The Digital Business Marketplace Catalyst - Phase 3

The Secure Supply Chain Initiative

The market size of global supply chain management was $15.8bn in 2019 and predicted to reach $37.4bn by 2027 [alliedmarketresearch], however, the supply chain remains vulnerable to issues such as theft, fraud, loss, damage and delays.

In addition, the 4th industrial revolution and Smart X scenarios are being constrained by market segment fragmentation, and with costly and risk-prone, labour-intensive processes. As a result, Industry 4.0 and Smart X deployments will struggle to scale until the supply chain evolves into an ecosystem that can repeatedly deliver secure devices, services and solutions, which can be easily aggregated, offered, ordered, delivered, installed and managed online.

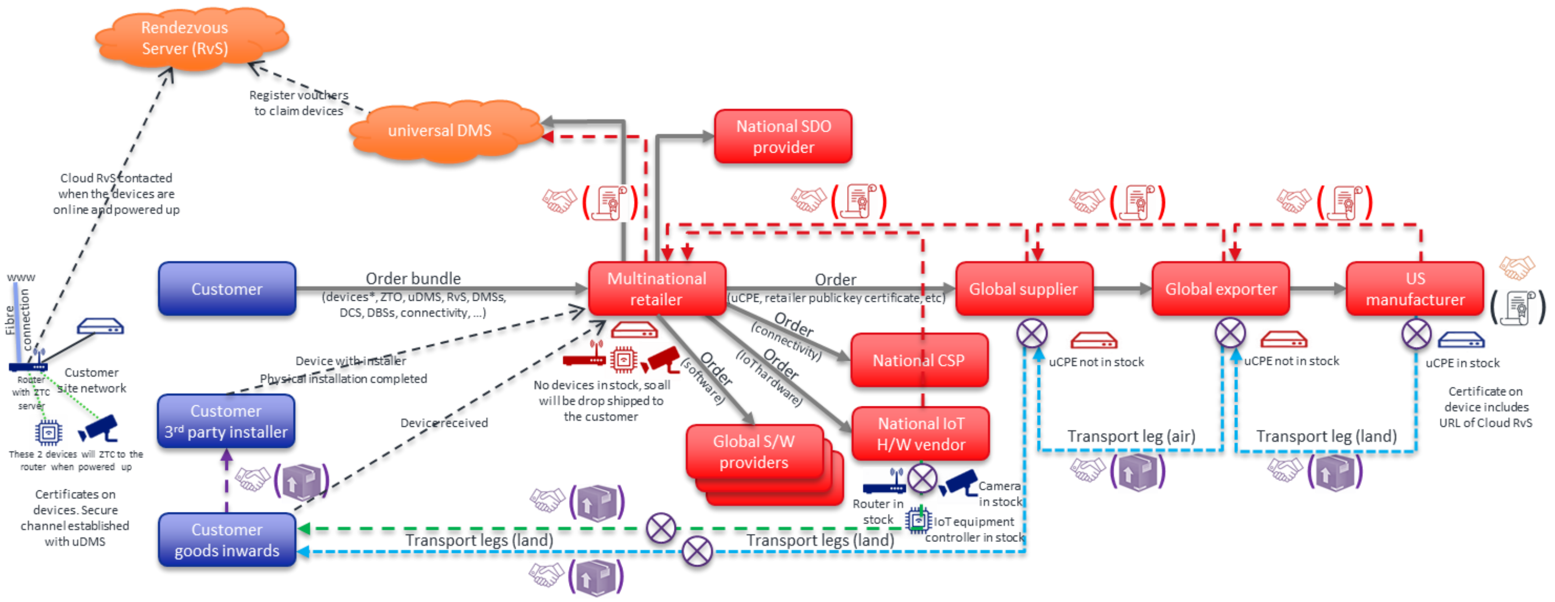
The DBM Catalyst secure supply chain initiative is actively addressing and mitigating these issues by combining a number of ecosystem, distributed ledger and zero-touch technologies that will deliver maximum growth for the supply chain business and for Industry 4.0 and Smart X solutions. As such, the secure supply chain initiative delivers part of an overall Smart Infrastructure which enables any of the Industry 4.0 and Smart X market sectors to deploy and manage their specific control systems and Artificial Intelligence, etc. on top.

Also, because of the criticality of supply chain security legal acts are now appearing to be mandated by a number of national governments. For example, an interim rule has been drafted by the U.S. Federal Acquisition Supply Chain Security Act to dictate how everything sold to the U.S Federal Government will need to be handled. https://www.federalregister.gov/documents/2020/09/01/2020-18939/federal-acquisition-supply-chain-security-act. The DBM Catalyst conforms to this interim rule.

In phase 1 and 2 of the DBM Catalyst, our focus wasn’t on the end-to-end secure supply chain but on enabling secure zero-touch deployment of devices; enabling a frictionless ecosystem of business partners; and providing an ecosystem-wide plug and play environment for product managers. In these earlier phases, we felt that these three capabilities would form the basis of a secure supply chain but we knew that there were gaps in our solution that needed to be addressed in phase 3.

So, what have we built in this phase, what’s new and how does it meet the requirements for a global and end-to-end secure supply chain?

Multinational secure supply chain architecture & user story scenario



For our secure supply chain demo we created a scenario where an enterprise customer wishes to purchase, in a secure and zero-touch way, a solution which is composed of a bundle of products and services that will be delivered through multiple supply chains.

