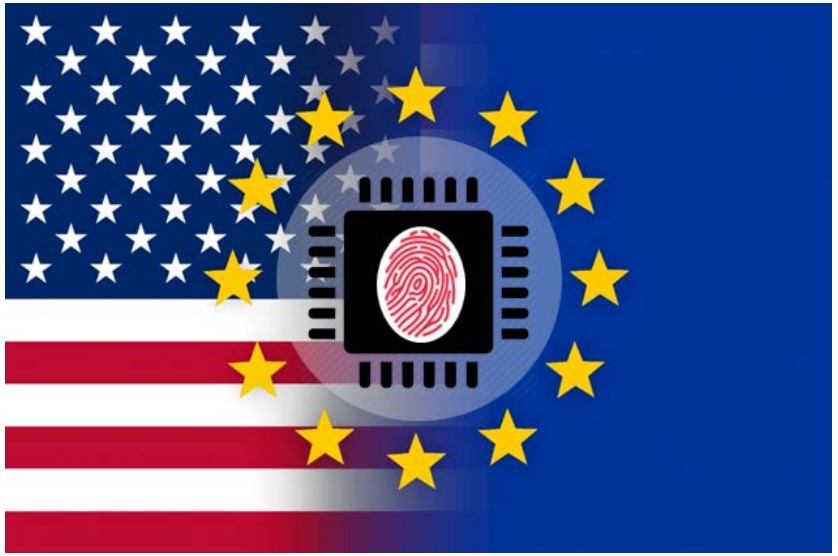


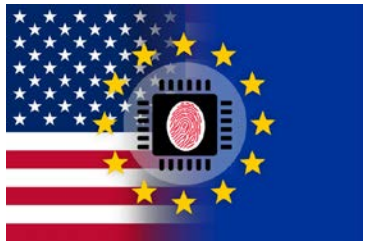
Global Chip Supply Chain Traceability Initiative

Global Unique and Immutable Numbers / A Trans-Atlantic Initiative

As per Initiation Document October 2, 2024

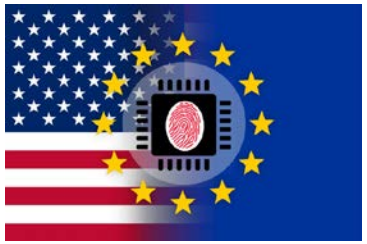
Workshop / November 19, 2024

Code of conduct TEAMS meeting



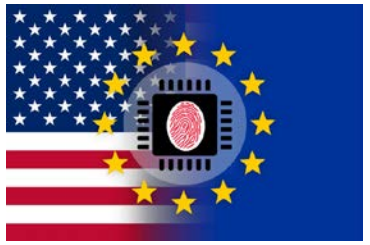
- **Mute When Not Speaking**: Keep your microphone muted when you're not speaking to minimize background noise.
- **Respectful Communication**: Be courteous and respectful to all participants. Avoid interrupting others and use the "Raise Hand" feature if you need to speak.
- **Use Video Appropriately**: Turn on your video to create a more engaging environment, but ensure your background is appropriate and free from distractions.
- **Follow Security Protocols**: Do not share meeting links or passwords publicly
- **Transcript and outcomes** of the workshop will be made available to all registered participants
- **Chatham House rules** apply for this meeting (recording not to be distributed)
- **Introduce yourself via the chat** (name, function and interest for this topic), then introduce again when you are speaking

Agenda (V2)



13:00	13:15	• TEAMS setting up and welcome address
13:15	13:45	• Introduction of the workshop objectives 15’ • Importance of semiconductor traceability and unique identification in the global supply chain. 15’
13:45	14:45	**Session 1: Current Challenges and Opportunities** • Panel discussion with representatives from the eco-system (institutions, governments, and industry). • Topics: Current state of semiconductor traceability, existing challenges, and potential opportunities. Use case “export control enforcement”
14:45	15:15	**Session 2: Technological Solutions and Innovations** • Presentations on cutting-edge technologies and innovations in semiconductor traceability. • Q&A session.
15:15	15:30	**Coffee break**
15:30	16:00	**Session 3: Policy and Regulatory Frameworks** • Discussion on existing and proposed policies and regulations. • Case studies from Europe. Standards applicable
16:00	16:30	**Session 4: Data Privacy and Database Governance** • Discussion on data privacy concerns and governance of databases used in semiconductor traceability. • Best practices and compliance with international standards
16:30	17:00	**Session 5: Establishing a “supporting infrastructure”** • Discussion on the formation of an infrastructure to support and oversee the initiative. • Roles, responsibilities, and structure of the body
17:00	17:30	**Closing Remarks and Next Steps** • Summary of key takeaways and action items. • Outline of next steps and follow-up actions
17:30		**End of workshop**

Global Chip Traceability



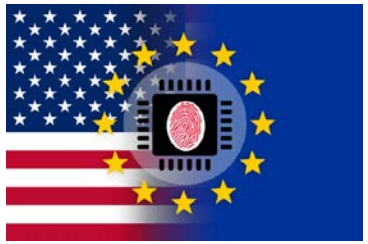
- The root problem solved by traceability of chips is ensuring the reliability, security, and accountability of chips as core in semiconductor components throughout their lifecycle.

- This addresses several highly interconnected challenges at the same time: Counterfeit, supply chain transparency (provenance), (cyber) security, regulatory compliance, data integrity and accountability, ethical sourcing and in the end also circularity of electronics.

- Traceability of chips provides a foundation for trust and efficiency in the whole semiconductor ecosystem, ensuring secure, reliable, and compliant use of critical components in industries ranging from consumer electronics to critical defense systems.

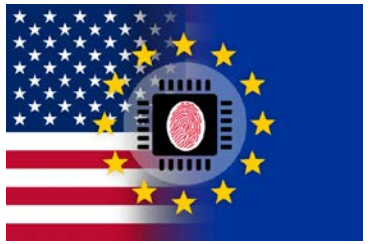
- The Global Chip Traceability initiative aims to provide a - Transatlantic driven but global in outreach - Ecosystem wide economic solution - By an evolution in perspective - From one central global database a global unique ID to in principle every chip.

Workshop objective November 19th



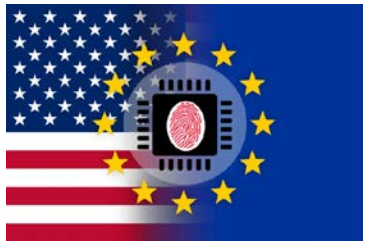
- **Workshop Purpose** is to assess the implementation of lifecycle traceability of individual chips, in a first use case, focusing on:
  - Export control enforcement as a use case
  - Defense and dual use chips
- **Key Focus Areas**:
  - Design of the Global Chip ID database
  - Traceability of chip from design to front-end & back-end over the life cycle
  - Testing of the use case in all aspects of the ecosystem
- **Workshop Outcome**:
  - Identify critical topics and questions related to individual chip traceability.
  - Prepare for future technical workshops and conferences
  - Get support from subject matter organizations and experts

Ecosystem Participants

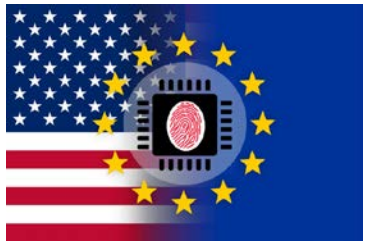


- **Roles and Responsibilities**:
  - **Design and Manufacture**: Ensure accurate documentation and traceability of chips from creation to production to delivery.
  - **Suppliers**: Maintain records of chip origins and ensure compliance with traceability requirements.
  - **Regulatory Bodies**: Oversee and enforce export control regulations, ensuring that all chips meet legal standards.
  - **End-Users**: Verify the traceability of chips received and ensure they are used in compliance with export control laws.
- **Focus on Defense and Dual-Use Applications**: Pay special attention to chips used in defense and dual-use technologies, ensuring strict adherence to export control regulations.

