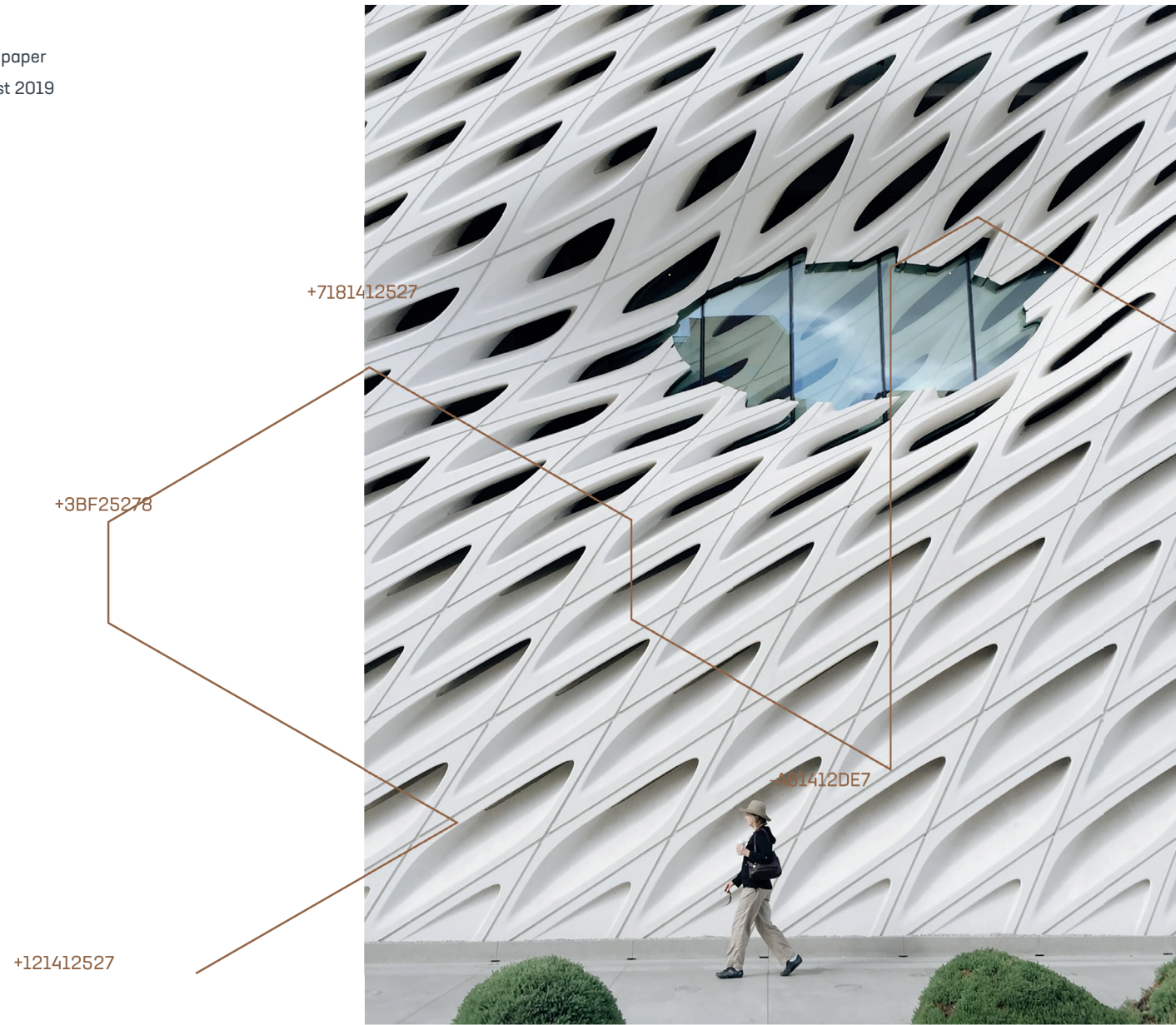
guardtime

guardtime.com

Enabling Multi Party Trust in the Era of 5G and Multi-Access Edge Computing

Whitepaper

August 2019



Introduction

Multi-access edge computing (MEC) and 5G are converging to become a revolutionary opportunity for telecom operators and their enterprise and government partners. A strategic race has begun for operators to be first movers in 5G and MEC, deploying infrastructure and service access in order to capture the rise of machine to machine, IoT connections and AI/ML decision inference.

This paper analyzes the challenges facing operators as the market moves from a centralized security model to a decentralized and federated model. We then introduce Guardtime MIDA, a security and trust platform optimized for 5G MEC convergence.

5G and MEC

Converged 5G networking and MEC promises support for massive scale device connections. MEC server platforms that are currently being deployed have to be able to deliver real-time provisioning, device/data management, scalable security and access/authentication/ authorization capabilities into and from decentralized architectures and networks.

Moving analytics and decisions to the edge also means that less data will be sent to the data center or cloud, promising greatly decreased costs for IoT and mobile ecosystem participants and addressing the walled gardens of the past that resulted in data silos and service monopolization. Elimination of these barriers, as well as the increased numbers of newly regulated ecosystem participants will greatly increase management and service complexity with 'many-of-many' new subscribers coming online to utilize, govern, orchestrate and secure MEC for value added services and new revenue streams. This evolution challenges telecom operators to move from a centralized security and data protection model to a decentralized and federated model.

While the convergence of 5G and MEC provides an opportunity to vastly open the ecosystem for new data-driven businesses, moving data faster and to more devices also requires a paradigm shift across many domains that include device and infrastructure provisioning, identity and subscription services, data protection and governance, and Machine Learning/Artificial Intelligence security.

