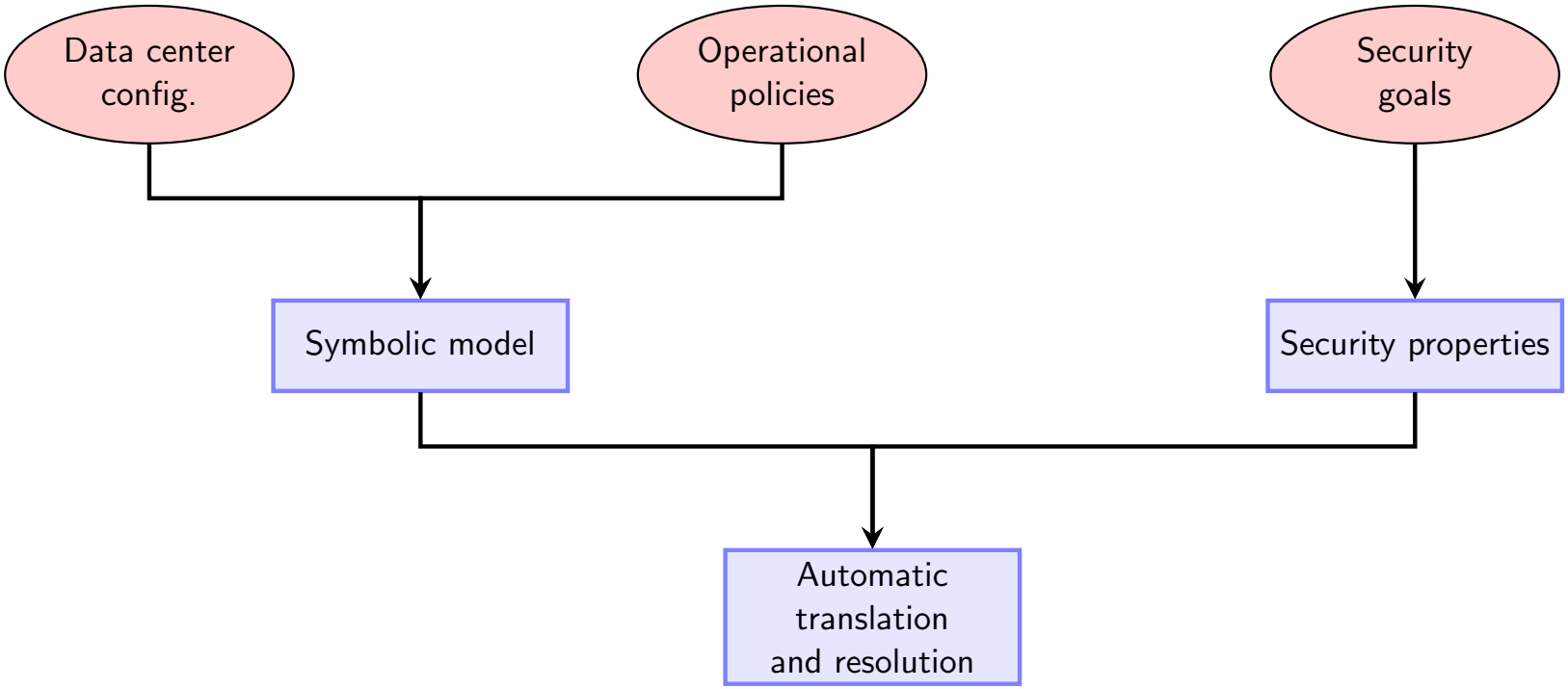
Workflow of the Proposed Approach



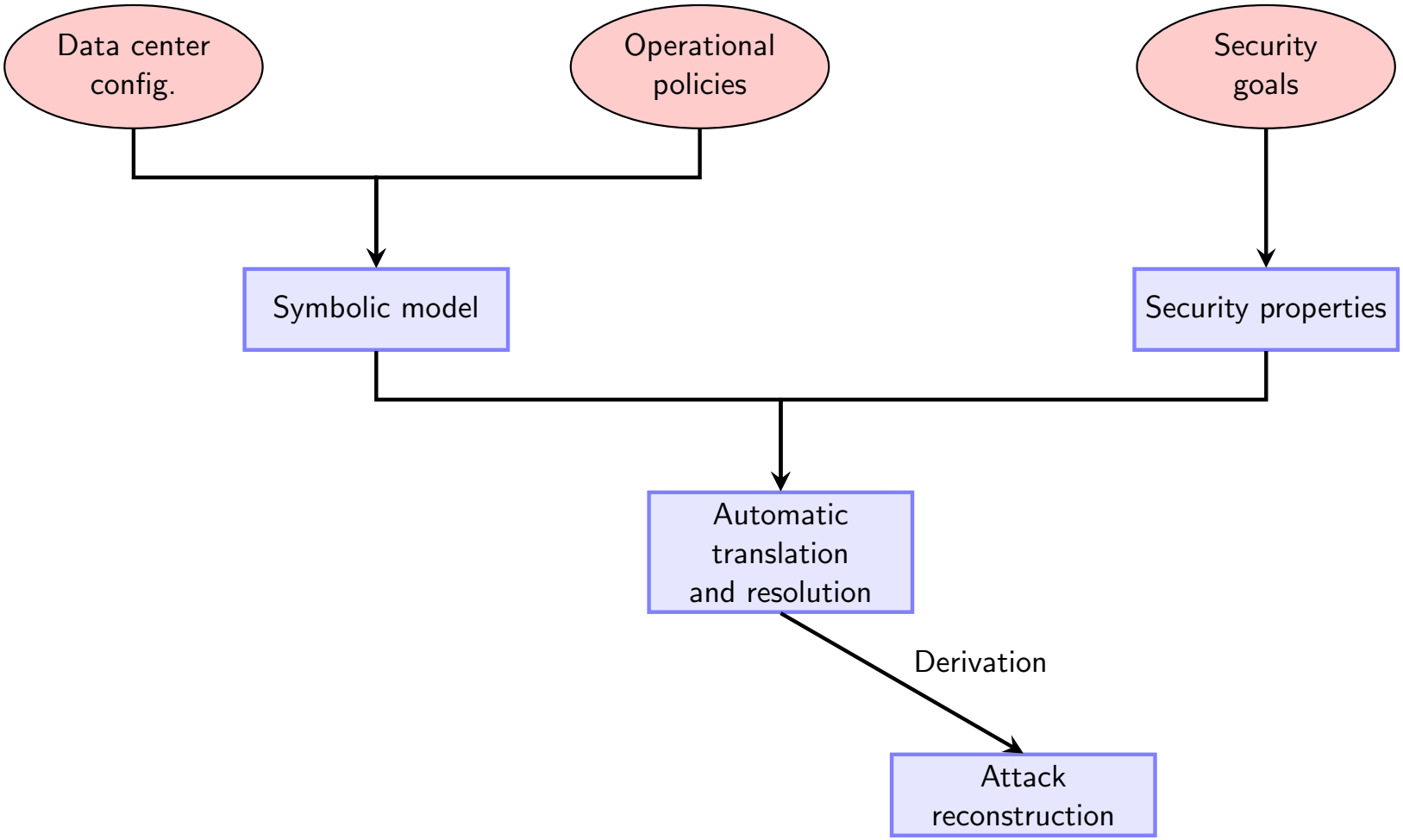
Workflow of the Proposed Approach



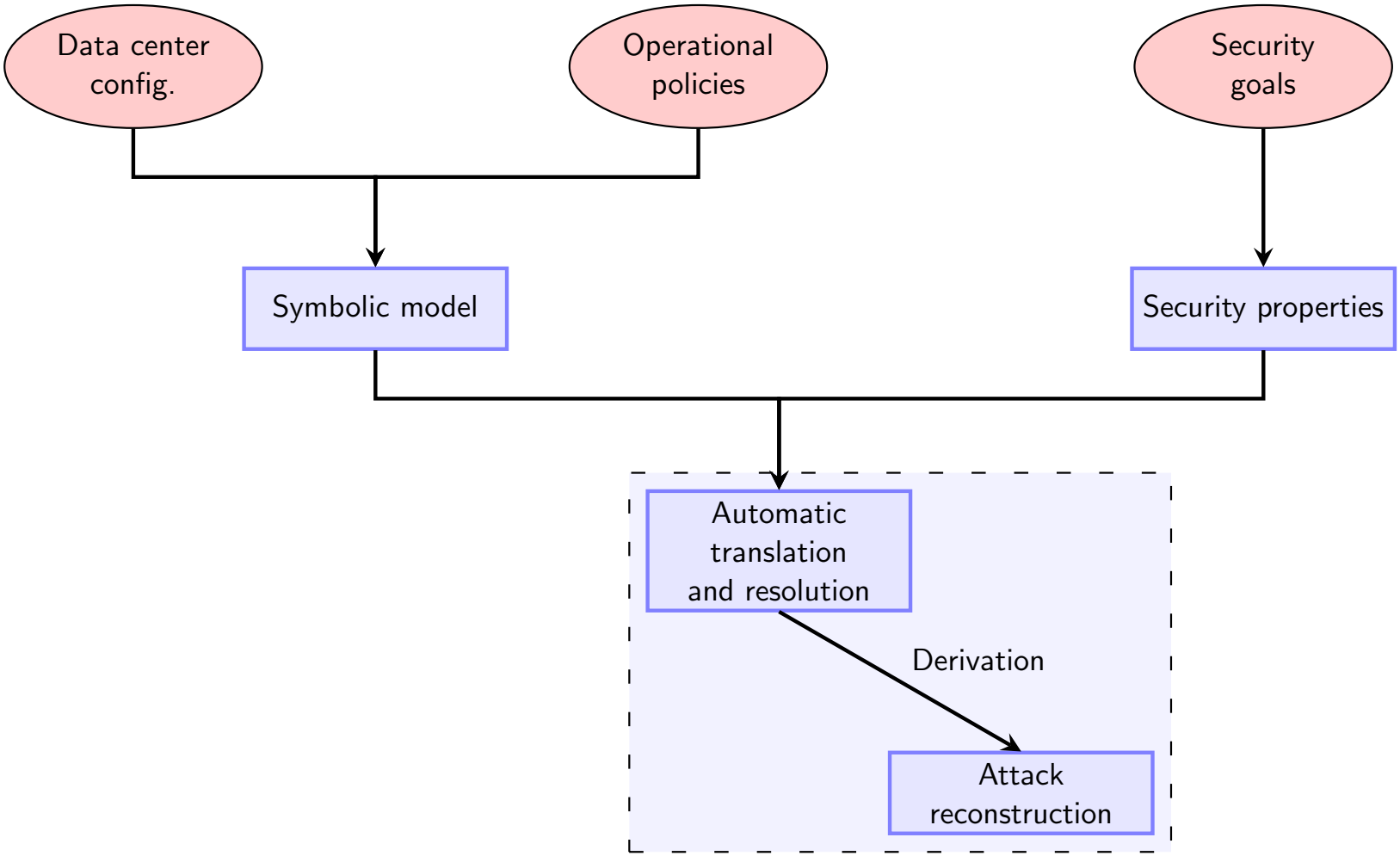
Workflow of the Proposed Approach