Pilot project

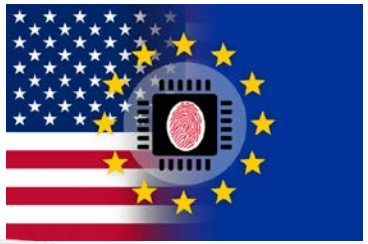


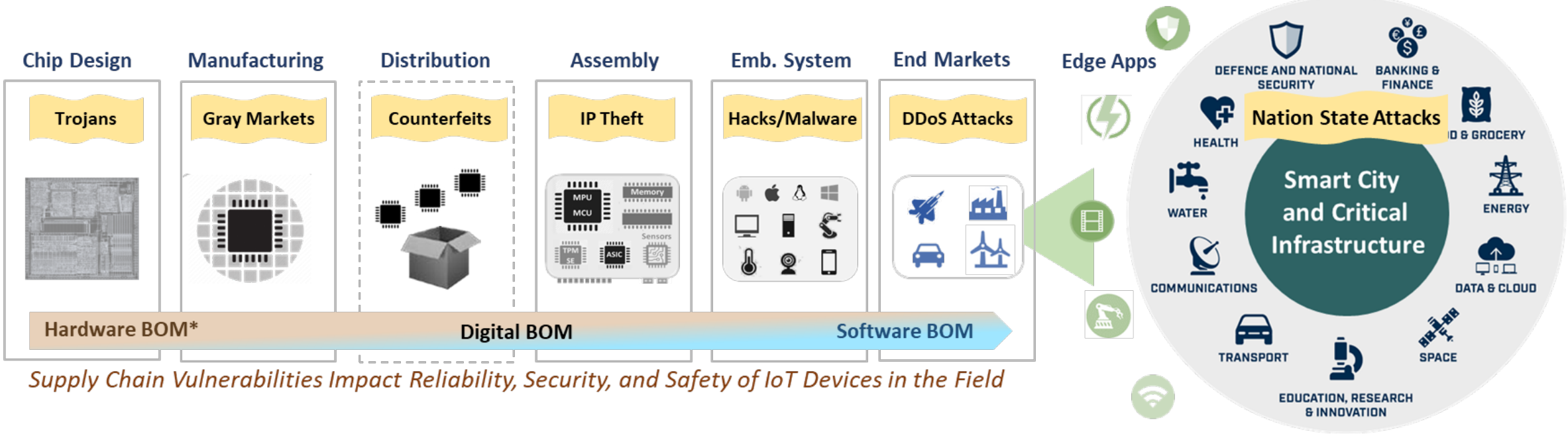
- This project aims developing a practical, comprehensive implementation plan for a practical use case.
- The initial focus will be on a traceability system designed and tested for export-import control and preventing the misuse of chips in advanced electronics for the aerospace-defense industries.
- This approach will facilitate a thorough analysis of the Global Chip ID's role across the entire ecosystem.
- The following key topics will be addressed in depth in Phase 0:
  - Database requirements and governance
  - Business Use case alignment
  - Standards alignment
  - Roadmap for implementation



Importance of semiconductor traceability and unique identification in the global supply chain

Importance of US-EU Initiative on Traceability



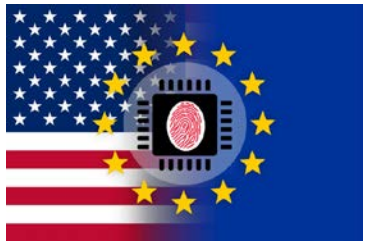


Supply Chain Vulnerabilities Impact Reliability, Security, and Safety of IoT Devices in the Field

- Safeguard allied nations' markets from being flooded by adversaries' legacy chips
- Strengthen export control and prevent western chips weaponized against our allies
- Drive resilience and new business models (analytics marketplaces, HaaS, AIoT)

*Source: NIST IoT Advisory Board Report Page 25

Why Chip Traceability Matters



Journey of chips though untrusted environments assembled with other chips into electronics products

1. China Rare Earth Metals
2. S. Korea Flash Memory
3. Germany Accelerometer
4. Netherlands NFC Controller
5. Japan Camera, LCD Screen
6. USA Wi-Fi & Audio Chips
7. Taiwan CPU/GPU Manufacturing
8. China Final Assembly & Test

Chip Supply Chain

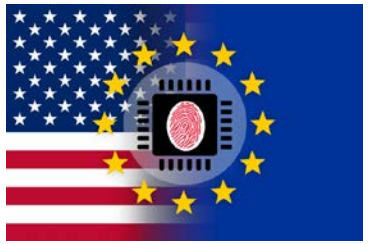
- Lack of visibility in fragmented supply chain
- Over 65% of electronics assembled in Asia
- Ineffective sanctions and customs controls
- Costly support, liabilities, and loss of value

Critical Infrastructure

- No security in Systems & Process Sensors
- Silos and no visibility in IT/OT convergence
- Nation state attacks infiltrating supply chains*
- Compromised equipment and human safety

https://www.bloomberg.com/news/articles/2024-09-19/exploding-pagers-sound-global-alarm-for-supply-chain-security

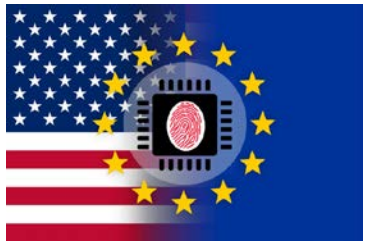
Global Chip Traceability Initiative



- **Purpose**: Establish a resilient supply chain through unique Global Chip IDs, ensuring traceability from design and manufacturing to edge applications
- **Vision**: Drive a global unique Chip ID, enabling assured supply, and opportunities for monetization to bolster national and economic security
- **Strategy**: Accelerate adoption through U.S.-EU collaboration with Global Chip IDs linked to infrastructure for secure SLM* and data analytics marketplaces
- **Objectives**: Improve transparency, security, and resilience across the supply chain and prevent market flooding or weaponization of chips by adversaries
- **Roadmap**: Convene workshops on traceability, initially on export-import control and business use cases that demonstrate the value of traceability

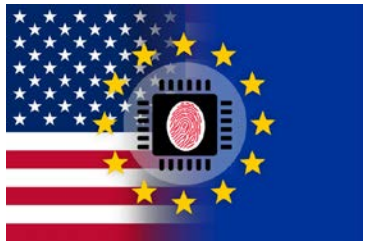
* Silicon Lifecycle Management

Benefits and Value of Chip Traceability



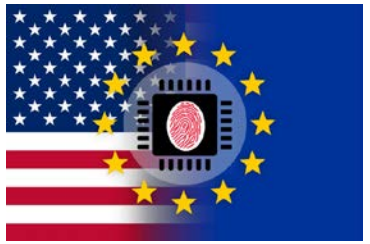
- **Transparency:** Enables clear visibility across the global chip supply chain, from design and manufacturing to deployment.
- **Security & Trust:** Protect critical infrastructure by preventing attacks to our critical infrastructure and weaponization of western chips by adversaries.
- **Resilience:** Strengthen the chip ecosystem against supply chain disruptions and enhances response capabilities.
- **Efficiency:** Optimize the trade, flow, management and field use of chips ensuring better lifecycle management and reduced risk.
- **Economic Growth:** Create opportunities for monetization and innovation with analytics marketplaces chip-enabled services.

Strategic Advantages for Stakeholders



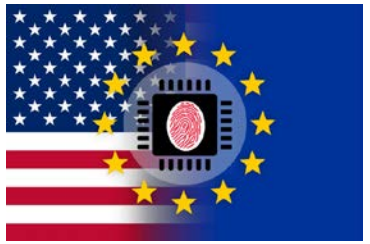
- **Governments:** Enhance export control mechanisms and protection of critical infrastructure through chip traceability, ensuring national and economic security
- **Industry:** Enable innovative business models and applications, to strengthen global competitiveness by ensuring authenticity and supply chain integrity
- **Cross-border Trade:** Foster unified U.S.-EU efforts, setting a foundation for worldwide industry adoption and creating a resilient and secure supply chain
- **Business Ecosystems:** Facilitate Chip ID connected value chains among chip companies, suppliers, and service providers to drive growth and innovation
- **Private-Public Partnerships**: Encourage investment and resource-sharing between governments and private sector accelerating economic growth

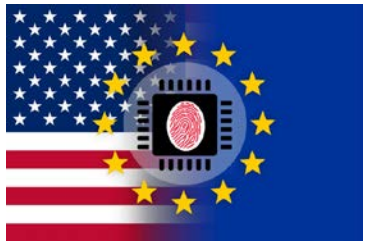
Call to Action



- **Act with Urgency:** Timing to secure our chip supply chain is now. Swift action is needed to address rising security risks and maintain global leadership.
- **Leverage Momentum:** Exploit on the massive investment in new fabs and infrastructure to drive traceability initiatives forward with industry-wide impact.
- **Start Collaborating:** Develop strong public-private partnerships. Unite industry leaders and governments to share resources and expertise
- **Accelerate Roadmap:** Start by driving awareness with workshops, launch pilot projects to validate and demonstrate the value of global Chip IDs.
- **Expand Networks:** Use trusted alliances to engage stakeholders, and drive adoption thorough business use case across the global value chains.