- The commercial actors in this ecosystem are the customer, the multinational retailer, the global supplier, the global exporter, the U.S. manufacturer, the national SDO provider, the national CSP, the national IoT hardware vendor and three global software providers.
- We continued to use the Infonova platform to underpin this commercial ecosystem not only because it can provide a full BSS capability-as-a-service to every business partner in the ecosystem, but, more importantly, because it allows chains of ecosystem partners to trade products and services with each other in a frictionless way – a quality that is paramount in supply chains
- In this scenario, the bundle being purchased consists of a Dell VEP uCPE, which is an edge compute node, a Teltonika router, an AWS DeepLens smart camera, a Raspberry Pi, which acts as an IoT controller, some network connectivity, and an assortment of software services running in the cloud and on edge devices. When the customer orders the bundle, we assume that no physical stock is held locally by the multinational retailer, the global supplier, or the global exporter. The U.S. manufacturer will therefore be drop-shipping the uCPE to the customer, while the national IoT hardware vendor will be supplying the router, camera and IoT controller. The national CSP will be providing the network connectivity, while the multinational retailer, national SDO provider and the three global software providers will be providing the assorted software services.
- The commercial supply chain runs from left to right as far as purchase ordering is concerned; right to left as far as invoicing is concerned; and again, left to right as far as payments are concerned.

- Delivery of the physical goods is done by a physical supply chain, which runs from right to left. Here, we have a short national supply chain from the national IoT hardware vendor to the Customer, and a longer international supply chain from the U.S. manufacturer to the Customer. Additional actors are brought into play, such as couriers, freight forwarders, transit sheds and customs, which could be added to the commercial ecosystem or, as in this case and for simplicity, regarded as supporting roles and were kept outside the scope of our automated commercial ecosystem but very much in scope as far as the physical supply chain is concerned.

- In phase 3, we introduced the use of the IOTA foundation DLT and Tangle network to underpin and immutably record transactions in this physical supply chain ecosystem because it is open source, fast, highly scalable, feeless, permission-less [because not all writers are known], and because there are a number of great track and trace services, such as Zebra and PING asset, that leverage the IOTA DLT, of which, we currently use Zebra for our physical supply chains.

- To deliver firmware, software, certificates, credentials and configuration to edge devices in a secure and zero-touch way, we continued to use Intel SDO and BT ZTO alongside the Infonova platform, however, we have added the R3 Corda DLT to address the security profile of this part of our solution.

- We continued to use Intel SDO because it supports chip-to-device-management-platform encrypted channels, because it enables devices to be provisioned at the point of installation rather than only at the point of manufacture, and because it offers something called “late binding” which allows customers the ability to choose their target device management platform at the time of ordering. Additionally, Intel is driving SDO into the Fast IDentity Online, or FIDO, IoT standards working group and is open-sourcing this work.

- Intel SDO uses an artefact called an ownership voucher that is needed for a cloud- or edge-based device management platform to claim ownership of a device before it is powered up. This ownership voucher originates at the device manufacturer and needs to be extended and passed on as the device’s ownership changes across the commercial supply chain towards the customer.

- Intel SDO assumes a secure supply chain in which to propagate the ownership voucher along the commercial supply chain. In phase 1 and 2, our solution assumed that SDO ownership vouchers were transferred across the supply chain in a secure way, however, in reality, this wasn’t the case and we knew that this gap needed to be plugged. So, in phase 3 we introduced the use of the R3 Corda DLT to plug these gaps. Corda provides us with a NIST (National Institute of Standards and Technology) cryptographic standards-compliant DLT that prevents ownership voucher replication (which is akin to double-spend in the Bitcoin world); that provides an immutable record and secure delivery of ownership voucher transactions and provenance across a distributed supply chain; and that is built around the use of Public Key Infrastructure (PKI) and Certificate Authorities (CAs) to manage business partner onboarding and permissions. Like IOTA, Corda is also open source, fast, highly scalable and feeless. Additionally, because Corda operates a permissioned DLT and supports the concept of a notary, it keeps information to a known network of commercial entities on a need-to-know basis, and enables business partners to quickly reach a consensus over transactions.

- Intel now also enable Bare Metal Onboarding with SDO, which phase 3 uses because it gives us the ability to do a complete secure, automated and human-free bare metal build from the cloud or edge.

- Whilst Intel SDO provides a single attestation technology and the ability for a single device management system, or DMS, to claim ownership of devices and, subsequently, manage them, there is a need to provide customer choice regarding attestation technologies and the ability to use multiple DMSs to manage various aspects of a device - for example, one DMS to manage the hardware, one to manage the software infrastructure, and one to manage each of the applications running on the device. We continued to use BT ZTO because it provides those such extra capabilities, permitting extra choice and flexibility over and above Intel SDO. In addition, and a big missing piece in device zero-touch capability, is the ability for devices to automatically find and securely connect to a network access point without requiring an administrator to manually log into the device and enter any network access point credentials, which is an error-prone, time-consuming and costly process, and which also opens up a number of cybersecurity attack surfaces. As BT ZTO enables this much-needed zero-touch connection capability for a range of network access technologies, such as Wi-Fi, NB-IoT, LoRa, 4 and 5G, we continued to use it in phase 3.

In summary, the team are confident that most supply chain issues relating to security, handling, tracking and tracing, device installation and management, and the commercial ecosystem wrapping have been solved by this solution.

The main solution components are either production-grade or already live products. Our innovation has centred on researching and merging several key technologies together in a way to minimise current supply chain and IoT business problems by raising automation, trust and customer experience levels whilst bringing down costs.

Because we chose to use production-grade components, we can immediately work on productising and ruggedising the solution as a whole. For example, our demo only showcases a happy path scenario, so we need to look at edge cases and how to handle fallout. We've also recently started "Red Teaming" our secure supply chain solution with the goal of improving the overall cybersecurity integrity of both the solution and also of the actors within the ecosystem by using the Intuitus SOC-as-a-service.