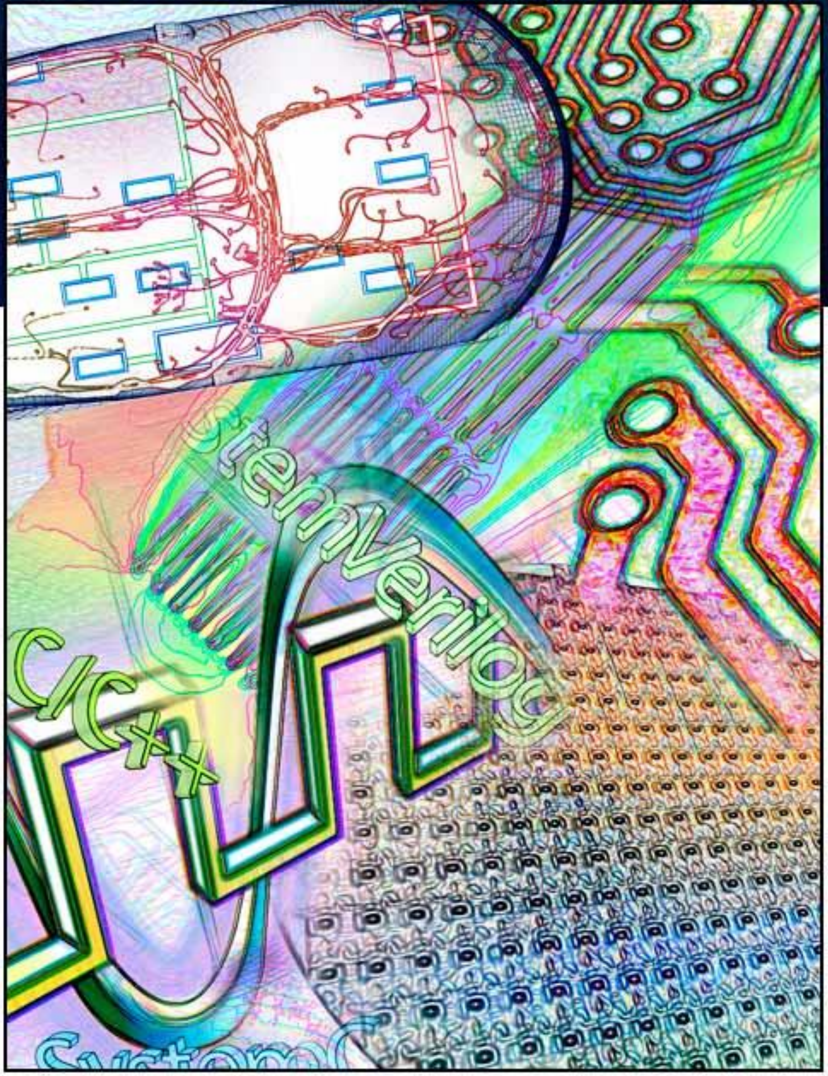


In Pursuit of Secure Silicon

Serge Leef

VP, New Ventures Division

Mentor Graphics Corporation

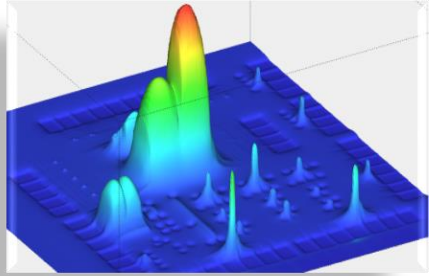
February 2017 – Version 1.0

Why is “Secure Silicon” an EDA problem?

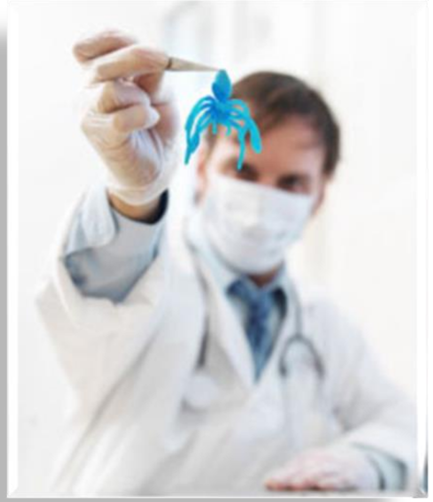
- Expertise in design tools, IP and methodologies
- Relationships with SoC and ASIC design communities
- Strong connections and process integration with silicon foundries
- Ability to interact with manufacturing and test equipment
- Willingness to leverage external inventions and innovations
- Sales channel capable of reaching all value chain participants
- Most important: EDA flow integration

- EDA companies are in a good position to make technical progress

Opportunities considered and rejected



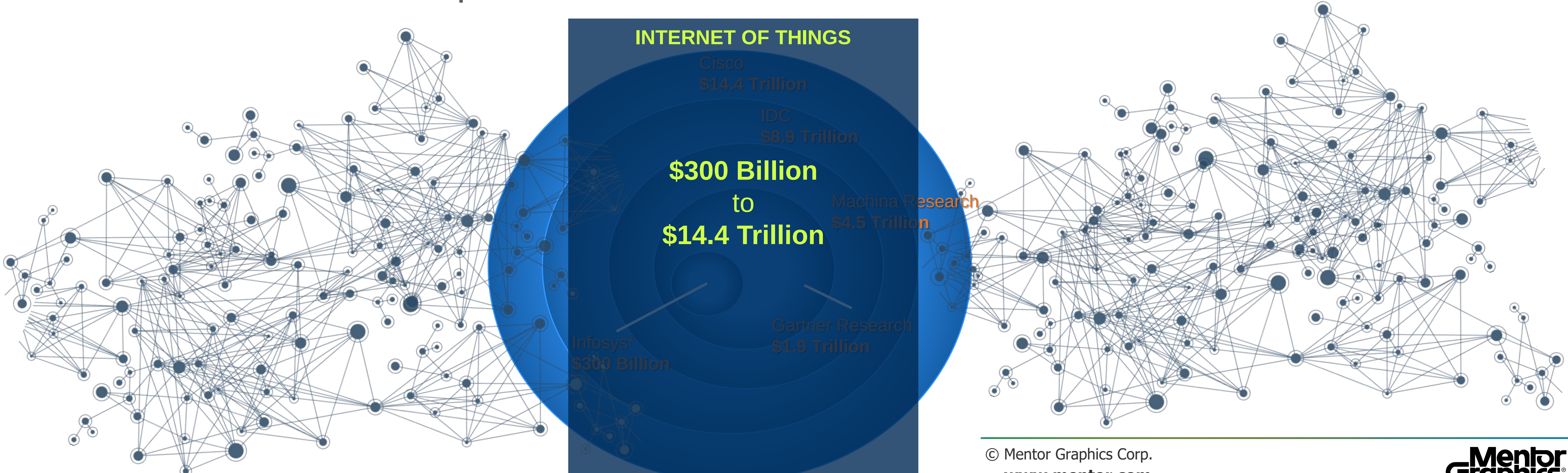
- **Side channel attacks – small, services oriented market**
  - Targeted devices: smart cards and set top boxes
  - Defensive strategies are well-understood
    - Incorporate randomness into cryptography
    - Use fixed-time algorithms to reduce data-related timing signatures
    - Camouflage structures to make relevant portions harder to find
  - Mostly services with estimated revenues of sub $50M



- **Hardware Trojans – no visible demand for a solution**
  - Trojan detection during design is a HARD problem
    - Search for unknown-unknowns
    - Trojan circuits look just like normal hardware
    - Further obfuscation occurs during synthesis
    - Low probability triggers can be hidden in the finite state machines
  - Most viable defense strategies are around “IP Protection”
  - Some level of run-time detection is possible

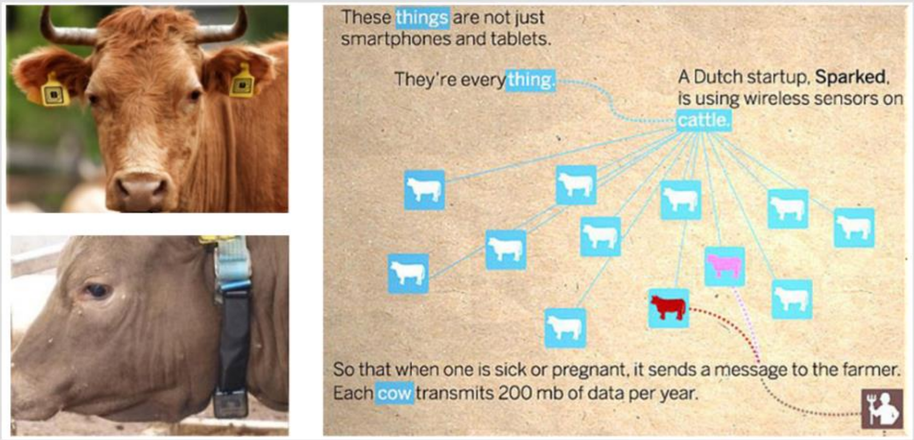
Commercial world of chip security

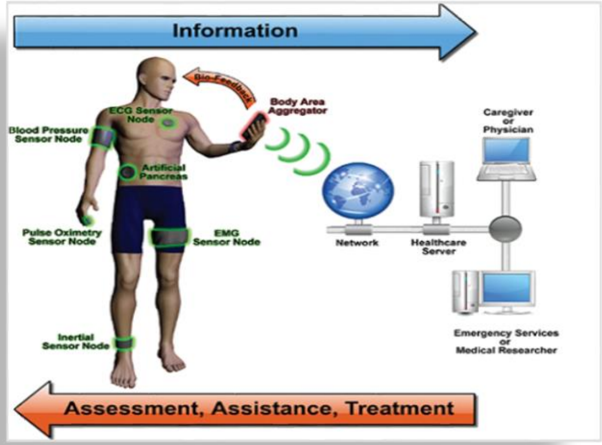
- Current activity is driven by the need to protect against economic damage in **banking** and **broadcast** application spaces
- New drivers will be related to deployment of 55B IoT edge nodes, some of which will have sufficient exposure to economic losses to warrant search for solutions