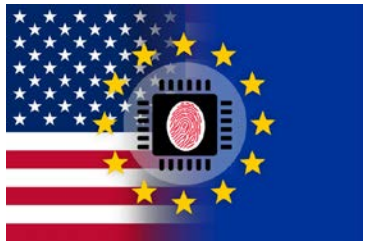
Time for discussion





Session 1: Current Challenges and Opportunities

Challenges About Chip Traceability



Industry CEO "*Traceability for Security should be our top priority... but many will turn a blind eye to security if it means even nominal higher costs. Education of the risk starts the conversation*."

- **Perception of Investment**: Our industry prioritizes cost-efficiency views traceability as a burden
  - **Change Mindset:** Promote *Traceability for Monetization* alongside security to justify economics.

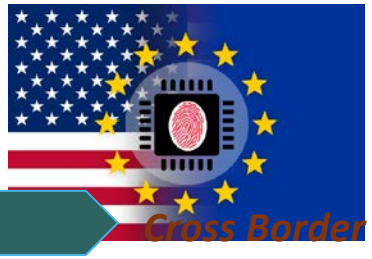
DG Connect: *"Cross-border chip supply chain traceability is very complex and needs to deal with a lot of highly sensitive data for security. Open standards can play a key role…"*

- **Complexity of Security & Data Sharing**: US and EU diversity on standards and regulations.
  - **Change Mindset:** Pursue methods enabling digital marketplaces facilitating private transactions

- **Value vs. Risk Conversation**: Frame traceability as a business opportunity that justifies ROI
  - Highlight economic benefits by focusing on business use cases with clear monetization
  - Engage executives on business models and thought leaders on strategy and roadmap.

Traceability for Security and Monetization

*Included in the report of the Department of Commerce appointed IoT Advisory Board report



Semiconductor Ecosystem → Electronics Ecosystem → IoT Ecosystem

Applications

Trusted Fab ROI | Power & Speed | Actual Value/Cost | Connectivity SLAs | XaaS Platforms | Circular Economy

U.S. Cyber Trust Mark

Digital Marketplaces

Trusted Digital Twins — Trusted Data Analytics

Asset Tracking

QR | RFID | Beacons

Public Private Partnerships

Chip Design & Mfg | Packaging & Test | Embedded System | Vertical Markets | Edge Applications | Environments

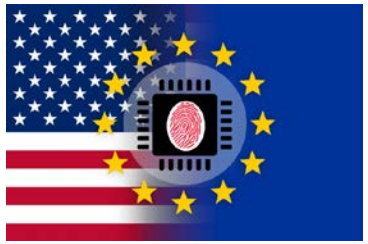
Trusted Digital Thread — Trusted Digital Transformation

EU Digital Passport

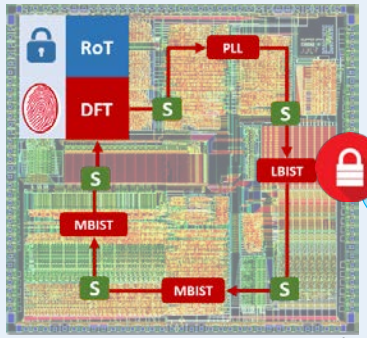
Infrastructure

Trustworthiness | Cybersecurity | Market Access | Confidentiality | Secure Onboard | Interoperability

Business Use Case Examples



Automotive - Silicon Lifecycle Management (SLM)



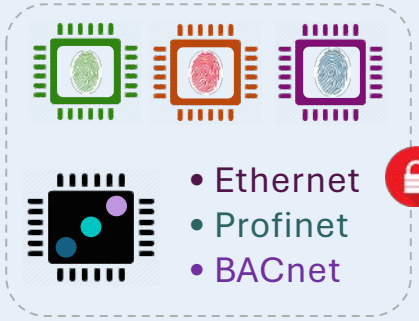
Functional Safety

Fleet Monitoring



*Source: Semiconductor Eng

Industrial - Chip Licensing & Multi Market Product



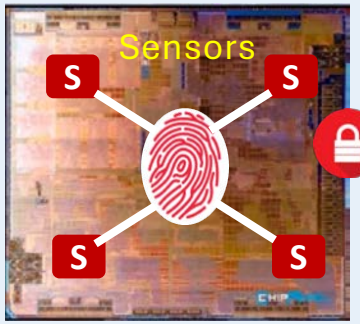
HW + SW Provisioning



*Sources: Intel - Pay-as-you-go Chip Licensing, Samsung - Memory Chip Rental Service

Global Chip ID

Aerospace & Defense - Manufacturing Integrity

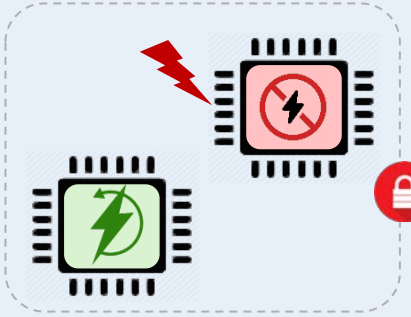


Failure Prevention



Source: ERI Summit 2020

Supply Chain - Monitoring & Regulating Field Use

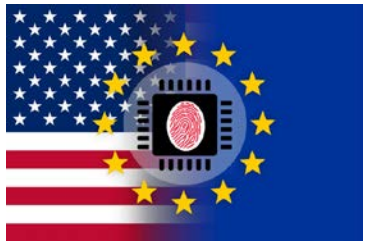


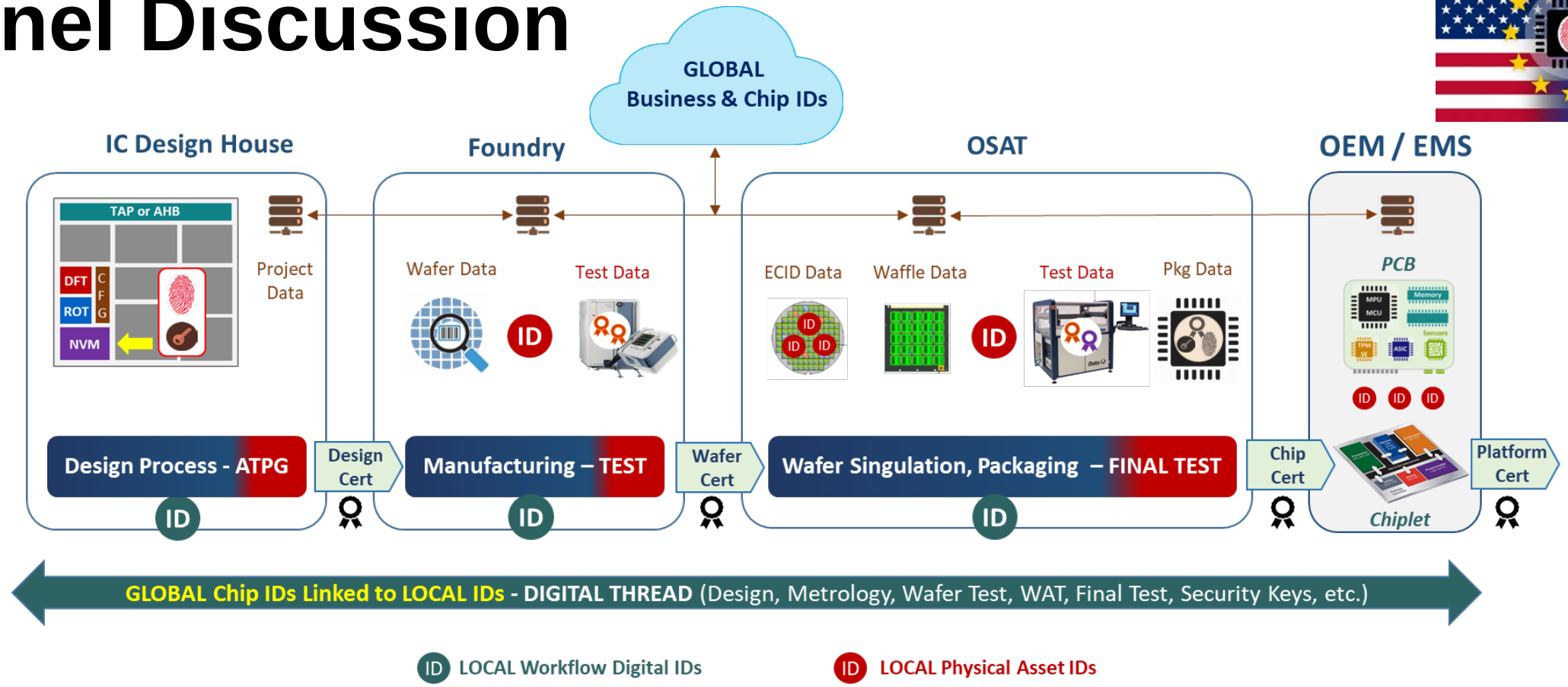
Disable Adversary



Sources: Reuters - Western chips in Russian drones, WSJ - Cheap drones in battlefields