Current challenges in 5G and MEC

With the almost constant attacks on telecom infrastructure and management systems, every network hardware OEM using the same commodity security frameworks is exploring new solutions to harden and secure their products and customer data at the edge.

The adoption of "always-on" architectures, coupled with the proliferation of edge compute and IoT devices has rapidly changed the landscape in which businesses and telecom operate. With almost every sensor, edge device and electronic control unit now directly or indirectly connected to a network or the Internet, the attack surface has increased significantly. Traditional tools are not equipped to detect, defend, and remediate attacks at scale, in an acceptable time frame, and at an appropriate cost.

In order to keep up with the scale, distributed nature, and complex heterogeneous ecosystems of today's connected edge landscape, a paradigm shift is needed. The common systemic issue is the lack of a common trust fabric from the edge, to the consumption of the data, and finally at the management plane to make decisions about this data.

Worldwide data creation is estimated to grow to a staggering 163 Zettabytes by 2025. In IoT alone, there will be a predicted 42Bn IoT devices online. While organizations will seek to monetize and analyze more and more services on top of this data, protecting it will also grow exponentially more complex.

Some of the challenges faced in MEC are:

+ PKI Challenges: In the 5G era, PKI as a provisioning (access, authorization and accounting) scheme will be challenged at scale with the many counterparties and service providers who require device or edge service access and may conceivably have no business relationship (federation or geographic/regulatory restrictions to share credentials or certificates). Given the sheer density of devices, provisioning and revocation using PKI becomes complex and costly.

+ Privacy concerns - In the past, companies had on-premise centralized networks that only trusted people were allowed to access. Today, many companies have infrastructure in their private cloud and utilize public cloud resources. By moving processing of traffic and services from a centralized cloud to the edge, it becomes imperative to address privacy on regulated information such as health and financial records and in real-time before dissemination.

  Associated privacy and compliance requirements have become regionalized with heavy levies for misuse as defined by the data protection standards like GDPR. Governance, risk and compliance for this data will be an enormous challenge considering 50% of organizations have not updated their data security strategy in 3 or more years.

+ Credential Compromise - Current exploits against credentialing applications are catastrophic considering 5G router and edge platform capacities. Consider that 5G MECs push computing capabilities closer to the Radio Access Network (RAN) and in turn closer to subscribers achieving device densities approximating 1 million devices for every square kilometer. Credential compromise of device management and control systems will lead to exploitation at scales that industries have not previously experienced via man-in-the-middle or lateral access attacks. Current deployments are attempting to use traditional credentials in a highly decentralized architecture, reused and weak credentials are exposed to compromise, effecting large amounts of devices with little awareness or ability to revoke credentials.

+ Lack of multi-party trust - Moving data faster and to more devices will not be effective without business and consumer confidence in their devices and data. If this new data driven economy is to flourish and grow, decentralized participants will have to obtain access to and manage edge resources. Decentralization also means federation between participants. For 5G to deliver better outcomes, new flexible multi-party Authentication, Authorization, and Accounting (AAA) platforms and trust anchors will be needed that work at scale, are more secure, while reducing management complexity.

+ Lack of scalability in identity management - With the billions of devices coming online, 5G MEC infrastructures needs a secure way to subscribe and manage the identities of each IoT device on network as well as a scalable way to govern the data being transacted off the device in accordance with sovereignty regulations like the EU GDPR.

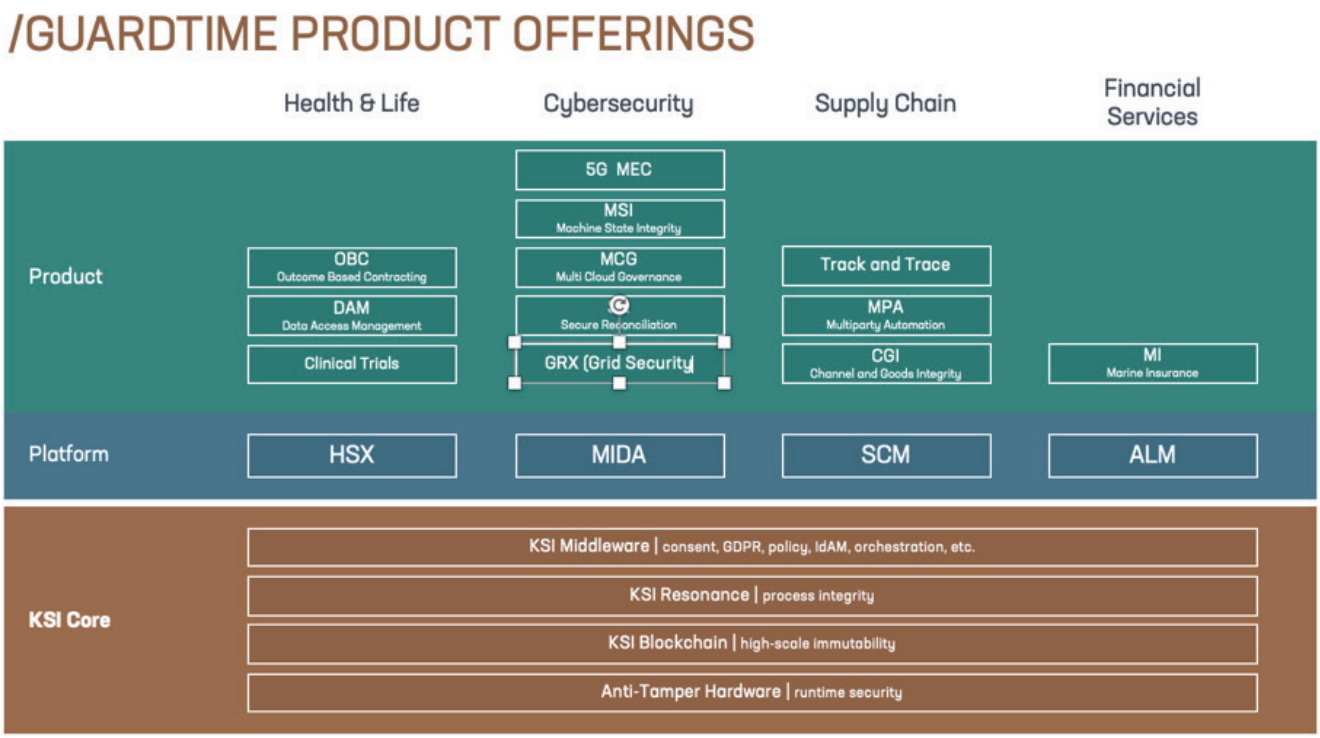
+ Data manipulation - IoT/Sensor data is collected at scale and can be manipulated during transport or in storage without detection, during collection to upstream business intelligence and AI decision toolchains. Unverified IoT/sensor data consumed by and/or shared among untrusting parties can lead to an additional liability of providing services and making decisions on manipulated data.

