Pacific Northwest
NATIONAL LABORATORY

PNNL-28237

Keyless Infrastructure Security Solution (KISS): Examining Security and Trust Gaps

Cybersecurity for Energy Delivery Systems (CEDS) Research and Development

November 2018

ME Mylrea, Pacific Northwest National Laboratory
SNG Gourisetti, Pacific Northwest National Laboratory
J Plummer, Guardtime
R Bishop, Guardtime
A Moralez, Guardtime
V Tatireddy, Guardtime
A Hahn, Washington State University
K Kaur, Washington State University
C Allwardt, Pacific Northwest National Laboratory
R Singh, Pacific Northwest National Laboratory

U.S. DEPARTMENT OF ENERGY

Prepared for the U.S. Department of Energy
under Contract DE-OE0000190

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor Battelle Memorial Institute, nor any of their employees, makes **any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights**. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof, or Battelle Memorial Institute. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
email: orders@ntis.gov <http://www.ntis.gov/about/form.aspx>
Online ordering: http://www.ntis.gov

This document was printed on recycled paper.
(8/2010)

ACKNOWLEDGMENTS

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000190.

Revision History

Revision	Date	Deliverable (Reason for Change)	Release #
#	11/2/2018	Original Report	enter text.

Contents

Figures

1.0 Introduction

The following cyber security gaps analysis focuses on opportunities and challenges related to applying a unique Keyless Infrastructure Security Solution (KISS) to increase the trustworthiness and integrity of energy delivery systems (EDSs) in electricity infrastructure.

2.0 Background

The KISS platform, being developed as part of the U.S. Department of Energy's Cyber Security for Energy Delivery Systems (CEDS) program, focuses on improving the state of the state of art of monitoring energy delivery systems (EDS) at the grid's edge through an innovative application of blockchain technology.

The KISS platform consists of VOLTTRON™—an agent-based distributed control system—enabled with KSI blockchain[1] to increase the trustworthiness and integrity of EDS operating at the grid's edge. The KSI blockchain provides a highly redundant, distributed, and secure platform for which entities can leverage to access and participate in the cryptographic signing of events. To improve trust and integrity of complex energy transactions, KISS provides a mathematical proof of the time of signature, the identity of the data signer, and the authenticity of the data. [2]

To create a KSI signature, KSI credentials must be provisioned to the device, to guarantee that only known good devices are interacting with the infrastructure. This relationship allows the classification of two groups of devices: credentialed, known good devices, and non-credentialed, rogue devices. The identification of rogue devices allows control over which devices can participate in device-to-device interaction through the KSI blockchain and whether continued participation is allowed.

3.0 Security and Trust Gaps

In examining various known security and trust gaps in electricity infrastructure, the KISS team is initially focusing on critical communications exchanges and storage between the distribution management system (DMS) and the historian. Addressing these gaps will enhance the trustworthiness of the data as well as the ability to perform continuous monitoring of critical EDS. The KSI blockchain solution applied makes the data inherently immutable[3] and ideal

[1] Note: distributed ledger technology (DLT)/blockchain consists of different categories of technology implementations, the discussion on blockchain presented in this paper centers on the Guardtime blockchain technology.

[2] Buldas, A., A. Kroonmaa, R. Laanoja. 2013. *Keyless signatures infrastructure: How to build global distributed hash-trees*. In: H. Riis Nielson and D. Gollmann (Eds.): NordSec 2013, LNCS 8208, pp. 313–320.

[3] For purposes of the KISS research, the term *immutability* is the root idea of the level of difficulty and complexity involved in changing the content on the blockchain. The phrase blockchain originates from the fundamental idea of blocks that are cryptographically connected where the hash of previous block is part of the hash generation process of the current block. For an attacker to change the blockchain data without being detected means changing every block and the hash from that point of time to the present.

situation for this gap. The potential mitigations for blockchain applications in this EDS context are provided in Section 4.0 of this document.

- Identify how trust is established and can be improved across EDS interconnections, specifically where KSI blockchain can help increase security:
    - DMS and device exchange of commands: there is no verification layer that checks that the information received is exactly the same as it is from the point of origin.
    - Validation is the data trustworthy and verifiable across disparate systems.
    - Provisioning and establishing trust relationship: Current devices are inherently trusted; there is no securing the identity of the device.
    - Corrective Actions and Remediation: Upon detection of changes.

3.1 Security Issues and Mitigation

3.1.1 KISS Security Features[4]

Through the ability to register the devices in the blockchain and securing both data-at-rest and data-in-transit, the KISS subsystem may facilitate the utilities' ability to employ protections for components or subcomponent products and services through the supply chain. KISS may afford real-time quality control and tamper detection (manipulation) of baseline changes in software such as source code, compiled binaries, and/or firmware, which can be verified in real-time for audit/investigative/configuration/ control actions. Such quality control and tamper detection will be achieved by enabling the systems to register with the blockchain to validate the transmitted data between the systems. KISS may further allow organizations to independently detect the occurrence of, reduce the likelihood of, and mitigate the consequences of unknowingly using products containing counterfeit components or malicious functions.

By signing critical software functions, configuration files, and software with KISS, counterfeit/malicious components may be quickly compared and contrasted against known good states and validated in real-time without the reliance on a trust anchor, especially in automated and abstracted management environments.

The impact of using KISS in this manner could ensure that users (power grid utilities) of this technology can strengthen their EDS, detect vulnerabilities through rigorous test and evaluation capabilities while observing the data, including developmental, acceptance, and operational testing. By signing critical functions and using KISS, counterfeit and malicious components may be compared/contrasted against approved release states and validated independently in real-time in coordination with governance policy rules. Such ability to provide log file integrity and

Since changing the entire content of the blockchain needs immense computation power, the research team is identifying KISS as inherently immutable as determined by the blockchain user community.

[4] Mylrea, M., S. Gourisetti, R. Bishop. M. Johnson. 2017. “Keyless Signature Blockchain Infrastructure: Facilitating NERC CIP Compliance and Responding to Evolving Cyber Threats and Vulnerabilities to Energy Infrastructure”, IEEE PES Transmission and Distribution Conference.

change detection is second to none. Below subsections are tailored to detail certain security features that are beneficial to realize secure EDS environment.

3.1.1.1 Security Feature – I

KISS provides a distributed ledger that records all transactions in a way where the data receives: immutable data authenticity, verification of signing entity and signing time. The first security layer is KISS cryptographic technology—the atomic outputs of participation are also called KISS Signatures.

- Assigns a data signer, authenticity of the data, and time of signing to a data asset.
- This is represented by including the hash of the data in the signature. The data format being signed can be anything in a digital format.

3.1.1.2 Security Feature – II

The second security layer of the KISS is the stack. This provides a highly redundant, distributed, and secure platform for which entities can leverage to access and participate in the cryptographic signing events.

- This stack can be distributed to individual customer premises or leveraged in a managed service or cloud approach depending on customer requirements, use case.
- Because of the combination of both the cryptographic signing events and distributed infrastructure, multiple customers can leverage the same widely witnessed information with no overlap in infrastructure if needed, while still having the ability to cryptographically verify the other entities data when needed, creating a true cross boundary trust mechanism.

3.1.2 Potential Risks

The use of KSI Infrastructure to sign and verify data being exchanged can help address some of the following cyber security issues:

- **Spoofing:** Since the KSI checks for the signer’s identification when authenticating a client, an attacker cannot masquerade as the DMS or Historian and send malicious information. Even if they manage to send information to the receiver, it will not pass the verification as the resultant root will not match the root of the publicly published hash calendar that was formed using the original data.
- **Tampering:** In case an attacker changes anything in the data in transit, the hash of the data would not match the hash calculated using the hash calendar. This inconsistency would alert the receiver that the data is not correct.
- **Repudiation:** The identity check of the sender prohibits them from denying that the data was sent by them. It can also help identify if there is some inside attacker who sent the data from the DMS.
- **Information Disclosure:** While the use of hash calendar adds another chain of communication, it does not add any threats to the data since only hashes are transmitted to the hash calendar system. If a hash from the tree is intercepted, it cannot be used. The data is hashed using one-way hash function and cannot be generated from the stolen hash.

3.1.3 Real World Use Case

The KISS research team has been using the BlackEnergy cyberattack[5] as a reference towards the development, testing, and for this section of the document. In the BlackEnergy cyberattack, the adversaries executed a multi-staged attack. Understanding each phase of the attack provides valuable insight into potential cyber security gaps and how KISS could mitigate some of those challenges. Figure 1 provides a visualization of the BlackEnergy cyberattack and Figure 2 provides a detailed incident mapping of the attack. The attack started with a spear phishing attack to gain access to the business networks. Next the adversary stole credentials from the business networks and increased their access using VPNs to enter the utilities ICS network. With this access, they were able to use existing remote access tools within the environment to issue commands directly from a remote station similar to an operator of the human machine interface (HMI). Using native controls for the supervisory control systems (such as the HMI) and operator screens, the adversaries were able operate the EDSs and deploy this malicious firmware to the serial-to-ethernet devices without alerting the respective security operations teams. This firmware allowed them to take field devices at substations offline, prevented remote commands to be issued to the substations from the operator workstations even after they were brought back online, and finally deleted all the logs of their activities along with the master boot record (when applicable) of the devices preventing them from functioning. Attackers used a modified KillDisk to erase the historian, which made cyber forensics and recovery very difficult.[6] The KISS team determined that the location of the data manipulation was an area to integrate KSI blockchain due to importance of immutability of this data set.