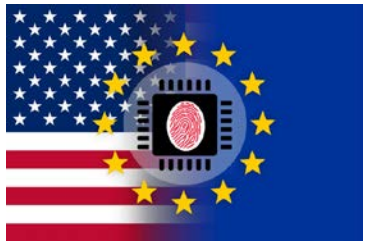
Panel Discussion





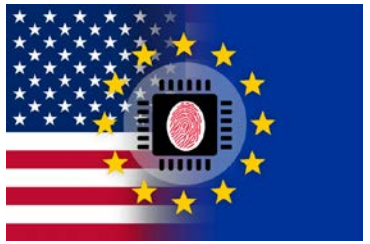
- **Ecosystem Participants:** Institutions, Governments, and Industries
- **Main Topics:** Current state of traceability challenges and opportunities.
- **Initial Use case:** Cross-border Traded and Export Control Enforcement

Questions & Feedback



- What do you think is needed for import-export control, from your perspective?
- What are your biggest challenges regarding the traceability initiative?
- How to orchestrate a pilot solution with initial public-private partnership?
- How can you participate in delivering pieces of what is needed for the pilot?
- What would be your most important deliverable outcome from this project?
- What challenges do you foresee that we need to address to be successful?

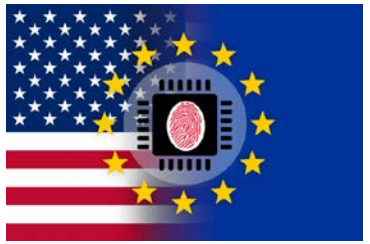
Information provided by participants

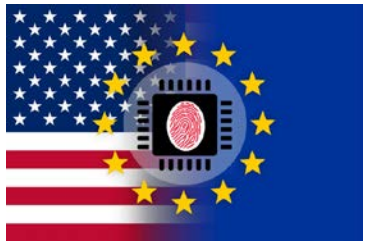


- Netherlands Government

- NXP

Time for discussion





Session 2: Technological Solutions and Innovations

Needs for Adoption of Traceability



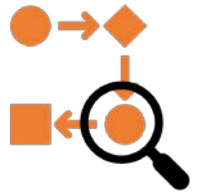
Policy and Market Behavior

- **Drive demand** tied to assurance to increase production capacity
- **Establish market incentives, policies and standards** that reduce risk of supply disruption
- **Promote the monetization of security** through traceability that can be valued by end users and consumers



Trusted Digitization Solutions

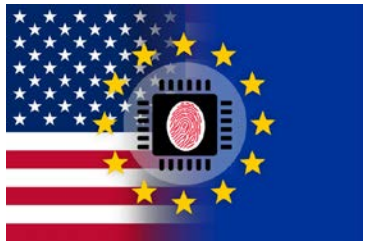
- **Illuminate supply chain** through provenance (e.g., trusted certificates, blockchain, etc.)
- **Model market risks** including non-market forces
- **Create the infrastructure** to monetize assured supply and security
- **Measure the impact of assured supply** to end-markets through market-level traceability and preference



Physical Traceability & Supply Chain

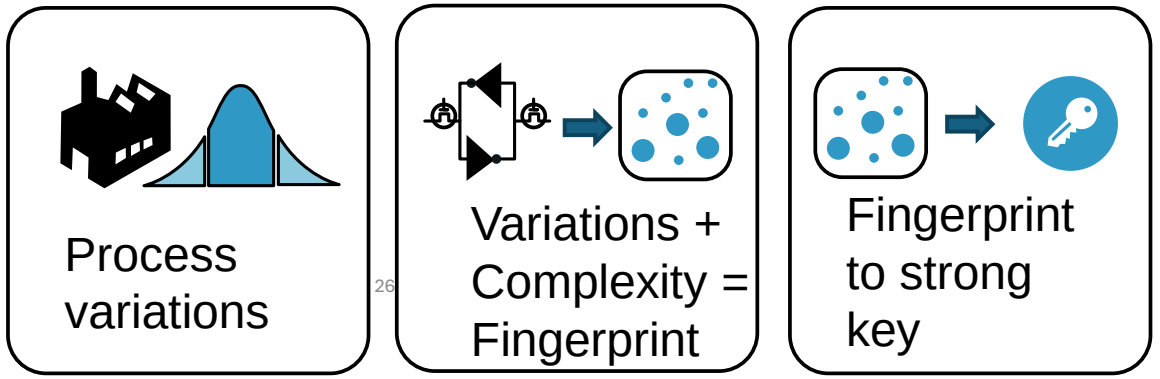
- **Implement immutable physical traceability** and validation infrastructure industry-wide
- **Standardize and validate root of trust** and hardware as a service to deliver differentiated technology through assured supply chain
- **Promote consumer level traceability tools** and marketplace

Sources of Provenance for Assurance



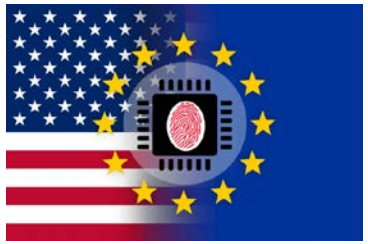
- Entropy
  - Natural/physical sources for randomness
  - Foundry processes battle and carefully measure effects of entropy
  - Entropy and variation is embedded as a fingerprint in each device

- Complexity
  - Encryption
  - Obfuscation
  - Unique marking
  - Large number of states



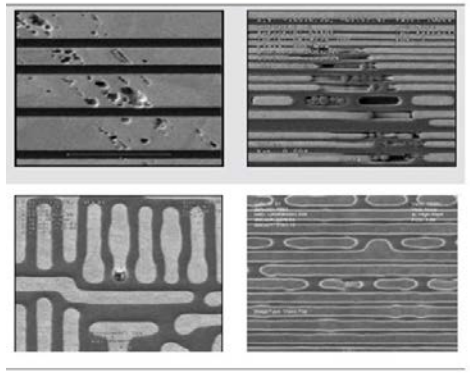
- Multi-factor contemporaneous Data
  - Temporal - when did the occur, how does it vary, etc.
  - Spatial – where was my wafer, distribution of physical variation, etc.
  - Spectral – visible, acoustic, electrical, radiation, etc.

Examples of Intrinsic Process Variation -Fingerprint



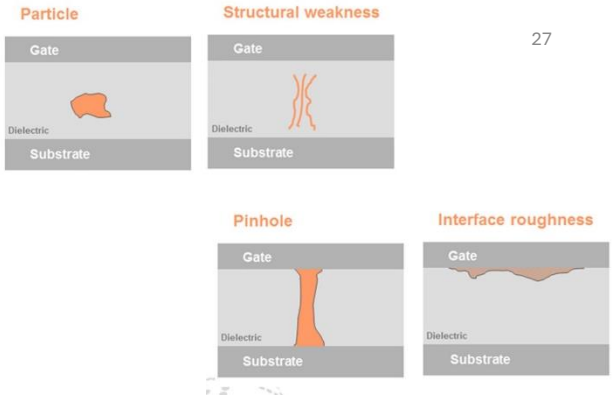
Metals

- Grain variations on small feature sizes
- Lithographic variations



Oxides

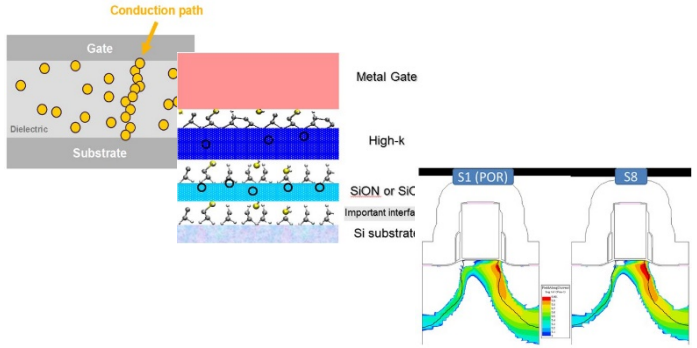
- Oxides thickness variation
- Gate Oxide variations cause performance changes