+ Lack of proof of provenance - Uncertainty over a meaningful data provenance trail for the data – where did it come from, can the quality of the data be trusted, and was the ingest treated with the same governance and compliance criteria that define liability.

MIDA: 5G MEC Data Governance and Security

In this section we introduce Guardtime's MIDA Platfrom, a data governance and security platform based on the KSI Blockchain, a globally available trust anchor capable of transacting at the scale and speed necessary to address the challenges for 5G MEC convergence. Benefits to the 5G MEC ecosystem include enhanced security, reduced device management complexity, interoperability and real-time measurement/monitoring forensics in and out of MEC to third party systems, thereby enhancing participant data orchestration, governance and compliance activities across the many federated networks utilizing MEC services.

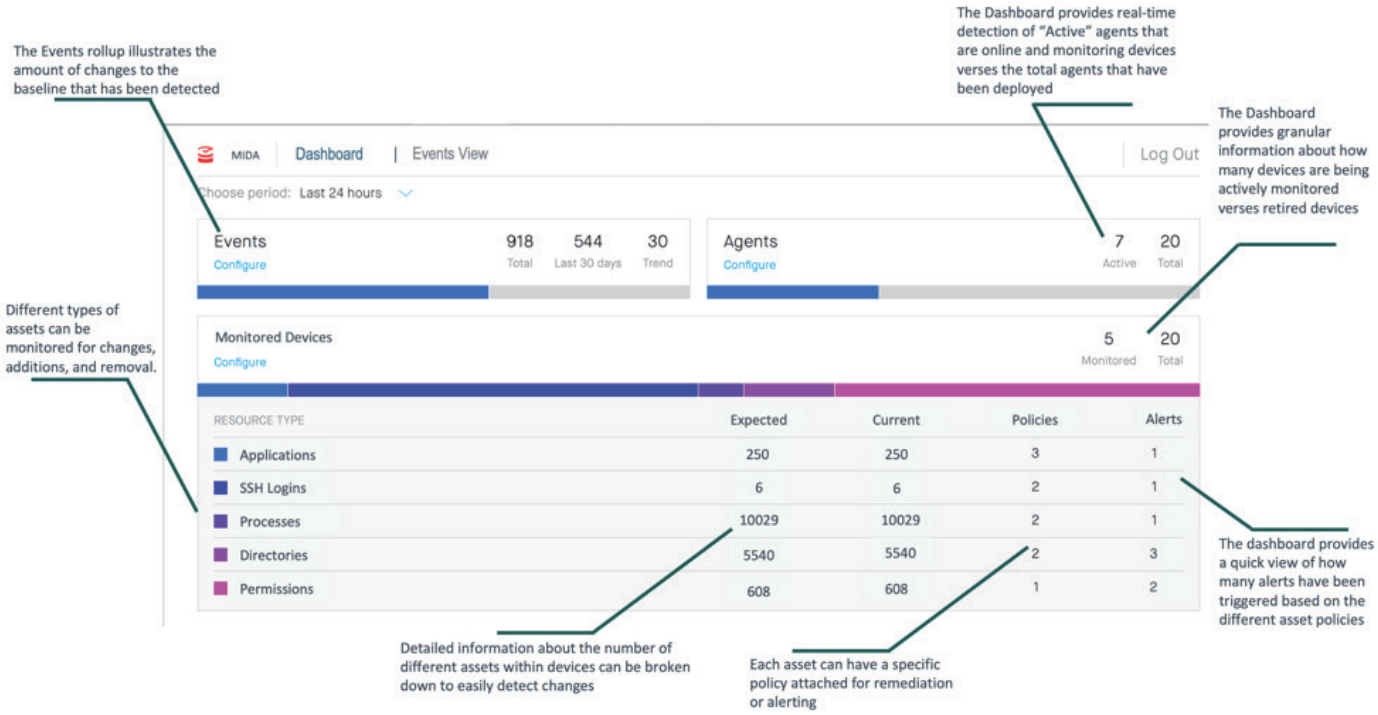
MIDA is a platform that sits on top of the KSI blockchain stack. Developers are able to take the MIDA security APIs and build products designed to solve specific security challenges – including OT/IT convergence in energy grid security, multi-cloud governance, secure reconciliation and 5G MEC data governance. Appendix I gives a high-level overview of the stack and in this paper we focus on the MIDA platform and 5G MEC data governance.



