



---

REF: 2004-2-INF-65 v1  
Difusión: Público  
Fecha: 20.01.2006

Creado: CERT3  
Revisado: TECNICO  
Aprobado: JEFEAREA

---

## INFORME DE CERTIFICACION

---

Expediente: 2004-2 KEY ONE 3.0

---

### Referencias:

EXT-18 Solicitud de Certificación, 09-07-2004  
EXT-125 Informe Técnico de Evaluación, 29-12-2005  
CCRA Arrangement on the Recognition of Common Criteria  
Certificates in the field of Information Technology Security,  
May 2000.

---

Informe de certificación del producto KeyOne 3.0, una solución software de infraestructura de clave pública (PKI), versión 3.0, release 04S2R1 con parches 3.0\_04S2R1\_B01, 3.0\_04S2R1\_B02, 3.0\_04S2R1\_B03, 3.0\_04S2R1\_B04, 3.0\_04S2R1\_B05, 3.0\_04S2R1\_B06 y 3.0\_04S2R1\_B07, tal y como se solicitó por [EXT-18], y evaluado por el CESTI-INTA, como se detalla en el Informe Técnico de Evaluación [EXT-125], recibido el 11 de enero de 2006, según lo especificado por el [CCRA].



## Índice

<b>RESUMEN EJECUTIVO</b> .....	<b>3</b>
RESUMEN DEL TOE.....	4
REQUISITOS DE GARANTÍA DE SEGURIDAD .....	5
REQUISITOS FUNCIONALES DE SEGURIDAD .....	6
<i>Requisitos expresados conforme a [CC_P2]:</i> .....	6
<i>Requisitos aumentados por el perfil de protección [CIMC]:</i> .....	6
<b>IDENTIFICACIÓN</b> .....	<b>8</b>
<b>POLÍTICAS DE SEGURIDAD</b> .....	<b>8</b>
<b>HIPÓTESIS Y ACLARACIONES DEL ALCANCE</b> .....	<b>8</b>
HIPÓTESIS DE USO .....	8
<i>Personal</i> .....	8
<i>Conectividad</i> .....	10
HIPÓTESIS DE ENTORNO .....	10
<i>Hipótesis físicas</i> .....	10
<i>Usuarios del TOE</i> .....	10
<i>Entornos de uso posibles</i> .....	11
ACLARACIONES SOBRE EL ALCANCE .....	11
<i>Amenazas de Usuarios Autorizados</i> .....	11
<i>Amenazas de Sistema</i> .....	12
<i>Amenazas relacionadas con la Criptografía</i> .....	12
<i>Amenazas debidas a ataques externos</i> .....	13
FUNCIONALIDAD DEL ENTORNO. ....	13
<i>Requisitos expresados conforme a [CC_P2]:</i> .....	14
<i>Requisitos extendidos:</i> .....	14
<b>INFORMACIÓN SOBRE LA ARQUITECTURA</b> .....	<b>16</b>
KEYONE CA. AUTORIDAD DE CERTIFICACIÓN .....	16
KEYONE LRA: AUTORIDAD LOCAL DE REGISTRO .....	16
KEYONE VA. GESTIÓN DE CERTIFICADOS REVOCADOS .....	16
KEYONE TSA SERVER. AUTORIDAD DE SELLADO DE TIEMPO .....	16
ARQUITECTURA FÍSICA .....	17
ARQUITECTURA LÓGICA .....	19
<b>DOCUMENTACIÓN</b> .....	<b>20</b>
<b>PRUEBAS DEL PRODUCTO</b> .....	<b>20</b>
<b>CONFIGURACIÓN EVALUADA</b> .....	<b>21</b>
<b>RESULTADOS DE LA EVALUACIÓN</b> .....	<b>22</b>
<b>COMENTARIOS Y RECOMENDACIONES DE LOS EVALUADORES</b> .....	<b>22</b>
CONCLUSIONES .....	22
RECOMENDACIONES .....	23
<b>RECOMENDACIONES DEL CERTIFICADOR</b> .....	<b>25</b>
<b>GLOSARIO</b> .....	<b>25</b>
<b>BIBLIOGRAFÍA</b> .....	<b>26</b>
<b>SECURITY TARGET</b> .....	<b>26</b>



## Resumen Ejecutivo

Informe de certificación del producto KeyOne 3.0, una solución software de infraestructura de clave pública (PKI), versión 3.0, release 04S2R1 con parches 3.0\_04S2R1\_B01, 3.0\_04S2R1\_B02, 3.0\_04S2R1\_B03, 3.0\_04S2R1\_B04, 3.0\_04S2R1\_B05, 3.0\_04S2R1\_B06 y 3.0\_04S2R1\_B07.

**Fabricante:** Safelayer Secure Communications, S.A.

**Sponsor:** Safelayer Secure Communications, S.A.

**Organismo de Certificación:** Centro Criptológico Nacional (CCN)

**ITSEF:** Centro de Evaluación de la Seguridad de las TI (CESTI), del Instituto de Técnica Aeroespacial “Esteban Terradas”(INTA).

**Perfiles de Protección:** [CIMC], Certificate Issuing and Management Components Family of Protection Profiles v1.0, Level 3, EAL 3+, october 2003.

**Nivel de evaluación:** EAL4+ (ALC\_FLR.2)

**Fortaleza de funciones:** Basic

**Fecha del Informe Técnico de Evaluación:** 2006-01-11

Todos los componentes de garantía requeridos por el nivel EAL4+ (aumentado con ALC\_FLR.2, SOF basic) han sido asignados un veredicto “PASA”. Consecuentemente, el laboratorio (CESTI /INTA) asigna el veredicto “PASA” al conjunto de la evaluación debido a que todas las acciones del evaluador se satisfacen para la metodología EAL4+, como define la Common Criteria [CC-P3] y la Common Methodology [CEM].

Considerando las evidencias obtenidas durante la instrucción de la solicitud de certificación del producto KeyOne 3.0, versión: 3.0, release 04S2R1 con parches 3.0\_04S2R1\_B01, 3.0\_04S2R1\_B02, 3.0\_04S2R1\_B03, 3.0\_04S2R1\_B04, 3.0\_04S2R1\_B05, 3.0\_04S2R1\_B06 y 3.0\_04S2R1\_B07, se propone estimar de forma positiva la resolución.