27

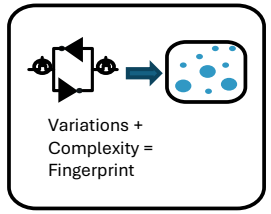
Transistors

- Time dependent breakdown
- Bias Temp instability
- Hot carrier injection



Intrinsic variation can be easily measured per die through process monitors and “canary” structures

Examples Extrinsic Variation





Die Markings

- Wafers are all marked
- Opportunity for die level marking using direct write and femto-lasers, dust, etc.
- Must be cost effective and have a high level of complexity or hash to other data

One-time-programmable

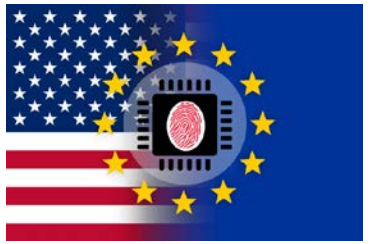
- One-time programmable (OTP) memory allows for unique state or electrically read labels
- Transistor elements that are programmable/unstable in state of operation can help with obfuscation and can be leveraged for uniqueness

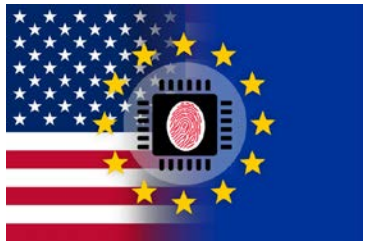
Tagging /data embedment

- Direct write of certain mask levels can create highly complex labels and embed data
- Can support electrical, optical, radiation, and other readout mechanisms
- Easy to read after packaging to tie provenance back to die

Extrinsic variation can increase ability to uniquely mark die and hash other data into the physical part

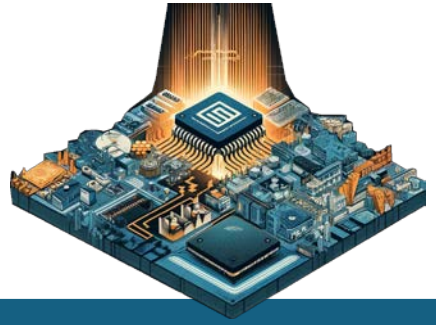
Time for discussion





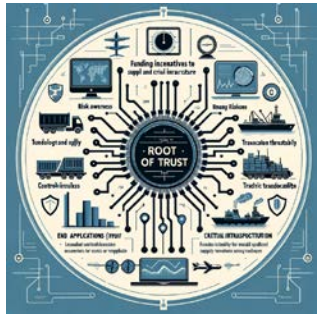
Session 3: Policy and Regulatory Frameworks

Problems



Economic

- Unlevel playing field & Asia dominance in microelectronics
- Dumping of state of practice semiconductors by China
- No market preference for assured supply to critical infrastructure (lowest cost wins)



Technology

- Lack of awareness of risks to supply & critical infrastructure
- Traceability from R&D into assured supply needs funding incentives
- Control (root of trust) of end technology at risk



Defense

- Limited assured supply of semiconductors
- Defense and critical infrastructure are linked
- Export control and foreign military controls of technology challenging

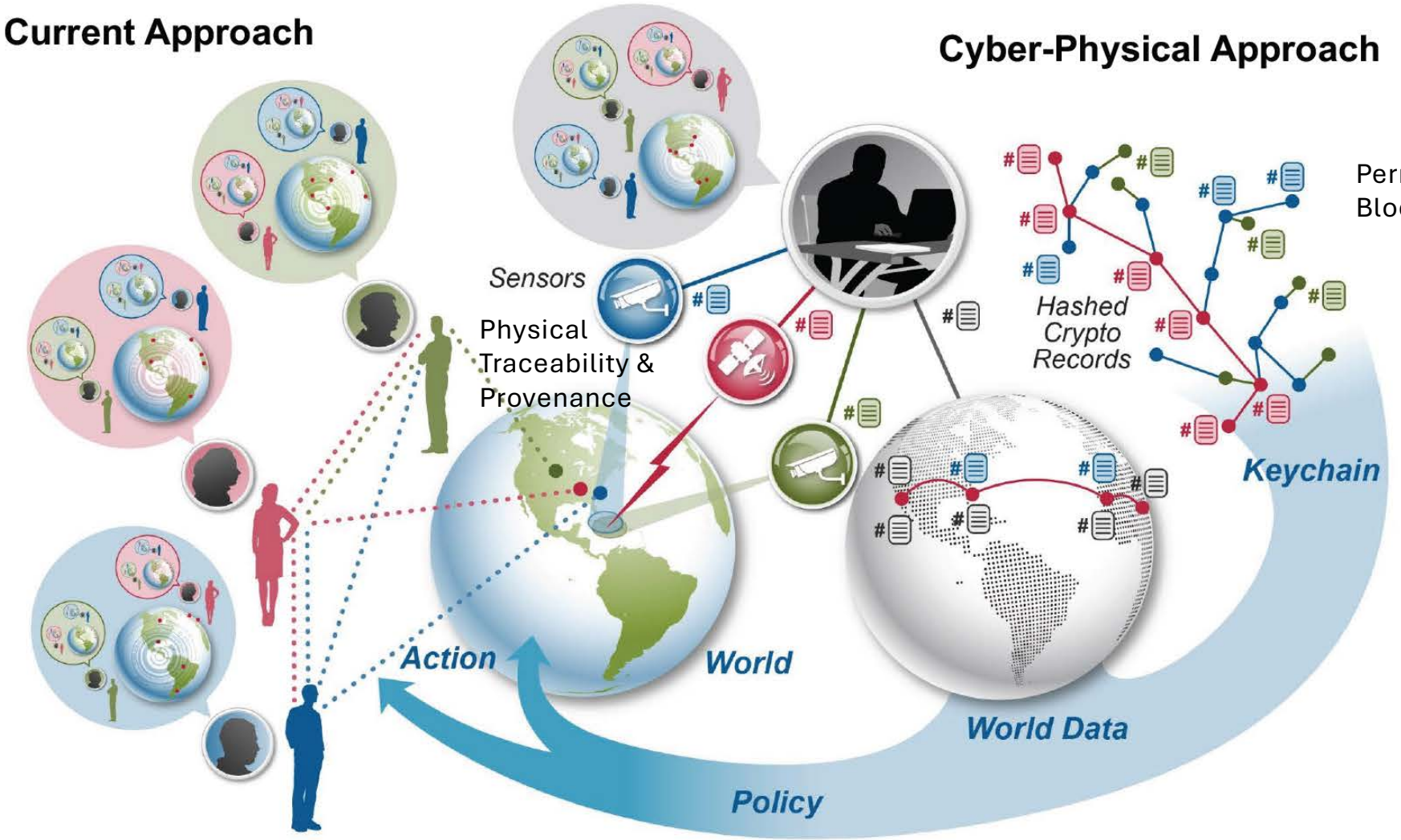


Policy

- EU/US CHIPS supply side investments can benefit from coordination
- Lack of demand side incentives to sustain supply investments
- Lack of coordinated US/Allied technology policy (Trade and Common Defense)

* Icons generated from CHATGTP4o, don't look too closely....

Modern Supply Chain Assurance



Permissioned
Block-chain?