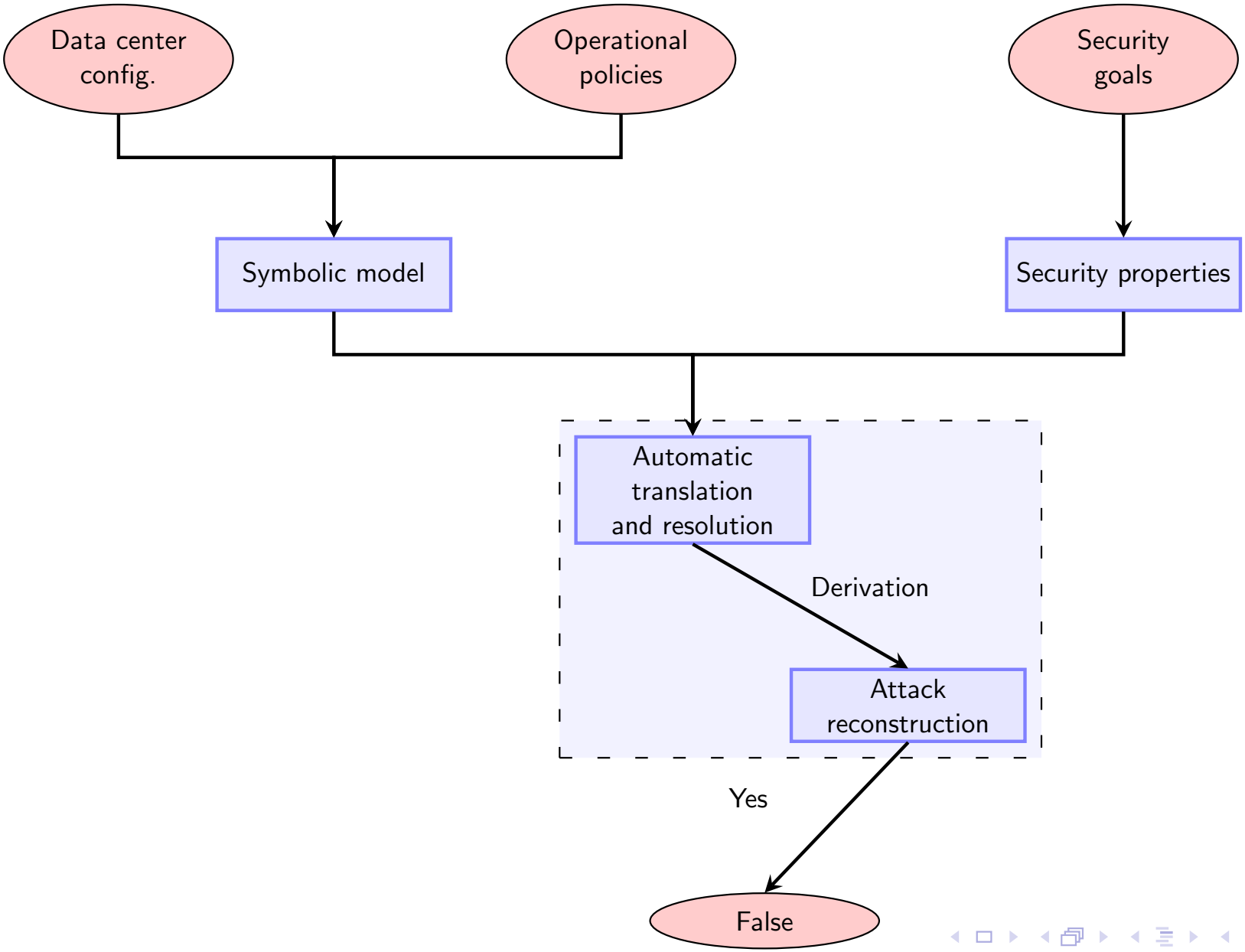
Workflow of the Proposed Approach



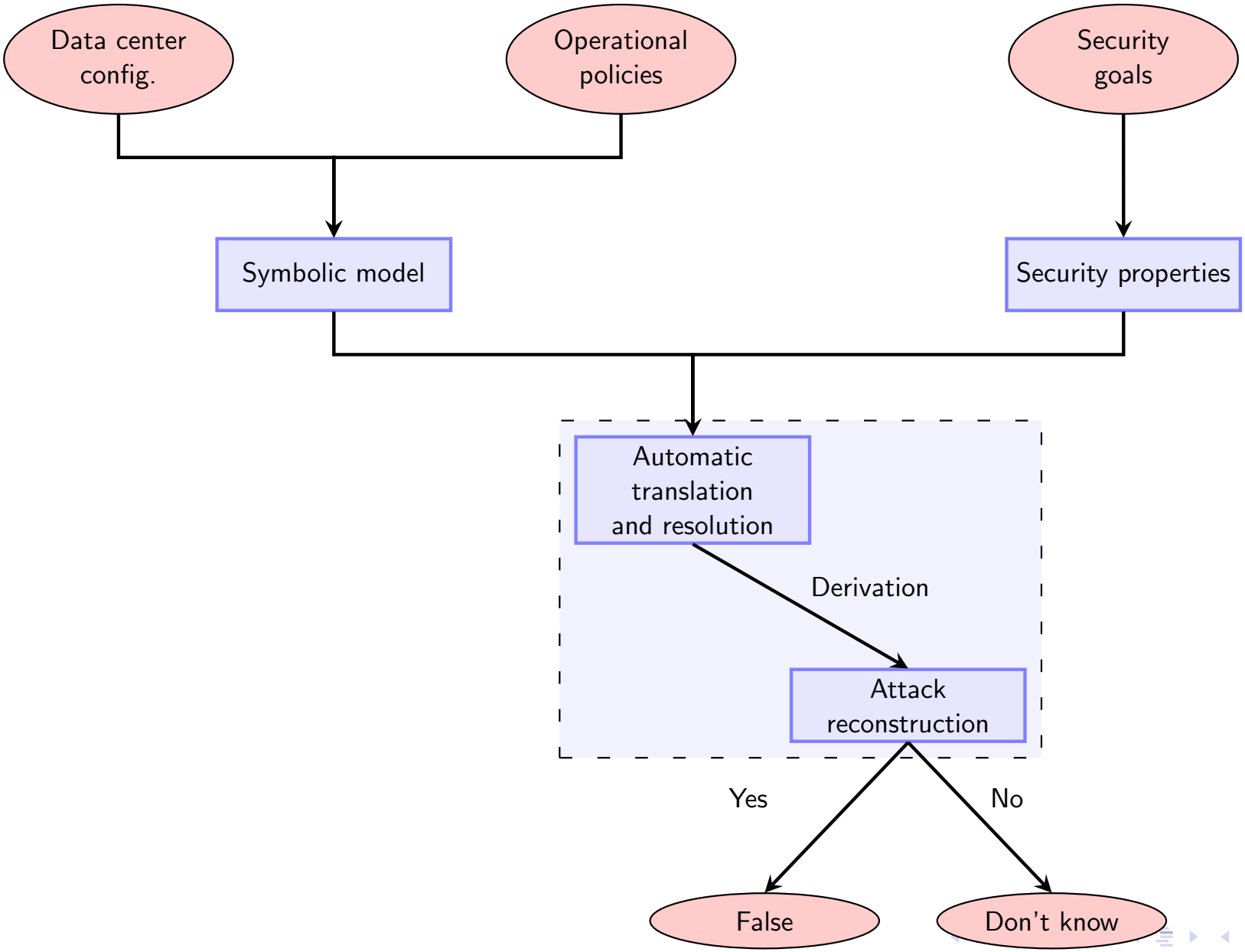
Workflow of the Proposed Approach



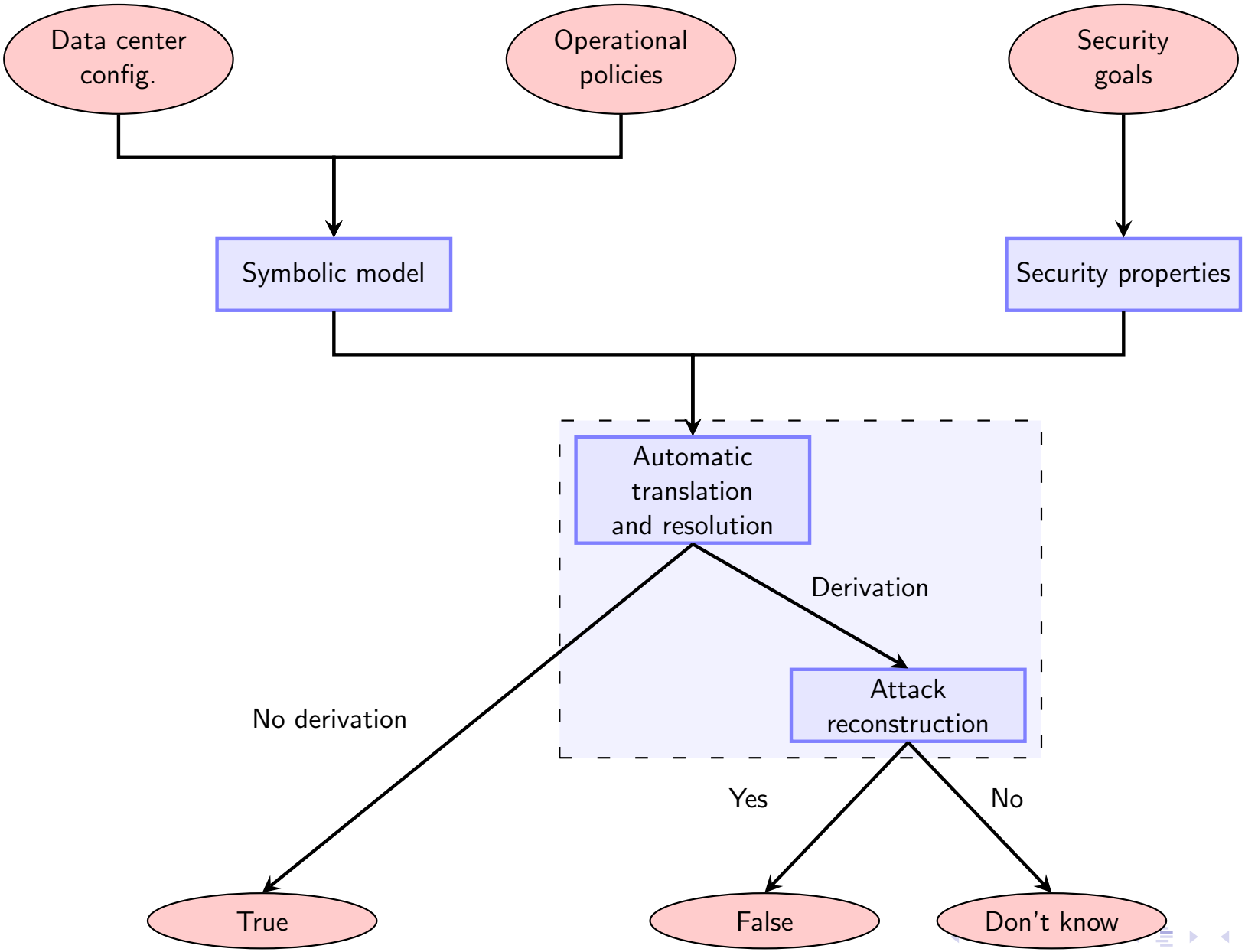
Workflow of the Proposed Approach



Workflow of the Proposed Approach



Workflow of the Proposed Approach



Symbolic Model (DCAP)

App Enclave

Symbolic Model (DCAP)

App Enclave

Application

Symbolic Model (DCAP)

App Enclave

Application

QE

Symbolic Model (DCAP)