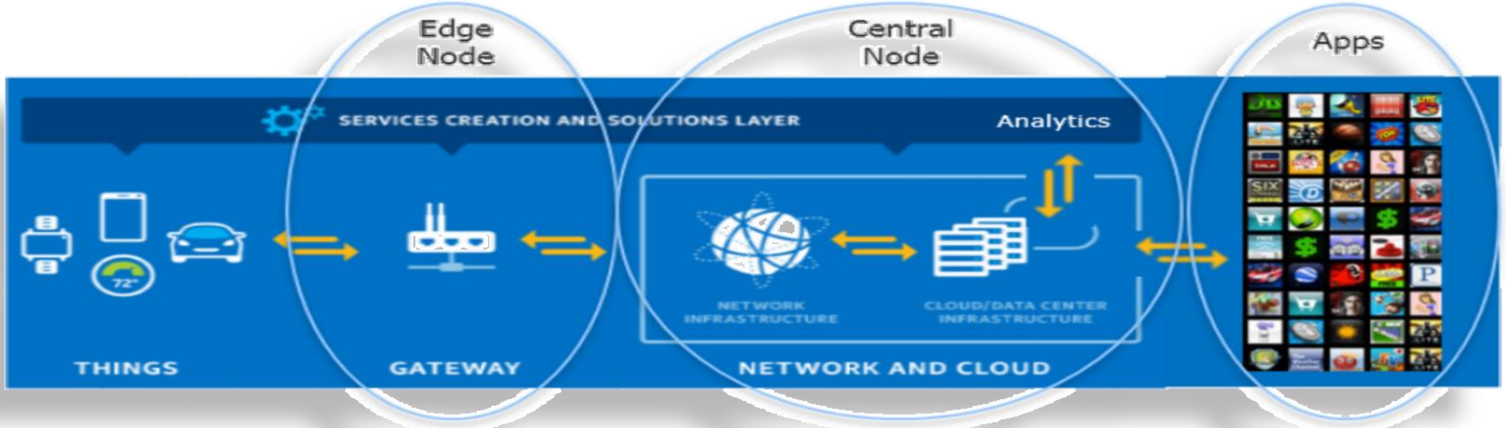


Which IoT applications warrant investment in secure chips?

It will be dictated by economics of E2E application security





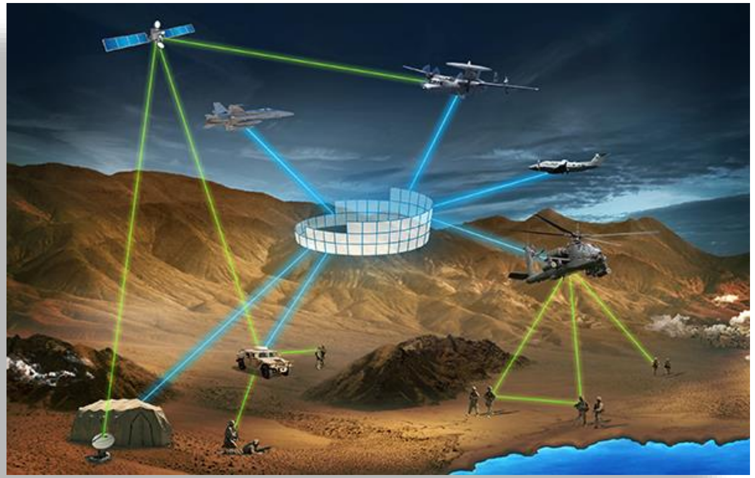


Key factors that drove demand in banking and broadcast:

- Loss of revenue
- Liability exposure

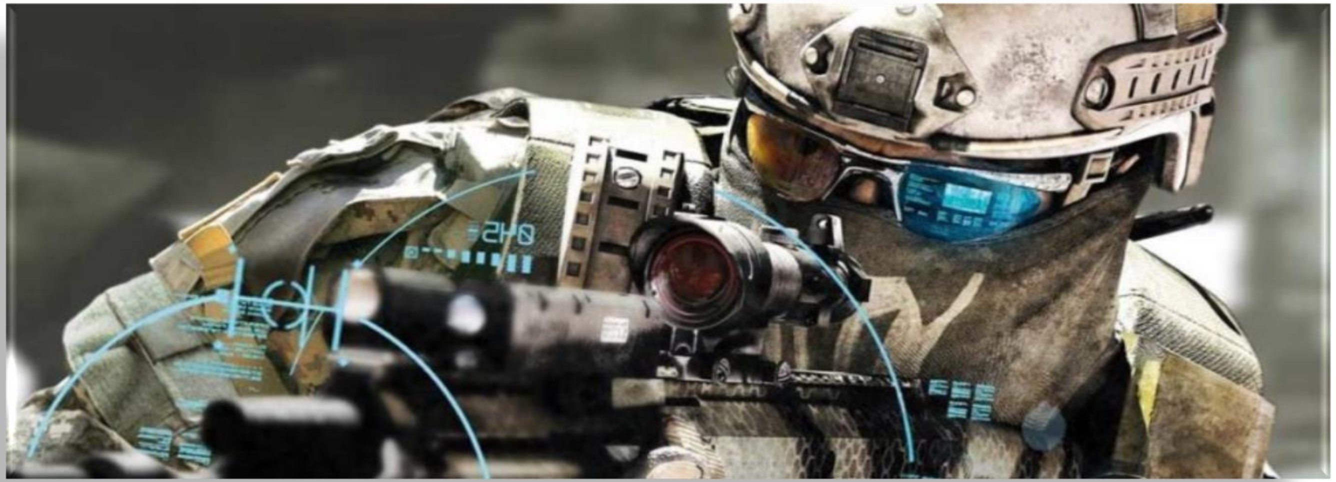
Which National Security applications warrant investment in secure chips? *All of them?*