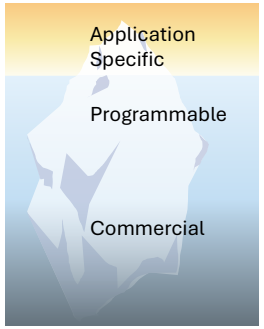
Analytic Marketplace

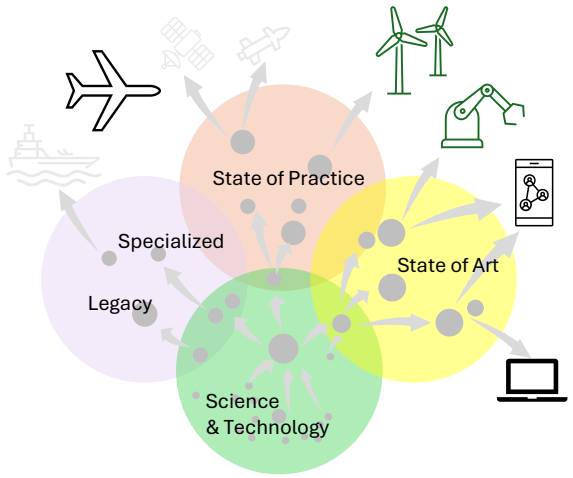
$$T = \sum \frac{A_m}{M_m}$$

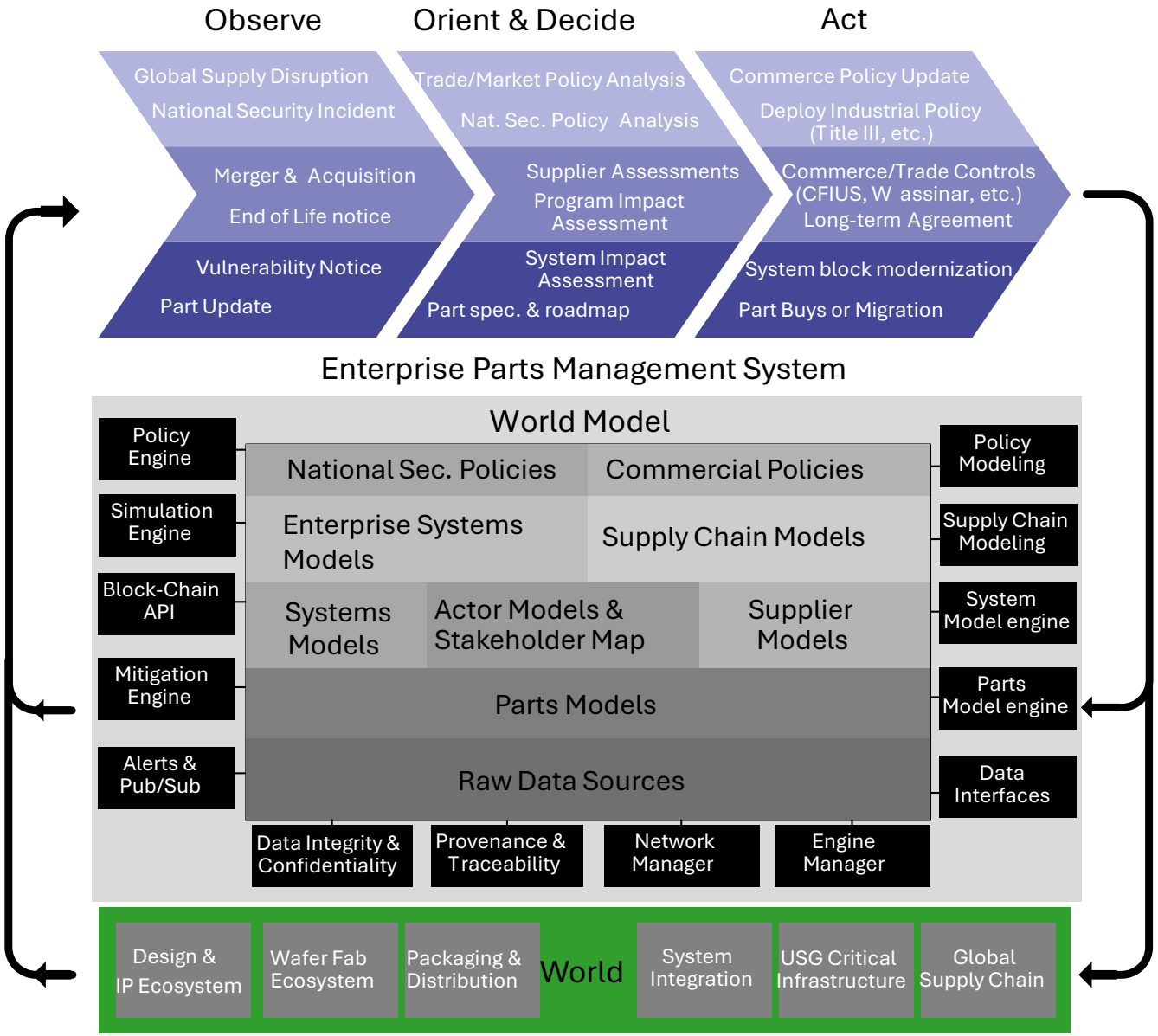
Industry and consumers adopt and USG values traceability and supply chain assurance

Architecture for Enterprise Management

Observe, Orient, Decide, Act to Manage Parts & Supply Chains







Digitalization of Value Chain: Data Marketplaces



Trusted Data Analytics

Monitor & Analyze

Visibility and Traceability

Digitalization Supplier A

Local Storage

RECOVER
IDENTIFY
PROTECT
DETECT
RESPOND
FRAMEWORK

Trust Pillar

Authority Endorser

Trust Nucleus

Asset Trust Anchor

Meta Data

ID-1 ID-2 ID-3 ID-4

Data → Task & Logs → Data → Task & Logs → Data → Task & Logs → Data

Supplier B

Local Storage

- Trust Pillar
- Metadata
- Identifiers

Supplier C

Local Storage

- Trust Pillar
- Metadata
- Identifiers

Field Use

Trusted Assets

Cryptographic Linking

Cryptographic Linking

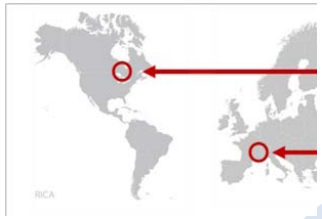
Cryptographic Linking

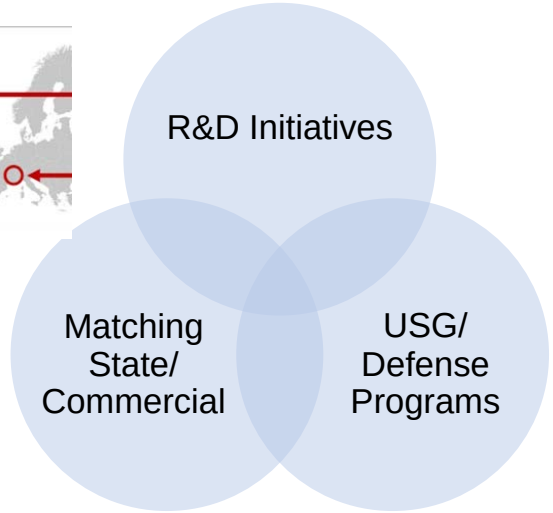
*Source: GSA TIES reply to NIST RFI on Cybersecurity Framework and Supply Chain Risk Management

Assurance USG/Industry Opportunities

Dual Use Roadmap

- Senior Leader Directive & funding
- Funded dual-use roadmap (Services, DIB, ME Supply Chain, etc.) secure supply map
- Identify Assured Supply Chain mappings to Critical Infrastructure (EPMS, AMARO, MQA, DHS, etc.)

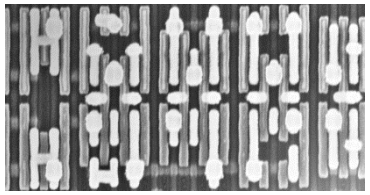




Assured Prototype Programs

- Restock Obsolescence replacement
- Attritable Systems
- New Capability for legacy program (critical infrastructure)





Reverse Engineering

Verification & Validation



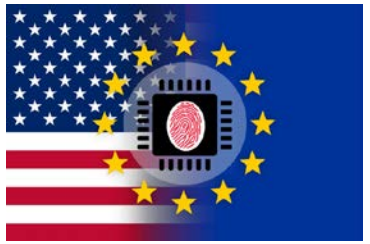
Acquisition/R&D Policy

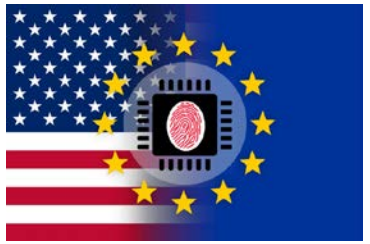
- SWAP-C, where A = Assurance of mission, supply chain, tech overmatch, obsolescence avoidance, etc.
- 15% of Program budget for ME dedicated to demo of new ME tech every 2 years (don't have to buy it)
- Policy and Budget reform in phases to support R&D, Rapid Prototyping, Obsolescence Avoidance through assured R&D ecosystem



