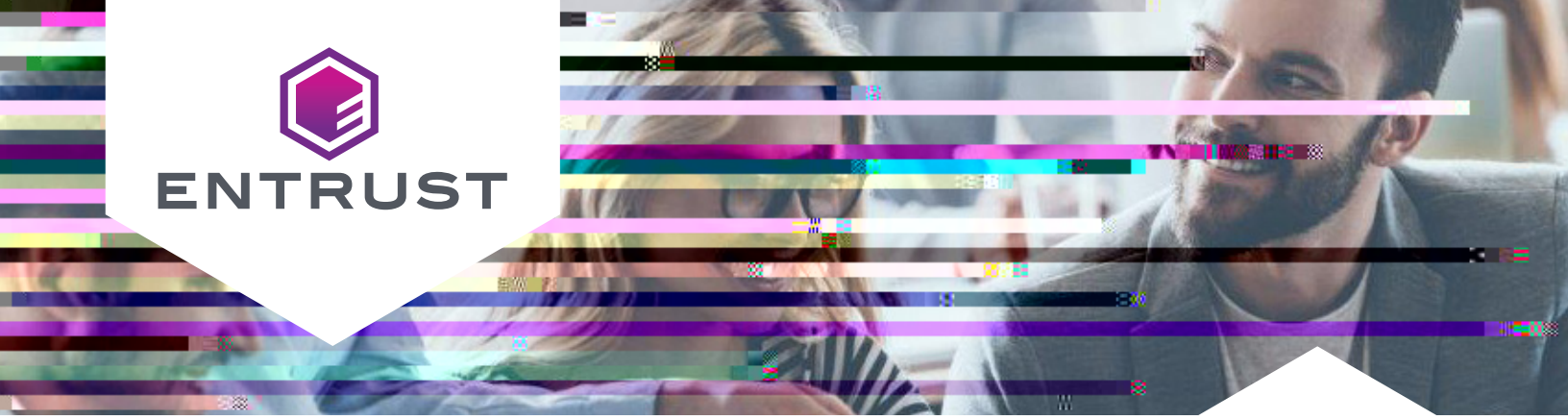

S
E R H C S

Generar confianza para la infraestructura de clave pública (PKI)

CARACTER STICAS PRINCIPALES

Ampl e la eg idad de Red Ha Ce izca e S em pa a la ol cione come ciale de la NSA pa a aplicacione cla izcada (CSfC)

Fo alece el ma co de eg idad ge ionando la iden idade de lo a io man eniendo la p i acidad de la com nicacione

P o ege la an accione la aplicacione habili ada pa a la PKI

U ilice m d lo de eg idad de ha d a e (HSM) nShield de En ce izcado po NIST FIPS 140-2

El problema: las KPI organizacionales se están ampliando para cumplir con un número cada vez mayor de aplicaciones comerciales

A medida q e la b echa de da o e el en oz icada , la o gani acione han ec ido a PKI pa a p o ege con ola el acce o a aplicacione c ica da o conzdenciale . Den o de na PKI, la a o idad de ce izcaci n (CA) emi e c edenciale elec nica pa a alida la iden idade en l nea hace c mpli lo con ole de acce o. Anali a la can idad de ce izcado digi ale ili ado , la impo ancia el alo de la aplicacione q e admi en i la aplicacione e n je a a ni ele al o de e c inio debido al c mplimien o no ma i o del gobie no o de la ind ia, on fac o e c ico pa a ga an i a q e la PKI p eda a i face la c ecien e demanda .

S E
Clave de firma privada protegida por HSM

S C t

Dispositivos de usuario final

Dispositivos de usuario final

APRENDA M S EN ENTRUST.COM/HSM

P R H

El desafío: establecer una raíz de confianza para los controles de identidad y acceso

La p o ecci n de la in eg idad eg idad de la CA q e en a na PKI e de i al impo ancia pa a ga an i a la conzan a en la aplicacione come ciale en lo da o q e p o egen. Dado q e la PKI admi en cada e n la opolog a cambian e de acce o de lo a io , incl ido lo di po i i o m ile de aiga p opio di po i i o (BYOD, po igla), la o gani acione deben a eg a e de q e la cla e c ip og zca p i ada e n p o egida ean ge ionada de mane a conzable.