Source: Orbital ATK



Source: internet

Source: LucasFilm

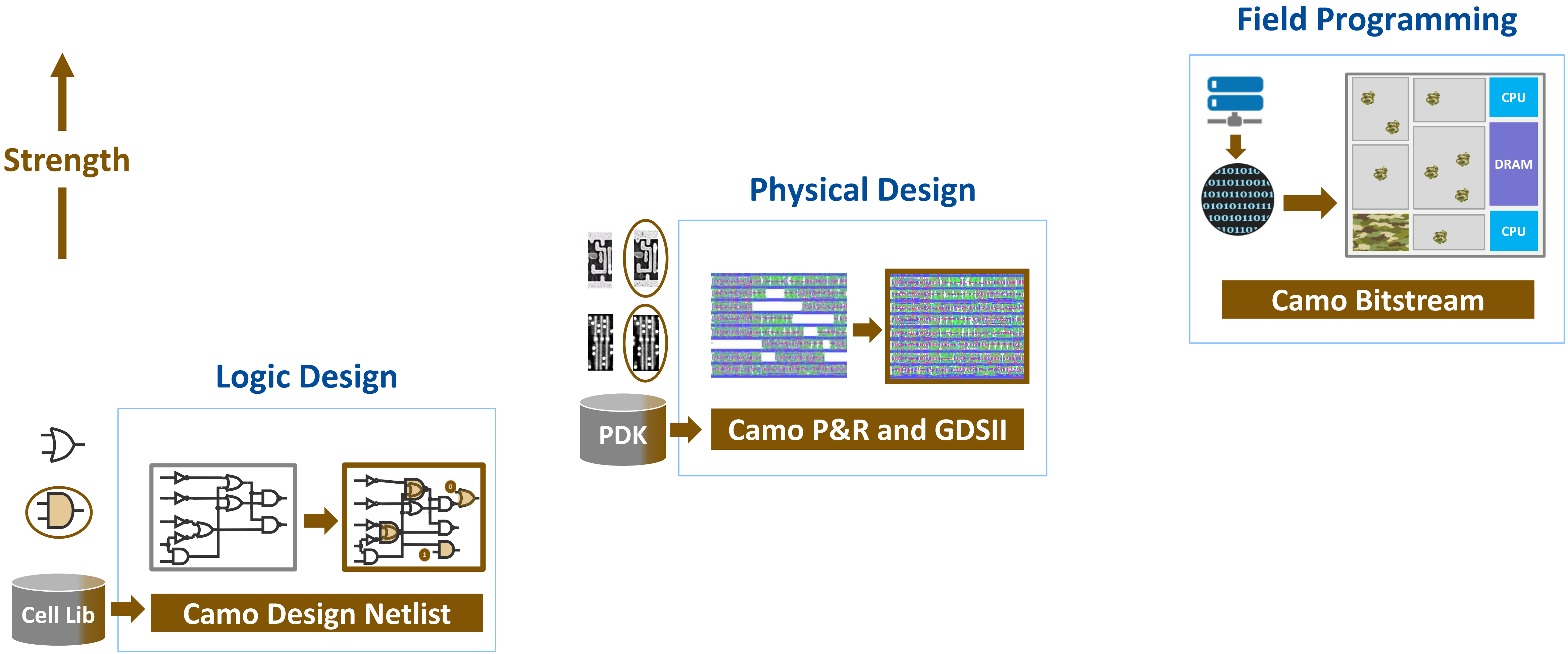


Source: thestack.com

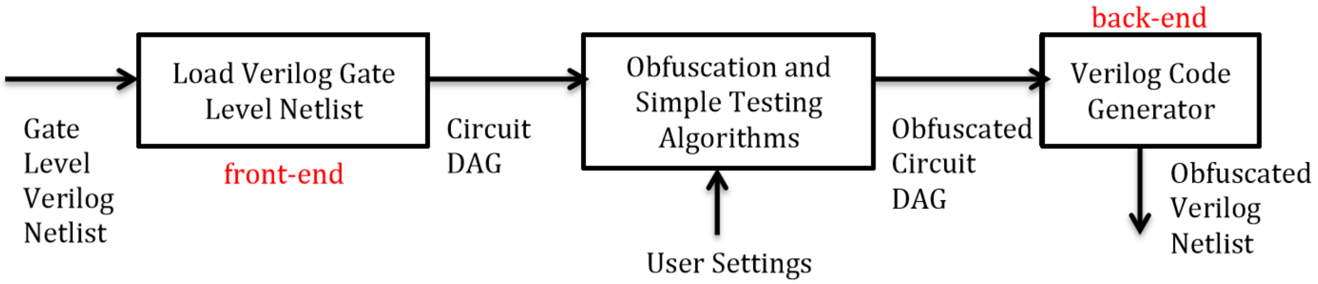
Key factors in National Security applications:

- Component provenance
- System integrity/assurance
- Reverse engineering resistance

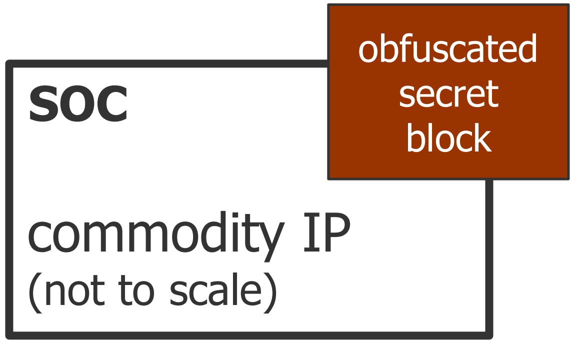
Anti Reverse Engineering:
End to End Camouflaging Methodology



Anti Reverse Engineering:
Obfuscation of key design IP blocks

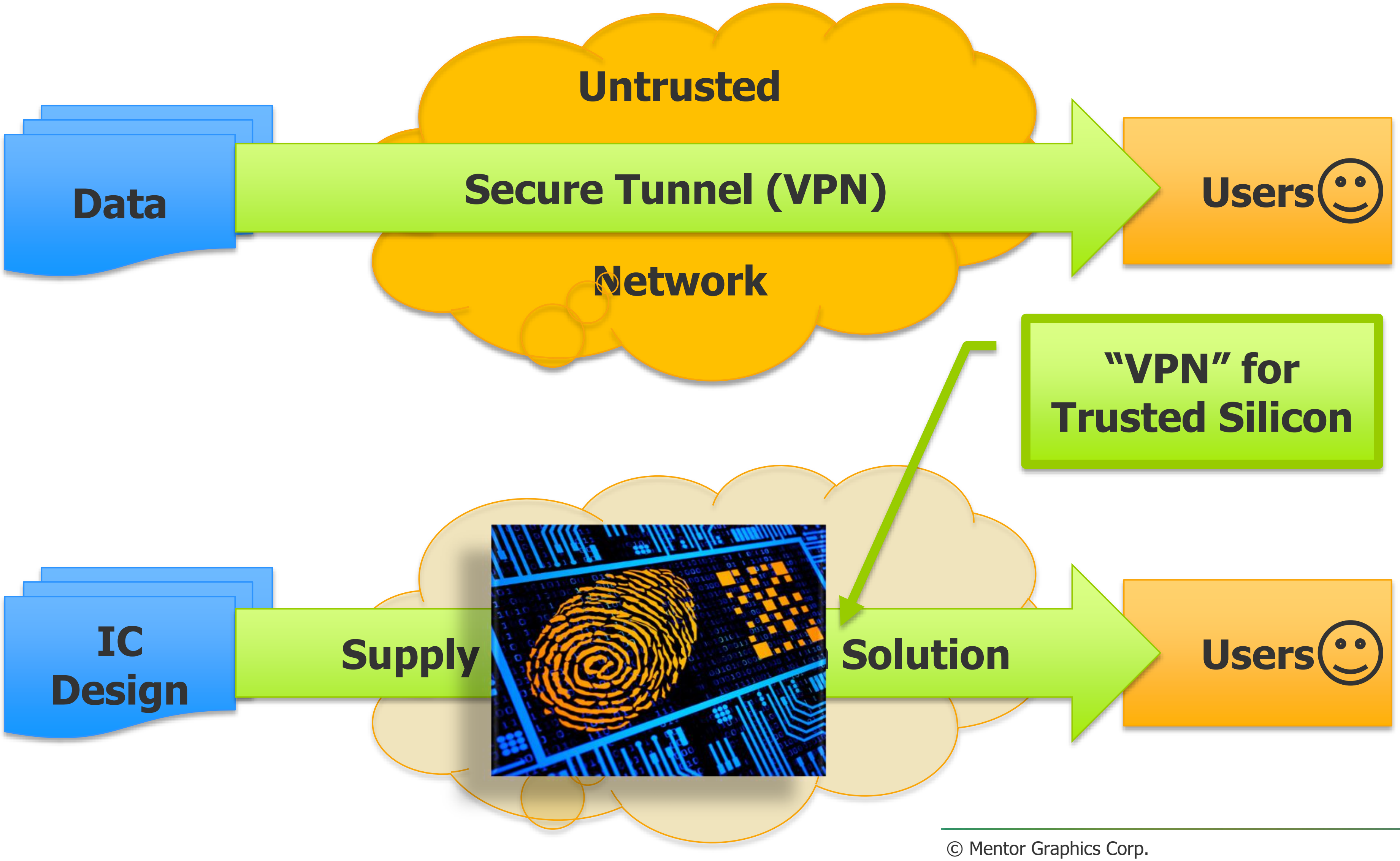


- Logic encryption/obfuscation engine
  - Inserting logic in areas to be protected
  - Additional logic elements are injected at hard-to-find sites to obscure the operational intent
  - Connected to a key of arbitrary length that can turn these elements into pass-throughs
  - Added area (cost) may not be prohibitive (i.e. 5% for 250M gate design)
  - Strong obfuscation makes it difficult to reverse engineer the IC
  - Potential solution to mitigate for limited availability of trusted foundries

