Announcing the SAG-CTR(TM) Community Trust Registry for Digitally Signed Software

SAG-CTR(TM) enables software customers to verify trust between a software supplier and digital signer of software to satisfy Executive Order C-SCRM requirements

WESTFIELD, MA, USA, June 29, 2021 /EINPresswire.com/ -- Reliable Energy Analytics, LLC (REA) has taken another significant step to improve the trustworthiness of software supply chains by announcing availability of the Software Assurance Guardian™ (SAG™) Community Trust Registry™ (SAG-CTR™). SAG-CTR™ implements a community trust model that allows REA Customers of the SAG-PM™ C-SCRM solution to register their trust in a

SAG Logo

software package/digital signature combination within the registry, enabling other REA Customers to view the list of trusted software objects, along with the trusting parties that have registered their trust within the registry. SAG-CTR™ addresses a known issue within the software supply chain preventing a software customer from verifying the trust relationship between the original software supplier of a software package and the party that signs a software package. Today's digital code signing and verification practices allow any party with a properly issued code signing certificate to sign a software package owned by any other party. Only legitimate, parties and signing keys authorized by the original software supplier should be allowed to digitally sign software packages on behalf of a software supplier in order to establish a trust worthy bond between the parties and a software package, which a software customer can verify. SAG-CTR™ provides software customers with the ability to perform this verification function, through an easy-to-use Web based API/URL.

The dangers present within a software package have received widespread media attention, such as the SolarWinds incident. The Cybersecurity Executive Order, released on May 12, 2021, emphasizes the risks emanating from the software supply chain and the immediate need for solutions to detect and mitigate these risks as part of a Cybersecurity Supply Chain Risk Management (C-SCRM) program. Software customers are becoming victims of malware induced cyber-crimes that can be prevented through the application of effective C-SCRM solutions that implement NTIA supported SBOM formats SPDX and CycloneDX, such as SAG-PM™ and the SAG-

CTR™ community trust methodology, described in the SAG™ patent application, [16/933161](#).

Never trust software, always verify and report! ™

Dick Brooks
Reliable Energy Analytics LLC
+1 978-696-1788
email us here

This press release can be viewed online at: https://www.einpresswire.com/article/545051889