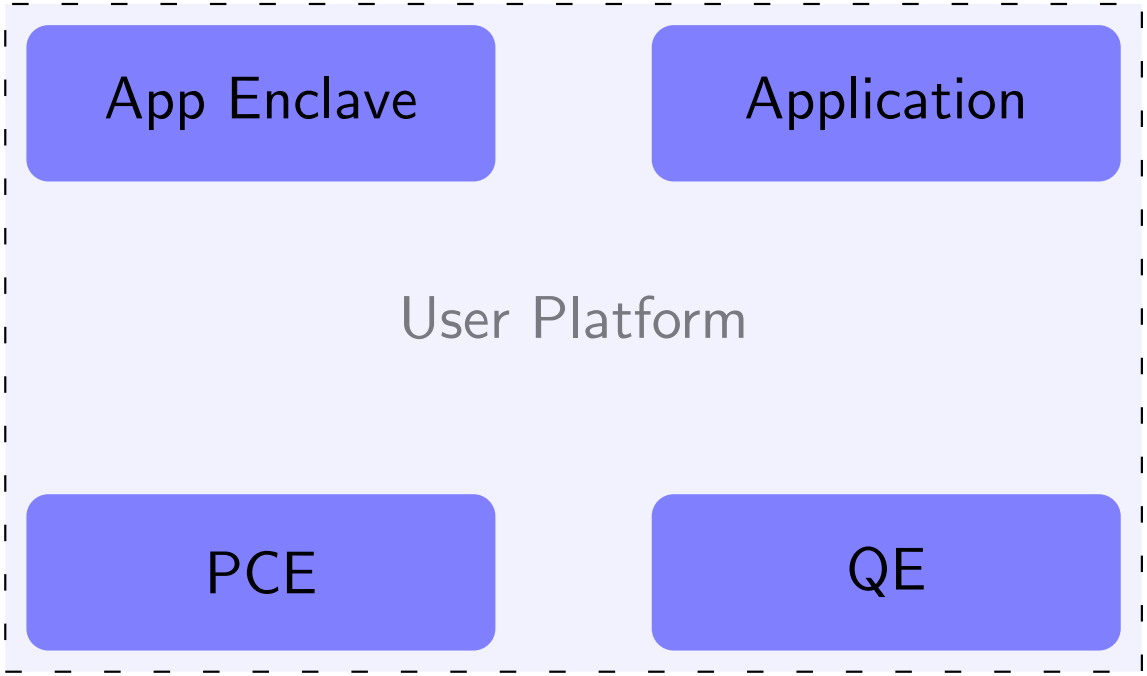
App Enclave

Application

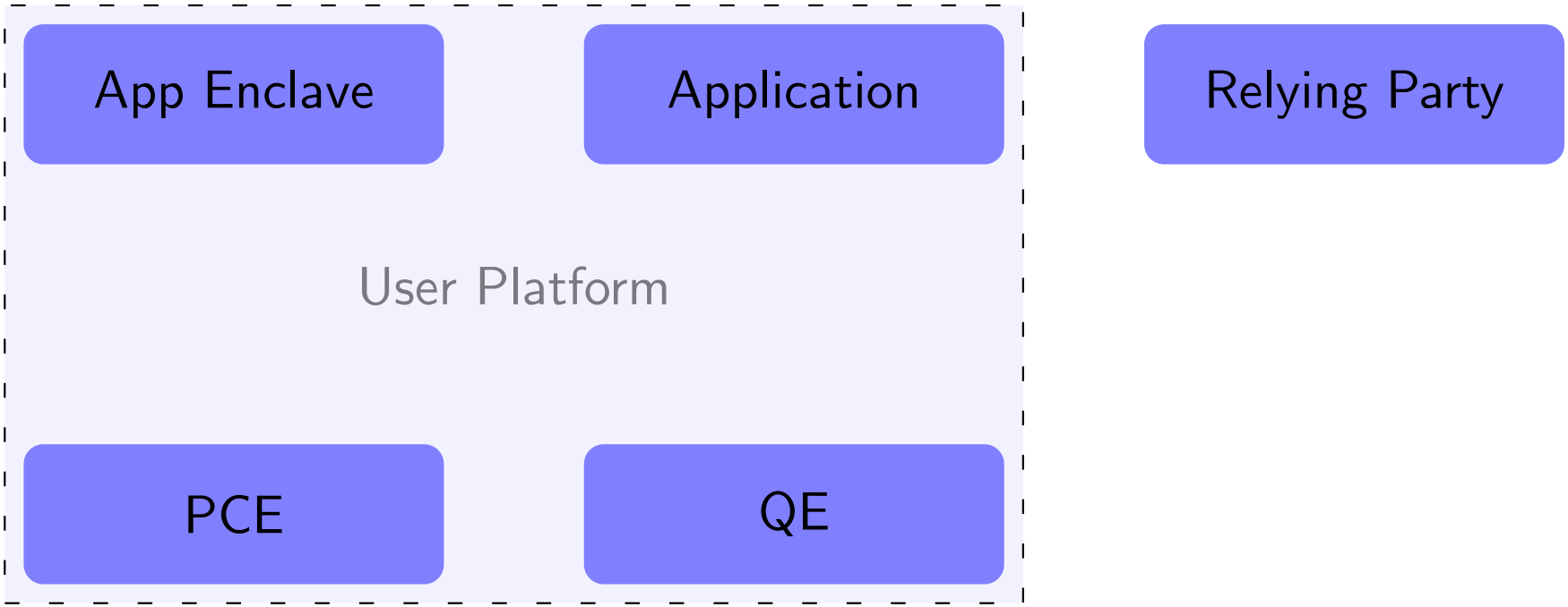
PCE

QE

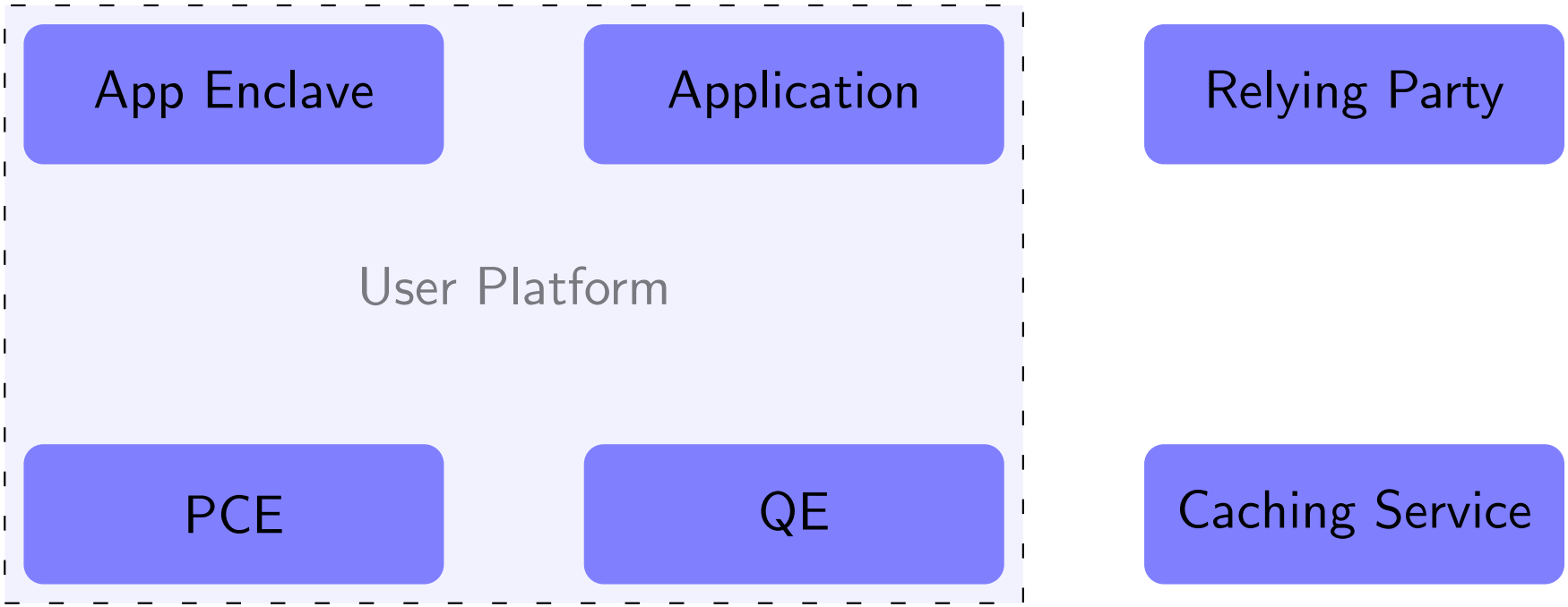
Symbolic Model (DCAP)



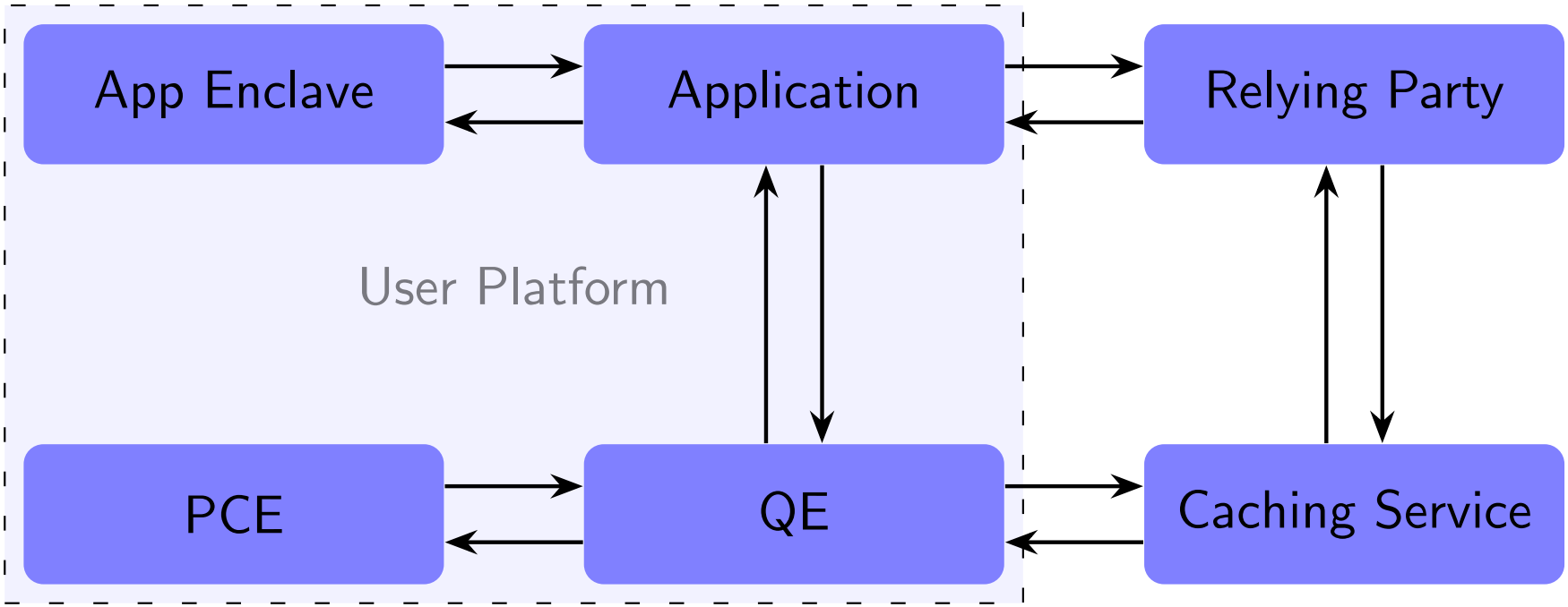
Symbolic Model (DCAP)



Symbolic Model (DCAP)



Symbolic Model (DCAP)



Challenges in Specification

- Costan and Devadas[4] claim about padding for report key derivation

[4] Victor Costan and Srinivas Devadas. "Intel SGX Explained". In: *IACR Cryptology ePrint Archive*. https://www.semanticscholar.org/paper/Intel-SGX-Explained-Costan-Devadas/a42e086f2382d518a0213879050e344539c2bcfa. 2016, pp. 83–85.

Challenges in Specification

- Costan and Devadas[4] claim about padding for report key derivation
  - EREPORT instruction → Hard-coded

[4] Costan and Devadas, "Intel SGX Explained".

Challenges in Specification

- Costan and Devadas[4] claim about padding for report key derivation
  - EREPORT instruction → Hard-coded
  - EGETKEY instruction → SECS

[4] Costan and Devadas, "Intel SGX Explained".

Challenges in Specification

- Costan and Devadas[4] claim about padding for report key derivation
  - EREPORT instruction → Hard-coded
  - EGETKEY instruction → SECS
  - In fact, the reverse![5]

[4] Costan and Devadas, "Intel SGX Explained".

[5] Intel. "Intel® 64 and IA-32 Architectures: Software Developer's Manual". In: https://software.intel.com/sites/default/files/managed/39/c5/325462-sdm-vol-1-2abcd-3abcd.pdf. Oct. 2019.