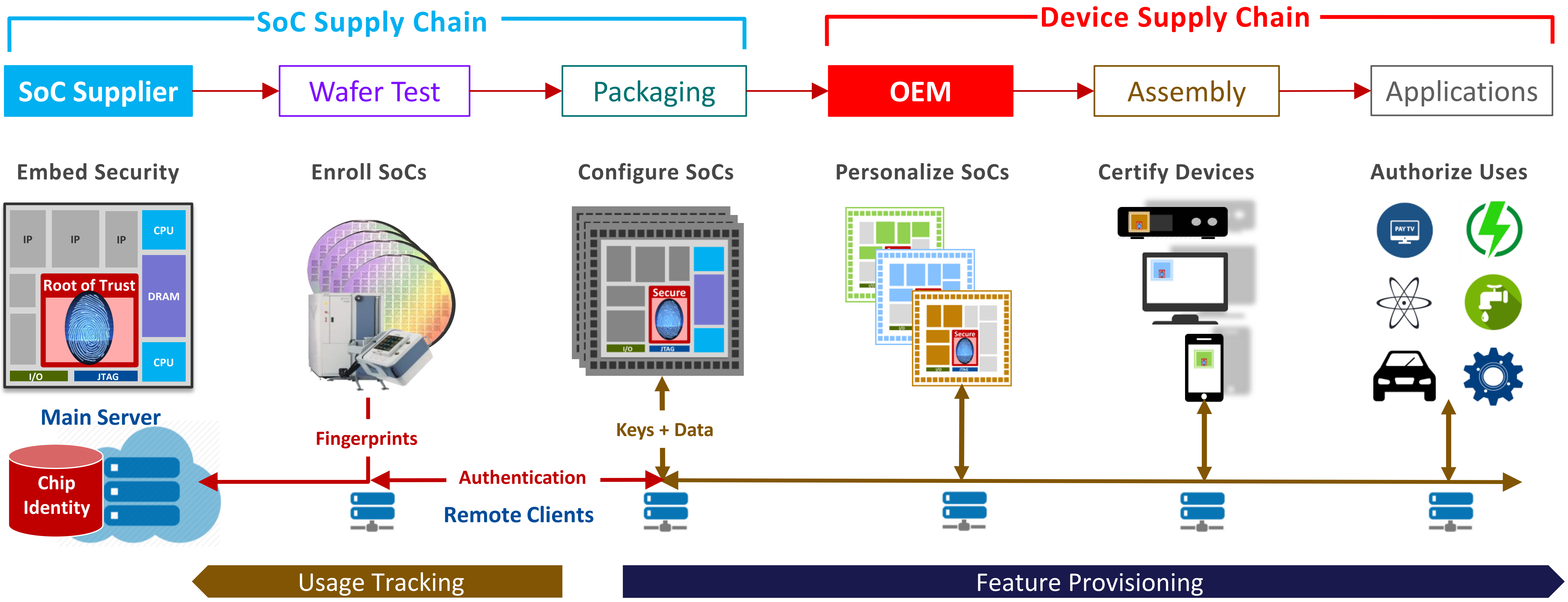


- Challenges
  - Selection of injections sites to be made in context of minimal impact on size, performance, power, observability, etc
  - Structure and size of these elements can also vary substantially and s related to reverse engineering resistance properties

Creating Secure Silicon in an Untrusted Environment — VPN for Silicon



End-to-End Solution Strategy for the Value Chain



Server Grades and Use Models

DoD Controlled

Mil-Aero IC Suppliers

DoD Security

Analytics

FP Data

Analytics

Parts DB

On Premises

Large IC Suppliers

Analytics

Parts DB

FP Data

Foundries & OSATs

Device Manufacturer

Device DB

FP Data

Dev. Cert

EMS Vendor

OEM1

OEM2

OEM3

Multi Tenant

Small IC Suppliers

FP Data

Parts DB1

Parts DB2

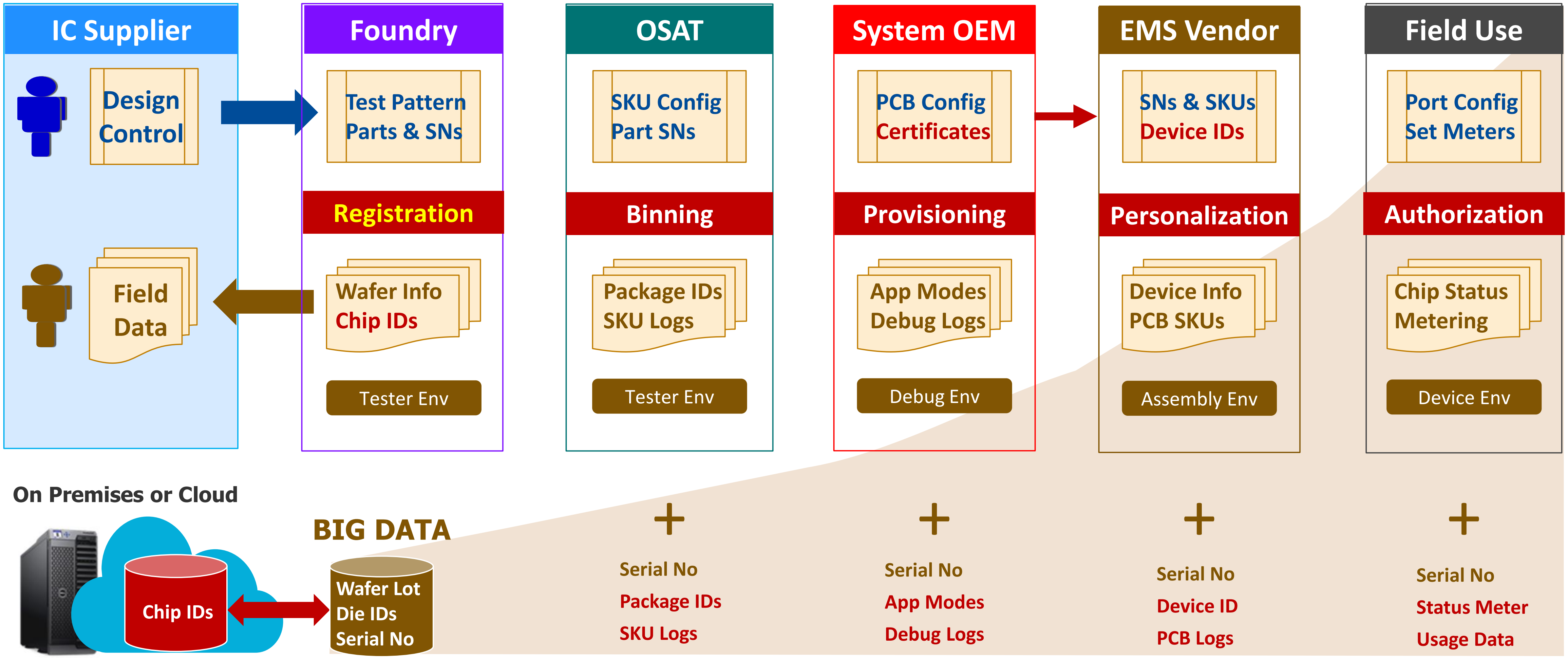
Parts DB3

Status & Provisioning UI

Analytics

Notifications

Increasing Value With Big Data Analytics

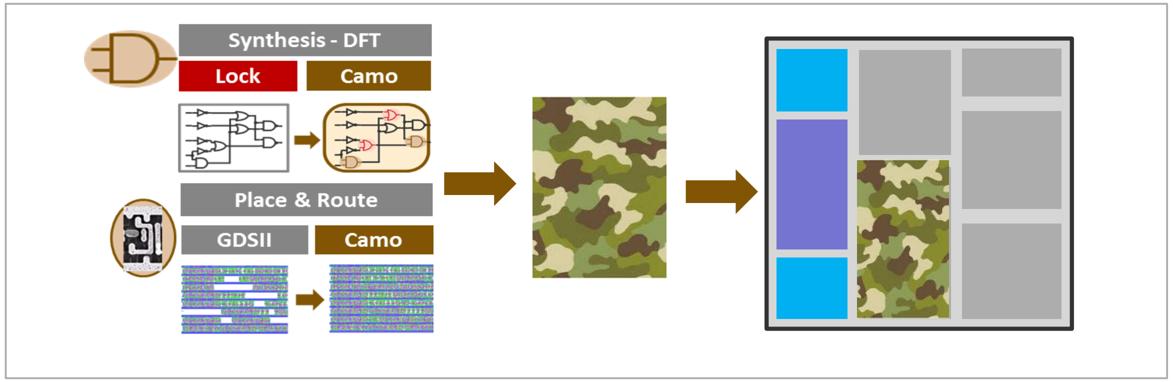


Enabling Several Identity Strategies

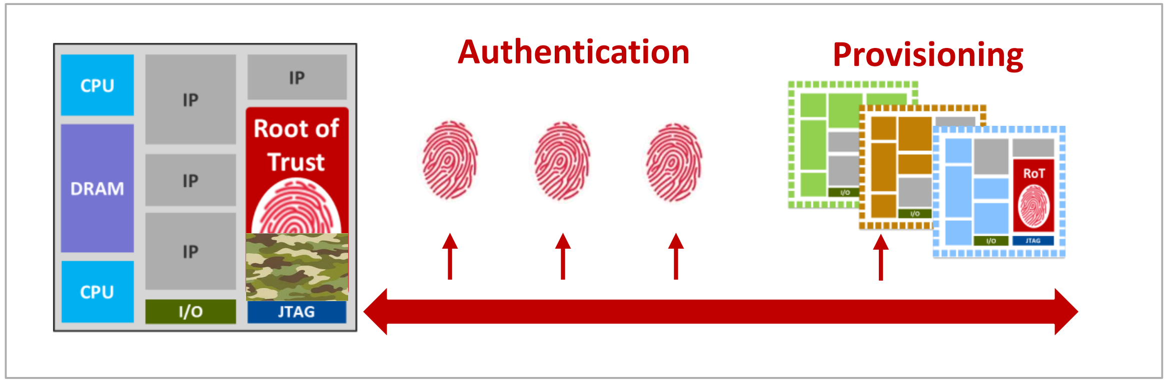
- Include into SoC comprehensive subsystem with inborn identity
  - Pro: enables authentication, provisioning, tracking, metering, very small attack surface, guarantee of silicon authenticity
  - Con: significantly impacts chip design, size too big for some chips
- Include into SoC a storage structure with programmable identity
  - Pro: small and easy to incorporate into designs, common current method
  - Con: requires trust injection event, can't distinguish counterfeits
- Include identity structure into chip packaging
  - Pro: non-invasive, can be added to old chips
  - Con: requires a trust attachment event, only supports authentication

