NIOC
NG9-1-1 INTEROPERABILITY
OVERSIGHT COMMISSION

The NG9-1-1 Interoperability Oversight Commission (NIOC), the independent oversight body for standards-driven interoperability programs for NG9-1-1, is proud to announce approval and signature of a Master Services Agreement (MSA) with DigiCert for the US PSAP Credentialing Agency (PCA) on July 17, 2020 (In Canada, the CRTC mandated that NG9-1-1 network providers are to provide PCAs).

The MSA directs DigiCert, under the oversight of the NIOC, to create and host the Root Certificate that establishes the heart of the chain of trust for secure, interoperable NG9-1-1 communications in the United States as specified in the NENA i3 Standard. With the MSA in place, DigiCert will procure the specialized hardware to host the Root Certificate so that the issuance of Intermediate Certificates to NG9-1-1 in accordance with the Certificate Policy can begin at the appropriate time. The signing of the MSA is a monumental milestone in establishing a Public Key Infrastructure (PKI) for NG9-1-1. The PKI is required by the prevailing standards for NG9-1-1 and will provide PSAPs and ECCs with the level of security and assurance recommended by leading industry groups such as the Federal Communications Commission (FCC) Task Force on Optimal PSAP Architecture (TFOPA).

Every PKI requires an independent governance structure; for the NG9-1-1 PKI, that is NIOC. NIOC was convened in March, 2020, and began conducting official business in April 2020.

“On behalf of the NIOC Commissioners, we are excited that another foundational step in the evolution of Next Generation 9-1-1 has been achieved.” says NIOC Chair Rick Blackwell, ENP, E9-1-1 Director for Greenville County, South Carolina. “Having a Master Services Agreement in place exemplifies concrete action in establishing the PKI and the Root Certificate for NG9-1-1. This agreement establishes the secure foundation sought through years of hard work by so many at NENA, including the Board of Directors, staff, Development Steering Council, and all the volunteers who contributed to the organization’s working groups.”

The NIOC is finalizing the Certificate Policy for the PKI that is at the heart of the PCA operation, with the goal of entering NG9-1-1 PKI production in 2020 with DigiCert and their partner, Eonti.

The NIOC Commissioners individually and independently approved the competitive, sealed-bid Request for Proposals (RFP) process that led to the award of a contract to DigiCert for the PKI. The RFP solicited multiple proposals for the PCA and after a review and scoring of proposals by a committee of public and private volunteers, following industry best practices for procurement, a contract award decision was reached. A summary overview of the process NIOC followed in awarding the contract through this fair and open process is available on the NIOC website (www.ng911ioc.org).

In its role as a governance body, the NIOC shall oversee operation of the PCA as a revenue neutral body to NIOC and NENA. Under NIOC governance, DigiCert will sign issuing certificates to trusted entities such as ESInet operators like government entities and NG911 Core Services providers as defined in the future PKI Certificate Policy, NG91-1 PKI Extended Validation Policy, and an approved Certificate Practice Statement. PSAPs and ECCs will benefit from the higher level of trust the PCA will bring to NG9-1-1 through certificates traceable to the PCA root certificate. As the MSA signing is the first of multiple steps, the NIOC will continue to provide transparency and information of the value and increased level of security the PCA affords NG9-1-1 operations. NIOC notes that this root certificate is intended to provide for interoperability within the United States at this time, but ultimately must be compatible with similar mechanisms in Canada, Europe and elsewhere.

A PKI is a common best practice in critical infrastructure industries for establishing trusted interoperability. Effectively, a PKI provides a system of policies, procedures and technologies to establish a chain of trust among users based on the real-time exchange of security certificates between disparate systems. In building a PKI for

NG9-1-1 model, NIOC and NENA looked to other telecommunications and public safety approaches including those taken by SHAKEN/STIR, state and Federal Government and local Councils of Government (COGs). Learn more about how a PKI works in this informational video from NENA.

NIOC consists of stakeholders from the public and private sectors that are affected by standards-driven interoperability programs. More information is available here.