Challenges in Specification

- Costan and Devadas[4] claim about padding for report key derivation
  - EREPORT instruction → Hard-coded
  - EGETKEY instruction → SECS
  - In fact, the reverse![5]
- Ambiguous statements, such as "The QE Report is a report when the QE Report is certified."[6]

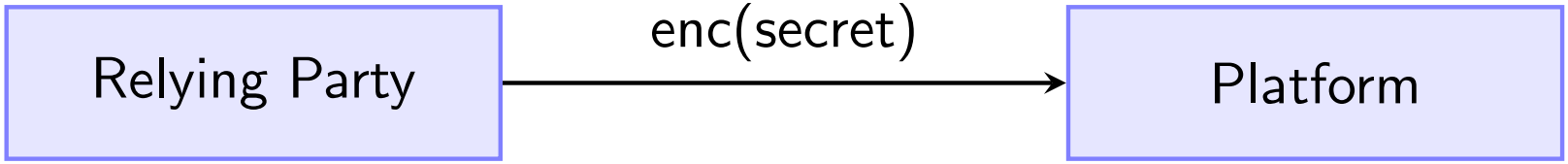
[4] Costan and Devadas, "Intel SGX Explained".

[5] Intel, "Intel® 64 and IA-32 Architectures: Software Developer's Manual".

[6] Intel. *Intel® Software Guard Extensions (Intel® SGX) Data Center Attestation Primitives: ECDSA Quote Library API*. Revision March 2020, updated 08-07-2020, last accessed on 07-08-2020. URL: https://download.01.org/intel-sgx/sgx-dcap/1.7/linux/docs/Intel_SGX_ECDSA_QuoteLibReference_DCAP_API.pdf.

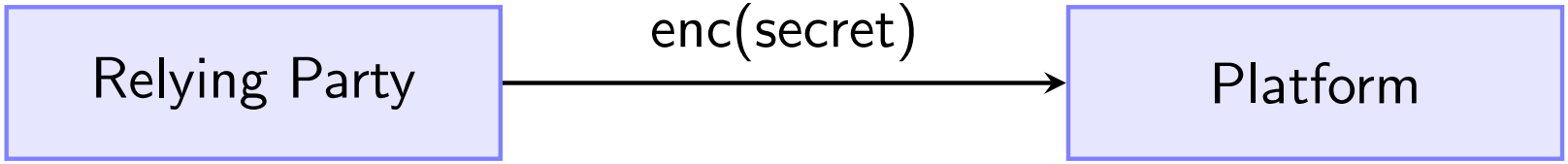
Specification of Security Goals

- Confidentiality



Specification of Security Goals

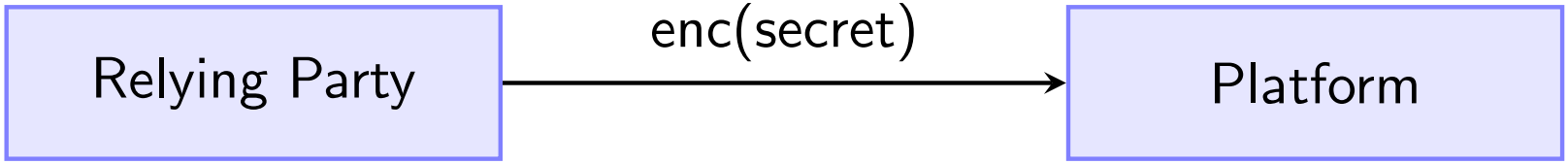
- Confidentiality



  - Formalized as a reachability property

Specification of Security Goals

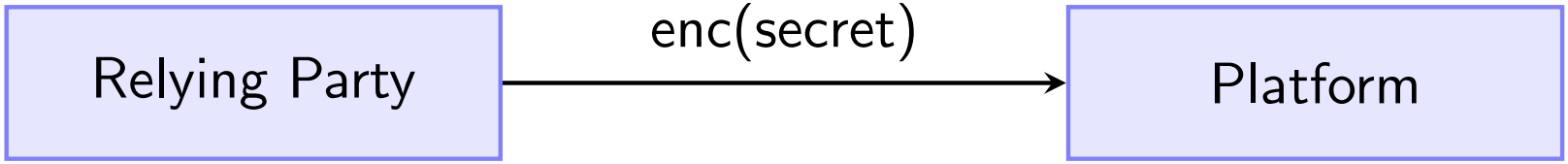
- Confidentiality



  - Formalized as a reachability property
- Integrity

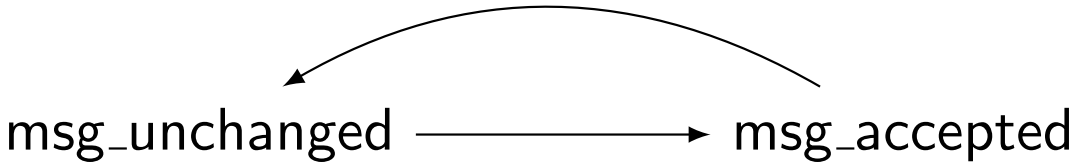
Specification of Security Goals

- Confidentiality



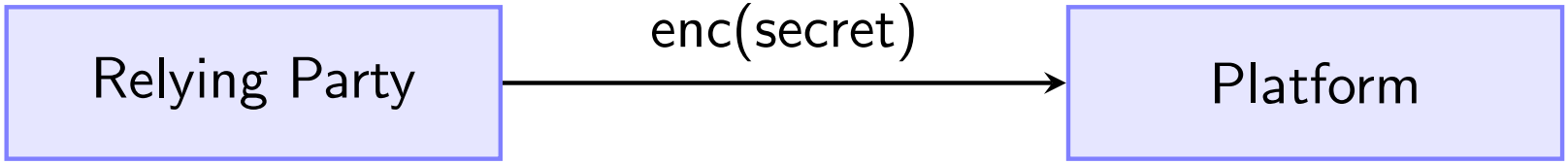
  - Formalized as a reachability property