## **Resumen del TOE**

El OE (Objeto de Evaluación) o TOE (Target Of Evaluation) es el producto Keyone 3.0 o KTS (Keyone Trusted System). Se trata de un producto software que implementa una infraestructura de clave pública (PKI).

Para implementar los servicios, el sistema KeyOne consta de los siguientes subsistemas componentes:

- KeyOne LRA. Autoridad Local de Registro
- KeyOne RA. Autoridad de Registro
- KeyOne CA. Autoridad de Certificación
- KeyOne VA. Autoridad de Validación
- KeyOne TSA. Autoridad de sellado de tiempo

Para realizar sus funciones, este producto proporciona los siguientes servicios.

### **Servicios principales**

- Servicio de Registro. Verifica la identidad y los atributos del solicitante de certificado. Los resultados de este servicio se pasan al servicio de generación de certificado.
- Servicio de Generación de Certificado. Crea y firma los certificados entregados por la autoridad de registro.
- Servicio de Gestión de Revocación de Certificado. Gestiona la petición de suspensión de certificados cuando se considera que la clave privada correspondiente ya no es segura.
- Servicio de Estado de Revocación de Certificado. Aporta información sobre el estado de revocación de un certificado a la parte confiable. Esta información se actualiza periódicamente.

### **Servicios adicionales**

- Servicio de Provisión de Dispositivos. Proporciona un dispositivo de creación de firma a los usuarios.
- Servicios de Sellado de Tiempo. Proporciona la capacidad para generar sellos de tiempo para la validación temporal de los datos.



MINISTERIO DE DEFENSA  
CENTRO NACIONAL DE INTELIGENCIA  
CENTRO CRIPTOLÓGICO NACIONAL  
ORGANISMO DE CERTIFICACIÓN



La relación entre los servicios que proporciona el sistema y el componente donde reside cada uno se describe en la siguiente tabla.

<b>Subsistema</b>	<b>Servicios</b>
KeyOne LRA	Servicio de Registro Servicio de Provisión de Dispositivo de Titular
KeyOne RA	Servicio de Registro
KeyOne CA	Servicio de Generación de Certificado Servicio de Gestión de Revocación
KeyOne VA	Servicio de Estado de Revocación
KeyOne TSA	Servicio de Estampado de Tiempo

### ***Requisitos de garantía de seguridad***

El producto se evaluó con todas las evidencias necesarias para la satisfacción del nivel de evaluación EAL4, más las requeridas para el componente adicional, ALC\_FLR.2.

<b>Clase de requisitos</b>	<b>Componente</b>
Gestión de configuración	ACM AUT.1, ACM CAP.4, ACM SCP.2
Distribución y operación	ADO DEL.2, ADO IGS.1
Desarrollo	ADV_FSP.2, ADV_HLD.2, ADV_IMP.1, ADV_LLD.1, ADV_RCR.1, ADV_SPM.1
Manuales	AGD ADM.1, AGD USR.1
Ciclo de vida	ALC DVS.1, ALC LCD.1, ALC FLR.2, ALC TAT.1
Pruebas	ATE COV.2, ATE FUN.1, ATE IND.2, ATE DPT.1
Análisis de vulnerabilidades	AVA SOF.1, AVA VLA.2, AVA MSU.2



### ***Requisitos funcionales de seguridad***

La funcionalidad de seguridad del producto satisface, con la colaboración del entorno, el perfil de protección [CIMC], Certificate Issuing and Management Components Family of Protection Profiles v1.0, Level 3, EAL 3+, october 2003.

Los requisitos funcionales que satisface el producto son los siguientes:

### **Requisitos expresados conforme a [CC\_P2]:**

- FAU\_GEN.1 Audit data generation
- FAU\_GEN.2 User identity association
- FAU\_SEL.1 Selective Audit
- FAU\_STG.1 Protected audit trail storage
- FAU\_STG.4 Prevention of audit data loss
- FPT\_STM.1 Reliable time stamps
- FMT\_MOF.1 Management of security functions behavior
- FDP\_ACC.1 Subset access control
- FDP\_ACF.1 Security attribute based access
- FDP\_ITT.1 Basic internal transfer protection
- FDP\_UCT.1 Basic data exchange confidentiality
- FPT\_RVM.1 Non-bypassability of the TSP
- FPT\_ITC.1 Inter-TSF confidentiality during transmission
- FPT\_ITT.1 Basic internal TSF data transfer protection
- FIA\_UAU.1 Timing of authentication
- FIA\_UID.1 Timing of identification
- FIA\_USB.1 User-subject binding

### **Requisitos aumentados por el perfil de protección [CIMC]:**

- FPT\_CIMC\_TSP.1 Audit log signing event
- FDP\_ACF\_CIMC.2 User private key
- FDP\_ACF\_CIMC.3 User secret key
- FDP\_SDI\_CIMC.3 Stored public key integrity monitoring and action
- FDP\_ETC\_CIMC.5 Extended user private and
- FDP\_CIMC\_BKP.1 CIMC backup and recovery
- FDP\_CIMC\_BKP.2 Extended CIMC backup and recovery
- FDP\_CIMC\_CSE.1 Certificate status export
- FDP\_CIMC\_CER.1 Certificate Generation
- FDP\_CIMC\_CRL.1 Certificate revocation list
- FDP\_CIMC\_OCSP.1 OCSP basic response
- FCO\_NRO\_CIMC.3 Enforced proof of origin and verification of origin
- FCO\_NRO\_CIMC.4 Advanced verification of origin
- FMT\_MTD\_CIMC.4 TSF private key confidentiality protection
- FMT\_MTD\_CIMC.5 TSF secret key confidentiality protection
- FMT\_MTD\_CIMC.7 Extended TSF private and secret key export



MINISTERIO DE DEFENSA  
CENTRO NACIONAL DE INTELIGENCIA  
CENTRO CRIPTOLÓGICO NACIONAL  
ORGANISMO DE CERTIFICACIÓN



- FMT\_MOF\_CIMC.3 Extended certificate profile management
- FMT\_MOF\_CIMC.5 Extended certificate revocation list profile management
- FMT\_MOF\_CIMC.6 OCSP Profile Management
- FCS\_CKM\_CIMC.5 CIMC private and secret key



## Identificación

**Producto:** KeyOne 3.0, una solución software de Public Key Infrastructure, versión 3.0, release 04S2R1 con parches 3.0\_04S2R1\_B01, 3.0\_04S2R1\_B02, 3.0\_04S2R1\_B03, 3.0\_04S2R1\_B04, 3.0\_04S2R1\_B05, 3.0\_04S2R1\_B06 y 3.0\_04S2R1\_B07.