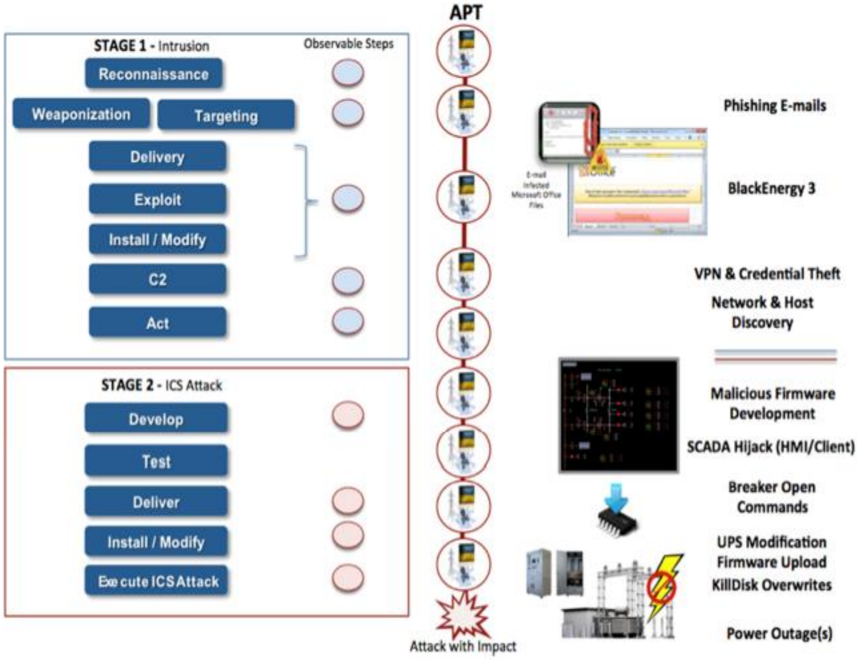
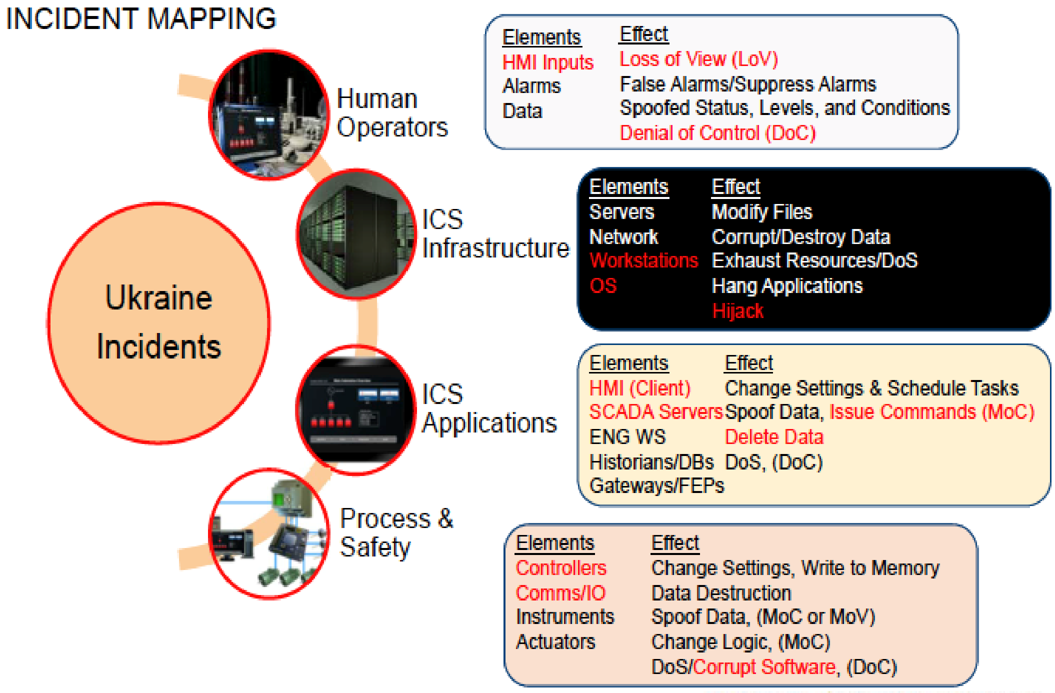


Figure 1. BlackEnergy Multi-stage Attack[6]

[5] On December 23, 2015, Ukrainian power companies experienced unscheduled power outages impacting a large number of customers. https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

[6] SANS (display on NERC webpage), Electricity Information Sharing and Analysis Center. 2016. *Analysis of the cyber Attack on the Ukrainian Power Grid, Defense Use Case*, https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf.



Elements	Effect
HMI Inputs	Loss of View (LoV)
Alarms	False Alarms/Suppress Alarms
Data	Spoofed Status, Levels, and Conditions
	Denial of Control (DoC)

Elements	Effect
Servers	Modify Files
Network	Corrupt/Destroy Data
Workstations	Exhaust Resources/DoS
OS	Hang Applications
	Hijack

Elements	Effect
HMI (Client)	Change Settings & Schedule Tasks
SCADA Servers	Spoof Data, Issue Commands (MoC)
ENG WS	Delete Data
Historians/DBs	DoS, (DoC)
Gateways/FEPs	

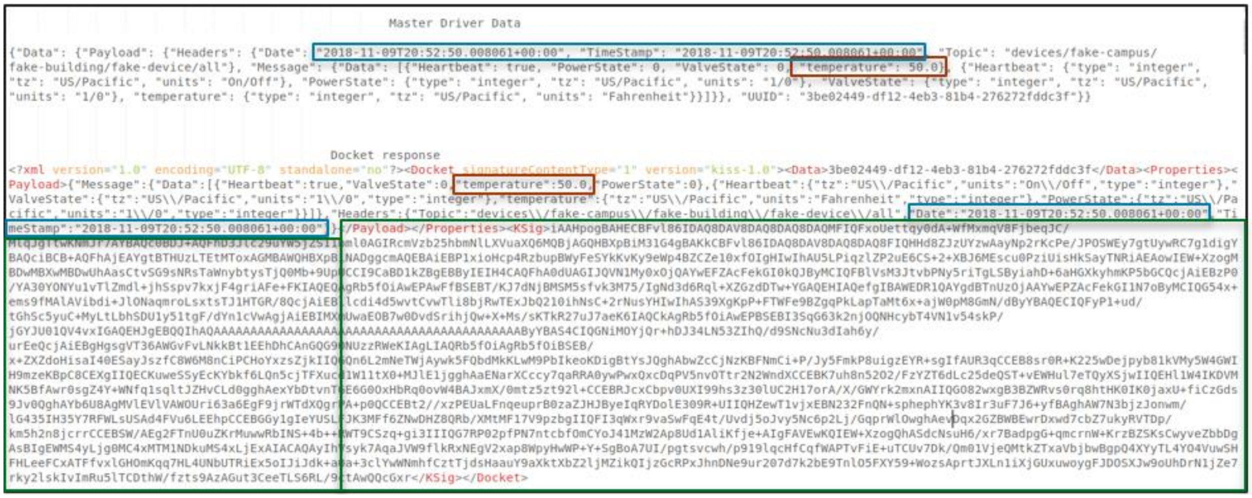
Elements	Effect
Controllers	Change Settings, Write to Memory
Comms/IO	Data Destruction
Instruments	Spoof Data, (MoC or MoV)
Actuators	Change Logic, (MoC)
	DoS/Corrupt Software, (DoC)

Figure 2. Incident Mapping of BlackEnergy Attack (developed based on the recent publication[7])

3.1.4 Mitigation Using KISS

For this project, we went through each phase of the BlackEnergy attack and focused on steps where KISS could provide increased security and help regulate future attacks. KISS will advance the trustworthiness and integrity of the SCADA data being stored and exchanged in a way that helps prevent spoofing, corrupting and destruction of these data sets. This will be achieved by creating dockets out of the historian data (captures both the past and the present). A docket is a cryptographically signed data structure or dictionary that is represented by a unique hash value. Dockets will be stored in a standalone database such as the VOLTTRON database which is immutable. The hash of the dockets are stored in the blockchain's immutable distributed ledger and at any given time, the validity of a docket can be verified by executing the KISS docket-verification software that recalculates the hash of the docket and compares with the hash on the blockchain. If the hash values match, that implies that the docket is not manipulated since the date of creation. If the hash values fail to match, it indicates that the docket and/or the data value in the docket is manipulated or corrupted. The KISS team performed a docket creation test using illustrative temperature data emulated from a VOLTTRON sensor (see Figure 3 and Figure 4 for the illustration). Relating this with the BlackEnergy attack, an important element of that attack was the loss of logs and historical data. That particular event made it extremely difficult to perform any forensics or attempt to regulate the data. Through the KISS solution, even the utility in-house historian is compromised, the

[7] Whitehead, D., K. Owens, D. Gammel, J. Smith. 2018. "Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies", Sensible Cybersecurity of Power Systems: A Collection of Technical Papers Representing Modern Solutions, available at: https://cdn.selinc.com/assets/Literature/Publications/Technical%20Papers/6774_UkraineCyber_DEW_20170130_Web7.pdf?v=20181015-210831.