- Integrity



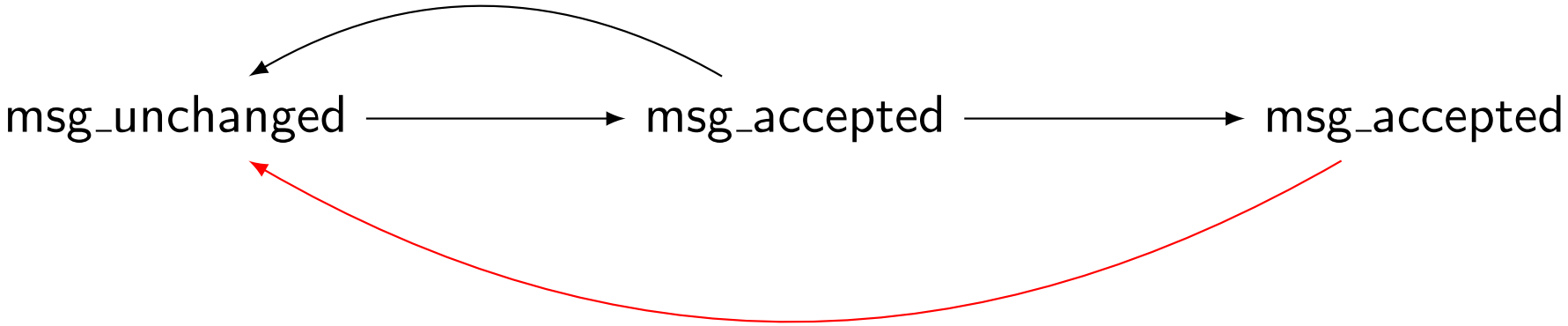
Specification of Security Goals

- Confidentiality



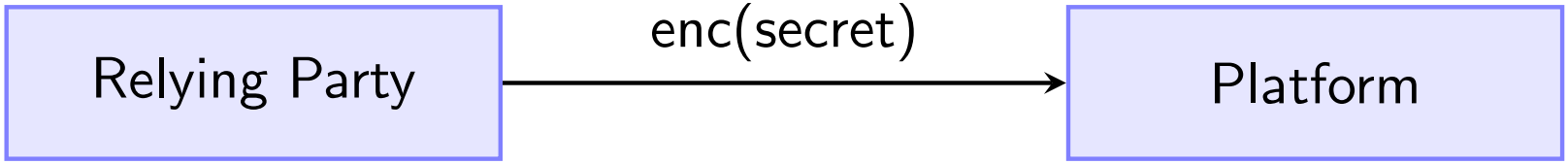
  - Formalized as a reachability property

- Integrity



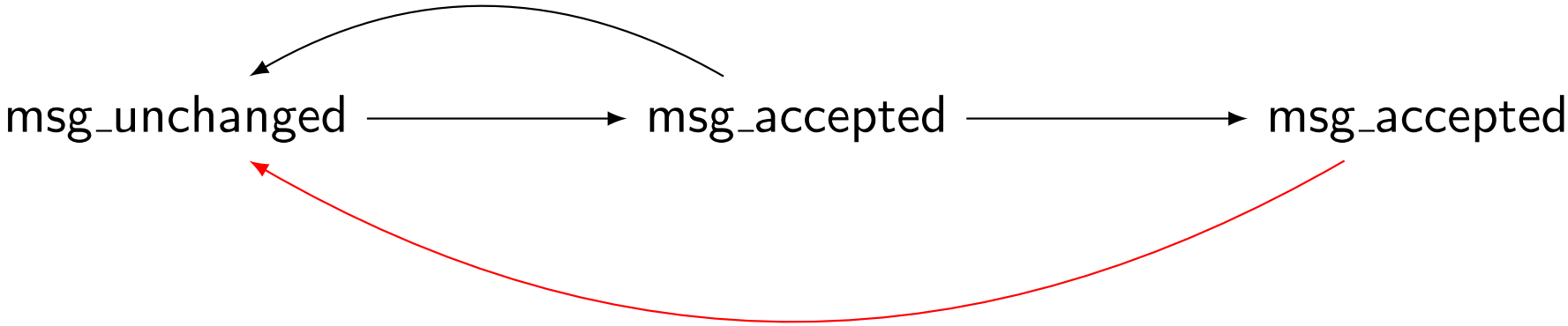
Specification of Security Goals

- Confidentiality



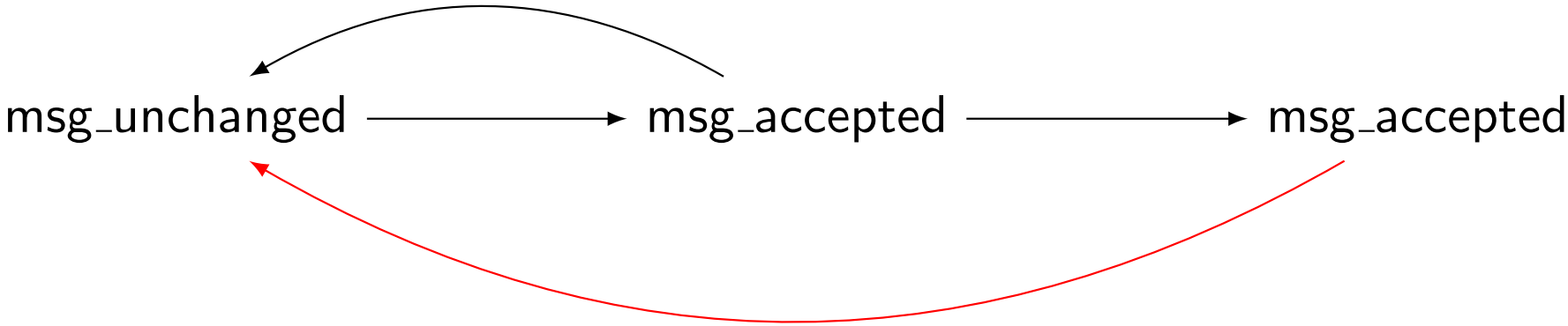
  - Formalized as a reachability property