**Declaración de Seguridad:** Declaración de Seguridad KeyOne 3.0 (7BFD7697), 1.9.

**Perfiles de Protección:** CIMC, Certificate Issuing and Management Components Family of Protection Profiles v1.0, Level 3, EAL 3+, october 2003.

**Nivel de Evaluación:** EAL4+ (ALC\_FLR.2)

**Fortaleza de funciones:** Basic

**Fecha del Informe Técnico de Evaluación:** 2006-01-11

## Políticas de Seguridad

La instalación del TOE y su operación deben cumplir con las siguientes políticas de seguridad como se indica en [CIMC]:

### **P. Uso autorizado de la Información**

La información sólo podrá ser utilizada para propósitos autorizados.

### **P. Criptografía**

Se utilizarán funciones criptográficas conformes con FIPS o recomendadas por el NIST, para todas las operaciones criptográficas.

## Hipótesis y aclaraciones del alcance

### ***Hipótesis de uso***

Las hipótesis de uso se clasifican en tres categorías: de personal, de conectividad y físicas. Éstas últimas se describirán en el apartado sobre hipótesis de entorno.

### **Personal**

Se trata de supuestos sobre las actividades de los administradores y usuarios del sistema, así como cualquier otro agente, que puedan implicar una amenaza.



### ***A.Auditoría de Revisión de Logs***

Es necesario recoger los registros de auditoria relativos a eventos de seguridad y éstos deben ser revisados por los Auditores.

### ***A.Gestión de Datos de Autenticación***

Se sigue una política de gestión de datos de autenticación que garantice que los usuarios actualizan sus datos de autenticación periódicamente y con los valores adecuados (ej. longitudes de clave adecuada, históricos, variaciones, etc.). Nota: esta hipótesis no aplica a datos de autenticación biométricos.

### ***A.Auditores, Oficiales de Seguridad, Operadores y Administradores competentes***

Se designarán Auditores, Oficiales de Seguridad, Operadores y Administradores competentes para gestionar el OE y la seguridad de la información que trata.

### ***A.Declaración de Prácticas de Certificación***

Todos los Auditores, Oficiales de Seguridad, Operadores y Administradores están familiarizados con la política de certificación (PC) y la declaración de prácticas de certificación (DPC), bajo las cuáles opera el TOE. Esta documentación es conforme a la política de certificación de la Nato (NPKI).

### ***A.Eliminación de los Datos de Autenticación***

Siempre que se elimina un acceso se realiza un borrado seguro de los datos de autenticación y privilegios asociados (ej.: finalización de contrato de trabajo, cambio de responsabilidades).

### ***A.Código malicioso sin firma***

El código malicioso no está firmado por una entidad de confianza.

### ***A.Notificación a las Autoridades de los temas de seguridad***

Auditores, Oficiales de Seguridad, Operadores y Administradores y demás usuarios notifican a las Autoridades pertinentes de cualquier tema de seguridad que pueda tener impacto en sus sistemas, para minimizar posibles pérdidas o compromiso de los datos.

### ***A.Educación en Ingeniería Social***

Los Usuarios, Auditores, Oficiales de Seguridad, Operadores y Administradores son formados en técnicas para frustrar ataques de ingeniería social.



### ***A. Usuarios coordinados***

Los usuarios requieren un entorno informático seguro para llevar a cabo ciertas tareas o grupos de tareas. Los usuarios requieren acceso al mínimo de información del TOE y se espera que actúen de forma coordinada.

## **Conectividad**

Se trata de supuestos sobre otros sistemas de información necesarios para un funcionamiento seguro del TOE.

### ***A. Sistema Operativo***

El sistema operativo seleccionado proporciona las funciones requeridas por el CIMC, para contrarrestar las amenazas detectadas para el nivel 3 del Perfil de Protección, tal y como se identifica en la Declaración de Seguridad (DS).

### ***A. Cliente NTP***

Todas las máquinas que componen el TOE tienen instalado un cliente NTP para sincronizar sus relojes con el tiempo universal coordinado (UTC) proporcionado por un reloj fiable.

## ***Hipótesis de Entorno***

### **Hipótesis físicas**

Se trata de supuestos sobre el emplazamiento físico del TOE o de cualquier dispositivo periférico conectado al mismo.

### ***A. Protección de las Comunicaciones***

El sistema está adecuadamente protegido frente a pérdidas de la comunicación.

### ***A. Protección Física***

El hardware, software y firmware del OE críticos para el cumplimiento de la política de seguridad será protegido frente a modificaciones físicas no autorizadas.

## **Usuarios del TOE**

Los pretendidos usuarios de los distintos servicios que ofrece este producto se clasifican en dos grupos principales.

### ***Usuarios externos***

La Entidad de Certificado/Usuario Final, es el sujeto del certificado que asocia su identidad con su clave pública. Hay otros tipos de



MINISTERIO DE DEFENSA  
CENTRO NACIONAL DE INTELIGENCIA  
CENTRO CRIPTOLÓGICO NACIONAL  
ORGANISMO DE CERTIFICACIÓN



entidades que se pueden certificar, por ejemplo, aplicaciones o servicios.

Las Partes de Confianza, usuarios o agentes o cualquier servicio externo de confianza que confía en los datos de un certificado al hacer las decisiones, siguiendo los procesos de comprobación y limitaciones establecidos en las políticas de certificado para cada tipo de certificados publicados por KTS.

Los Auditores, que requieren acceder al registro de auditoría para evaluar y revisar las prácticas de certificación.