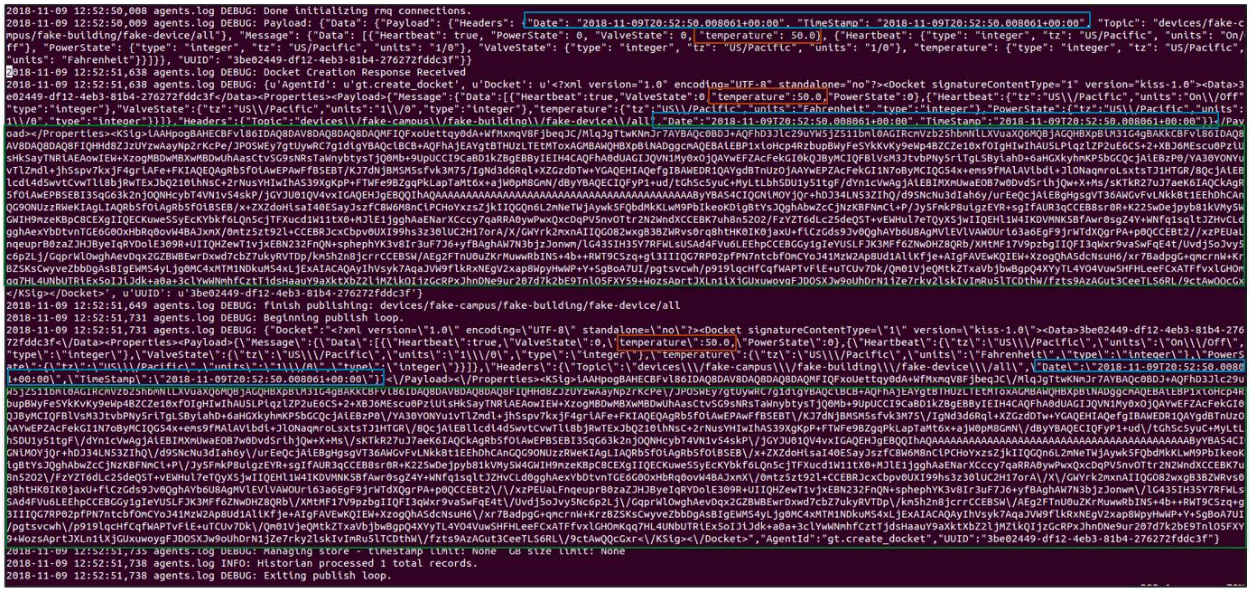
```
                              Master Driver Data

{"Data": {"Payload": {"Headers": {"Date": "2018-11-09T20:52:50.008061+00:00", "TimeStamp": "2018-11-09T20:52:50.008061+00:00", "Topic": "devices/fake-campus/
fake-building/fake-device/all"}, "Message": {"Data": [{"Heartbeat": true, "PowerState": 0, "ValveState": 0, "temperature": 50.0}, {"Heartbeat": {"type": "integer",
"tz": "US/Pacific", "units": "On/Off"}, "PowerState": {"type": "integer", "tz": "US/Pacific", "units": "1/0"}, "ValveState": {"type": "integer", "tz": "US/Pacific",
"units": "1/0"}, "temperature": {"type": "integer", "tz": "US/Pacific", "units": "Fahrenheit"}}]}}, "UUID": "3be02449-df12-4eb3-81b4-276272fddc3f"}}


                            Docket response
<?xml version="1.0" encoding="UTF-8" standalone="no"?><Docket signatureContentType="1" version="kiss-1.0"><Data>3be02449-df12-4eb3-81b4-276272fddc3f</Data><Properties><
Payload>{"Message":{"Data":[{"Heartbeat":true,"ValveState":0,"temperature":50.0,"PowerState":0},{"Heartbeat":{"tz":"US\\/Pacific","units":"On\\/Off","type":"integer"},"
ValveState":{"tz":"US\\/Pacific","units":"1\\/0","type":"integer"},"temperature":{"tz":"US\\/Pacific","units":"Fahrenheit","type":"integer"},"PowerState":{"tz":"US\\/Pa
cific","units":"1\\/0","type":"integer"}}]},"Headers":{"Topic":"devices\\/fake-campus\\/fake-building\\/fake-device\\/all","Date":"2018-11-09T20:52:50.008061+00:00","Ti
meStamp":"2018-11-09T20:52:50.008061+00:00"}}</Payload></Properties><KSig>iAAHpogBAHECBFvl86IDAQ8DAV8DAQ8DAQ8DAQMFIQFxoUettqy0dA+WfMxmqV8FjbeqJC/
MlqJgTtwKNmJr7AYBAQc0BDJ+AQFhD3Jlc29uYW5jZS11bml0AGIRcmVzb25hbmNlLXVuaXQ6MQBjAGQHBXpBiM31G4gBAKkCBFvl86IDAQ8DAV8DAQ8DAQ8FIQHHd8ZJzUYzwAayNp2rKcPe/JPOSWEy7gtUywRC7g1digY
BAQciBCB+AQFhAjEAYgtBTHUzLTEtMToxAGMBAWQHBXpBiNADggcmAQEBAiEBP1xioHcp4RzbupBWyFeSYkKvKy9eWp4BZCZe10xfOIgHIwIhAU5LPiqzlZP2uE6CS+2+XBJ6MEscu0PziUisHkSayTNRiAEAowIEW+XzogM
BDwMBXwMBDwUhAasCtvSG9sNRsTaWnybtysTjQ0Mb+9UpUCCI9CaBD1kZBgEBByIEIH4CAQFhA0dUAGIJQVN1My0xOjQAYwEFZAcFekGI0kQJByMCIQFBlVsM3JtvbPNy5riTgLSByiahD+6aHGXkyhmKP5bGCQcjAiEBzP0
/YA30YONYu1vTlZmdl+jhSspv7kxjF4griAFe+FKIAQEQAgRb5fOiAwEPAwFfBSEBT/KJ7dNjBMSM5sfvk3M75/IgNd3d6Rql+XZGzdDTw+YGAQEHIAQefgIBAWEDR1QAYgdBTnUzOjAAYwEPZAcFekGI1N7oByMCIQG54x+
ems9fMAlAVibdi+JlONaqmroLsxtsTJ1HTGR/8QcjAiEBllcdi4d5wvtCvwTli8bjRwTExJbQ210ihNsC+2rNusYHIwIhAS39XgKpP+FTWFe9BZgqPkLapTaMt6x+ajW0pM8GmN/dByYBAQECIQFyP1+ud/
tGhSc5yuC+MyLtLbhSDU1y51tgF/dYn1cVwAgjAiEBIMXmUwaEOB7w0DvdSrihjQw+X+Ms/sKTkR27uJ7aeK6IAQCkAgRb5fOiAwEPBSEBI3SqG63k2njOQNHcybT4VN1v54skP/
jGYJU01QV4vxIGAQEHJgEBQQIhAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABbyYBAS4CIQGNiMOYjQr+hDJ34LN53ZIhQ/d9SNcNu3dIah6y/
urEeQcjAiEBgHgsgVT36AWGvFvLNkkBt1EEhDhCAnGQG9ONUzzRWeKIAgLIAQRb5fOiAgRb5fOiBSEB/
x+ZXZdoHisaI40ESayJszfC8W6M8nCiPCHoYxzsZjkIIQGQn6L2mNeTWjAywk5FQbdMkKLwM9PbIkeoKDigBtYsJQghAbwZcCjNzKBFNmCi+P/Jy5FmkP8uigzEYR+sgIfAUR3qCCEB8sr0R+K225wDejpyb81kVMy5W4GWI
H9mzeKBpC8CEXgIIQECKuweSSyEcKYbkf6LQn5cjTFXucd1W11tX0+MJlE1jgghAaENarXCccy7qaRRA0ywPwxQxcDqPV5nvOTtr2N2WndXCCEBK7uh8n52O2/FzYZT6dLc25deQST+vEWHul7eTQyXSjwIIQEHl1W4IKDVM
NK5BfAwr0sgZ4Y+WNfq1sqltJZHvCLd0gghAexYbDtvnTGE6G0OxHbRq0ovW4BAJxmX/0mtz5zt92l+CCEBRJcxCbpv0UXI99hs3z30lUC2H17orA/X/GWYrk2mxnAIIQGO82wxgB3BZWRvs0rq8htHK0IK0jaxU+fiCzGds
9Jv0QghAYb6U8AgMVlEVlVAWOUri63a6EgF9jrWTdXQgrPA+p0QCCEBt2//xzPEUaLFnqeuprB0zaZJHJByeIqRYDolE309R+UIIQHZewT1vjxEBN232FnQN+sphephYK3v8Ir3uF7J6+yfBAghAW7N3bjzJonwm/
lG435IH35Y7RFWLsUSAd4FVu6LEEhpCCEBGGy1gIeYUSLFJK3MFf6ZNwDHZ8QRb/XMtMF17V9pzbgIIQFI3qWxr9vaSwFqE4t/Uvdj5oJvy5Nc6p2Lj/GqprWlOwghAevDqx2GZBWBEwrDxwd7cbZ7ukyRVTDp/
km5h2n8jcrrCCEBSW/AEg2FTnU0uZKrMuwwRbINS+4b++RWT9CSzq+gi3IIIQG7RP02pfPN7ntcbfOmCYoJ41MzW2ApBUd1AliKfje+AIgFAVEwKQIEW+XzogQhASdcNsuH6/xr7BadpgG+qmcrnW+KrzBZSKsCwyveZbbDg
AsBIgEWMS4yLjg0MC4xMTM1NDkuMS4xLjExAIACAQAyIhVsyk7AqaJVW9flkRxNEgV2xap8WpyHwWP+Y+SgBoA7UI/pgtsvcwh/p919lqcHfCqfWAPTvFiE+uTCUv7Dk/Qm01VjeQMtkZTxaVbjbwBgpQ4XYyTL4YO4VuwSH
FHLeeFCxATFfvxlGHOmKqq7HL4UNbUTRiEx5oIJiJdk+a0a+3clYwWNmhfCztTjdsHaauY9aXktXbZ2ljMZikQIjzGcRPxJhnDNe9ur207d7k2bE9TnlO5FXY59+WozsAprtJXLn1iXjGUxuwoygFJDOSXJw9oUhDrN1jZe7
rky2lskIvImRu5lTCDthW/fzts9AzAGut3CeeTLS6RL/9ctAwQOcGxr</KSig></Docket>
```

Figure 3. Illustration of docket creation from the emulated sensor data (orange boxes show the data value, blue boxes show the timestamps, and green boxes show the hash value)