Use Case: Digital Media End-to-End Solution

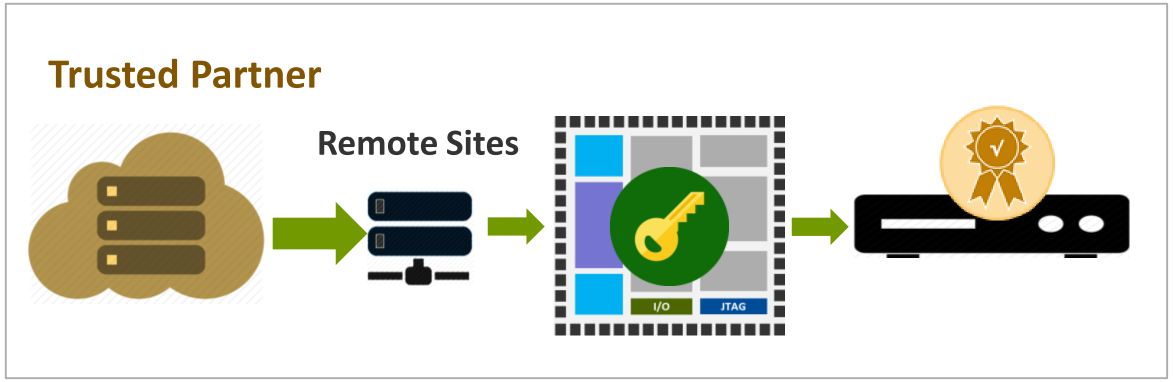
Prevent SoC Reverse Engineering



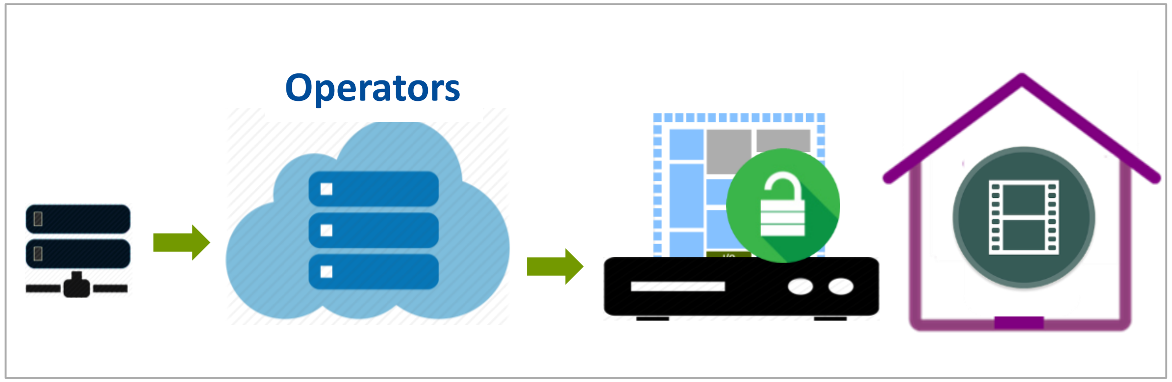
Embed, Hide & Enroll RoT



Inject Keys or Codes to Provision SoC