### ***Usuarios Internos***

Los Administradores de la PKI, que pueden configurar y administrar las diferentes aplicaciones sostenidas por el TOE: Registro, Autoridad de Certificado, Autoridad de Validación, Autoridad de Estampado de Tiempo.

El Oficial de Registro es responsable de la operación de la Autoridad de Registro Ligera y de la Autoridad de Registro, según los procedimientos de registro establecidos.

### **Entornos de uso posibles**

La funcionalidad de este producto, presentada en su Declaración de Seguridad, puede resolver una gran variedad de casos, que van desde la identificación de usuario y control de acceso hasta la protección de recursos internos, comercio electrónico u otros muchos sectores del mercado.

Sin embargo, el uso de este producto es más conveniente en determinados esquemas de registro. Esta configuración se adapta perfectamente a:

- Entornos de registro distribuido, debido al rápido y fácil despliegue de diferentes RAs, sin incrementar las necesidades de mantenimiento.
- Registros móviles o ambulantes, garantizando la seguridad del servicio de registro sin unas medidas de protección física muy restrictivas.

### ***Aclaraciones sobre el alcance***

Las siguientes amenazas, organizadas en cuatro categorías (usuarios autorizados, sistema, criptografía, y ataques externos) son cubiertos por el TOE o por el entorno, o por ambos de ellos.

### **Amenazas de Usuarios Autorizados**

#### ***T.Errores de omisión administrativa***

Los Auditores, Oficiales de Seguridad, Operadores y Administradores no realizan correctamente las funciones críticas para la seguridad.



***T.Abuso de autorización del usuario que recopila y/o envía datos***

El usuario abusa de las autorizaciones concedidas para recopilar y/o enviar datos sensibles o críticos para la seguridad.

***T.Error de usuario que provoca la inaccesibilidad de los datos***

El usuario accidentalmente borra datos del usuario que los hace inaccesibles.

***T.Audidores, Oficiales de Seguridad, Operadores y Administradores incurren en errores o acciones hostiles***

Un Auditor, Oficial de Seguridad, Operador o Administrador Incurre en errores que cambian la política de seguridad del sistema o la aplicación o modifican intencionadamente la configuración del sistema para permitir que se produzcan violaciones de seguridad.

## **Amenazas de Sistema**

***T.Fallo de componente crítico para el sistema***

El fallo de uno o más componentes del sistema provoca una pérdida de la funcionalidad crítica del sistema.

***T.Ejecución de código dañino***

Un usuario autorizado, sistema informático, o hacker obtiene y ejecuta código dañino que da lugar a procesos anormales que violan la integridad, disponibilidad o confidencialidad de los activos del sistema.

***T.Modificación del contenido de un mensaje***

Un hacker modifica la información que es interceptada por la línea de comunicación entre dos entidades autorizadas, antes de que llegue a su destinatario.

***T.Código defectuoso***

El desarrollador del sistema o aplicaciones entrega código que no está de acuerdo con las especificaciones o que contiene fallos de seguridad.

## **Amenazas relacionadas con la Criptografía**

***T.Revelación de claves privadas y secretas***

Una clave privada o secreta es revelada de forma inapropiada.



### ***T.Modificación de claves privadas/secretas***

Una clave privada/secretas es modificada.

### ***T.El remitente niega el envío de información***

El remitente de un mensaje niega el envío del mismo para evitar responsabilidades derivadas del envío del mensaje y acciones secundarias o falta de acciones.

## **Amenazas debidas a ataques externos**

### ***T.Un hacker consigue el acceso***

Un hacker se hace pasar por un usuario autorizado para realizar operaciones que serán atribuidas al usuario o proceso del sistema autorizado, o consigue acceso al sistema sin ser detectado debido a una falta, una vulnerabilidad y/o una implementación incorrecta del control de acceso ocasionando posibles violaciones de integridad, confidencialidad, o disponibilidad.

### ***T.Acceso físico de un hacker***

Un hacker interacciona directamente con el sistema para explotar vulnerabilidades del entorno físico, comprometiendo la seguridad a su capricho.

### ***T.Ingeniería Social***

Un hacker usa técnicas de ingeniería social para obtener información sobre la entrada al sistema, el sistema del usuario, diseño del sistema u operación del sistema.

Cualquier otra amenaza no incluida en esta sección NO está cubierta por el TOE evaluado, y no se hace ninguna declaración de resistencia por la certificación.

## ***Funcionalidad del entorno.***

El producto requiere de la colaboración del entorno para la satisfacción de los requisitos del perfil de protección [CIMC], Certificate Issuing and Management Components Family of Protection Profiles v1.0, Level 3, EAL 3+, october 2003.

Los requisitos funcionales que se deben satisfacer por el entorno de uso del producto son los siguientes:



### Requisitos expresados conforme a [CC\_P2]:

- FAU\_GEN.1 Audit data generation
- FAU\_GEN.2 User identity association
- FAU\_SAR.1 Audit review
- FAU\_SAR.3 Selectable audit review
- FAU\_SEL.1 Selective Audit
- FAU\_STG.1 Protected audit trail storage
- FAU\_STG.4 Prevention of audit data loss
- FPT\_STM.1 Reliable time stamps
- FPT\_SEP.1 TSF domain separation
- FPT\_RVM.1 Non-bypassability of the TSP
- FPT\_ITC.1 Inter-TSF confidentiality during transmission
- FPT\_ITT.1 Basic internal TSF data transfer protection
- FPT\_AMT.1 Abstract machine test
- FMT\_SMR.2 Restrictions on security roles
- FMT\_MOF.1 Management of security functions behavior
- FMT\_MSA.1 Management of security attributes
- FMT\_MSA.2 Secure security attributes
- FMT\_MSA.3 Static attribute initialisation
- FMT\_MTD.1 Management of TSF data
- FMT\_SMF.1 Specification of Management Functions
- FDP\_ACC.1 Subset access control
- FDP\_ACF.1 Security attribute based access
- FPT\_ITT.1 Basic internal TSF data transfer protection
- FDP\_UCT.1 Basic data exchange confidentiality
- FIA\_ATD.1 User attribute definition
- FIA\_UAU.1 Timing of authentication
- FIA\_UID.1 Timing of identification
- FIA\_USB.1 User-subject binding
- FIA\_AFL.1 Authentication failure handling
- FTP\_TRP.1 Trusted path
- FCS\_CKM.1 Cryptographic key generation
- FCS\_CKM.4 Cryptographic key
- FCS\_COP.1 Cryptographic operation