(Note that the data value, timestamp, digital signature and the cryptographic hash values are all part of the docket. The docket is stored in a standalone historian, and a copy of the hash is stored in the blockchain's immutable distributed ledger)



```
2018-11-09 12:52:50,008 agents.log DEBUG: Done initializing rmq connections.
2018-11-09 12:52:50,009 agents.log DEBUG: Payload: {"Data": {"Payload": {"Headers": {"Date": "2018-11-09T20:52:50.008061+00:00", "TimeStamp": "2018-11-09T20:52:50.008061+00:00", "Topic": "devices/fake-c
mpus/fake-building/fake-device/all"}, "Message": {"Data": [{"Heartbeat": true, "PowerState": 0, "ValveState": 0, "temperature": 50.0}, {"Heartbeat": {"type": "integer", "tz": "US/Pacific", "units": "On/
ff"}, "PowerState": {"type": "integer", "tz": "US/Pacific", "units": "1/0"}, "ValveState": {"type": "integer", "tz": "US/Pacific", "units": "1/0"}, "temperature": {"type": "integer", "tz": "US/Pacific",
"units": "Fahrenheit"}}]}}, "UUID": "3be02449-df12-4eb3-81b4-276272fddc3f"}}
2018-11-09 12:52:51,638 agents.log DEBUG: Docket Creation Response Received
2018-11-09 12:52:51,638 agents.log DEBUG: {u'AgentId': u'gt.create_docket', u'Docket': u'<?xml version="1.0" encoding="UTF-8" standalone="no"?><Docket signatureContentType="1" version="kiss-1.0"><Data>3
e02449-df12-4eb3-81b4-276272fddc3f</Data><Properties><Payload>{"Message":{"Data":[{"Heartbeat":true,"ValveState":0,"temperature":50.0,"PowerState":0},{"Heartbeat":{"tz":"US\\/Pacific","units":"On\\/Off"
"type":"integer"},"ValveState":{"tz":"US\\/Pacific","units":"1\\/0","type":"integer"},"temperature":{"tz":"US\\/Pacific","units":"Fahrenheit","type":"integer"},"PowerState":{"tz":"US\\/Pacific","units":
1\\/0","type":"integer"}}]},"Headers":{"Topic":"devices\\/fake-campus\\/fake-building\\/fake-device\\/all","Date":"2018-11-09T20:52:50.008061+00:00","TimeStamp":"2018-11-09T20:52:50.008061+00:00"}}</Pav
oad></Properties><KSig>iAAHpogBAHECBFvl86IDAQ8DAV8DAQ8DAQ8DAQMFIQFxoUettqy0dA+WfMxmqV8FjbeqJC/MlqJgTtwKNmJr7AYBAQc0BDJ+AQFhD3Jlc29uYW5jZS11bml0AGIRcmVzb25hbmNlLXVuaXQ6MQBjAGQHBXpBiM31G4gBAKkCBFvl86IDAQ8
AV8DAQ8DAQ8FIQHHd8ZJzUYzwAayNp2rKcPe/JPOSWEy7gtUywRC7g1digYBAQciBCB+AQFhAjEAYgtBTHUzLTEtMToxAGMBAWQHBXpBiNADggcmAQEBAiEBP1xioHcp4RzbupBWyFeSYkKvKy9eWp4BZCZe10xfOIgHIwIhAU5LPiqzlZP2uE6CS+2+XBJ6MEscu0PziU
sHkSayTNRiAEAowIEW+XzogMBDwMBXwMBDwUhAasCtvSG9sNRsTaWnybtysTjQ0Mb+9UpUCCI9CaBD1kZBgEBByIEIH4CAQFhA0dUAGIJQVN1My0xOjQAYwEFZAcFekGI0kQJByMCIQFBlVsM3JtvbPNy5riTgLSByiahD+6aHGXkyhmKP5bGCQcjAiEBzP0/YA30YONYu
vTlZmdl+jhSspv7kxjF4griAFe+FKIAQEQAgRb5fOiAwEPAwFfBSEBT/KJ7dNjBMSM5sfvk3M75/IgNd3d6Rql+XZGzdDTw+YGAQEHIAQefgIBAWEDR1QAYgdBTnUzOjAAYwEPZAcFekGI1N7oByMCIQG54x+ems9fMAlAVibdi+JlONaqmroLsxtsTJ1HTGR/8QcjAiEB
lcdi4d5wvtCvwTli8bjRwTExJbQ210ihNsC+2rNusYHIwIhAS39XgKpP+FTWFe9BZgqPkLapTaMt6x+ajW0pM8GmN/dByYBAQECIQFyP1+ud/tGhSc5yuC+MyLtLbhSDU1y51tgF/dYn1cVwAgjAiEBIMXmUwaEOB7w0DvdSrihjQw+X+Ms/sKTkR27uJ7aeK6IAQCkAgR
5fOiAwEPBSEBI3SqG63k2njOQNHcybT4VN1v54skP/jGYJU01QV4vxIGAQEHJgEBQQIhAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABbyYBAS4CIQGNiMOYjQr+hDJ34LN53ZIhQ/d9SNcNu3dIah6y/urEeQcjAiEBgHgsgVT36AWGvFvLNkkBt1EEhDhCAn
QG9ONUzzRWeKIAgLIAQRb5fOiAgRb5fOiBSEB/x+ZXZdoHisaI40ESayJszfC8W6M8nCiPCHoYxzsZjkIIQGQn6L2mNeTWjAywk5FQbdMkKLwM9PbIkeoKDigBtYsJQghAbwZcCjNzKBFNmCi+P/Jy5FmkP8uigzEYR+sgIfAUR3qCCEB8sr0R+K225wDejpyb81kVMy5W
GWIH9mzeKBpC8CEXgIIQECKuweSSyEcKYbkf6LQn5cjTFXucd1W11tX0+MJlE1jgghAaENarXCccy7qaRRA0ywPwxQxcDqPV5nvOTtr2N2WndXCCEBK7uh8n52O2/FzYZT6dLc25deQST+vEWHul7eTQyXSjwIIQEHl1W4IKDVMNK5BfAwr0sgZ4Y+WNfq1sqltJZHvCLd
gghAexYbDtvnTGE6G0OxHbRq0ovW4BAJxmX/0mtz5zt92l+CCEBRJcxCbpv0UXI99hs3z30lUC2H17orA/X/GWYrk2mxnAIIQGO82wxgB3BZWRvs0rq8htHK0IK0jaxU+fiCzGds9Jv0QghAYb6U8AgMVlEVlVAWOUri63a6EgF9jrWTdXQgrPA+p0QCCEBt2//xzPEUaL
nqeuprB0zaZJHJByeIqRYDolE309R+UIIQHZewT1vjxEBN232FnQN+sphephYK3v8Ir3uF7J6+yfBAghAW7N3bjzJonwm/lG435IH35Y7RFWLsUSAd4FVu6LEEhpCCEBGGy1gIeYUSLFJK3MFf6ZNwDHZ8QRb/XMtMF17V9pzbgIIQFI3qWxr9vaSwFqE4t/Uvdj5oJvy5
c6p2Lj/GqprWlOwghAevDqx2GZBWBEwrDxwd7cbZ7ukyRVTDp/km5h2n8jcrrCCEBSW/AEg2FTnU0uZKrMuwwRbINS+4b++RWT9CSzq+gi3IIIQG7RP02pfPN7ntcbfOmCYoJ41MzW2ApBUd1AliKfje+AIgFAVEwKQIEW+XzogQhASdcNsuH6/xr7BadpgG+qmcrnW+Kr
BZSKsCwyveZbbDgAsBIgEWMS4yLjg0MC4xMTM1NDkuMS4xLjExAIACAQAyIhVsyk7AqaJVW9flkRxNEgV2xap8WpyHwWP+Y+SgBoA7UI/pgtsvcwh/p919lqcHfCqfWAPTvFiE+uTCUv7Dk/Qm01VjeQMtkZTxaVbjbwBgpQ4XYyTL4YO4VuwSHFHLeeFCxATFfvxlGHOm
qq7HL4UNbUTRiEx5oIJiJdk+a0a+3clYwWNmhfCztTjdsHaauY9aXktXbZ2ljMZikQIjzGcRPxJhnDNe9ur207d7k2bE9TnlO5FXY59+WozsAprtJXLn1iXjGUxuwoygFJDOSXJw9oUhDrN1jZe7rky2lskIvImRu5lTCDthW/fzts9AzAGut3CeeTLS6RL/9ctAwQOcGx
</KSig></Docket>', u'UUID': u'3be02449-df12-4eb3-81b4-276272fddc3f'}
2018-11-09 12:52:51,649 agents.log DEBUG: finish publishing: devices/fake-campus/fake-building/fake-device/all
2018-11-09 12:52:51,731 agents.log DEBUG: Beginning publish loop.
2018-11-09 12:52:51,731 agents.log DEBUG: {"Docket":"<?xml version=\"1.0\" encoding=\"UTF-8\" standalone=\"no\"?><Docket signatureContentType=\"1\" version=\"kiss-1.0\"><Data>3be02449-df12-4eb3-81b4-276
72fddc3f<\/Data><Properties><Payload>{\"Message\":{\"Data\":[{\"Heartbeat\":true,\"ValveState\":0,\"temperature\":50.0,\"PowerState\":0},{\"Heartbeat\":{\"tz\":\"US\\\/Pacific\",\"units\":\"On\\\/Off\",
\"type\":\"integer\"},\"ValveState\":{\"tz\":\"US\\\/Pacific\",\"units\":\"1\\\/0\",\"type\":\"integer\"},\"temperature\":{\"tz\":\"US\\\/Pacific\",\"units\":\"Fahrenheit\",\"type\":\"integer\"},\"PowerS
tate\":{\"tz\":\"US\\\/Pacific\",\"units\":\"1\\\/0\",\"type\":\"integer\"}}]},\"Headers\":{\"Topic\":\"devices\\\/fake-campus\\\/fake-building\\\/fake-device\\\/all\",\"Date\":\"2018-11-09T20:52:50.0080
61+00:00\",\"TimeStamp\":\"2018-11-09T20:52:50.008061+00:00\"}}<\/Payload><\/Properties><KSig>iAAHpogBAHECBFvl86IDAQ8DAV8DAQ8DAQ8DAQMFIQFxoUettqy0dA+WfMxmqV8FjbeqJC\/MlqJgTtwKNmJr7AYBAQc0BDJ+AQFhD3Jlc29u
W5jZS11bml0AGIRcmVzb25hbmNlLXVuaXQ6MQBjAGQHBXpBiM31G4gBAKkCBFvl86IDAQ8DAV8DAQ8DAQ8FIQHHd8ZJzUYzwAayNp2rKcPe\/JPOSWEy7gtUywRC7g1digYBAQciBCB+AQFhAjEAYgtBTHUzLTEtMToxAGMBAWQHBXpBiNADggcmAQEBAiEBP1xioHcp4R
bupBWyFeSYkKvKy9eWp4BZCZe10xfOIgHIwIhAU5LPiqzlZP2uE6CS+2+XBJ6MEscu0PziUisHkSayTNRiAEAowIEW+XzogMBDwMBXwMBDwUhAasCtvSG9sNRsTaWnybtysTjQ0Mb+9UpUCCI9CaBD1kZBgEBByIEIH4CAQFhA0dUAGIJQVN1My0xOjQAYwEFZAcFekGI0
QJByMCIQFBlVsM3JtvbPNy5riTgLSByiahD+6aHGXkyhmKP5bGCQcjAiEBzP0\/YA30YONYu1vTlZmdl+jhSspv7kxjF4griAFe+FKIAQEQAgRb5fOiAwEPAwFfBSEBT\/KJ7dNjBMSM5sfvk3M75\/IgNd3d6Rql+XZGzdDTw+YGAQEHIAQefgIBAWEDR1QAYgdBTnUzO
AAYwEPZAcFekGI1N7oByMCIQG54x+ems9fMAlAVibdi+JlONaqmroLsxtsTJ1HTGR\/8QcjAiEBllcdi4d5wvtCvwTli8bjRwTExJbQ210ihNsC+2rNusYHIwIhAS39XgKpP+FTWFe9BZgqPkLapTaMt6x+ajW0pM8GmN\/dByYBAQECIQFyP1+ud\/tGhSc5yuC+MyLtL
hSDU1y51tgF\/dYn1cVwAgjAiEBIMXmUwaEOB7w0DvdSrihjQw+X+Ms\/sKTkR27uJ7aeK6IAQCkAgRb5fOiAwEPBSEBI3SqG63k2njOQNHcybT4VN1v54skP\/jGYJU01QV4vxIGAQEHJgEBQQIhAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABbyYBAS4CI
GNiMOYjQr+hDJ34LN53ZIhQ\/d9SNcNu3dIah6y\/urEeQcjAiEBgHgsgVT36AWGvFvLNkkBt1EEhDhCAnGQG9ONUzzRWeKIAgLIAQRb5fOiAgRb5fOiBSEB\/x+ZXZdoHisaI40ESayJszfC8W6M8nCiPCHoYxzsZjkIIQGQn6L2mNeTWjAywk5FQbdMkKLwM9PbIkeoK
igBtYsJQghAbwZcCjNzKBFNmCi+P\/Jy5FmkP8uigzEYR+sgIfAUR3qCCEB8sr0R+K225wDejpyb81kVMy5W4GWIH9mzeKBpC8CEXgIIQECKuweSSyEcKYbkf6LQn5cjTFXucd1W11tX0+MJlE1jgghAaENarXCccy7qaRRA0ywPwxQxcDqPV5nvOTtr2N2WndXCCEBK7u
8n52O2\/FzYZT6dLc25deQST+vEWHul7eTQyXSjwIIQEHl1W4IKDVMNK5BfAwr0sgZ4Y+WNfq1sqltJZHvCLd0gghAexYbDtvnTGE6G0OxHbRq0ovW4BAJxmX\/0mtz5zt92l+CCEBRJcxCbpv0UXI99hs3z30lUC2H17orA\/X\/GWYrk2mxnAIIQGO82wxgB3BZWRvs0
q8htHK0IK0jaxU+fiCzGds9Jv0QghAYb6U8AgMVlEVlVAWOUri63a6EgF9jrWTdXQgrPA+p0QCCEBt2\/\/xzPEUaLFnqeuprB0zaZJHJByeIqRYDolE309R+UIIQHZewT1vjxEBN232FnQN+sphephYK3v8Ir3uF7J6+yfBAghAW7N3bjzJonwm\/lG435IH35Y7RFWLs
SAd4FVu6LEEhpCCEBGGy1gIeYUSLFJK3MFf6ZNwDHZ8QRb\/XMtMF17V9pzbgIIQFI3qWxr9vaSwFqE4t\/Uvdj5oJvy5Nc6p2Lj\/GqprWlOwghAevDqx2GZBWBEwrDxwd7cbZ7ukyRVTDp\/km5h2n8jcrrCCEBSW\/AEg2FTnU0uZKrMuwwRbINS+4b++RWT9CSzq+g
3IIIQG7RP02pfPN7ntcbfOmCYoJ41MzW2ApBUd1AliKfje+AIgFAVEwKQIEW+XzogQhASdcNsuH6\/xr7BadpgG+qmcrnW+KrzBZSKsCwyveZbbDgAsBIgEWMS4yLjg0MC4xMTM1NDkuMS4xLjExAIACAQAyIhVsyk7AqaJVW9flkRxNEgV2xap8WpyHwWP+Y+SgBoA7UI
\/pgtsvcwh\/p919lqcHfCqfWAPTvFiE+uTCUv7Dk\/Qm01VjeQMtkZTxaVbjbwBgpQ4XYyTL4YO4VuwSHFHLeeFCxATFfvxlGHOmKqq7HL4UNbUTRiEx5oIJiJdk+a0a+3clYwWNmhfCztTjdsHaauY9aXktXbZ2ljMZikQIjzGcRPxJhnDNe9ur207d7k2bE9TnlO5FXY
9+WozsAprtJXLn1iXjGUxuwoygFJDOSXJw9oUhDrN1jZe7rky2lskIvImRu5lTCDthW\/fzts9AzAGut3CeeTLS6RL\/9ctAwQOcGxr<\/KSig><\/Docket>","AgentId":"gt.create_docket","UUID":"3be02449-df12-4eb3-81b4-276272fddc3f"}
2018-11-09 12:52:51,735 agents.log DEBUG: Managing store - timestamp limit: None  GB size limit: None
2018-11-09 12:52:51,738 agents.log INFO: Historian processed 1 total records.
2018-11-09 12:52:51,738 agents.log DEBUG: Exiting publish loop.
```