Configurable and Tailored MIDA Dashboards

MIDA provides dashboards that provide concise and actionable information to the end users. In order to provide this data in the most meaningful manner, the dashboards can be tailored and configured based on the specific type of asset, device or data being monitored, updated or protected. The image below illustrates the MIDA dashboard showing device monitoring wherein various data points are captured in a single pane of glass approach. The dashboard allows end users to configure which data points are relevant for their infrastructure, providing a precise and actionable holistic view of their infrastructure and its current state.

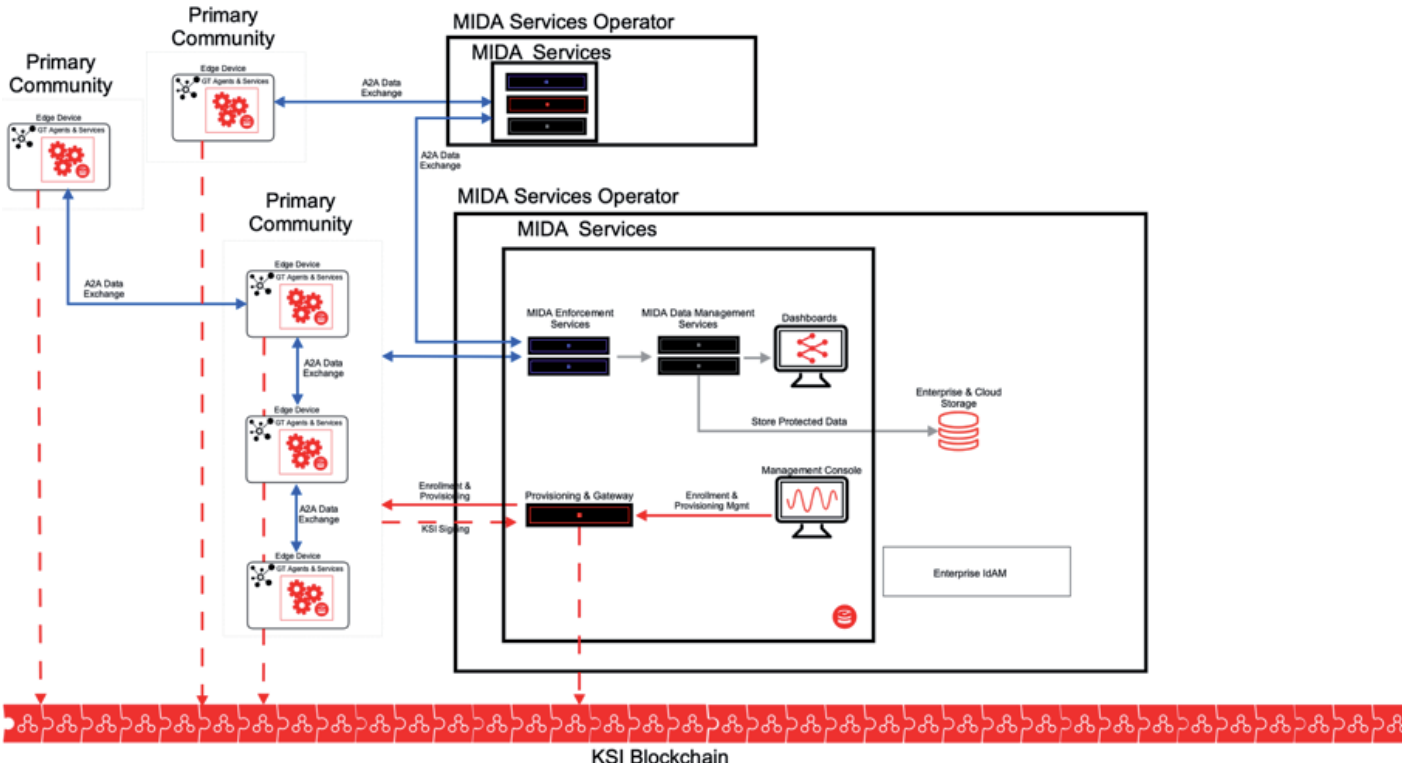
For this example, the illustration below provides more detail on the various aspects of the dashboard.



MIDA Logical Architecture

The image blelow illustrates an example logical architecture for a MIDA Edge deployment. In the logical architecture:

1. Data can be distributed in the any-to-any model between edge devices.
2. Devices are individually enrolled and provisioned with the ability to participate in the KSI blockchain
3. The MIDA Service Operator can create and distribute trusted updates to specific devices or groups of devices.



