Prestador de Servicios de Certificación VIT S.A.

POLÍTICA DE SERVICIOS DE VALIDACIÓN DE CERTIFICADOS EN LÍNEA DE VITSA

(POLÍTICA VA VITSA)

Documento: POLITICA VA VITSA
Fecha: martes, 12 de agosto de 2014
Versión: 0.1
Estado: PRELIMINAR
OID: en trámite

Clasificación: PRIVADO
Archivo: Politica VA VITSA 1.docx
Nº de páginas: 14
Preparado por: VITSA

Tabla de contenido

1. INTRODUCCIÓN

El presente documento establece las políticas generales implementadas por la Autoridad de Validación de VITSA para la emisión de respuestas OCSP.
De esta manera se proporciona información fehaciente del estado de los certificados confiables para VITSA
En la presente política se establecen los participantes en los procesos de validación de certificados, especificando sus responsabilidades, derechos y ámbito de aplicación.
El presente documento puede ser utilizado por terceros verificadores y los suscriptores de los servicios proporcionados por VITSA como base para garantizar la confianza en los servicios que se describen a continuación.
Esta política se basa en la criptografía de clave pública, fuentes de tiempos fiables y certificados x.509 v3.

IDENTIFICACIÓN DEL DOCUMENTO

La presente política de Autoridad de Validación de VITSA se identifica de la siguiente forma:

Nombre del Documento	Politica de Autoridad de Validación de VITSA
Versión	1.0
OID	EN TRAMITE
Fecha de Creación	07/05/2014

DEFINICIONES Y ACRONIMOS

DEFINICIONES

VA (ValidationAuthority)	La Autoridad de Validación es el componente que tiene como tarea suministrar información sobre la vigencia de los certificados electrónicos que, a su vez, hayan sido registrados por una Autoridad de Registro y certificados por la Autoridad de Certificación.
Hash	Valor numérico de longitud fija que identifica datos de forma unívoca. Los valores hash se utilizan para comprobar la integridad de los datos.
HSM (Hardware Security Module)	Es un dispositivo hardware con capacidades criptográficas que permiten generar y almacenar de manera segura claves criptográficas.
Subscriptor	Persona o entidad que solicita los servicios proporcionados por la Autoridad de Validación de VITSA
Usuario	Destinatario de una respuesta OCSP y que confía en la misma.

ACRÓNIMOS

CA	Autoridad de Certificación
VA	Autoridad de Validación
CEN	Comité Européen de Normalisation (Comité Européo de Normalización)
CRL	CertficateRevocation List
CWA	CEN Workshop Agreement
DPC	Declaración de Prácticas de Certificación
ETSI	EuropeanTelecommunications Standard Institute
FIPS	Federal InformationProcessing Standard
HSM	Hardware Security Module.
IETF	Internet EngineeringTaskForce
OID	Objectidentifier
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastructure
RFC	Request For Comments

REFERENCIAS

- Políticas de Certificación VITSA oid [EN TRAMITE] https://www.efirma.com.py
- Prácticas de Certificación VITSA oid [EN TRAMITE] https://www.efirma.com.py
- Políticas de Certificación Autoridad Certificadora Raíz del Paraguay. oid []www.acraiz.gov.py/documentación/politicas.pdf
- [**RFC2560**] "Internet X.509 Public Key Infrastructure – Online Certificate Status Protocol - OCSP"
- [**RFC5280**] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- [**SR002176**] ETSI SR 002 176 "Algorithms and Parameters for Secure Electronic Signatures"

2. CONCEPTOS GENERALES

AUTORIDAD DE VALIDACIÓN

La Autoridad de Validación de VITSA es la encargada de suministrar información sobre la vigencia de los certificados electrónicos emitidos por la Autoridad Certificadora "CA VIT SA" y con aquellas autoridades certificadoras con las que VITSA mantenga acuerdos de cooperación.

El certificado de la Autoridad de validación cuenta con el siguiente certificado inicial:

Emisor	CN= CA VITSA O = VIT SA SERIALNUMBER = RUC 80080099-0 C =PY
Titular	CN= Autoridad Validación VIT SA O = VIT SA C =PY
Número de Serie	[PENDIENTE]
Periodo de Validez	**Desde** XXX **hasta** XXX+6 meses
Huella (SHA1)	[PENDIENTE]
Algoritmo de firma	pkcs1-sha1withRsaSignature

El mismo será renovado cada 6 meses.
El servicio se presta en la siguiente dirección: https://www.efirma.com.py

SUSCRIPTORES

Los suscriptores a los servicios de validación son todos aquellos organismos o personas físicas que hayan suscripto el correspondiente acuerdo con VIT S.A para la utilización del servicio.