Figure 4. Multiple Dockets Are Shown with VOLTTRON Debug Messages in A Created Docket (orange boxes show the data value, blue boxes show the timestamps, and green boxes show the hash value)

immutable docket-historian will be available to retrieve the lost data (while verifying the authenticity through hash-check with the blockchain). Note that from the instant KISS solution is adopted into a utility network, the data from then to the final date of decommission of the KISS system, the docket creation process will be performed in an autonomous fashion. The KISS system can also take the existing data in the historian (the past) and create the dockets using that data. However, KISS will assume that the past is true and unchanged since the KISS system does not have any means to verify the data prior to the deployment and installation of

KISS in a utility. This is a gap that may need other means to address and this particular gap falls beyond the scope of KISS objective.

Key attributes from the BlackEnergy attack that will be potentially addressed through KISS:

1. By creating a historian of dockets that can only be accessed or changed by being compliant with the rulesets defined by KISS, under an attack such as in BlackEnergy attack where the historian logs were lost, the historian data can be accessed through the KISS docket historian. Note that having administrative access may not be sufficient to access (read or write) the KISS docket historian.

2. System registration and system-to-system verification in the blockchain that could potentially regulate attack propagation. Beyond the data integrity use-cases, the KISS team will be exploring means to capture device *static* information in the blockchain. KISS will be used to define rules to identify device-to-device communication restrictions. For example, if device A sends a message to device B, device B will verify the authenticity of device A before accepting the data packet from device A. Such features may not completely eliminate an attack but can at least regulate the attack from propagating any further.

Attributes from the BlackEnergy attack that may not be addressed by KISS and that are potentially out of scope for KISS (**trust gaps**):

1. KISS may not have been able to completely prevent the BlackEnergy attack. The goal of KISS is to attempt to regulate such an attack, ensuring the data and logs are not lost. Aspects of the BlackEnergy attacks such as telephone line tampering is beyond the scope of this project. However, attacks executed targeting the changes of breaker statues could be potentially stopped through KISS (see #2 above).

2. If KISS is deployed in a utility, it will be expected to verify, validate, and secure the data from a moment in time. KISS will have the capability to secure the historical data, validate and verify from that moment in time. However, KISS may not be able to *tell* if the historical data is corrupted and such verification is beyond the scope of this project.

3. For purposes of the KISS research, the term immutability is the root idea of the level of difficulty and complexity involved in changing the content on the blockchain. The phrase blockchain originates from the fundamental idea of blocks that are cryptographically connected where the hash of previous block is part of the hash generation process of the current block. For an attacker to change the blockchain data without being detected means changing every block and the hash from that point of time to the present. Since changing the entire content of the blockchain needs immense computation power, the research team is identifying KISS as inherently immutable as determined by the blockchain user community. However, quantifying the immutability factor is beyond the scope of the project.

Since grid modernization continues to increase connectivity and automation, it makes it challenging to manually provision, secure, and manage all EDS. Outside of the basic cyber security controls and policies (e.g., IT/OT segmentation, patch management) that aid mitigation, KISS aims to shift the paradigm in decentralized and distributed security by leveraging KSI Blockchain to provide flexible and scalable device enrollment and credentialing. Regardless if it is between edge devices, substations, or communicating to the cloud, KISS will help provide more resilient data structures for immutable and portable data exchange using a common trust anchor. This structure ensures secure device management and technology agnostic data normalization allowing for cross organizational and technology identity management and verified, multi-directional data exchange as shown in Figure 5.