MIDA Platform Components

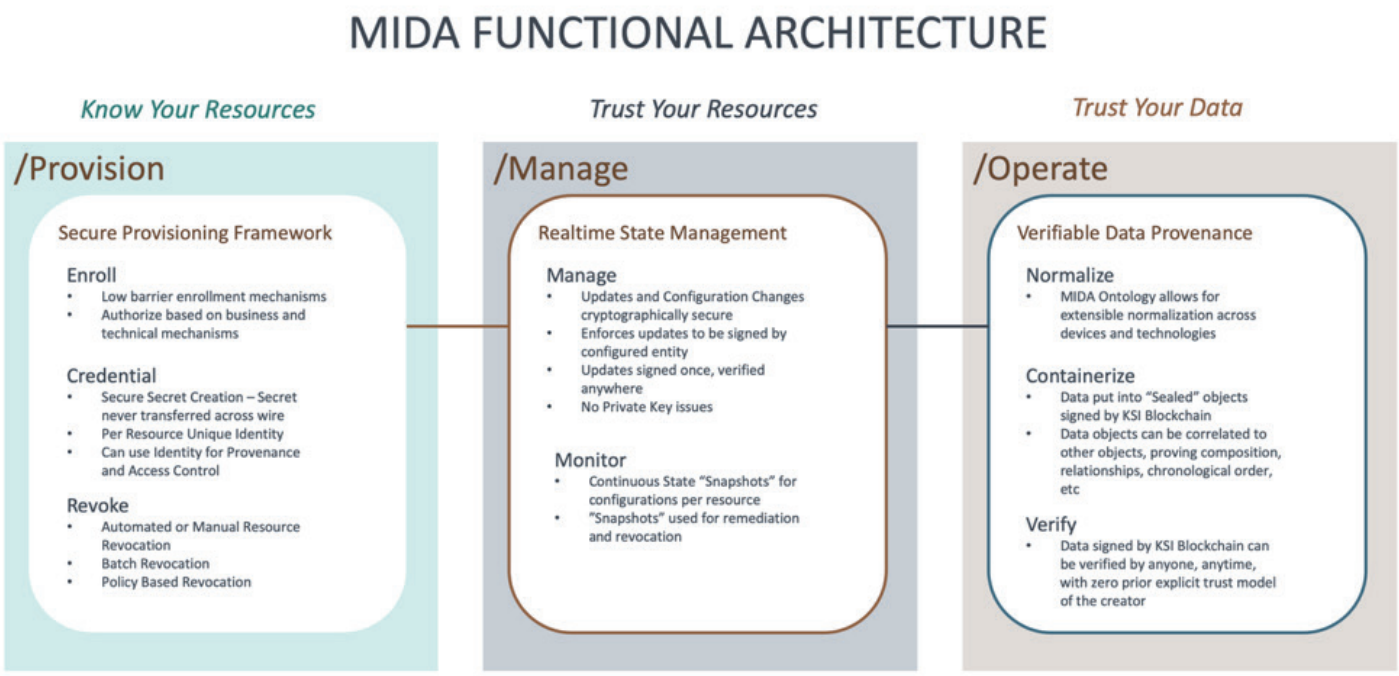
MIDA converges device management and monitoring with scalable data protection. The MIDA platform achieves this in a modular manner, the components of which are:

+ Provision - Provides the ability to "Know Your Devices", or enroll, provision and revoke devices.

+ Manage - Provides the ability to "Trust Your Devices", or manage updates and changes as well as continuous state monitoring.

+ Operate - Provides the ability to "Trust Your Data", or create cryptographically verifiable data.

These modules are combined to provide the full end-to-end security for edge computing operators.



Provisioning Module – Credential and Provision Devices

The Provisioning Module provides the ability for flexible enrollment mechanisms as well as credentialing and revoking devices. With this module, owners and operators can leverage MIDA to index and authenticate devices in order to mitigate against rogue device attacks in a decentralized and heterogeneous environment.

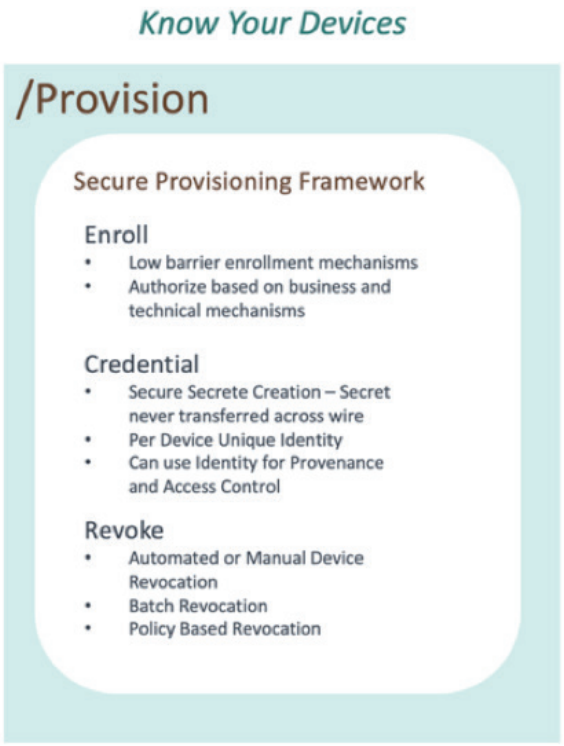


Figure 1 - Guardtime MIDA: Provisioning Module

Provisioning Functionality

+ Operators have the ability to configure the devices with a trusted enrollment token. These can come in the form of a manufacturer key, a license key, or a form of PKI.

+ Devices will leverage that enrollment token to gain access to a unique credential allowing the devices to participate in the KSI Blockchain.

+ Devices can then leverage the KSI Blockchain Identity to authenticate with backend systems, or sign data that is being sent to the backend system, attributing data uniquely to individual devices.

+ At the device end of life or in the event of a compromise, automated workflows or semi-autonomous workflows can revoke these credentials, disallowing these devices to participate as trusted devices.

Functional Components

+ MIDA Enrollment Services: These services provide the necessary backend components to configure enrollment methods, revocation, and authentication of devices.