La solución: Red Hat y Entrust brindan juntos una protección sólida de las identidades digitales

Red Ha Ce izca e S em emi e, ge iona alida la iden idade digi ale q e e ili an pa a inc la pe ona , di po i i o o e icio a cla e p i ada co e pondien e . La alide de cada ce izcado emi ido depende de la p o ecci n de la cla e CA q e emi e la iden idade . C ando el p oce o de emi i n e ejec a en n e ido ili ando na cla e almacenada localmen e en n a chi o, e a cla e p ede e lne able a la d plicaci n, modizcaci n i ci n. Ho en d a, la ma o a de la CA e ili an pa a emi i ce izcado pa a o den o de na o gani aci n. In e namen e, lo ce izcado e ili an no malmen e pa a eali a a en icaci n po cable e ine mb ica, cone ione de eg idad de capa de cone i n/ an po e eg o (SSL/TLS) a en icaci n de ed p i ada i al (VPN). Dado q e la aplicacione en e pan i n nece i an lo e icio de na PKI, la demanda de la CA la nece idad de na eg idad mejo ada on p imo diale .

Lo HSM nShield de de En a men an el ni el de eg idad de la PKI al p o ege la a p i ada la cla e de CA de z ma. Lo HSM nShield p o egen lo p oce o de emi i n, ge i n alidaci n, lo q e le pe mi e a la o gani acione fo alece la ol ci n de iden idad acce o. Lo HSM nShield e in eg an f cilmen e con Ce izca e S em de Red Ha ili ando in e face de p og amaci n de aplicacione c ip og zca e nda (CAPI). C ando e ili an lo HSM nShield de En odo el p oce amien o de alidaci n emi i n de ce izcado e p od ce den o de lo l mi e p o egido del HSM. La cla e de z ma a p i ada n nca on acce ible o en n fo ma o legible f e a del HSM. Incl o d an e lo p oce o de copia de eg idad, a chi o ec pe aci n, lo HSM nShield ga an i an q e la cla e p i ada no ean cep ible de manip laci n /o comp omi o.

P R H

¿Por qué utilizar HSMs de Entrust con Certificate System de Red Hat?

La iden izcaci n de b echa , la ec pe aci n λ la planizcaci n de con ingencia on pa o impo an e q e e p eden oma pa a fo alece la eg idad de na PKI. Una PKI efo ada λ de al a eg idad p opo ciona n en o no q e p o ege la cla e c ica pa a la eg idad con a obo λ o indebido . Vinc la la emi i n de ce izcado a la e izcacione λ ap obacione de iden idad ili ando n HSM nShield de En , ha ido na lecci n impo an e ap endida de lo comp omi o de eg idad de CA an e io e .

Ce izcado eg n e ic o e nda e de eg idad, incl ido FIPS 140-2 Ni el 3λ Common C i e ia EAL4+, lo HSM nShield:

- Almacene la cla e pa a z ma λ emi i ce izcado digi ale en n en o no eg o λ e i en e a manip lacione indebida
- Ge ione el acce o de admini ado e con na pol ica ba ada en a je a in eligen e λ a en icaci n de do fac o e
- C mpla con lo eq i i o no ma i o del ec o p blico, lo e icio znancie o λ la emp e a

HSMs de Entrust

Lo HSM de En nShield e enc en an en e la ol cione de HSM de ma o endimien o, ma eg a λ f cile de in eg a q e e enc en an di ponible , lo c al facili a el c mplimien o no ma i o λ of ece lo ni ele ma al o de eg idad de da o λ aplicacione pa a o gani acione emp e a iale , znancie a λ g be namen ale . N e a e cl i a a q i ec a de ge i n de cla e Sec i λ Wo ld p opo ciona con ole lido λ g an la e ob e el acce o λ o de cla e .

Red Hat

Red Ha e el p o eedo m ndial l de de ol cione de c digo abie o pa a emp e a . Adema de i ema de ce izcacione de Red Ha , la ol cione incl λ en la pla afo ma Red Ha En e p i e Lin , Red Ha OpenS ackλ Red Ha OpenShif , en e na amplia gama de e icio λ admini aci n. Lo HSM nShield de En e n ce izcado con Red Ha Ce izca e S em. **www.redhat.com**

Más información

Pa a abe ma ob e lo HSM nShield de En i i e **entrust.com/HSM**. Pa a abe ma ob e la ol cione de eg idad digi al de En pa a iden idade , acce o, com nicacione λ da o , i i e **entrust.com**