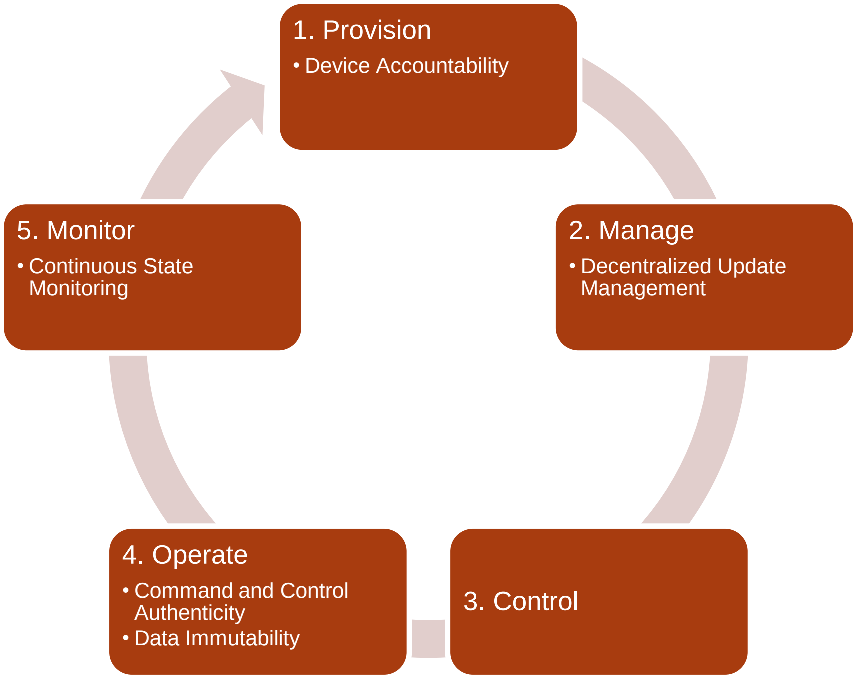

1. Provision
• Device Accountability
2. Manage
• Decentralized Update Management
3. Control
4. Operate
• Command and Control Authenticity
• Data Immutability
5. Monitor
• Continuous State Monitoring

Figure 5. Security Device Management through KISS

Each piece of data is cryptographically tied to a specific device. Thus, data analytics and correlation can be used to detect anomalies, errant data, and misbehaving devices. When a misbehaving device is discovered, various actions can be taken (e.g., deletion of errant data, revocation of credentials, and deployment of personnel to inspect the device physically). If a security operations center wanted to continue monitoring a misbehaving device, various tests and segmentation could be implemented to allow the device to continue communicating in a controlled manner without effecting the rest of the infrastructure.

A KISS subsystem can also be installed directly on some Energy Delivery Systems (EDS). The KISS subsystem can be configured to monitor and detect the configuration and state of the device, allowing it to send an alert on any configuration change, any new connection (i.e., secure socket shell or SSH), or even physical tampering or access. This KISS agent can be used to install secure updates—allowing only those updates that have proper KSI signatures of their own—and to send an alert if unauthorized changes are being made.

As shown in Figure 6, KISS uses existing provisioning services, such as a username and password, Active Directory, public key infrastructure (PKI), security assertion markup language (SAML), etc. Once a provisioning service verifies the device, a device-specific KSI key is generated (see Figure 7). This key is used to generate a hash-based message authentication code (HMAC) to obtain a KSI signature from the KISS Gateway. The KISS Gateway authenticates the device every time the device requests a KSI signature for the data to be signed. A docket (i.e., a cryptographic envelope that contains the data and signature as shown in Figure 8), which provides the previously mentioned cryptographic link between the fingerprint of the device and the data itself, is then generated and passed on to the KISS infrastructure. This process can be automated, allowing for zero-touch provisioning in real-time

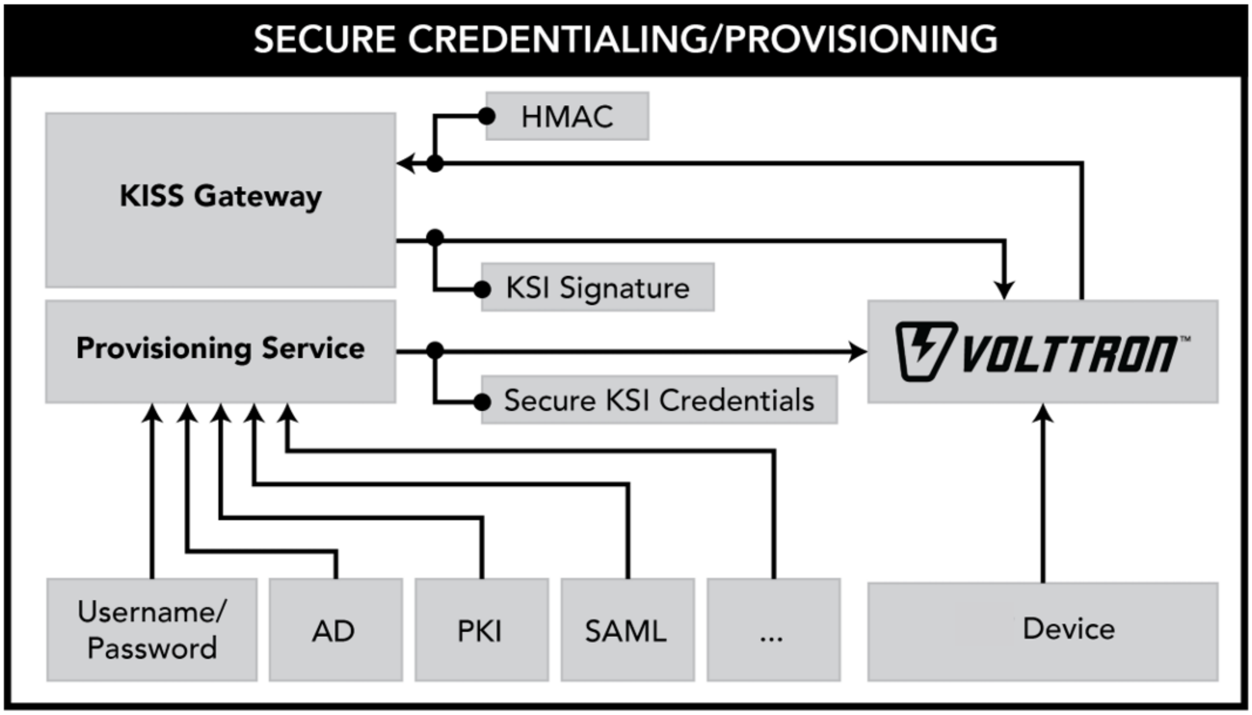


Figure 6. Securing Credentialing/Provisioning through KISS

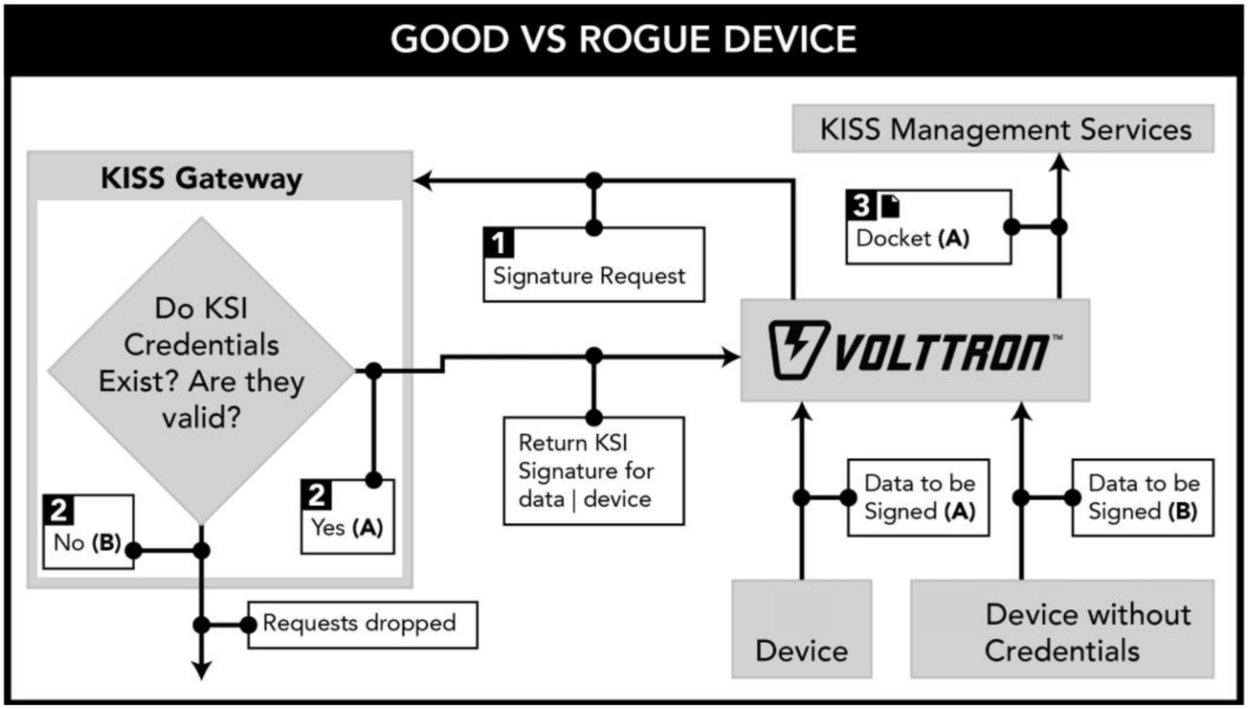


Figure 7. Good Device vs Rouge Device Identification through KISS

If a device has not received its credentials, the request for a signature will be dropped, and the data will not be ingested into KISS. In the case of a malicious device masquerading as a good device, the HMAC will not match, and once again the request will be dropped. Thus, if an attacker plants his or her own devices, or swaps good devices for maliciously configured ones, those devices will be prohibited from communicating and interacting with the rest of the infrastructure. This process is briefly illustrated in Figure 9 and Figure 10.

