Palatine, Illinois and Stockholm, Sweden, 16th July, 2018 - Diamond Key Security™ (DKS) and the CrypTech Project are announcing the recent launch of the DKS website, dkey.org. The website is the online home for DKS and will become a place where customers, potential customers, OEMs, and licensees of Internet and general IT security solutions based on CrypTech technology can find the latest information related to DKS's product and service offerings. It will be a centralized location where one can learn about applying the DKS Hardware Security Module (HSM) to DNSSEC, identity management, and credential management as well as other HSM applications that provide trust by securing digital information through encryption, authentication, and signing.

"DKS and the CrypTech team are trying to fill the need for trustworthy cryptography for Internet infrastructure; they both want the open security platform to proliferate the market. DKS is in a unique position to create a sustainable, long-term business relationship for the open hardware design and open-source firmware that runs on it", said Russ Housley, of the CrypTech business team.

Whereas the CrypTech website is the place for developers to find the open-source specifications, code, and documentation for its security module, DKS's website will be the go-to place to find application-specific, educational, and support materials for its solutions, including products and services based on CrypTech. It will also be a place where corporate and institutional stakeholders and individuals can learn the benefits of financially supporting this open-source initiative.

According to W. Stuart Jones, Managing Director, Operations at DKS, "DKS is well positioned to assist, in particular, under-served industry segments, in protecting information and privacy. One important example is the burgeoning CrypTech Project, and DKS is becoming, for the transparent, open-source CrypTech technology, the not-for-profit equivalent of what Red Hat, Inc. is to Linux. The launch of our website is an important step towards this goal."

About DKS

Diamond Key Security™, based in Palatine, Illinois, was formed in March 2017 as a not-for-profit corporation described under Section 501(c)(3) of the United States Internal Revenue Code. Its educational, charitable, and scientific purposes include conducting scientific research in the development, enhancement and deployment of transparent, auditable cryptographic technologies to help safeguard the Internet for the public good, educating the general public concerning cryptographic technology,

facilitating initiatives to enhance the security and stability of the Internet, encouraging the effective use of cryptographic technologies in educational and other nonprofit organizations, and making reliable cryptographic security technologies widely available.

DKS's initial activities involve research, study, and scientific experimentation related to the CrypTech open-source cryptographic module. Specifically, its work researches the sustainability, development, and support of the CrypTech module for widely-available and inexpensive use among the general public through testing, evaluation, development of support, reference and developer support materials, and through the creation of viable hardware and software solutions that utilize this technology in under-served spaces, where such security technology is neither readily available nor currently affordable. DKS's website is at dkey.org.

About CrypTech

The CrypTech Project is a worldwide initiative started in late 2013. The CrypTech project was originally formed in response to the Snowden revelations of mass surveillance and to indications that the hardware implementations of key cryptographic algorithms and functions have been systematically targeted in an effort to weaken and subvert their utility. The goal of the project was to create an open-source design for a hardware cryptographic engine for Hardware Security Modules (HSMs) and an associated reference implementation that allows anyone to deploy and audit a secure, low-cost cryptographic engine in their environments. Possible examples of key security infrastructure that could utilize CrypTech technology include Domain Name System Security Extensions (DNSSEC), Resource Public Key Infrastructure (RPKI), TOR Consensus, Pretty Good Privacy (PGP), Identity Federations, and the Let's Encrypt Certificate Authority (CA). CrypTech is funded through contributions and support from varying industry and global partners. Additional information can be found at the CrypTech website at cryptech.is.