MICROELECTRONICS COMMONS
BRIDGING THE GAP FROM LAB TO FAB

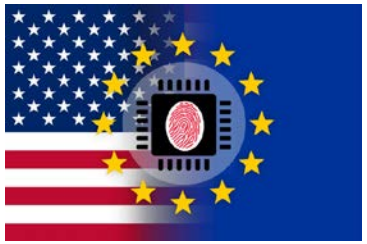
Time for discussion

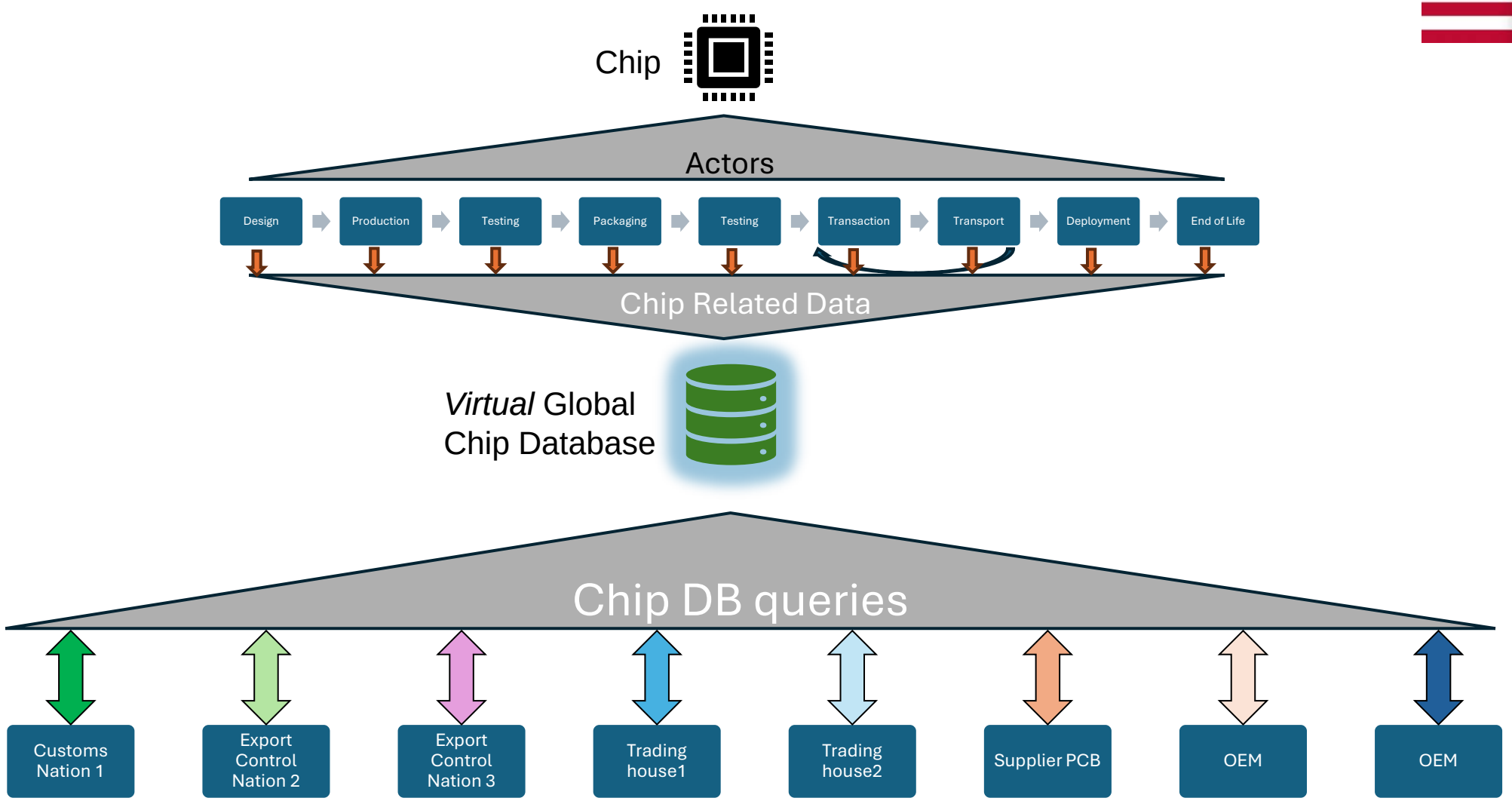




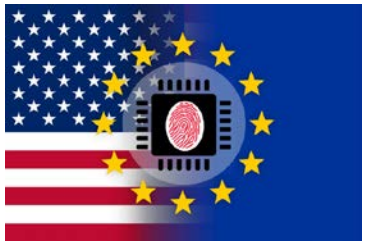
Session 4: Data Privacy and Database Governance

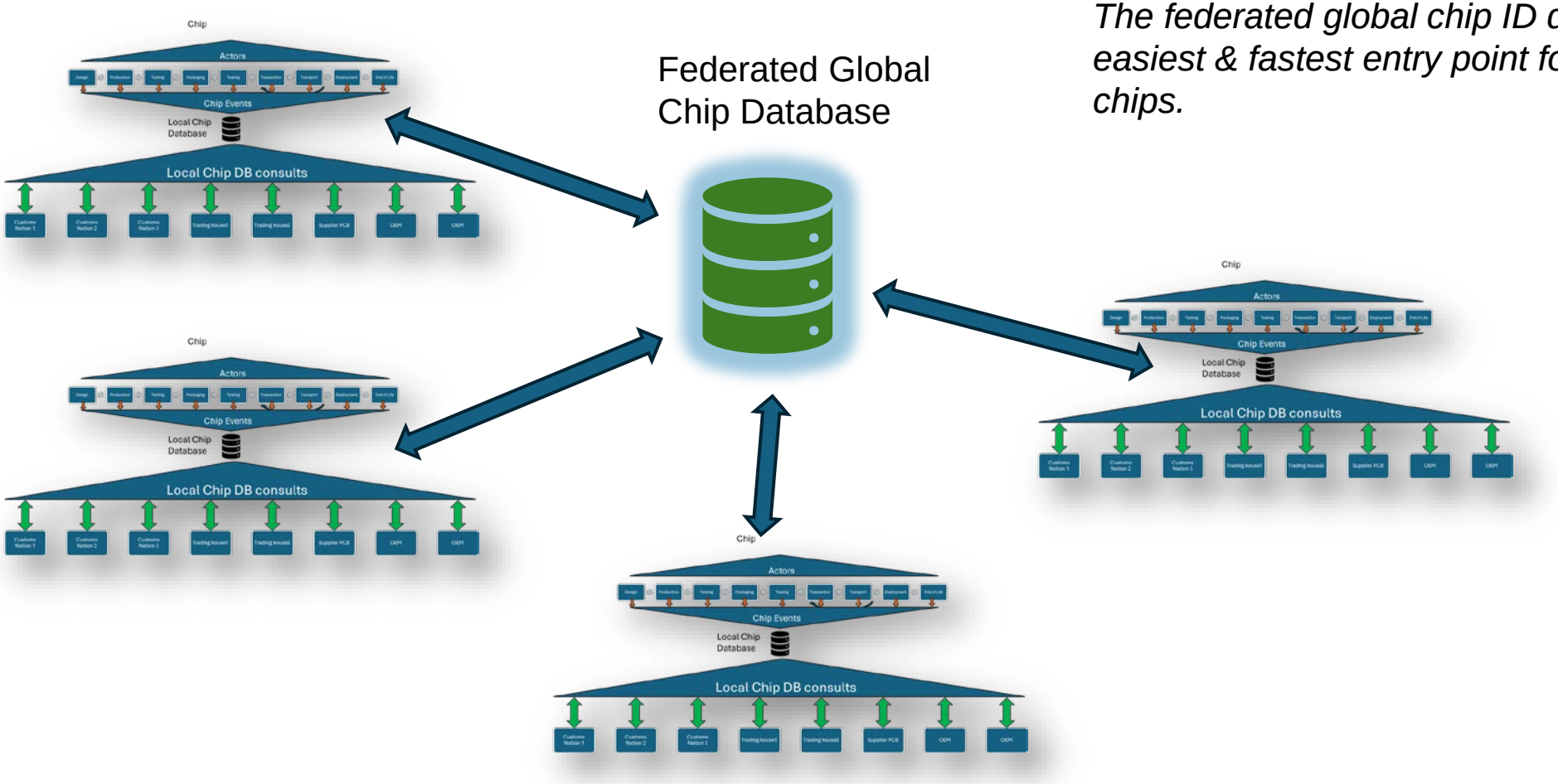
Virtual Global Chip ID Database





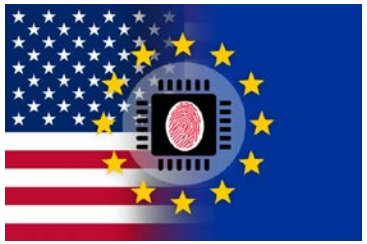
Federated Global Chip ID Database unites existing local databases





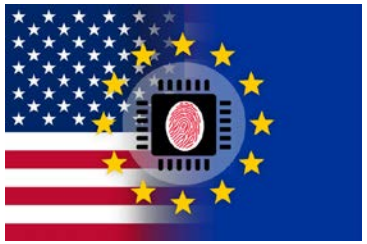
The federated global chip ID database is the easiest & fastest entry point for traceability of chips.

