

V-Key Autenticación Multifactorial

La única solución MFA que necesita para todas sus aplicaciones en la nube, VPN y sistemas

Autenticador para gobernar a todos



Basado en el elemento seguro virtual V-OS patentado a nivel mundial, el V-Key Smart Authenticator proporciona una solución MFA basada en la nube para Android e iOS. Con la confianza de bancos y super aplicaciones, y diseñado para admitir múltiples plataformas de productividad, personalice el Authenticator para la marca de su empresa.

BENEFICIOS

- La ausencia de hardware de token se traduce en un menor coste de aprovisionamiento, gestión y renovación.
- Modelo de licencia simple, una licencia cubre el uso de los modos cliente y sin cliente.
- Aprovechar las tendencias actuales en materia de informatización en el lugar de trabajo.
- Mejore las tasas de adopción de los usuarios a través de la facilidad de uso y la falta de tokens incrementales.
- La personalización permite una experiencia de usuario con la marca de la empresa.
- Las claves de token nunca se almacenan en un tercero o proveedor de tokens que no sea de confianza. Sin posibilidad de compromiso.
- Las cuentas se pueden suspender si se pierde el teléfono y luego se pueden restablecer cuando se encuentra el teléfono.

RESÚMENES

- Elemento seguro virtual con certificación FIPS 140-2.
- Implementación sencilla.
- Potente gestión administrativa.
- Protección de todas las soluciones.
- Panel de control visualizado.
- Migración de autenticación avanzada.
- Múltiples factores de forma: token de software, OTP, huella dactilar, caraID, TouchID y SMS.
- Tokens blandos para iPhone y Android.
- Modelo de precios inteligente: un precio por usuario al año, independientemente del factor de forma.
- Compatibilidad con ADFS/RADIUS, SAML+ y OCID
- Portal web intuitivo para el auto aprovisionamiento de usuarios.
- Informes integrales y motor de cumplimiento.
- Inicio de sesión único.
- Simplifique el inicio de sesión en aplicaciones desde dispositivos de confianza.
- Notificación push móvil para un inicio de sesión rápido sin OTP.
- Servidor de autenticación disponible como servicio en la nube y servicio gestionado.
- Opciones de integración y migración disponibles.

CASOS DE USO

- Mejore RADIUS o Active Directory o Entra ID.
- Autenticación de servicios basados en la nube.
- Autenticación RDS.
- Inicio de sesión sin contraseña.
- Proteja los PC con Windows.
- Acceso Seguro a Microsoft Always On VPN.
- Acceso seguro a VDI.
- Escritorio remoto Seguro.



Elemento seguro virtual de V-OS

En el corazón de las soluciones de V-Key se encuentra V-OS, el primer elemento seguro virtual del mundo que cumple con la norma FIPS 140-2 (US NIST), alcanza los objetivos de seguridad FIDO y cuenta con la certificación Common Criteria EAL3+ . V-OS crea un entorno virtual aislado dentro de las aplicaciones móviles para almacenar de forma segura claves criptográficas y otra información importante.

CARACTERÍSTICAS PRINCIPALES

- Solución de nivel enterprise.
- Funciona en la nube y en las instalaciones.
- Admite servidores de autenticación de terceros.
- Protecciones de seguridad móvil avanzadas de varias capas.
- Soporta estándares de criptografía simétricos y asimétricos.
- Aprovechamiento de varios tokens dentro de una sola aplicación.
- PKI y OTP seguras.
- Cumple con el estándar FIDO.
- Certificación CC EAL3+ y FIPS 140-2.
- Tiempo de confianza.
- Superposición y detección de espejo de pantalla.
- Bloqueo remoto.
- Enlace de dispositivos protegido contra copia.
- Verdadero cifrado de extremo a extremo.
- API segura.
- CaraID, huella dactilar, bloqueo de PIN.
- Proveedor de servicios múltiples.
- Multidispositivo.
- Acceso físico.
- Protección de aplicaciones integrada.
- Panel de inteligencia de amenazas.
- Interfaz de usuario personalizable.
- Capaz de operar en dispositivos rooteados/liberados.

Sección	Funciones
Funcionalidades	PKI Auth
	PKI Transaction validation
	OTP
	Proveedor de servicios múltiples
	Multidispositivo
	Acceso físico
	Mensajería segura
	Acceso seguro a VPN
	Acceso seguro a O365
	Personalizar el soporte de la aplicación
	Soporte lingüístico global
Experiencia de usuario	Experiencia de usuario intuitiva
	WYSIWYS (Lo que ves - lo que firmas)
	Activación flexible
	Fácil personalización
	Localización
	Gesto de 2 pasos
Otros	Certificación/Cumplimiento
	Patente- FIPS 140-2, CC EAL3+, SOC 2, OATH

Sección	Funciones
Seguridad	Política de contraseñas personalizable
	Inteligencia de amenazas
	FaceID, FingerPrint, PIN Lock
	Protección de la información de las transacciones
	Canal seguro
	RASP (Run time ASP)
	Jailbreak & Root Detection
	Tamper Detection & Anti Cloning
	Auditorías Externas
	Elemento seguro virtual (V-OS)
	Fuerte protección de claves criptográficas y semillas OTP
	Depurador, simulador, detección de emulador de hardware
	Detección de ganchos
	Secure Channel to the application server
	Alertar a los sistemas de supervisión de que se ha producido un ataque
	Detección de malware (e.g., accessibility-enabled malware)
	Anti-captura de pantalla
Seguridad (Monitoring)	



Celestix Networks, Inc.
2603 Camino Ramon #200
San Ramon, CA 94583
www.celestix.com

Americas : +1 510.668.0700
EMEA : +44 (0203) 900 3737
Asia : +65 6958 0822
sales@celestix.com