3. Política de la Autoridad de Validación

La presente política tiene como cometido dictar las reglas de emisión y control de las respuestas OCSP, adicionalmente regula el nivel de seguridad de la Autoridad de Validación.
El perfil de certificado de la autoridad de validación se ajusta a las normas [RFC 2560] y [RFC 5280].

La siguiente tabla especifica los campos del certificado de la Autoridad de Validación:

Campo x509v3	Nombre	Valor
Version	Versión de X509	Versión 3
SerialNumber	Número de serie	Aleatorio, asignado por la CA VITSA
SignatureAlgorithm	Algoritmo de firma digital del certificado	pkcs1-sha1withRsaSignature
Issuer	C (País)	PY
	O (Organización)	VIT SA
	SERIALNUMBER	RUC 80080099-0
	CN (Nombre)	CA VITSA
Validity	NotBefore	[Fecha Inicio validez]
	NotAfter	NotBefore + 6 meses
Subject	C (País)	PY
	O (Organización)	VIT SA
	CN (Nombre)	Autoridad Validación VIT SA
subjectyPublicKeyInfo	Clave pública	Clave RSA – tamaño 2048
Extensiones estándar		
subjectKeyIdentifier	Ident. de clave pública del sujeto	Hash de la clave pública generado automáticamente
authorityKeyIdentifier	Identificador de la clave pública del emisor	Calculado de forma automática – Mismo valor que la extensión subjectKeyIdentifier del certificado de la CA VITSA
keyUsage	Uso de la clave	DigitalSignature
Extended KeyUsage	Uso extendido de la clave	OCSP Signing
CertificatePolicies	PolicyIdentifier	OID [EN TRAMITE]
	CPS Pointer	https://www.efirma.com.py
BasicConstraints	CA	False
	PathLenConstraint	Ninguno
CRLDistributionPoints	Punto de distribución de la CRL	URL=https://www.efirma.com.py
ocspNoCheck	No comprobar por OCSP	Null

Las respuestas OCSP firmadas por la Autoridad de validación cumplen con la norma IETF RFC 2560.

ÁMBITO DE APLICACIÓN

Las respuestas OCSP emitidas por la Autoridad de Validación de VITSA pueden ser utilizadas para garantizar las transacciones y el no repudio en los procesos en los cuales intervenga VITSA y las entidades que hayan formalizado convenios de certificación con VITSA

4. Obligaciones y Responsabilidades

OBLIGACIONES DE LA AUTORIDAD DE VALIDACIÓN

VITSA como prestador de servicios de Certificación en la emisión de respuestas OCSP tiene como obligaciones:

- Operar de acuerdo a la presente política.
- Proteger y custodiar sus claves privadas
- Seguir procedimientos y buenas prácticas que garanticen la confianza de los suscriptores y la seguridad de las claves.
- Emitir respuestas OCSP confiables y conformes a la información conocida al momento de la emisión.
- Emitir respuestas libres de errores de entrada de datos.
- Utilizar sistemas y productos fiables protegidos contra alteraciones y que garanticen la seguridad técnica y criptográfica.
- Garantizar que se puede determinar con precisión la fecha y hora en que se emitió una respuesta OCSP.
- Garantizar que todos los requerimientos de la Autoridad de Validación, incluidos los procedimiento y practicas relativos a la emisión OCSP son conformes a los procedimientos de VITSA

La Autoridad de Validación actúa de acuerdo a los procedimientos y no se permiten exclusiones a la regulación.
En el Capítulo 9.6 de la Declaración de Practicas de Certificación de VITSA se pueden encontrar las obligaciones pertinentes a VITSA y a los suscriptores.

OBLIGACIONES DE LOS SUSCRIPTORES

En el proceso de obtención de una respuesta OSCP es obligación de los suscriptores validar la firma electrónica de la misma.

OBLIGACIONES DE TERCERAS PARTES VERIFICADORAS

Al igual que los suscriptores deberán verificar la firma de las respuestas OCSP.
Podrán comprobar el estado del certificado de la cadena de certificación de la Autoridad de Validación de VITSA y los periodos de validez de las diferentes entidades de la cadena.
En el caso de la verificación de una respuesta OCSP, después de la expiración del certificado de la VA, podrán:

- Verificar que el número de serie del certificado de la VA no se encuentra en la CRL que correspondiera en el momento de la emisión de la respuesta OCSP, o determinar la validez del certificado de la VA por otros mecanismos que articule VITSA
- Verificar que las funciones y algoritmos criptográficos usados son todavía seguros, y que el tamaño de la clave usada garantiza esta seguridad.