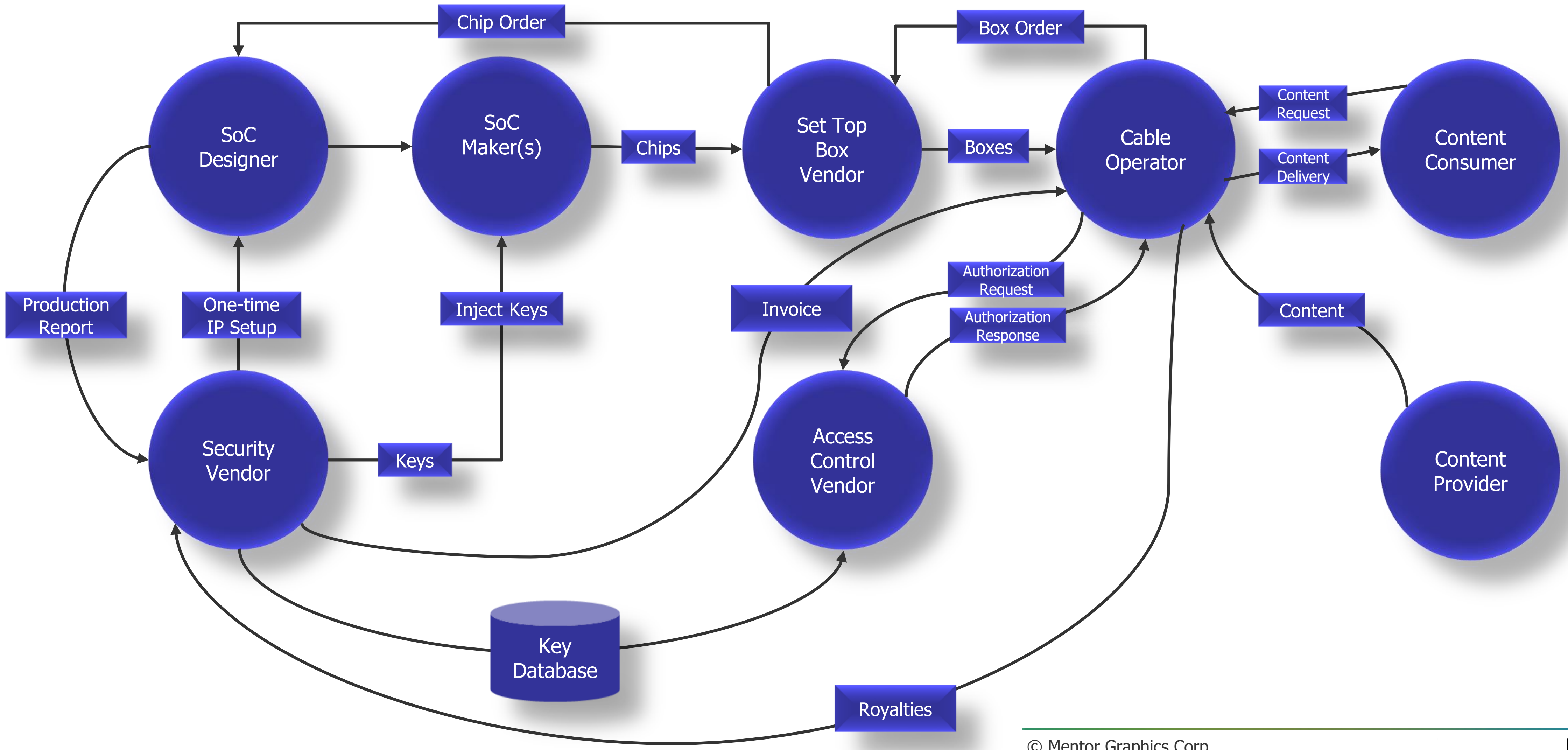


Distribute & Unlock Content from SoC

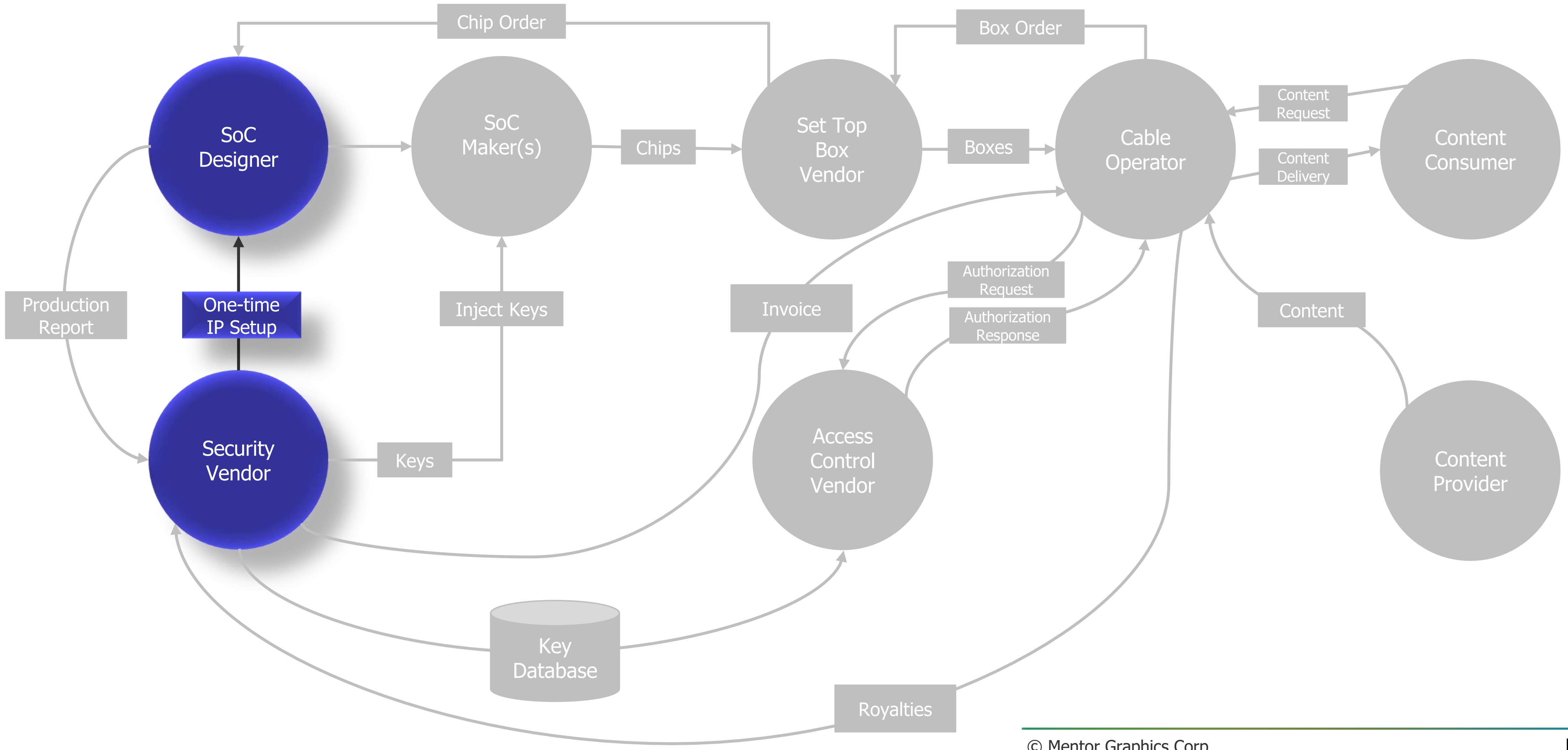


*With Trusted Ecosystem Partners

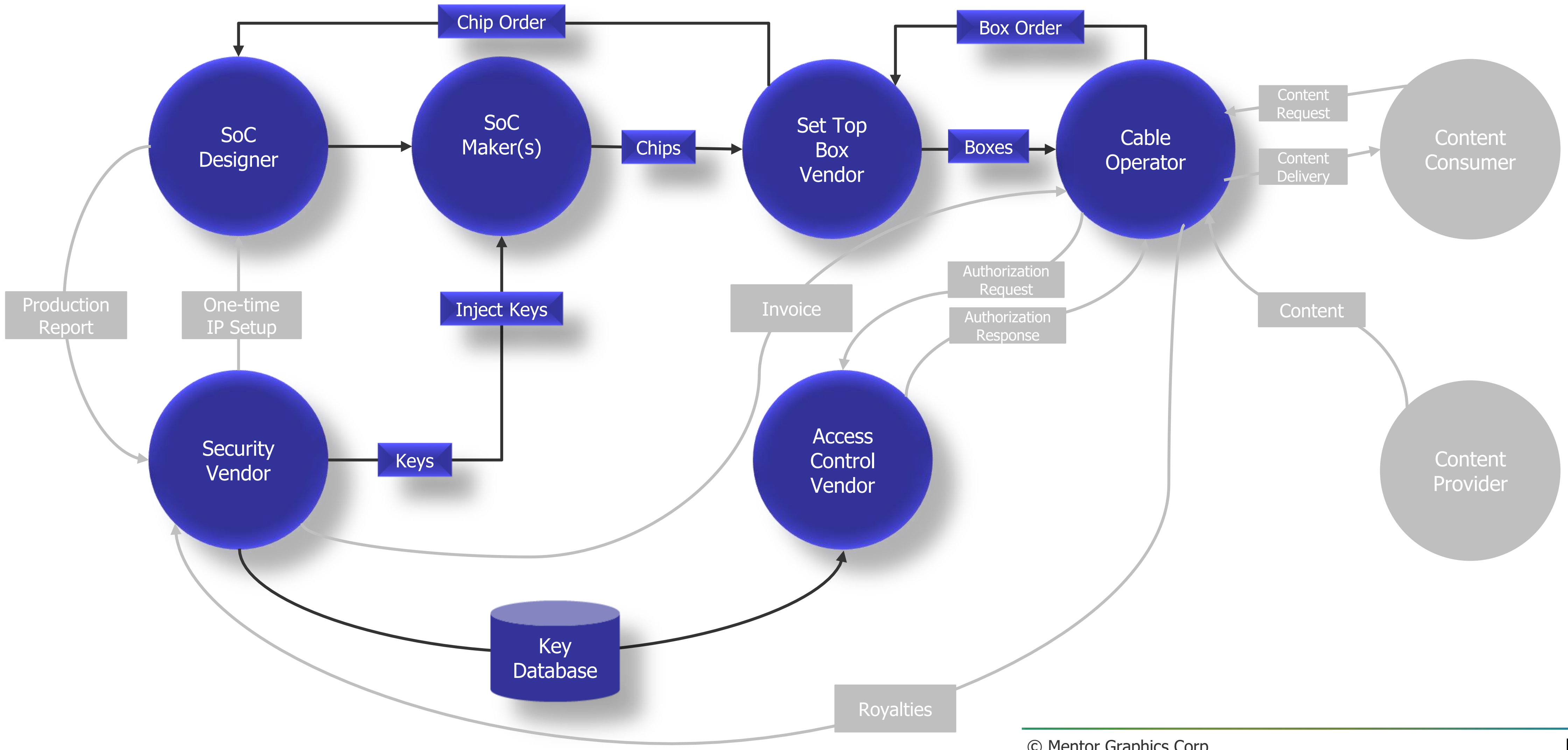
Relationships in the Digital Media Ecosystem



