61 THE CHIPS TO SYSTEMS CONFERENCE

SHAPING THE NEXT GENERATION OF ELECTRONICS

JUNE 23-27, 2024

MOSCONE WEST CENTER
SAN FRANCISCO, CA, USA

61 THE CHIPS TO SYSTEMS CONFERENCE
SHAPING THE NEXT GENERATION OF ELECTRONICS
JUNE 23-27, 2024
MOSCONE WEST CENTER
SAN FRANCISCO, CA, USA

Formal System-in-Package Security Architecture

Speakers: Sylvain Guilley (Secure-IC) & Junie Um (Cadence Design Systems)

Venue: DAC 2025

Benefits of chiplet paradigm

- **Increased yield**: Chiplets are less prone to manufacturing defects due to smaller die size and better wafer utilization at the edges thereby increasing the number of known good die available.
- **Less over-specification and/or better fit to purpose**: Chiplets reduce costs by enabling mixing and matching of dies from leading and mature nodes.
- **Improved performance**: Chiplets are optimized for specific tasks, bringing about performance improvements above and beyond traditional processing gains. For example, integrated photonics in a multi-die package have been shown to provide 20 times the bandwidth density at half the cost and power consumption.
- **Increased chip area**: Maximum size of a chip is typically limited by the reticle size. Chiplets bypass this limit by reducing die sizes relative to monolithic designs.
- **Less power consumption**: Chiplets also reduce power requirements by shortening interconnection distance between chips and decreasing power lost through data transfer.
- **More flexible product development**: Modularity allows nimbler adjustments to their product portfolios and re-use of existing designs for new use cases. It also de-risks sophisticated SoC development by shortening the design time and enabling greater confidence in hitting application specs. In other words, the increased modularity makes companies more adept at meeting specific requirements of applications.

Works only if the chiplets within the system-in-package is secure!

Security features for chiplets

Compared to monolithic SoC, disaggregated SiP requires trustworthiness of any chiplet, which are of different provenance.

Important chiplet-level security features:

- **`[SiP secure boot]`** Verifying that the SiP is made up of secure chiplets:
  - It is the extension of the secure boot from chip(let)s to SiP
  - It can be seen as the verification of the **H**ardware **B**ill **o**f **M**aterial (**HBOM**)
- **`[SiP SBOM remote attestation]`** Verifying that the **S**oftware **B**ill **o**f **M**aterial (**SBOM**) is genuine and at correct version:
  - It is the distributed attestation, aggregated for reporting to the SiP owner
  - Optionally, extend what is checked to encompass also config data (e.g., PLL) and trimming values

`[SiP secure boot]`

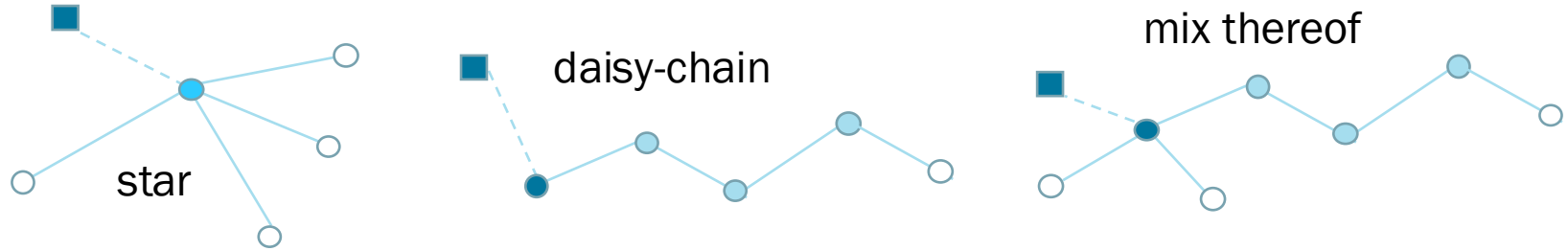
- Ensure the properties that:
  - Each chiplet boots properly
  - The inventory is correct, based on an ad hoc PKI
- Is a service required by NIST FIPS 140-3

`[SiP SBOM remote attestation]`

- On top of **`[SiP secure boot]`**
- Allows to verify that firmware has not been tampered with
- Is a requirement by EU CRA / CC ALC_FLR

Topology for SiP secure boot & SiP SBOM remote attestation

- There is usually one distinguished chiplet, termed the *base system chiplet*
  - ARM **C**hiplet **S**ystem **A**rchitecture (**CSA**) names it « Primary Trusted Security Agent »
- The order of HBOM and SBOM verifications can be varied



Topology caption:

- host
- base system chiplet
- intermediate chiplets
- leaf chiplets

Example of pairing protocols	Example of distributed attestation protocols
USB	TCG DICE
Bluetooth	IETF EAT (draft-ietf-rats-eat-11) / PSA attestation certified API
etc.	etc.