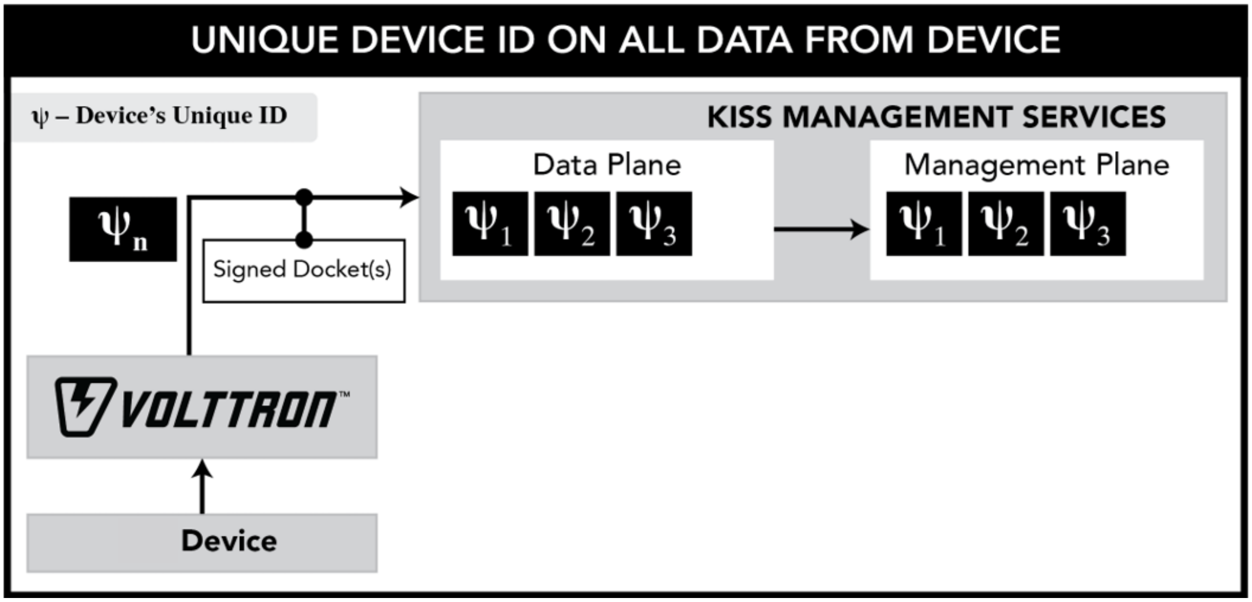


Figure 8. Illustration to Show Unique Device ID on All The Data from The Device

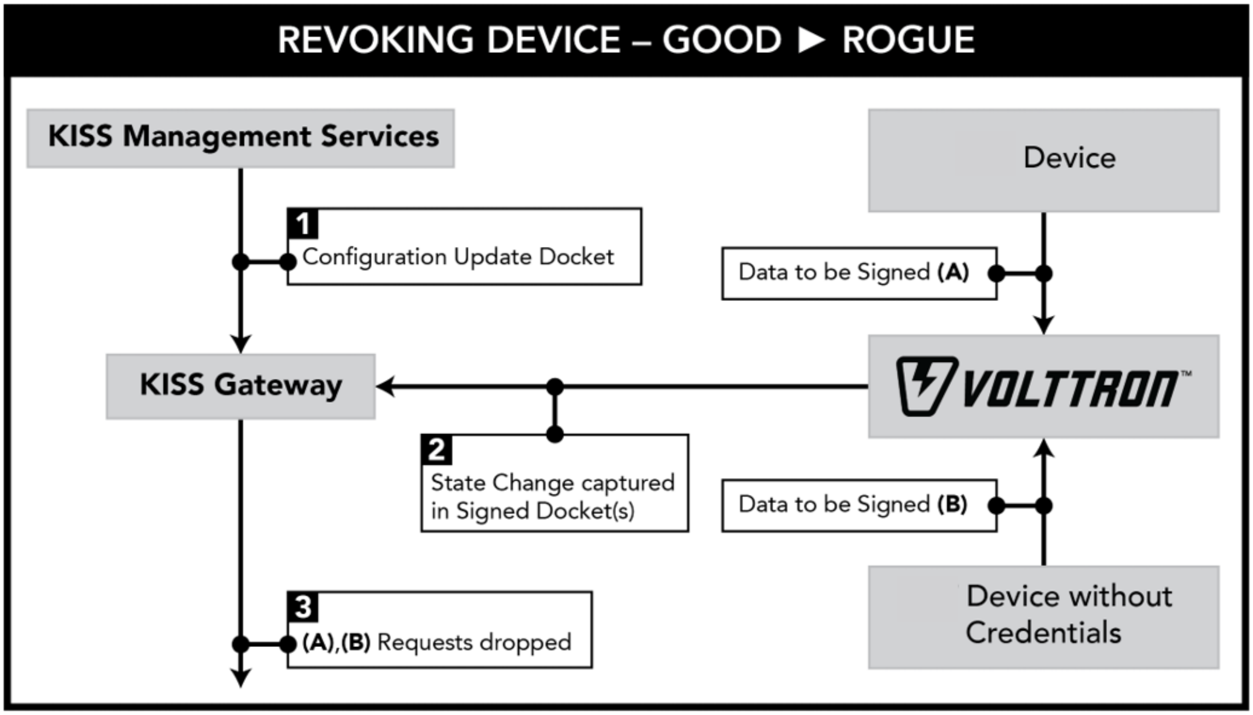

REVOKING DEVICE – GOOD ▶ ROGUE
KISS Management Services
Device
1 Configuration Update Docket
Data to be Signed (A)
KISS Gateway
VOLTTRON™
2 State Change captured in Signed Docket(s)
Data to be Signed (B)
Device without Credentials
3 (A),(B) Requests dropped

Figure 9. Workflow of Device Revocation (good device vs rouge device)

Once a device is properly credentialed and communicating, every piece of data it sends will forever be stamped with its unique fingerprint. Whether the data is moved to a data plane to run analytics (see Figure 10), or ingested into a correlation engine, this fingerprint will follow the data wherever it goes. Individual devices and their data can be queried (i.e., using XPATH or some other query, depending on infrastructure) to find data at any given time or over any given period.

If data analysis uncovers an issue, whether due to malicious intent or simple malfunction, a device's credentials can be revoked immediately, putting it into a rogue state and preventing further communication until further actions are taken.

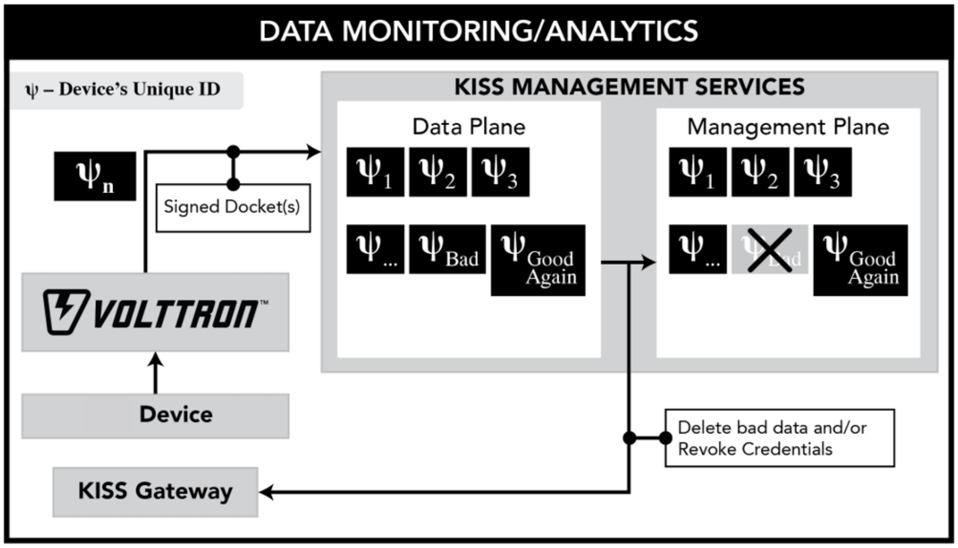

DATA MONITORING/ANALYTICS
ψ – Device's Unique ID
KISS MANAGEMENT SERVICES
Data Plane
Management Plane
ψ_1 ψ_2 ψ_3
$\psi_{...}$ ψ_{Bad} $\psi_{Good Again}$
ψ_1 ψ_2 ψ_3
$\psi_{...}$ ψ_{Bad} $\psi_{Good Again}$
ψ_n
Signed Docket(s)
VOLTTRON™
Device
KISS Gateway
Delete bad data and/or Revoke Credentials

Figure 10. Data Monitoring and Analytics through KISS

Because specific devices and device data can be queried at any time, a device transmitting errant data can be expediently remediated. In cases of simple error, such data can be removed from the database. Then, the device can be monitored further to make certain it is not consistently incorrect and thus needs to be replaced (see Figure 10 and Figure 11).

