

nCipher enables Red Hat to meet rigorous Common Criteria standard

nShield hardware security modules (HSMs) protect cryptographic keys underpinning security of Red Hat Certificate System

Cambridge, UK – August 15, 2019 – [nCIPHER Security](#), an Entrust Datacard company and provider of trust, integrity and control for business-critical information and applications, announces that Red Hat, the world's leading provider of open source solutions, has achieved Common Criteria validation for its Red Hat Certificate System using nCipher nShield hardware security modules (HSMs).

The international Common Criteria (CC) standard was developed to unify and supersede national IT security certification schemes from different countries, including the US, Canada, Germany, UK, France, Australia, and New Zealand. Common Criteria certified solutions are required by governments and enterprises around the globe to protect their mission-critical infrastructures.

The Red Hat Certificate System is a public key infrastructure (PKI) used by some of the world's largest organizations to manage user identities and help keep communications private. PKIs are the hardware, software, policies, procedures and processes that issue and manage digital credentials across enterprise systems. PKIs are underpinned by a Certificate Authority (CA), a core component responsible for establishing a hierarchical chain of trust. Consequently, they are often the focus of sophisticated, targeted attacks.

To obtain its [Common Criteria certification](#), Red Hat was required to protect the critical root CA keys with FIPS 140-2 Level 3 certified hardware – the industry benchmark in cryptographic security. A long-standing nCipher partner, Red Hat used the nShield HSM to meet this requirement and provide a root of trust.

The new certified system offers joint customers a root of trust for the protection of cryptographic signing keys underpinning the Red Hat Certificate System. As customers embrace new digital initiatives such as the Internet of Things (IoT), PKIs are being deployed to support the increasing volume of digital certificates needed to validate the identities of devices and applications.

John Grimm, senior director of strategy and business development, nCipher Security says:

“The use of nCipher nShield HSMs is a best practice to provide a root of trust for business-critical applications, facilitating customer compliance with ever stricter data security and privacy regulations. According to the [2019 Global Encryption Trends Study](#), the use of HSMs grew at a record year-on-year level, from 41% in 2018 to 47%, indicating a requirement for a hardened, tamper-resistant environment with higher levels of trust, integrity and control for both data and applications. In its [ongoing collaboration](#) with nCipher, Red Hat continues to proactively address customer security needs in both enterprise and cloud environments.”

Amy Farley, product manager, Identity Management, Red Hat says:

“We're pleased to have worked with nCipher Security to achieve Common Criteria certification for Red Hat Certificate System 9.4. nCipher nShield HSMs helped us to more effectively meet the required levels of IT security for sensitive and classified environments as we pursued the certification.”

About nCipher Security

nCipher Security, an Entrust Datacard company, is a leader in the general-purpose hardware security module (HSM) market, empowering world-leading organizations by delivering trust, integrity and control to their business critical information and applications. Today's fast-moving digital environment enhances customer satisfaction, gives competitive advantage and improves operational efficiency – it also multiplies the security risks. Our cryptographic solutions secure emerging technologies such as cloud, IoT, blockchain, and digital payments and help meet new compliance mandates. We do this using our same proven technology that global organizations depend on today to protect against threats to their sensitive data, network communications and enterprise infrastructure. We deliver trust for your business critical applications, ensure the integrity of your data and put you in complete control – today, tomorrow, always. www.ncipher.com

Follow us on [LinkedIn](#), [Twitter](#), [Facebook](#) and [Instagram](#) – search nCipherSecurity.

###

For more information please contact:

nCipher Security

Megan Nemeš megan.nemeh@ncipher.com +1 408 887 5064

Liz Harris liz.harris@ncipher.com +44 7973 973648

Red Hat is a trademark or registered trademark of Red Hat, Inc. or its subsidiaries in the U.S. and other countries.