- Integrity

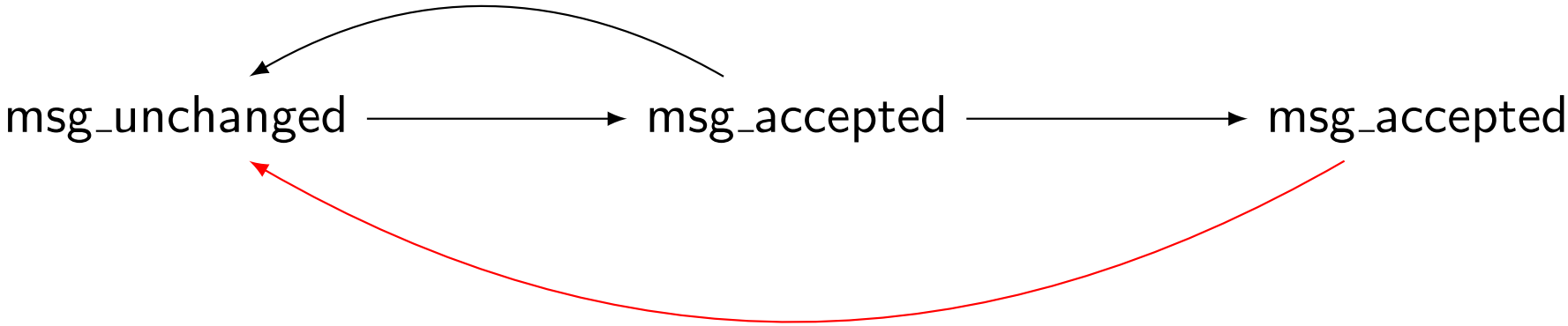


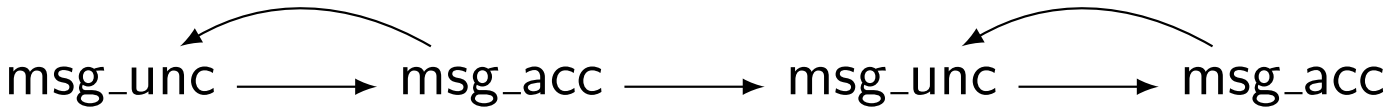
  - Correspondence assertions

Integrity

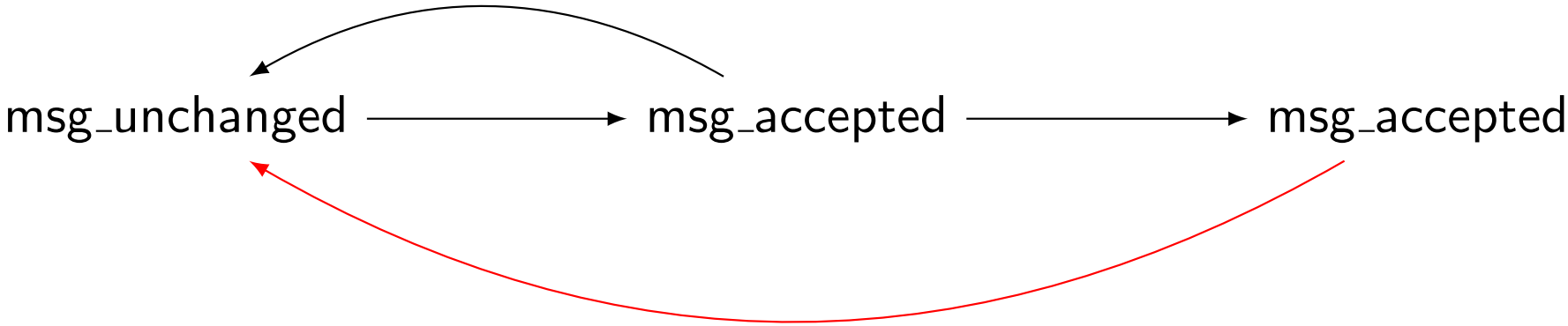


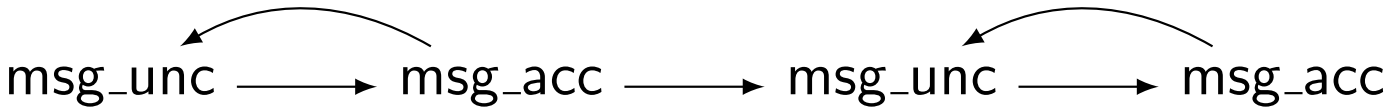
Integrity


msg_unchanged
msg_accepted
msg_accepted


msg_unc
msg_acc
msg_unc
msg_acc

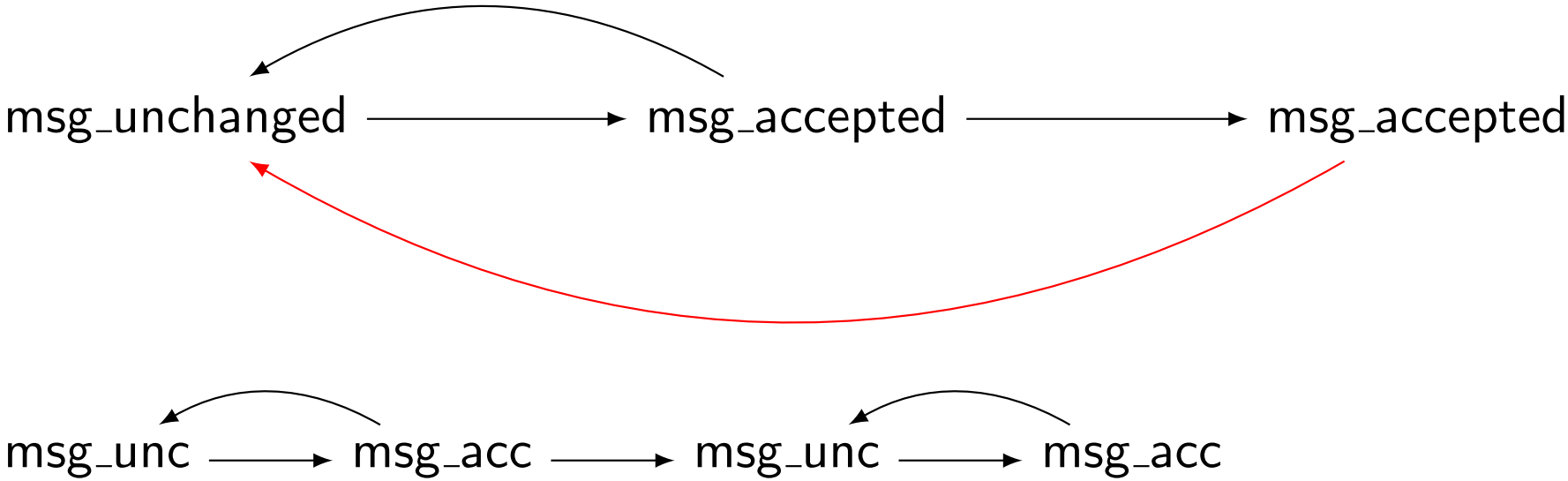
Integrity





- Injective correspondence assertions

Integrity



- Injective correspondence assertions
- Additional check: Reachability of `msg_accepted`

Summary and Future Work

- Specification of Intel SGX DCAP

Summary and Future Work

- Specification of Intel SGX DCAP
- Discovery of various discrepancies

Summary and Future Work

- Specification of Intel SGX DCAP
- Discovery of various discrepancies
- Confidentiality and Integrity

Summary and Future Work

- Specification of Intel SGX DCAP
- Discovery of various discrepancies
- Confidentiality and Integrity
- Future work:

Summary and Future Work

- Specification of Intel SGX DCAP
- Discovery of various discrepancies
- Confidentiality and Integrity
- Future work:
  - Consider side-channels

Summary and Future Work

- Specification of Intel SGX DCAP
- Discovery of various discrepancies
- Confidentiality and Integrity
- Future work:
  - Consider side-channels
  - Other TEEs (e.g., ARM TrustZone)

Key References

Costan, Victor and Srinivas Devadas. "Intel SGX Explained". In: *IACR Cryptology ePrint Archive*. https://www.semanticscholar.org/paper/Intel-SGX-Explained-Costan-Devadas/a42e086f2382d518a0213879050e344539c2bcfa. 2016, pp. 83–85.

Fraer, Ranan et al. "From visual to logical formalisms for SoC validation". In: *2014 Twelfth ACM/IEEE Conference on Formal Methods and Models for Codesign (MEMOCODE)*. ACM/IEEE. 2014, pp. 165–174.

Goel, Amit et al. "SMT-Based System Verification with DVF". In: *Satisfiability Modulo Theories*. Vol. 20. EasyChair, 2013, pp. 32–43.

Intel. "Intel® 64 and IA-32 Architectures: Software Developer's Manual". In: https://software.intel.com/sites/default/files/managed/39/c5/325462-sdm-vol-1-2abcd-3abcd.pdf. Oct. 2019.

— .*Intel®Software Guard Extensions (Intel®SGX) Data Center Attestation Primitives: ECDSA Quote Library API*. Revision March 2020, updated 08-07-2020, last accessed on 07-08-2020. URL: https://download.01.org/intel-sgx/sgx-dcap/1.7/linux/docs/Intel_SGX_ECDSA_QuoteLibReference_DCAP_API.pdf.

Leslie-Hurd, Rebekah, Dror Caspi, and Matthew Fernandez. "Verifying linearizability of Intel® software guard extensions". In: *International Conference on Computer Aided Verification*. Springer. 2015, pp. 144–160.

Thank You for Your Attention!

Questions and Comments?

Project updates here

Email: muhammad_usama.sardar@mailbox.tu-dresden.de