Component Pedigree

Industrial Technology Working Group

Michael J. Mossbarger

ENT Foundation Inc.

mike@ent.net

The following use case may be considered a grand challenge candidate and will explore tracking both title and possession of any asset in an authentic and legally defensible way. As title and possession changes throughout the scenario each new holder endorses with a cryptographically unique signature. Tracking begins at the moment of manufacture and follows the component through its integration into a composite device as well as to the eventual installation in the end use point. Secure component pedigree is an area of present concern given the amount of semiconductor manufacturing that occurs in locations with minimal regulation, such as China. Chain of possession is possible today through various technologies and vendors. However, ensuring strong chain of title is a more difficult proposition as a component moves through a variety of systems in the various stages of manufacture, integration, shipping, and installation.

If a component can be tracked and its title can be verified with a high degree of certainty then installation/discovery/provisioning of OEM devices/things into secure end points can be accomplished with both greater ease and a greater degree of security. The device may be assumed to be in a known state if both it and its components are traceable, and if systems are in place which use this traceability to provide anti-theft and anti-counterfeiting measures. Ideally, every component, machine, and device in secure systems would have complete chain of title and chain of possession that spanned its entire journey from manufacture to installation. Security, privacy, control, and ownership challenges converge in this use case.

Technology/Utilities/UC006: MPU is made and shipped with complete chain of title and possession	
Vignette	A new microprocessor is being manufactured and needs chain of possession and chain of title so that its pedigree can be verified at all stages of its lifecycle.
Actors	MPU Factory Shipper OEM Another shipper End User
Event	A new microprocessor has completed the physical manufacture process and is being prepared to exit the factory where it was made.
Pre-/Post-Conditions	Pre: Universal decentralized identifier system in place. This may not be one overarching system and may represent a standard way of identifying assets that is universal in all the systems that the asset touches.

	Post: Complete MPU chain of title & possession are established through the MPU's lifecycle. All subsequent title and possession becomes opaque to previous owners at the time of transfer.
Technology	Decentralized Identity system (Identifier + tracking)
Fit Criteria	Component title and authenticity can be established with certainty Component possession can be tracked with certainty Tracking/Information is limited to involved parties only (private).
Scenario	1. MPU manufacture is completed at the factory. MPU is engraved and/or hard coded with an identifier. This identifier is universally unique and opaque, ensuring the identifier doesn't reveal any information about the asset. Identifier establishes a legal means for authenticating its validity. 2. A digital record is established by the manufacturer for the MPU and can be considered the digital title for the MPU. Even if physical MPU is stolen the digital title cannot be stolen. The MPU now has a digital counterpart which is cryptographically protected. Initial title and possession of this digital MPU identity would be with the factory. Similar identifiers for the factory, lot, model, and workers that made the chip are included as information under the MPU's digital record. This information is useful in case the MPU is defective or in case it proves to be compromised later and needs investigation. 3. MPU is packaged into a box. The box has its own digital identity with chain of title and chain of possession. The box's digital record is updated with the identifier of the person who packed the box. MPU identifiers are nested in the box's digital record in the tracking system. Title and possession of all identities in this box are with the factory at this time. 4. Shipper takes possession of the boxes. Title of the boxes is still held by the factory but possession is transferred to the shipper's tracking systems, the digital record of the box may be updated to reflect this change. 5. Shipping company's driver and truck each have an identifier, chain of title, and chain of possession. If driver isn't the authorized driver for the truck, the system may create an alert. Boxes are nested under truck's identifier. If boxes are removed by any party other than the allowed party, the system may create an alert. This is all tracked via the same identifier standard. 6. Truck and its contents can be tracked wirelessly using their assigned identifiers to optimize logistics. Each location broadcast may be identified authentically as the truck's identifier. Identifiers are private, unique and authentic so that they may be monitored by both the shipper, manufacturer, and customer if desired and allowed by the appropriate parties. Optimal route, warehousing, supply chain planning, etc. can all be tracked and optimized by the manufacturer, shipping company, and customer using the same identifier system providing uniform vertical and horizontal integration. 7. Box is received by the OEM who knew exactly when the shipment would arrive thanks to tracking. OEM scans truck identifier and then each box identifier to verify all boxes are correct boxes. OEM then

	unpacks the boxes and scans each MPU identifier to verify all MPU's are correct for each box. If any boxes are missing from the truck or if any MPU's are missing from the boxes the manufacturer can be notified and the incident investigated. If any boxes are in the truck or MPU's are in the boxes that shouldn't be there, each can be set aside and investigated. OEM accepts receipt of goods by digitally signing. Manufacturer is able to verify receipt of shipment. 8. Complete chain of title and possession are visible to OEM. Once the OEM is satisfied with the MPU pedigree, both title and possession of MPU's transfer to OEM in tracking system (perhaps with payment). Chain of title (ownership of digital records) may now be hidden from previous owners but can still be passed on to subsequent owners to verify complete pedigree. Ideally, ownership is also opaque to all third parties and does not rely on a centralized system, which maximizes privacy. If boxes are disposable then they can be recycled and their identities transferred to the recycling bin (which also has an identity). This lets the recycling company know when to pick up the container… but that is another vignette. 9. OEM installs MPU's, along with other uniformly identified components into an OEM product. OEM also installs application into product and this application similarly has a standard, authentic identity. OEM product is given a new identity and digital record and title/possession of this product are assigned to the OEM. Components, MPU(s), and applications installed in product are nested under OEM product's identity. If in the future any of these mismatch, the system may create an alert. 10. OEM product is packaged with its identifier and goes into a box along with other products. 11. Similar tracking of title and possession for boxes, truck, and driver as detailed in steps 3, 4, 5, and 6 above. 12. Box is received by the end user who knew it was coming thanks to the broadcast tracking. End user scans the truck and driver identifiers, then each box identifier, then unpacks the boxes and scans each product identifier. If any of these identifiers are not nested with the correct sub-identifiers then the manufacturer/shipper can be notified and the incident investigated. If any products are in the box that should not be in the box, these are set aside and investigated. 13. Once end user is satisfied with title and possession pedigree of products, components in the products, and applications loaded on the products then all transfer to end user in tracking system (perhaps with payment). Previous owners now have no visibility except as allowed by end user. 14. 'Things' can now be installed in the millions or billions, scalable to any number, without individual discovery/provisioning. All devices, things, components, and applications have complete chain of title that is authentic.