+ Device Agents: These agents provide the on-device capabilities to provision, communicate with the KSI Blockchain and authenticate with the backend services.

Manage - Securely Manage and Monitor Your Devices

The Management Module provides the ability to manage devices and continuously monitor their state. The Management Module provides the ability to enforce only KSI Blockchain secured firmware and software updates to be executed on the device. The module also includes continuous monitoring capabilities, which provide real-time state attestation of firmware versions, software configurations and network configurations. The module also provides alerting based on baselines and thresholds. It provides semi-autonomous or autonomous revocation.

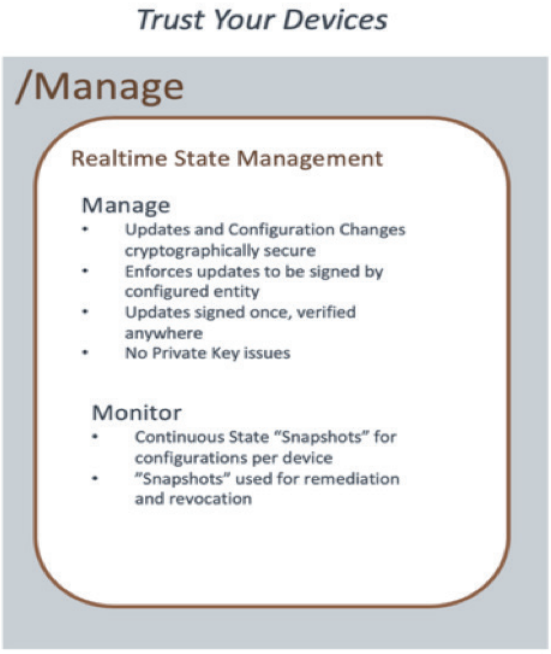


Figure 2 - Guardtime MIDA: Management Module

Provisioning Functionality

+ Operators have the ability to configure agents to monitor specific files, applications and performance metrics on the devices.

+ Operators will have the ability to set specific KSI Blockchain Identities to push updates and changes to the devices.

+ The devices will then create KSI Blockchain Signed state snapshots from the devices and send them to the backend services.

+ The backend services will capture and correlate the device state to thresholds and baselines.

+ If the devices state varies from the desired compliant state, alerts and revocation can take place.

+ During an update or change, Operators can create trusted update packages signed by the KSI Blockchain.

+ The trusted update packages can be sent to specific devices or groups of devices

+ Devices can leverage the configuration to validate the update before applying or executing the change

Guardtime MIDA monitors the entire ecosystem to give insight into the total number of resources being protected. With every event being cryptographically signed, there is traceability of entire environments down to granular events exposed to the end user.

Functional Components

+ MIDA Management Services: These services provide the necessary backend components to create trusted updates and software packages to be sent to devices. They also maintain and receive the state of the devices to provide the input into variations from configured baselines and thresholds.

+ Device Agents: These agents provide the on-device capabilities to verify incoming updates based on KSI Blockchain signatures and send configurable device state attestation to the backend.

Operate – Cryptographically Prove Event Relationships at Scale

The Operate Module creates trusted and accountable data from devices, protected by the KSI Blockchain signatures. This data is cryptographically "sealed" proving the entity that created it, time of creation, and protects against manipulation of the data. Because KSI signatures are independently verifiable across organizations and technologies, the data becomes highly portable, significantly increasing its data monetization and value for AI and Machine Learning processing.

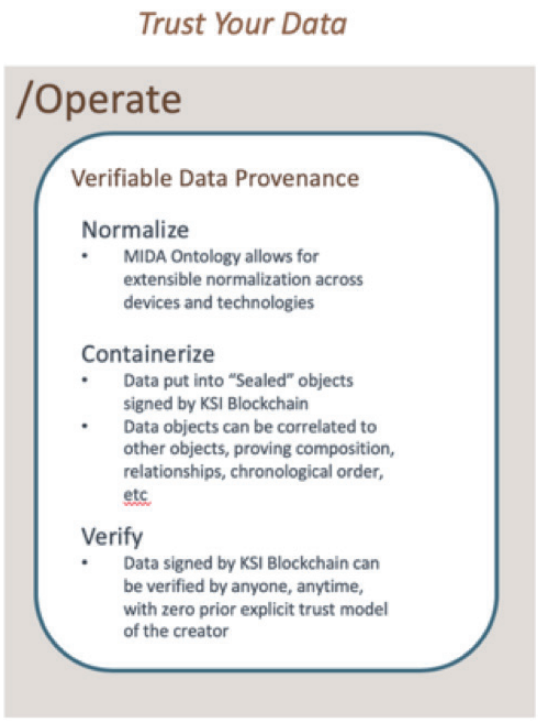


Figure 3 - Guardtime MIDA: Operate Module

Operate Functionality

+ Operators have the ability to configure the device to normalize and sign data based on operational needs
+ The devices will capture data and each data payload will be normalized and signed by the KSI Blockchain
+ The backend services will be able to receive the data and verify the validity of the data, mitigating any data manipulation as it is sent from the device using the KSI Signature
+ The backend services will also verify the validity of the data, using attributes and context such as time, or location before processing
+ The backend services can append useful information to the data received by the backend such as time of receipt or location of receipt.
+ Data varying from the ruleset can be KSI signed to denote suspicious or malformed data and can then be alerted and quarantined, or exchanged to another location
+ Data can be organized and processed in the backed for further analytics and business decision operations

Functional Components

+ MIDA Data Management Services - These services provide the necessary backend components to validate, alert and store data from the devices.
+ MIDA Data Capture Agents - These agents provide the on-device capabilities to create trusted data using the KSI Blockchain, based on configurable policies.