### Requisitos extendidos:

- AccessDatabaseTools Access to the Database Tools
- ControlDatabaseTools Control and supervision of the Database Tools
- FPT\_TST\_CIMC.2 Software/firmware integrity test
- FPT\_TST\_CIMC.3 Software/firmware load test



MINISTERIO DE DEFENSA  
CENTRO NACIONAL DE INTELIGENCIA  
CENTRO CRIPTOLÓGICO NACIONAL  
ORGANISMO DE CERTIFICACIÓN



Los detalles de la definición del entorno del producto (hipótesis, amenazas y políticas de seguridad), o de los requisitos de seguridad del OE se encuentran en la correspondiente Declaración de Seguridad.



## **Información sobre la Arquitectura**

Como se mencionó anteriormente el sistema está compuesto de los siguientes componentes.

### ***KEYONE CA. AUTORIDAD DE CERTIFICACIÓN***

El objetivo principal del KeyOne CA es la generación de certificados a partir de las peticiones solicitadas a través de la Autoridad de Registro. KeyOne CA genera, además, las listas de revocación, y ofrece el servicio de recuperación de claves.

La Autoridad de Certificación procesa lotes de entrada enviados por la Autoridad de Registro y genera lotes de salida con los certificados o las listas de revocación. Incluye un repositorio donde almacena los certificados y listas de revocación y ofrece servicios de recuperación de claves de cifrado y autenticación.

Los certificados y las listas de revocación de certificados que emite KeyOne CA se ajustan en su formato a lo establecido por X.509 v3 y "X.509 v2 CRL format" respectivamente.

### ***KEYONE LRA: AUTORIDAD LOCAL DE REGISTRO***

KeyOne LRA proporciona los servicios básicos para el registro de usuarios y para la solicitud de los certificados a la autoridad de certificación. Una vez recibido el certificado, lo almacena en una tarjeta inteligente. También es la autoridad encargada de enviar las peticiones de revocación de certificado a la Autoridad de Certificación.

### ***KEYONE VA. GESTIÓN DE CERTIFICADOS REVOCADOS***

KeyOne VA permite la consulta del estado de revocación de los certificados. El usuario solicita a través de una petición OCSP el estado de revocación de un certificado. KeyOne VA realiza una consulta en su base de datos interna, donde se encuentra actualizada la lista de certificados revocados, y devuelve al usuario un mensaje utilizando el protocolo OCSP. El mensaje devuelto se encuentra firmado y constituye una garantía de la validez del certificado.

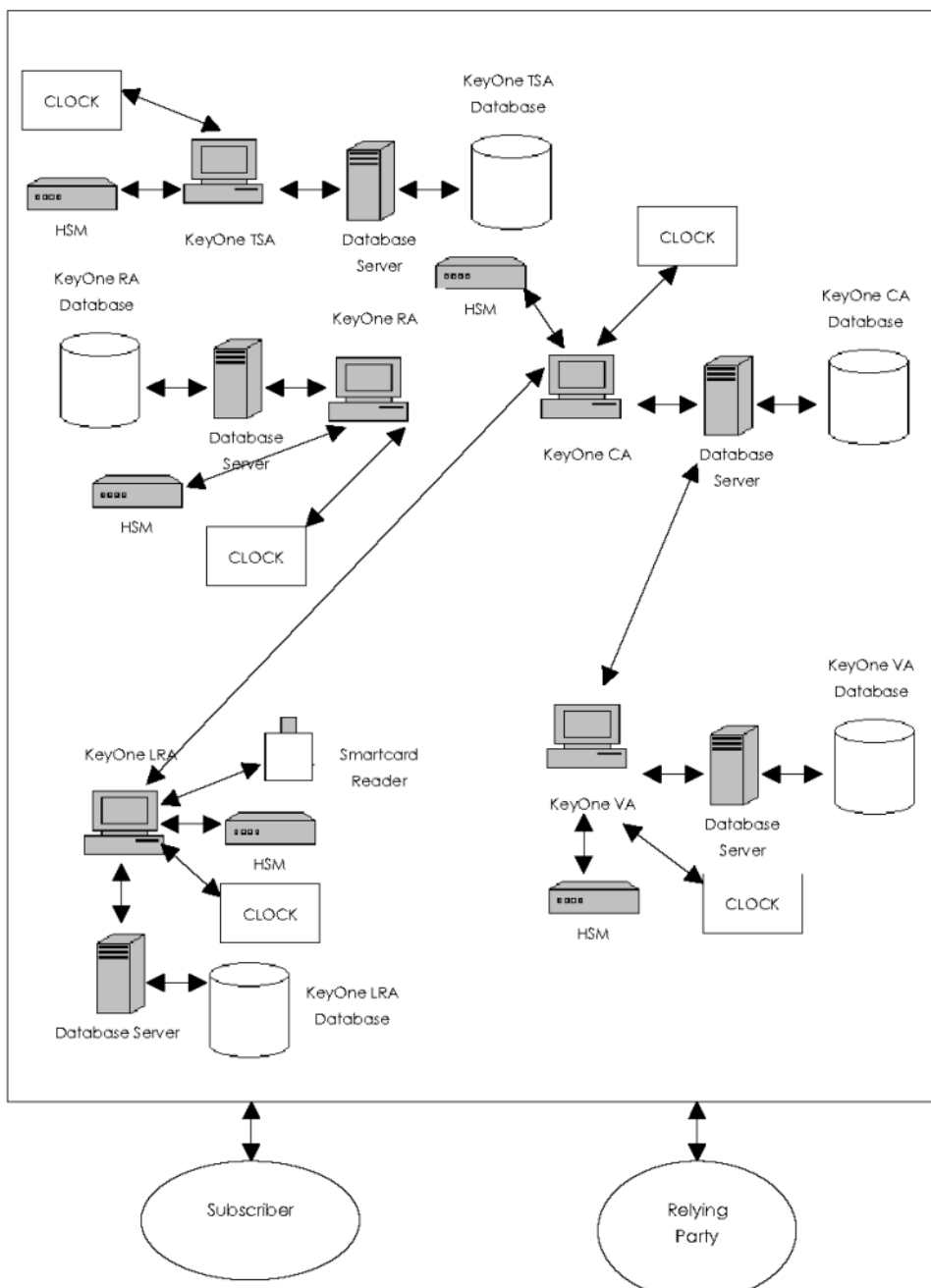
### ***KEYONE TSA SERVER. AUTORIDAD DE SELLADO DE TIEMPO***

KeyOne TSA Server implementa una autoridad de sellado de tiempo, creando tokens de sellado con la fecha y hora para indicar que unos determinados datos son válidos en la fecha indicada.