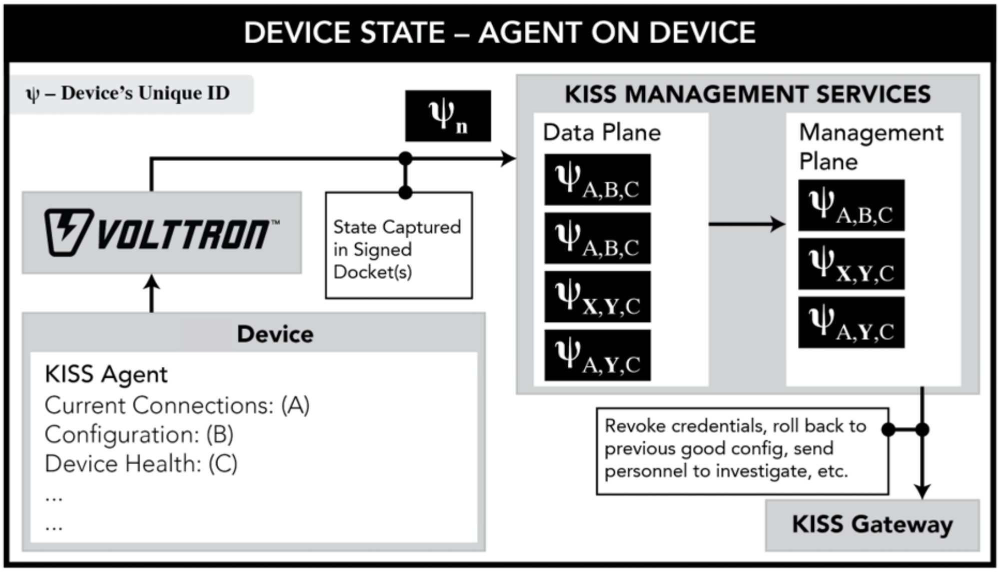


Figure 11. Depiction of Device State (KISS agent on device)

An IoT device that has a KISS agent installed on it allows even finer control and visibility into the device's state. A KISS agent on a device continuously captures and transmits the state of the device (See Figure 11), everything from its physical health and configuration to the connections it is making and who it is communicating with. If an unauthorized login occurs and a configuration file is changed, that change will be captured. In such a case, the devices credentials can be revoked, causing it to become a rogue device. The device would stay in a rogue state until it receives a new configuration or is rolled back to a known good state.

In addition, an agent on the device can reject any update from a source (see Figure 12) that has not been properly vetted and signed with a valid KSI signature. Further, the agent can prevent the device from communicating at all, leaving the device in a rogue state until its security posture meets the necessary requirements.

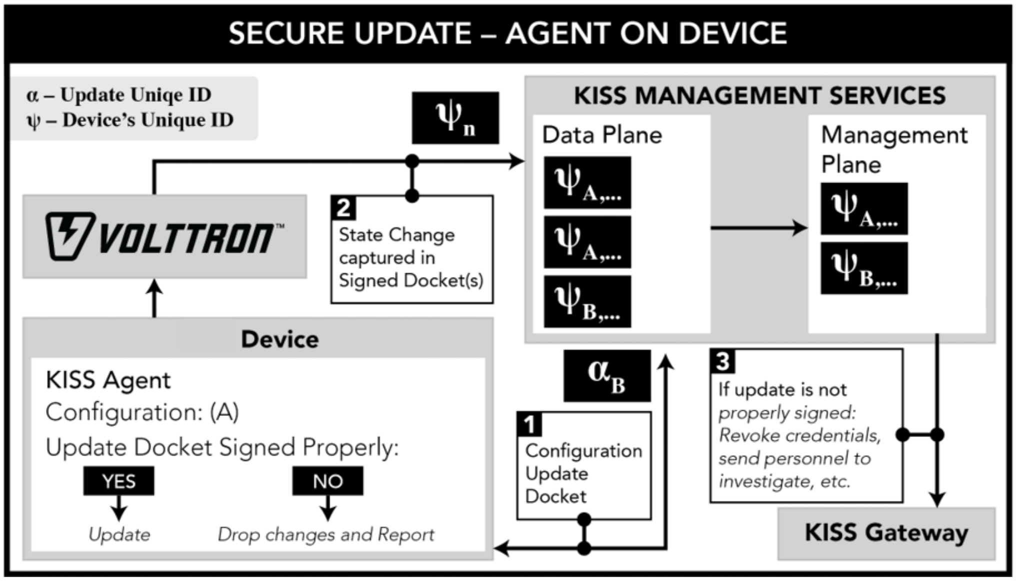

SECURE UPDATE – AGENT ON DEVICE
α – Update Uniqe ID
ψ – Device's Unique ID
ψ_n
KISS MANAGEMENT SERVICES
Data Plane
$\psi_{A,...}$
$\psi_{A,...}$
$\psi_{B,...}$
Management Plane
$\psi_{A,...}$
$\psi_{B,...}$
VOLTTRON™
2 State Change captured in Signed Docket(s)
Device
KISS Agent
Configuration: (A)
Update Docket Signed Properly:
YES
NO
Update
Drop changes and Report
α_B
1 Configuration Update Docket
3 If update is not properly signed: Revoke credentials, send personnel to investigate, etc.
KISS Gateway

Figure 12. Secure Updates and State Changes (KISS agent on device)

4.0 Prevention and Remediation

The KISS infrastructure can help increase the trustworthiness and integrity of EDS in electricity infrastructure by preventing misconfigured devices from connecting and communicating to the rest of infrastructure (Figure 7). If a device is tampered with, that device's analytics will detect the anomalies on the data coming from the device (Figure 10) and the device's credentials will be revoked (Figure 9). Then, a new device will be provisioned to take its place (Figure 6). Devices with KISS agent on them can step through the above process within seconds (Figure 10 and Figure 11). The cryptographic lineage of configurations, locations, and states of devices (Figure 8 and Figure 10), allows the replacement of an entire set of devices automatically with the zero-touch provisioning provided by KISS when the new devices are available (Figure 6, Figure 11, and Figure 12).

5.0 Use Case

The KISS team will perform initial set of use-cases as defined in the "Specifications and requirements document". Those use-cases will be performed on EMS and DMS connected systems at PNNL and WSU respectively and are targeted to test KISS sub-system to secure data-at-rest and data-in-transit. Beyond those use-cases, the KISS research team will continue to build upon those use-cases to perform a large scale complex inter-facility secure data exchange test through the developed KISS subsystem. This particular use-case will demonstrate all the elements discussed in previous sections that are related to immutability, non-repudiation, data provenance, and strengthening the system to address some elements of the BlackEnergy attack. Below subsection defines some of the technical elements associated with the use-cases along with the high-level architectural overview.

5.1 Utility to ISO Signing and Verification

This use case simulates data exchange between utilities and ISOs where Washington State University (WSU) acts as a power utility while VOLTTRON acts like an ISO collecting data from different utilities to device an efficient market environment. The DMS agent in the WSU Testbed collects topological data in the form of control switch statuses from the RTUs via DNP3 communication. This data would be in the form of data points that have been read and/or written and the function codes specifying the commands sent to them. This data is signed and sent to the agent at PNNL which verifies it using BlackLantern.[8] The DNP3 packets get hashed by a shared KSI agent before they are sent to the BlackLantern for signing. The ISO agent at PNNL might subscribe to other agents' topics that send switch statuses.

There can be a shared environment for the KSI agent which acts like a third party that signs and verifies the data or there could be two KSI agents – one to subscribe to the DMS agent for signing and the other to subscribe to the agent at PNNL for verification. Figure 13 gives an overview of the proposed use-case.

[8] Black Lantern Security Appliance is an integrated, anti-tamper hardware and software platform, purpose built to mitigate both remote and physical attacks against network infrastructure and applications.

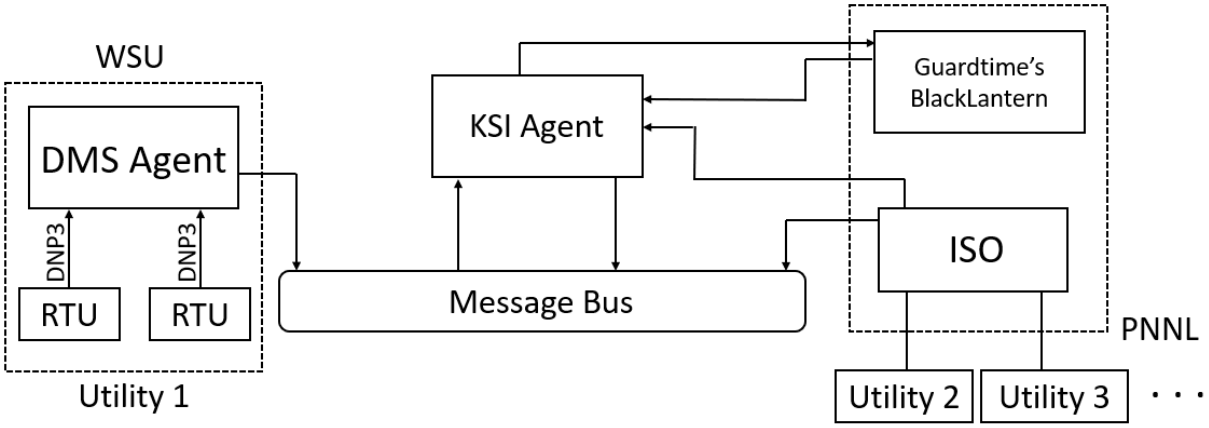


Figure 13. Utility Simulation Use Case

6.0 Conclusion

This gap analysis identified and number of cyber security opportunities and challenges in applying the Keyless Infrastructure Security Solution (KISS) to improve the state of the state of art of monitoring energy delivery systems (EDS) at the grid's edge through an innovative application of blockchain technology. The BlackEnegry cyberattack were a grim reminder of the potential impact of not closing these gaps. The proposed use cases were given that would help close security gaps currently found in electricity infrastructure in the U.S. and globally. Additional research by the KISS team may also show that KISS can improve that current state of the art in grid security by rapidly revoking and deprovisioning EDS that are misconfigured and or under attack. Improving this capability and closing these gaps is imperative for a timely and effective response to a large-scale outage, whether due to a natural disaster or a large-scale attack.

Pacific Northwest National Laboratory

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99352
1-888-375-PNNL (7665)

www.pnnl.gov