Along with protecting the actual data sent from edge devices, it expands upon traditional monitoring and command and control solutions to provide Owners, Operators, and Certifiers with enhanced control, cryptographic data verification and provable, real-time state attestation.

The combination of the three modules described above enables:

+ Scalable and Cost-Effective Device Management and Credentialing
+ Realtime Discovery of Misconfiguration or Device Changes
+ Provable and Real-Time Continuous State Integrity Monitoring
+ Scalable Data Protection and Cryptographic Verification

How MIDA solves the identified MEC challenges

- PKI Challenges - Using the MIDA Provisioning Module, Agents and Services leverage highly distributed credentials based on the KSI Blockchain. The KSI Blockchain credentials leverage KSI Signatures, removing the complexity and cost of managing a large set of keys and certificates. This allows each agent to create cryptographic data based on that unique credential. As each agent or service has its own unique credential, the origin, authenticity, and time of data creation can be proven in a scalable and secure manner using the KSI Signatures.

- Privacy concerns - Due to the ability to create trusted data at scale based on the KSI Signatures in a streamlined manner, data is highly attributed and portable. The MIDA Operate Module enables agents and services to create data that is cryptographically linked to device identities, context, and attributes in a single, verifiable construct. Thus, r consumers can enforce very granular policies for access to and distribution of the data.

- Credential Compromise - MIDA leverages KSI Credentials that are unique to each device and agent. By creating unique cryptographic credentials in a secure manner, attackers at best can only compromise a single agent, rather than having the ability to leverage a common credential across a fleet of devices.

- Lack of multi-party trust - MIDA creates widely available and independently verifiable data using the KSI Blockchain. Because multiple organizations and operators no longer need to explicitly trust each other, but can cryptographically prove data independently, the distributed trust model of the KSI Blockchain enables multiple parties to trust data across organizations and technologies.

- Lack of scalability in identity management - Because the cryptographic data used by MIDA is signed by KSI Blockchain, the key management complexities and cost are removed from the process. This enables a highly scalable and dynamic identity management environment where enrolling and revoking identities of devices does not increase cost and complexities.

- Data manipulation - MIDA leverages the KSI Blockchain to sign all data moving from or to the edge devices. Data, device snapshots, commands and updates to name a few are all signed with the KSI Signature. This provides data integrity at scale and detection of tampering down to the bit level.

- Lack of proof of provenance - The ability to create KSI Blockchain based signatures enables data to be "chained" together in a portable and interoperable manner. MIDA leverages this aspect of KSI to enable portable data provenance and lineage. For example, data moving from a sensor, to a processing node, and aggregated for the management plane can retain each "hop" along the path it took. Consumers of this data can use this attributed data to create a full history of where it came from and how it got to the current validating entity.

MIDA Use Cases At the Edge

MIDA aims to mitigate and defend connected edge architectures across many organizations and industries. In this section we explore a few specific use cases from different sectors:

Artificial Intelligence:

While training AI will remain in the cloud due to the massive compute and storage needed for training, inference applications of a trained algorithm can be pushed to the edge to reduce decision cost and enhance decision speed.

AI inference moving to the edge will be essential for data intensive applications, such as connected vehicles as the time penalties of moving data across transit infrastructure to and from the source and across geographies will be unacceptable.

Because decision-making will be moved to the edge of network the protection and trustworthiness of AI inference applications is key. Trustworthy AI has several components to it and blockchain security platforms such as MIDA can aid in certain aspects like governance, transparency via traceability, and accountability via auditability, providing an end to end chain of custody for the integrity of training data, algorithms and the resulting models.

Internet of Things:

MEC can be used to aggregate data generated by an increasing number of IoT devices, before they reach the main network. As the number of IoT connections increase, reduced latency and shorter transit times between device and server will be important for scalability and performance.

Medical IoT devices such as wearables etc. collect massive amounts of data, making it possible for more accurate diagnosis, offering precision healthcare. However, flooding the cloud with such a large amount of data, introduces latency and requires critical processing and AI inference to happen at the edge.

One of the biggest use cases for IoT is telemetry data. IoT devices used for telemetry tend to have low computing resources and low bandwidth. There also exists the problem of separation of useful data from noise. In most cases, it is useful to aggregate telemetry data from different sensors for intelligent analytics. In these cases, edge computing offers a way to filter data, perform aggregation, thereby providing a way to utilize the data for useful analysis.

IoT and edge sensors are gaining traction in creating the supply chains of the future. Due to the obvious value of having real-time information about goods moving across the globe, IoT and edge sensors are a natural choice to integrate into the world's largest supply chains. Operators are realizing that the problem with adopting these new technologies is trust. Once these devices are deployed, organizations are realizing that there is no visibility into which devices are trusted, have no awareness of the state of their own devices, and have trouble confidently leveraging the data coming from these sensors and devices.

MIDA brings the ability to trust these decentralized devices and increases confidence in the data originating from them. MIDA provides a user friendly and flexible platform to incorporate vast amounts of devices from many manufacturers into a common, trusted ecosystem. The data then becomes significantly more valuable for decision making and operations, streamlining and digitizing business with confidence.