## Arquitectura Física

La arquitectura física del sistema KEYONE 3.0 se muestra en la siguiente figura.



Todos los componentes de KeyOne están conectados a una Base de Datos donde está almacenada la información relacionada al servicio que ese componente proporciona.



MINISTERIO DE DEFENSA  
CENTRO NACIONAL DE INTELIGENCIA  
CENTRO CRIPTOLÓGICO NACIONAL  
ORGANISMO DE CERTIFICACIÓN



La base de datos relacionada con la componente KeyOne CA almacena certificados generados y CRLs, lotes de KeyOne y los registros generados por el subsistema KeyOne CA. Los lotes contienen los conjuntos de peticiones de certificación o revocación, o certificados, dependiendo de la entidad que los emite. El propósito principal de los lotes utilizados en KeyOne es enviar peticiones de certificación o revocación y recibir las respuestas entre el RA y el CA.

La base de datos relacionada con el componente KeyOne VA almacena el estado relativo a los certificados, los mensajes intercambiados con el componente KeyOne CertStatus (la parte del producto de KeyOne CA), y los registros generados por el subsistema de KeyOne VA.

La base de datos relacionada con el componente de KeyOne TSA almacena las peticiones y respuestas de TSTs, y los registros generados por el subsistema de KeyOne TSA.

La base de datos relacionada con el componente de KeyOne RA almacena certificados, lotes de KeyOne y registros generados por el subsistema de KeyOne RA.

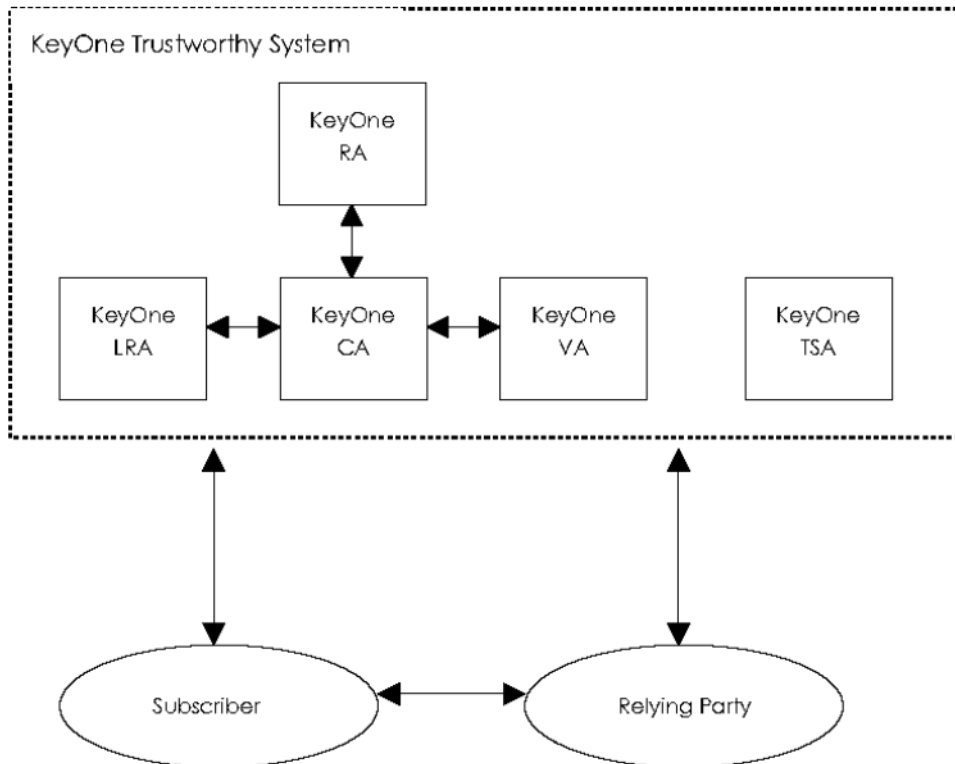
La base de datos relacionada con la componente KeyOne LRA almacena registros generados por el subsistema de KeyOne LRA.

Todos los componentes de KeyOne están conectados a un HSM (Módulo de Seguridad de Hardware) para generar y almacenar las claves relacionadas al servicio, y también ellos están conectados a un reloj que proporciona sellos fiables de tiempo para el uso del servicio.



## Arquitectura Lógica

La arquitectura lógica del sistema KEYONE 3.0 se muestra en la siguiente figura.





## Documentación

El producto tal y como se ha evaluado se empaqueta con la siguiente documentación requerida para la instalación y operación segura del TOE.

- KeyOne 3.0 Installation and Uninstallation Tool Manual, A98558AB 1.18
- KeyOne 3.0 Installation and Administration Manual, 65128EAB 1.6
- KeyOne 3.0 Signing scripts C3133BBD 1.4
- KeyOne 3.0 Batch Format Description, 269C9E2F 1.4
- KeyOne 3.0 CA Administration Manual, 40B3123A 1.23
- KeyOne 3.0 CA User Manual, 8B4B9CFE 1.31
- KeyOne 3.0 Certificate, Keys and CRL Management, EA99A2FE 1.14
- KeyOne 3.0 Console 3999D586 1.23
- KeyOne 3.0 I3D Database Management, DD01D2DA 1.3
- KeyOne 3.0 Logs Registration Administration, 1CBF9472 1.6
- KeyOne 3.0 Master Document, C7342558 1.32
- KeyOne 3.0 RA Administration and User Manual 1.8
- KeyOne 3.0 TSA Administration and User Manual, 7246994C 1.17
- KeyOne 3.0 Template Textual Specification Syntax, E204D730 1.4
- KeyOne 3.0 VA Administration and User Manual, F24E6F5E 1.20
- KeyOne 3.0 CRLA Manual EDFD484B 1.22
- KeyOne 3.0 LRA Administration and User Manual 513BE36C 1.19

## Pruebas del Producto

Tanto el fabricante como el laboratorio de evaluación realizaron pruebas exhaustivas al producto.