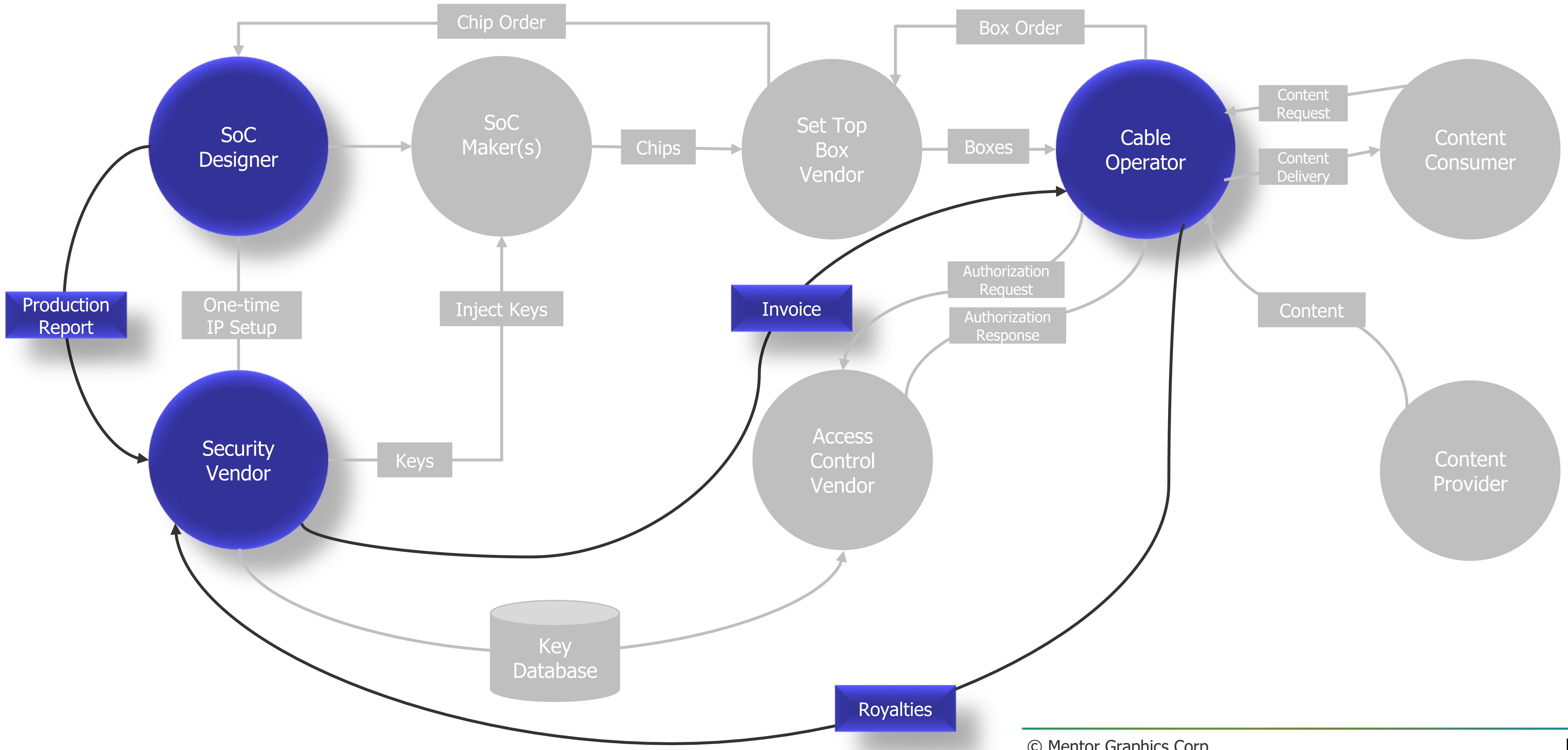
Digital Media Ecosystem: *Setup*



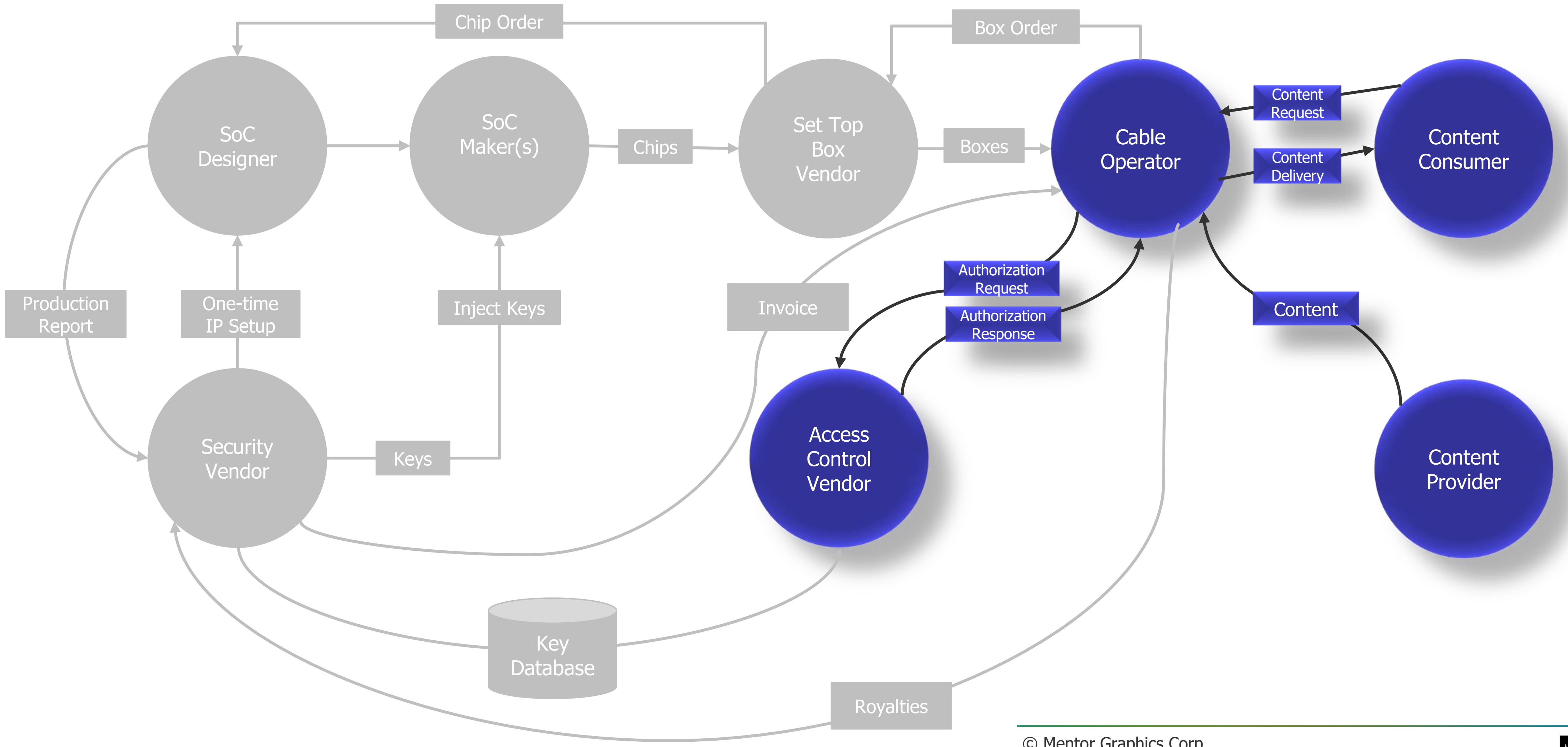
Digital Media Ecosystem: *Order Fulfilment*