Connected and Autonomous Vehicle Enablement:

Vehicles today are quickly becoming mobile devices with wheels or wings. With the adoption of open architectures and connected components, these vehicles are seeing a massive amount of code residing on the vehicles as well as the movement of data to and from the enterprise. Managing secure updates and configurations of multiple electronic control units is increasingly becoming complex and lacking effective and efficient security postures.

MIDA provides the automotive industry with a secure yet scalable solution to provide trusted updates to vehicles in a controlled manner.

Software Defined Networking and Network Function Virtualization:

MEC system specifications leverage Service Based Architecture (SBA) and rely heavily on Network Function Virtualization (NFV) and Software Defined Networking (SDN) paradigms.

Both NFV and MEC can be used in 5G networks to increase computing capacity to meet increased networking demands. MEC provides the ability to host virtualized network functions (VNF) closer to the end user devices thereby decreasing latency and enhancing performance. Use of Service function chaining (SFC) to connect VNFs can be used to boost security and efficient management of network slices. SDN controllers with built in support for machine learning can determine traffic loads and network utilization on specific SFC paths and accordingly offload the traffic processing to the edge.

Blockchain security platforms such as MIDA can be used to efficiently detection deviation in specified service function chain paths and also providing a cryptographically sound way to prevent a malicious attacker from bypassing nodes in the SFC, thereby preventing a malicious attacker from modifying the intended path[3].

Edge compute for Energy Grid:

With the convergence of OT/IT, many energy providers are looking to capitalize on pushing compute to the edge in, for example, substation devices. In order to fully realize the value, the devices must remain in compliance and provide trusted data.

MIDA provides scalable visibility into these devices while alerting on any compliance variances.

Enterprise Switching, Edge Servers, and Routing:

Large enterprises deploy considerable amounts of off the shelf switches, routers, and firewalls. Telecom is deploying large numbers of industrial routers and MEC servers. Controlling updates and configurations as well as making sure the data from the devices is accurate is paramount to protect their business.

MIDA provides agents and services that can enforce only authentic and trusted updates and configurations get deployed to each device.

Appendix I: KSI Blockchain

Guardtime's cryptographers and have been working on cryptographic protocols since the 1990s. They were the architects of e-Estonia digital society and in 2007 decided to take a different path from the cryptocurrency community. Specifically they wanted to build a system for the Estonian Government that would eliminate the need for trusted humans in the verification of information. The technology went in to production in 2012 and since then more and more functionality has been added to the stack.

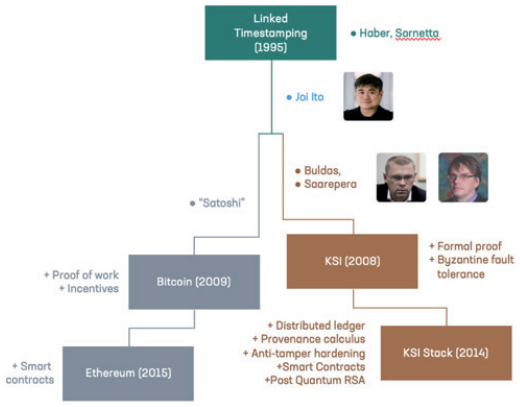
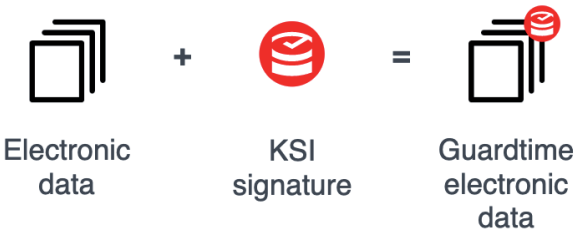


Figure 4 - Guardtime MIDA: Operate Module

Guardtime's KSI blockchain is designed to provide massively scalable digital signature based authentication for electronic data, machines and humans. Unlike traditional approaches that depend on asymmetric key cryptography, KSI uses only hash-function cryptography and does not rely on key based credentials, secrets or the human administrators that manage them. This enabling the verification of information to rely only on the security of hash-functions and the availability of a public ledger commonly referred to as a blockchain.

Guardtime KSI blockchain technology assigns a unique "keyless" signature to any type of data. The signature can be thought of as a tag or receipt. It can be stored with the data as an attribute or separately in different types of data container. This KSI signature can verify the time of creation, identity of creator, and integrity of the underlying data.



Importantly, (and in contrast to other blockchain infrastructure, platform, and software providers), the KSI blockchain does not require migrating the target data to the blockchain. There are three major benefits - scale and settlement time, interoperability, and data sovereignty. Guardtime's current public service can manage 1 trillion signatures derived from the KSI blockchain each second. Moreover, organizations using and consuming KSI Blockchain trust anchor services for identity and data management can leverage their existing IDAM, ERP, database, SEM, enterprise, cloud and mobile storage environments and services. The signatures are cryptographically immutable and used to verify data and service access where data naturally lives, is processed and needs to be governed, in turn supporting machine and business development operations, process workflow integrity, awareness, and real-time governance across zones that traditionally don't or can't share authoritative access.

The KSI blockchain has been in production since 2009 for the government of Estonia and then adopted by the US DoD and defense aerospace communities. Achieving NIAP accreditation for our customers means the KSI Blockchain and its associated components are proven, mature and battle-hardened.

References

+ [1] https://www.afcea.org/content/incoming-we-must-anticipate-5g-consequences-now

+ [2] Multi Party Trust Framework - A blockchain based system of decentralized trust and privacy at the edge from Intel

+ [3] Verification mechanism for network service chain paths, https://patents.google.com/patent/US20170346752A1/en