Estas pruebas se pueden dividir en 2 categorías: pruebas funcionales y pruebas de penetración.

### PRUEBAS FUNCIONALES

El laboratorio comprobó que las pruebas funcionales documentadas y realizadas por el fabricante eran suficientes para demostrar que el producto había sido sistemáticamente probado según su especificación funcional.

Por otra parte, el laboratorio realizó de forma independiente el mismo modelo de pruebas realizado por el fabricante, comprobando la exactitud de los resultados obtenidos por aquél.

### PRUEBAS DE PENETRACIÓN

El laboratorio realizó una batería de ataques al sistema, en busca de vulnerabilidades o intentando explotar aquellas vulnerabilidades declaradas por el análisis del fabricante.



Tras la realización de estas pruebas, el laboratorio concluyó que las vulnerabilidades encontradas o declaradas NO son explotables en el entorno de uso previsto para este producto.

## Configuración Evaluada

La configuración evaluada del producto se basa en la siguiente tabla:

Subsystem	OS	Database	HSM	SCD/SSCD
KeyOne CA	Microsoft Windows 2000	Oracle 9i	nCipher nShield F3 Ultrasign SCSI, firmware version 2.0.5, Hardware version nC4032W	STARCOS SPK 2.4
KeyOne LRA	Microsoft Windows 2000	Oracle 9i	nCipher nShield F3 Ultrasign SCSI, firmware version 2.0.5, Hardware version nC4032W	STARCOS SPK 2.4
KeyOne RA	Microsoft Windows 2000	Oracle 9i	nCipher nShield F3 Ultrasign SCSI, firmware version 2.0.5, Hardware version nC4032W	STARCOS SPK 2.4
KeyOne VA	Microsoft Windows 2000	Oracle 9i	nCipher nShield F3 Ultrasign SCSI, firmware version 2.0.5, Hardware version nC4032W	STARCOS SPK 2.4
KeyOne TSA	Microsoft Windows 2000	Oracle 9i	nCipher nShield F3 Ultrasign SCSI, firmware version 2.0.5, Hardware version nC4032W	STARCOS SPK 2.4



Adicionalmente, son necesarios los siguientes componentes:

- Cliente NTP instalado en el mismo *host* que los subsistemas KeyOne CA, KeyOne RA, KeyOne LRA, KeyOne TSA y KeyOne VA.
- Reloj fiable que obtiene obtains el Tiempo Universal Coordinado de una fuente fiable, y que sincroniza el reloj del sistema por medio del protocolo NTP, usando el cliente NTP instalado en la misma máquina que los subsistemas KeyOne CA, KeyOne RA, KeyOne LRA, KeyOne TSA y KeyOne VA.
- Windows 2000 Service Pack 4 para las componentes KeyOne CA, KeyOne LRA, KeyOne RA, KeyOne VA y KeyOne TSA.

## Resultados de la Evaluación

Todos los componentes de garantía requeridos por el nivel EAL4+ (aumentado con ALC\_FLR.2, SOF basic) han sido asignados un veredicto "PASA". Consecuentemente, el laboratorio (CESTI /INTA) asigna el veredicto "PASA" al conjunto de la evaluación debido a que todas las acciones del evaluador se satisfacen para la metodología EAL4+, como define la Common Criteria [CC-P3] y la Common Methodology [CEM].

La conformidad de este producto con el [CIMC], Certificate Issuing Management Components Family of Protection Profiles v1.0, Level 3, EAL3+, octubre 2003, también ha sido evaluada, y asignado el veredicto de "PASA".

## Comentarios y Recomendaciones de los Evaluadores

### Conclusiones

De acuerdo con los resultados de la evaluación realizada al producto KEYONE 3.0, el equipo evaluador dictó las siguientes conclusiones y recomendaciones.

- Todas las actividades de evaluación se cerraron con el veredicto de PASA. Por tanto, se otorga el veredicto final de PASA a la evaluación del producto KEYONE 3.0 04S2R1, con los parches B01, B02, B03, B04, B05, B06 y B07.
- El TOE KEYONE 3.0 04S2R1, con los parches B01, B02, B03, B04, B05, B06 y B07, satisface su Declaración de Seguridad, "Declaración de Seguridad del KEYONE 3.0. 7BFD7697 v1.9", de acuerdo con la norma Common Criteria, EAL4+ (ALC\_FLR.2), SOF Basic.



MINISTERIO DE DEFENSA  
CENTRO NACIONAL DE INTELIGENCIA  
CENTRO CRIPTOLÓGICO NACIONAL  
ORGANISMO DE CERTIFICACIÓN



- El TOE KEYONE 3.0 04S2R1, con los parches B01, B02, B03, B04, B05, B06 y B07, satisface los requisitos del perfil de protección CIMC Nivel 3.
- Los resultados de la evaluación y las presentes conclusiones son válidas exclusivamente para la configuración concreta del producto evaluado y la versión citada de la Declaración de Seguridad:
  - o Producto: KeyOne 3.0 04S2R1 con parches B01, B02, B03, B04, B05, B06 y B07.
  - o Declaración de Seguridad: “Declaración de Seguridad del KEYONE 3.0. 7BFD7697 v1.9”.

### **Recomendaciones**

Para cumplir con las garantías de seguridad EAL4+, correspondientes a la “Declaración de Seguridad del KEYONE 3.0. 7BFD7697 v1.9” el fichero de licencia usado en el TOE no tiene que permitir la ejecución de *scripts* en modo inseguro (activación del flag -unsecure).