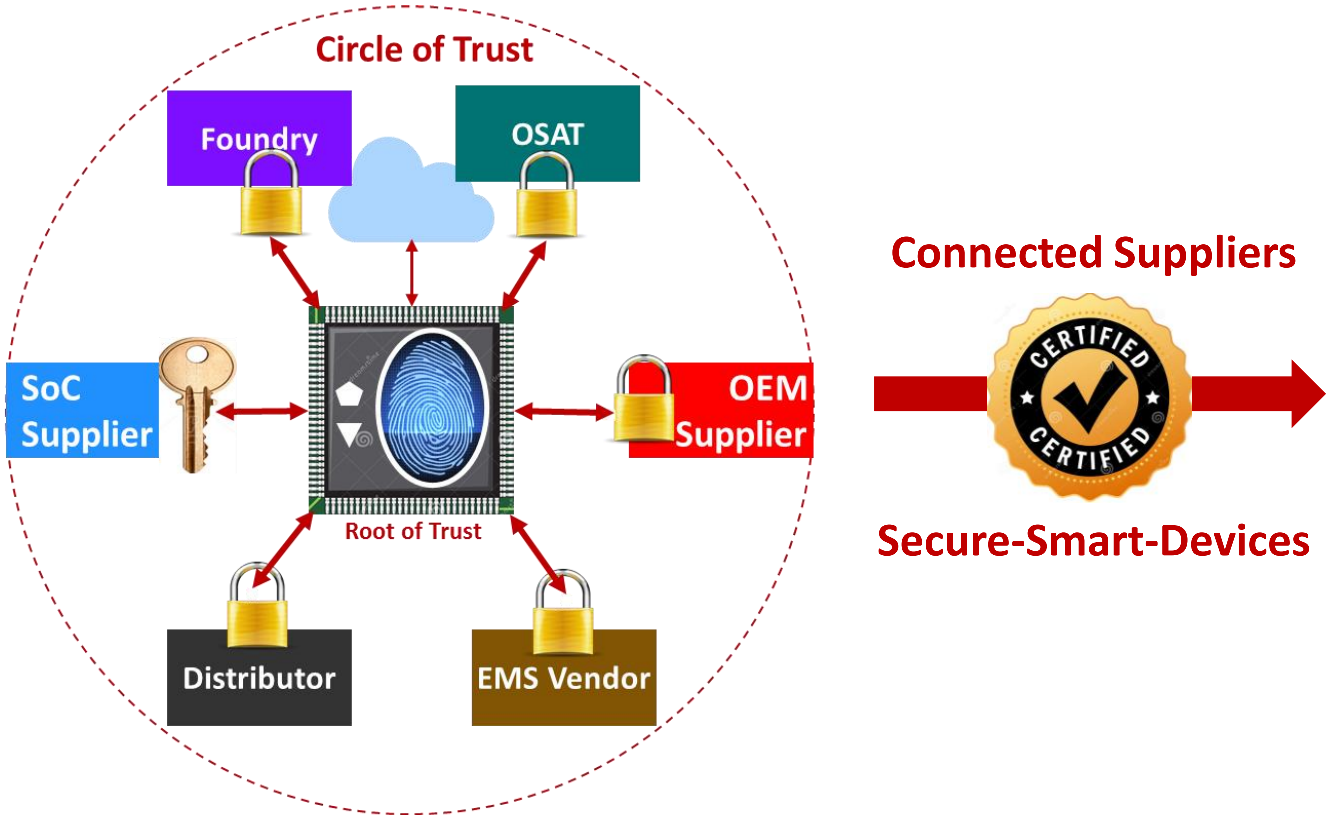
Digital Media Ecosystem: *Billing*

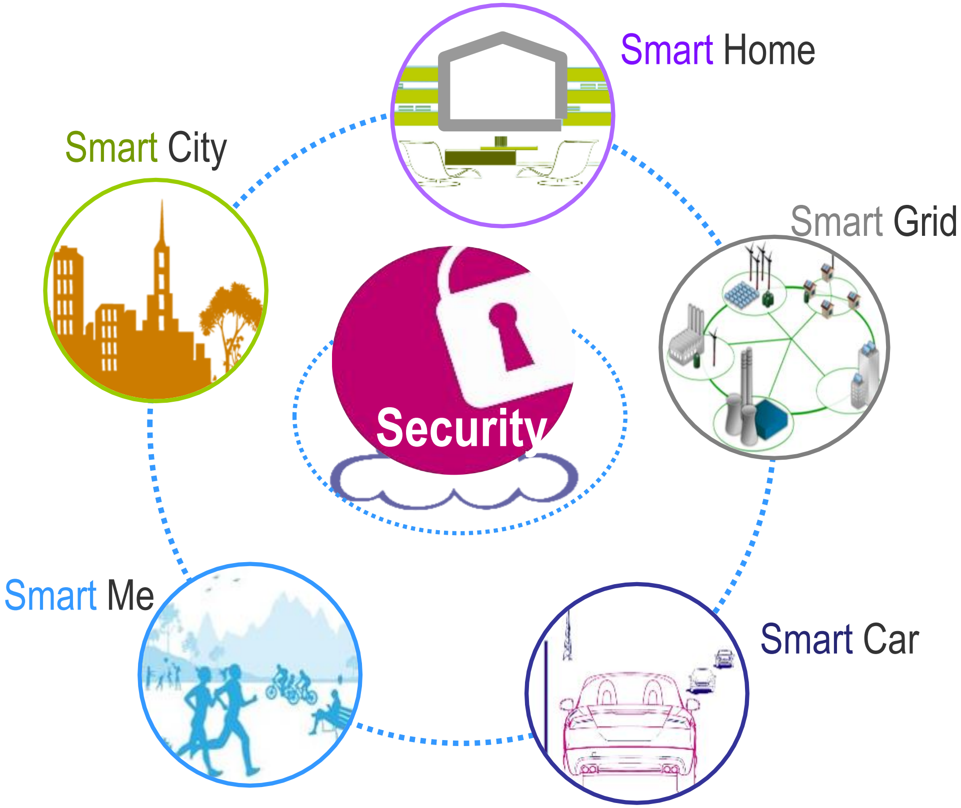


Digital Media Ecosystem: *Consumer Interaction*



Secure-Connected Collaboration Needed in
Vertical Markets Where Security has Clear Monetary and Legal Value





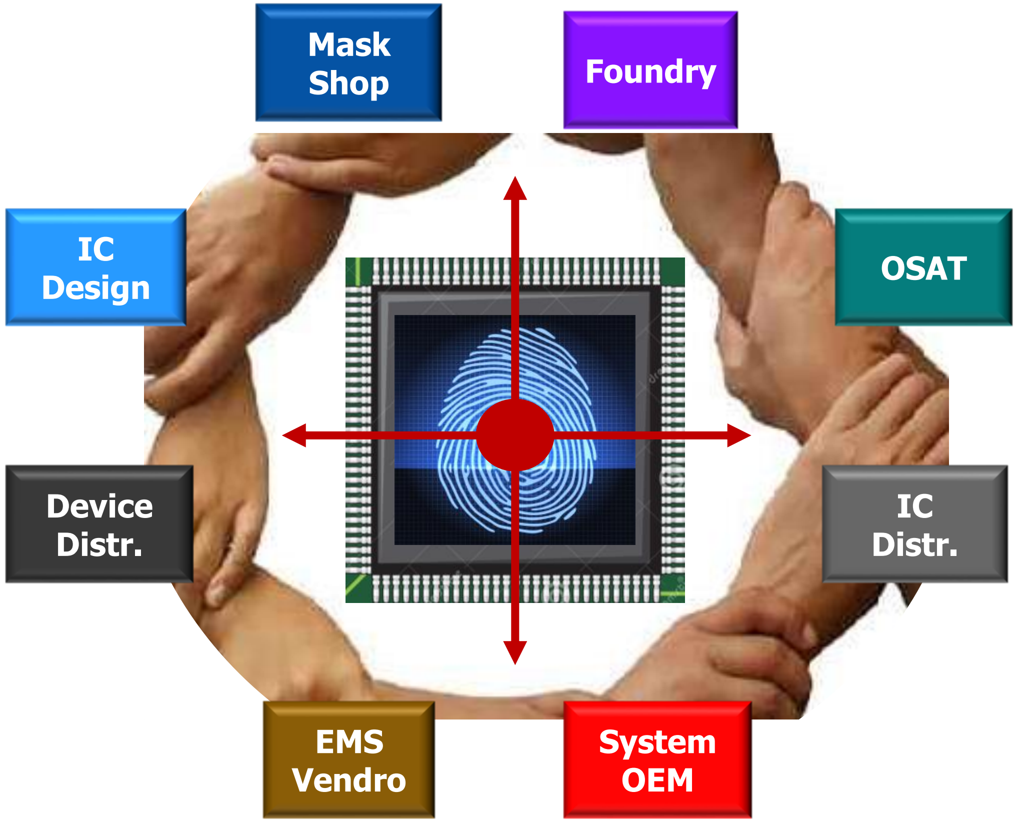
*Source: ST Microelectronics

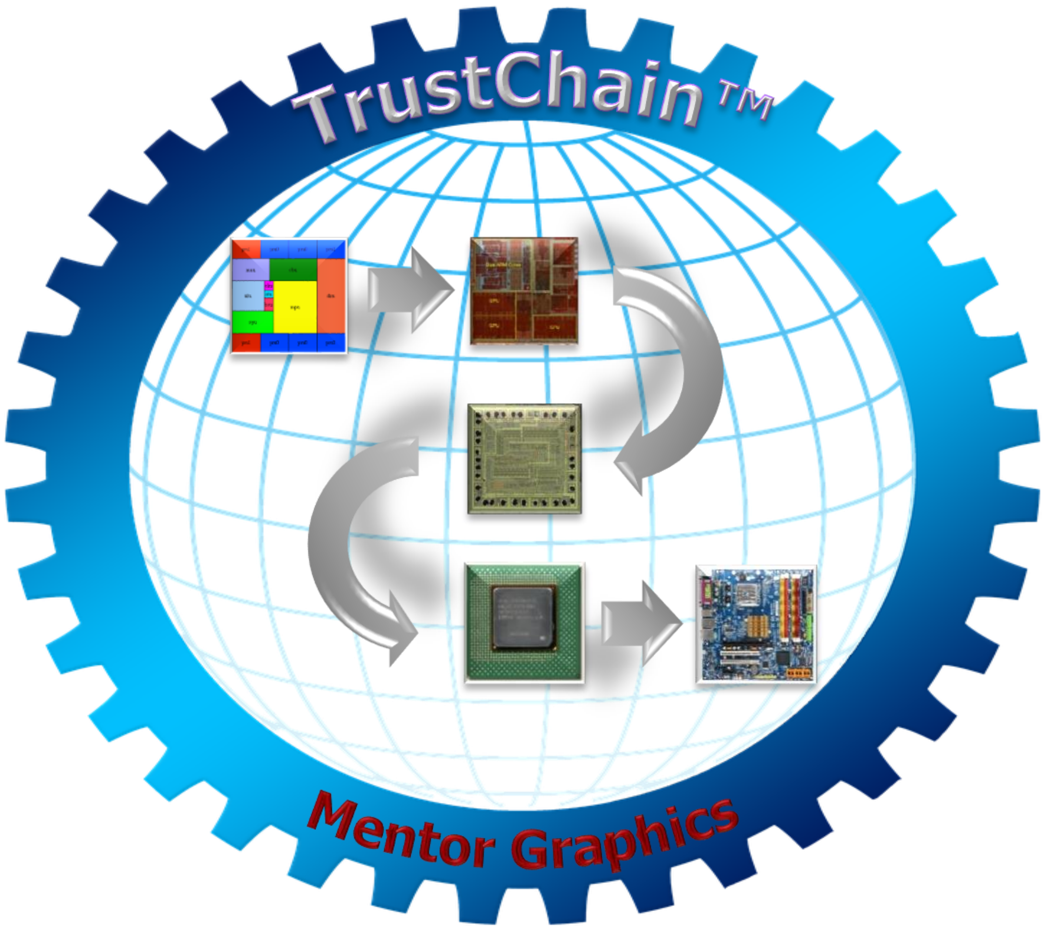
Supply Chain Trusted Ecosystem Alliance is essential for Security

Challenges observed and addressed in banking and broadcast markets

- **Reverse engineering** can be addressed with camouflaging and obfuscation
  - Can protect against mask theft and inspection based attacks
  - Approach
    - Camouflaging at functional and physical levels
    - Selective obfuscation of “secret” IP blocks
- **Unique identity** is an ideal root-of-trust for protecting the value chain
  - Can combat supply chain attacks:
    - Recycling, remarking, cloning, counterfeiting, overproduction
  - Approach
    - Enrollment, Provisioning, Authentication, Selective Logic Obfuscation
    - Metering, Data Analytics, Authentication-enabled Applications
- **Business models** needed to be created to provide value to all stakeholders
  - Approach
    - Parties along the value chain pay for participation (silicon vendors, system integrators, operators)
    - Party <u>at the end of the supply chain</u> with the greatest economic stake pays per chip royalties

TrustChain™ platform will be introduced at
Design Automation Conference 2017 | Austin, TX | June 18-22





Mentor Graphics®

www.mentor.com