Federated Database requirements (I)



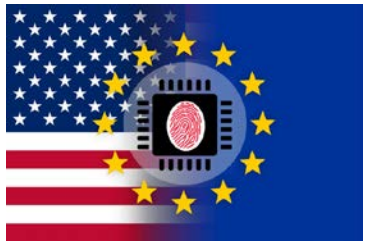
- Virtual Global Database
  - Global Unique Chip ID is the “**key” index** which will **unite** all chip related information
  - Establish **interoperability** and **compliance**
  - **Actual data** remains in **local databases** is owned by the various players in the eco system (sovereignty)
  - **Unified** data (format, semantics, rules etc.)
  - Determines what **information** can be found in which **local data base** using **links**
- What needs to be traced?
  - **Requirements** on shared information availability based **Use Cases**
  - Different **profiles** for different Chip categories
- Who needs to **record**?
  - **Provenance** of referenced **chips** verified by measured data of the chip
  - **Provenance** of entity (and the used tools) entering the information to be verified by **Trust System**
- Who has **access**?
  - Role and access rights based on **Trust system**

Federated Database requirements (II)



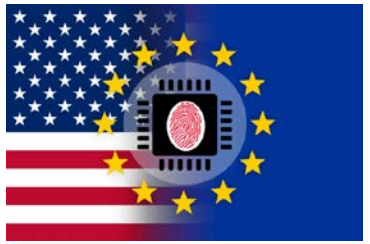
- Trust System
  - **Identification** of businesses and other actors in eco-system **based on existing systems**
  - **Digital Data Market Place** will require **more elaborate Trust system**
- Security
  - Confidentiality
    - *Real* Data is **stored** in local **databases**
    - **Meta Data** requires **less confidentiality**
    - **Access control** to *real* data is controlled by **data owners - Need to know basis**
  - Integrity
    - Ensure Data is always **correct** and **consistent**
    - Ensure Data **can not be changed** by malicious actors
  - Availability
    - Data is **always available** without delay (for entities that have access)
    - Data access is sufficiently **scalable**
    - Data is available **during life cycle of the chips** (40+ years)
  - Non-Repudiation
    - **Ensuring** parties entering data reflecting certain actions **can not deny** having performed those actions

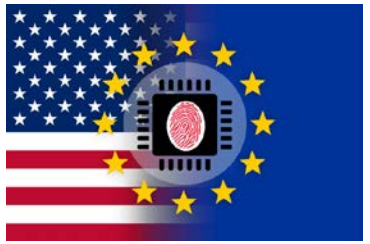
Federated Database Concepts



- Data Spaces Business Alliance
  - **Gaia-X** is a European initiative to create a **federated** and **secure** data infrastructure that promotes data **sovereignty**, **interoperability**, and innovation.
  - **I**nternational **D**ata **S**paces **A**ssociation (IDSA): secure, sovereign data sharing
  - **Fiware Foundation –** Building Smart Applications
  - Big Data Value Association: Innovation in big data and AI supporting Europe's data economy
  - 1,000+ leading key industry players, associations, research organizations, innovators, and policymakers worldwide.
- Similar concepts in other domains and countries
  - Catena-X (Automotive Industry, Europe)
  - ONC Trusted Exchange Framework and Common Agreement (TEFCA) (Healthcare, US)
  - Industrial Data Space (IDS) (Global/Europe)

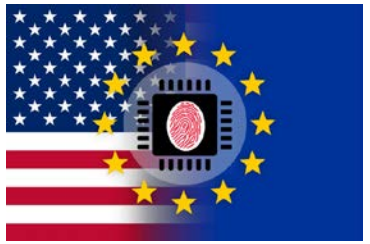
Time for discussion





Session 5: Support infrastructure

Session 5: Support infrastructure



“**Robust cross-border governance infrastructure”** has various levels.

- Vision on database function and
- Implementation of a global manufacturing and data handling infrastructure.

Vision

The Global ChipID strives to allocate a unique number for every chip.

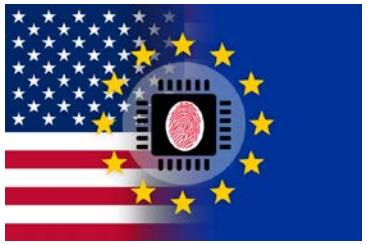
(with an inherent lifecycle use responsibility that can be transferred in the ecosystem)

The issuance, and management of the IDs is the framework and a strict public – non- profit function.

A “supranational” organization with strictest governance requirements.

Similar other industries. Needs to be benchmarked and investigated with top experts in this field.

Session 5: Support infrastructure



Supranational Governance Structure: A non-profit entity will lead, ensuring no single country or company controls the system. It will foster collaboration between allied nations under independent oversight, providing a neutral, secure platform for stakeholders.

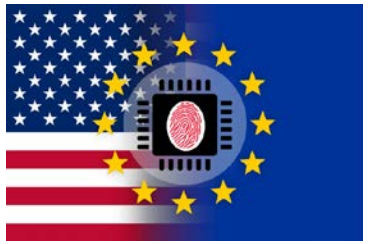
Trust Organization and Public Function: A trust organization will oversee the initial phase, leading to a "public function foundation" in the U.S. and Europe to coordinate stakeholders and ensure transparent, secure operations aligned with global standards.

Transparency and Accountability: Independent oversight will uphold high standards of transparency, ensuring governments, industries, and standards bodies comply with global regulations and build trust.

Government Role in Driving Growth: Governments will provide financial incentives, regulatory support, and public-private partnerships (PPPs) to promote private sector investment in trusted chips, balancing security, and innovation.

Dual Approach - Government Push and Industry Pull: Governments will set market preferences for trusted chips, while businesses across the value chain innovate to create value, fostering a resilient global chip ecosystem.

Session 5: Support infrastructure



The Global Chip ID Database has:

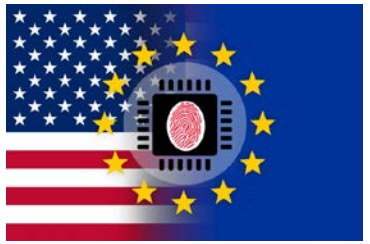
- Market info function – chip number confirmations and administration of the life cycle owner (in the ecosystem) – direct access to and fast response.

- Use case roadmaps – info and best practices for all market parties – not only to participating large organizations but also to new users e.g. SMEs, start ups associations and new countries.

- Manufacturing roadmaps – certification of “trusted” manufacturing lines (preventing rogue-fab operations).

- Financial aspects – t.b.d. see also chapter 5.4 Economic Value Creation.

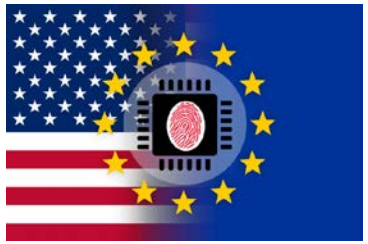
Session 5: Support infrastructure



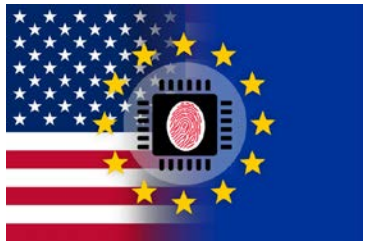
- Roles, responsibilities and next steps.
  - This is clearly the key topic that needs broad and deep investigation.

- Advisory board:
  - USA and EU (but will be extended)
  - Industry, government and public
  - Financial independence
  - Top experts to be involved

Time for discussion



Closing Remarks and Next Steps



- Wrap-up the result of the WS and key takeaways

- Work streams
  - Next meetings in EU & US
  - Technical workshops
  - Budget
  - Proof of concept (PPP)

Closing Remarks and Next Steps