Para utilizar de forma segura el TOE, hay que tener presente el cumplimiento de las hipótesis relativas al entorno incluidas en “Declaración de Seguridad del KEYONE 3.0. 7BFD7697 v1.9” sección 3 ‘Entorno de Seguridad del TOE” (esta sección incorpora todas las hipótesis sobre el entorno que aparecen en el CIMC, Certificate Issuing and Management Components Family of Protection Profiles v1.0, Level 3, EAL 3+, october 2003).

Para utilizar de forma segura el TOE, hay que tener presente el cumplimiento de los Objetivos de Seguridad para el entorno incluidos en “Declaración de Seguridad del KEYONE 3.0. 7BFD7697 v1.9” sección 4.2 “Objetivos de Seguridad para el entorno” y sección 4.3 “Objetivos de seguridad para el TOE y el entorno” (esta sección incorpora todos los objetivos de seguridad para el entorno que aparecen en el CIMC, Certificate Issuing and Management Components Family of Protection Profiles v1.0, Level 3, EAL 3+, october 2003.)

Para utilizar de forma segura el TOE, hay que tener presente el cumplimiento de los Objetivos de Seguridad para el entorno de TI incluidos en su Declaración de Seguridad “Declaración de Seguridad del KEYONE 3.0. 7BFD7697 v1.9” sección 5.2 “Requisitos de Seguridad para el entorno”. Para ello, es importante que el personal responsable de los elementos del entorno de TI (básicamente, sistema operativo, bases de datos y HSM) sepa cómo configurar dichos elementos de forma que se proporcione el adecuado apoyo al TOE.

En este sistema no se separa claramente el usuario ordinario del usuario administrador, sino que cada usuario tiene un role con unos privilegios asociados. Por tanto, cada usuario puede realizar, o no, una determinada acción, dependiendo de los privilegios que esta acción exija. Por otra parte, el fabricante no ha publicado manuales independientes para el administrador y para el usuario, sino un manual común de administración y uso. Por ello, se



MINISTERIO DE DEFENSA  
CENTRO NACIONAL DE INTELIGENCIA  
CENTRO CRIPTOLÓGICO NACIONAL  
ORGANISMO DE CERTIFICACIÓN



recomienda buscar la funcionalidad de la aplicación deseada, cuya descripción se recoge en el manual indicando, en cada paso, si es necesario un role específico para realizarlo.

Para una óptima comprensión de la documentación de pruebas del fabricante y del manual de uso, hay que tener en cuenta que este producto KeyOne 3.0 04S2R1 con parches B01, B02, B03, B04, B05, B06 y B07 ha sido desarrollado para trabajar con distintas políticas de seguridad definidas por el fabricante. Como mínimo, se pueden utilizar dos políticas de seguridad: la correspondiente a la normativa europea [CWA] o la relativa al [CIMC]. En el contexto de esta evaluación sólo aplica la política de seguridad definida en el [CIMC], pero en lo referente a nombres de roles, no se ha definido un uso concreto de los mismos y, por tanto, en esta evaluación se utilizan nombres de ambas políticas.

Para aclarar esta situación hay que tener en cuenta que, en la política CIMC hay cuatro roles: administrador, oficial, auditor y operador:

- El role de administrador correspondería a los de administrador del sistema y responsable de seguridad.
- El role de oficial correspondería al de responsable de registro.
- El role de auditor correspondería con el de auditor del sistema.
- El role de operador correspondería con el de operador del sistema.

El requisito de seguridad FPT\_CIMC\_TSP.1.3 es alcanzado debido a que para cada modificación (adición, actualización o borrado) de un registro de la base de datos, el mecanismo i3D asegura la generación de una firma digital que garantiza la integridad de la base de datos, y entonces el KeyOne funciona como si hubiese sido configurado para utilizar la máxima frecuencia posible, y por tanto la frecuencia más segura (refinamiento del requisito FPT\_CIMC\_TSP.1.3).



## Recomendaciones del Certificador

A la vista de los resultados de esta evaluación y tras comprobar que las características de seguridad del producto, así como la metodología de desarrollo del fabricante, cumplen con lo especificado en su Declaración de Seguridad, incluyendo la conformidad con el perfil de protección [CIMC], Certificate Issuing and Management Components Family of Protection Profiles v1.0, Level 3, EAL 3+, october 2003, se recomienda la certificación positiva del nivel EAL4+ (ALC\_FLR-2), según las normas CC/CEM 2.2, del KEYONE 3.0 identificado en el apartado 2.

## Glosario

CA	Certification Authority
CC	Common Criteria
CEM	Common Evaluation Methodology
CESTI	Centro de Evaluación de la Seguridad de las Tecnologías de la Información
CIMC	Certificate Issuing and Management Components
CPS	Certification Practices Statement
DPC	Declaración de Prácticas de Certificación
DS	Declaración de Seguridad
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
KTS	KeyOne Trusted System
INTA	Instituto Nacional de Técnica Aeroespacial
LRA	Local Registry Authority
NIST	National Institute of Standards and Technology
NPKI	NATO PKI
NTP	Network Time Protocol
OC	Organismo de Certificación
OCSP	On-line Certificate Status Protocol
OE	Objeto de Evaluación
PC	Política de Certificación
PKI	Public Key Infrastructure
PP	Perfil de Protección
RA	Registry Authority
TI	Tecnologías de la Información
TOE	Target Of Evaluation
TSA	Time Stamping Authority
UTC	Universal Time Coordinated
VA	Validation Authority



## Bibliografía

Las siguientes normas y documentos se han utilizado en la evaluación del producto:

[CC\_P1] Common Criteria for Information Technology Security Evaluation- Part 1: Introduction and general model, Version 2.2, rev 256, January 2004.

[CC\_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 2.2, rev 256, January 2004.

[CC\_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 2.2, rev 256, January 2004.

[CEM] Common Evaluation Methodology for Information Technology Security: Introduction and general model, Version 2.2, rev 256, January 2004.

[CIMC] Certificate Issuing and Management Components Family of Protection Profiles v1.0, Level 3, EAL 3+.

## Security Target

Se publica de forma conjunta con este informe de certificación la “Declaración de Seguridad del KEYONE 3.0. 7BFD7697 v1.9”.