- Asymmetric cryptography is favored to avoid systemic attacks
  - Each entity has its own private / public key pair

Chiplet lifecycle, incl. security

provisioning & manufacturing

mission mode

Chiplets secure pre-provisioning (standalone) in SiP

- `InitSecurityCfg`
- *Copy FW*

Chiplet enrollment (initiated by Master) of every chiplet

- `CreateEK`
- `CreateSRK`

SiP enrollment/registration #1

- *Master reads all chiplets EK* (`ReadPubEK`)

SiP enrollment/registration #2

- Master stores within itself PK of each slave

Chiplet control sequence broadcast

- Chiplets enrollment is closed (configuration lock)
- Master announces operational control sequence to slave chiplets

Chiplets ready

- Authorization control sequence of every chiplet is known depending upon connection topology (central RoT or next-in-command)

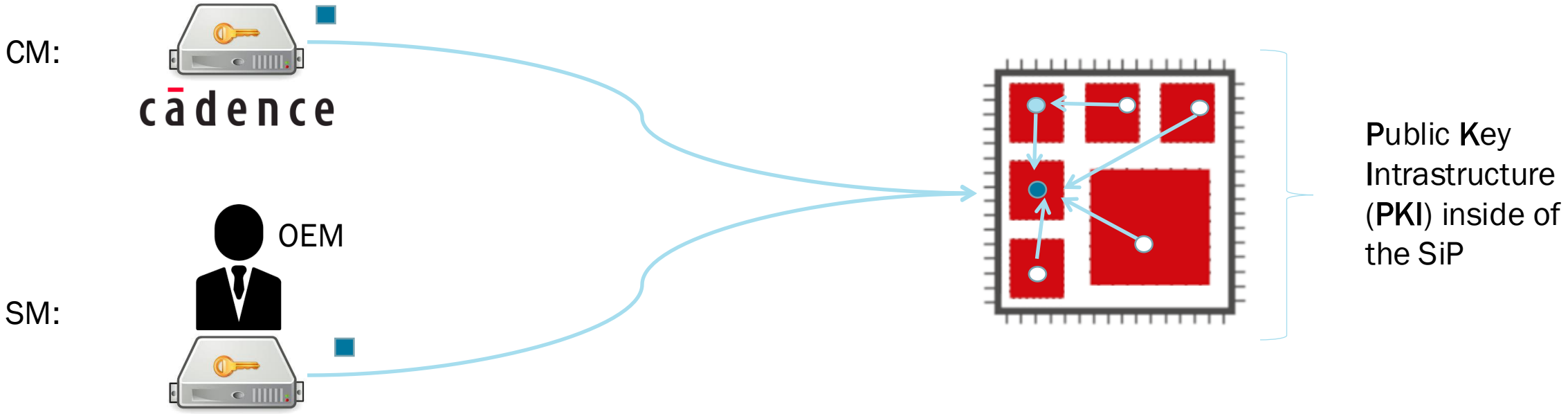
Chiplets verify

- Chiplets authenticate based on control sequence from either the RoT or next-in-command
- Only following authentication, FW remote attestation is carried out

Part of a draft **C**ommon **C**riteria (**CC**) **P**rotection **P**rofile (**PP**) we are preparing

SIP_VERIFY: Verification of HBOM and SBOM

- **Roles:**
  - Chip Manufacturer (CM): performs hierarchical HBOM inventory
  - System Manufacturer (SM): ensures that each chip can duly authenticate it(s) surrogate(s)
- **Both verifications are reported:**



- **Conclusion:**
  - Cadence / Secure-IC architecture, enables recreation of a RoT at SiP level
  - Our lifecycle management is generic / agnostic, hence adapts to Customer constraints