CAPACIDAD FINANCIERA

Según especificado en la Declaración de Prácticas de Certificación de VITSA.

5. Requerimientos de la Autoridad de Validación de Certificados

GESTIÓN DEL CICLO DE VIDA DE LAS CLAVES

GENERACIÓN DE CLAVES DE LA VA

La generación de claves de la Autoridad de Validación es realizada en dispositivos de hardware criptográfico seguro conformes a la norma FIPS 140-2 nivel 3 y durante el proceso se exige que haya un número mínimo de personas designadas por VITSA con privilegios de acceso.
El entorno de generación de las claves cumple los requisitos impuestos por VITSA en su Declaración de Practicas de Certificación y por la Autoridad Certificadora Raíz del Paraguay.
El algoritmo utilizado para la generación de las claves es RSA de 2048 bits.

PROTECCIÓN DE LA CLAVE PRIVADA

Los niveles de seguridad del HSM donde se almacena la clave se pueden ver en el punto 5.1.1 de la presente política.
La clave se dividida en 8 fragmentos y son necesarios 3 para poder recuperarla.

DISTRIBUCIÓN DE LA CLAVE PÚBLICA DE LA AUTORIDAD DE VALIDACIÓN

El certificado que contiene la clave pública de la Autoridad de Validación de VITSA se puede encontrar en la siguiente URL:
https://www.efirma.com.py
Dicho certificado se encuentra firmado por la Autoridad CA VIT SA subordinada a la Autoridad Certificadora Raíz del Paraguay.
En el punto 2 de las Prácticas de Certificación de VITSA se puede encontrar más información sobre los certificados y la documentación que los acompaña.

REGENERACIÓN DE LA CLAVE DE LA AUTORIDAD DE VALIDACIÓN

La regeneración de las claves de la Autoridad de Validación se lleva a cabo con una semana de antelación al vencimiento de las claves actuales, cuando fueron comprometidas o se descubrió alguna debilidad en el algoritmo de generación o en el largo de las claves.
Las claves privadas caducadas se almacenan por un período no menor a 10 años, siendo VITSA el que ejecuta el procedimiento y responsable de la decisión.

DESTRUCCIÓN DE LA CLAVE PRIVADA DE LA AUTORIDAD DE VALIDACIÓN

Las claves privadas son destruidas de forma que se impida su robo, modificación, divulgación no autorizada o uso no autorizado. En el caso de las claves almacenadas en tarjetas se procede a la destrucción física de las mismas.

GESTIÓN DE LOS HSM

VITSA verifica con herramientas del fabricante que los HSM no hayan sido manipulados y que cumplen con los requisitos necesarios para el correcto funcionamiento.

SERVICIO OCSP

La prestación de estos servicios de validación se realiza en base a **Online Certificate Status Protocol** (OCSP), lo que, en esencia, supone que un cliente OCSP envía una petición sobre el estado del certificado a la Autoridad de Validación, la cual, tras consultar su base de datos, ofrece - vía http - una respuesta sobre el estado del certificado.
La Autoridad de Validación del VITSA recoge de las fuentes puestas a disposición por parte de las Autoridades de Certificación a las que sirve un mecanismo de sincronización que garantiza que la información acerca del estado de los certificados que devuelve en sus repuestas es conforme con los periodos de gracia establecidos en las políticas y DPCs de dichas autoridades de certificación.
Las respuestas OCSP son firmados por la clave privada de la Autoridad de Validación, cuyo certificado asociado, campos y extensiones se encuentran descritas en el capítulo "3 Política de la Autoridad de Validación" del presente documento.
Estas claves y certificado han sido generados exclusivamente para este propósito por parte de la Autoridad Certificadora CA VITSA
La Autoridad de Validación establece todo el procedimiento asociado a la generación de las respuestas OCSP utilizando el protocolo descrito en [RFC2560].

OPERACIÓN Y GESTIÓN DE LA AUTORIDAD DE VALIDACIÓN

GESTIÓN DE SEGURIDAD

Todos los elementos relativos a la seguridad se describen en el punto 5.2 de la Declaración de Prácticas de Certificación de VITSA.

SEGURIDAD DEL PERSONAL

Las Características del personal y los controles que se establecen sobre el mismo son los descritos en la Declaración de Prácticas de Certificación de VITSA en el capítulo 5.3 Controles de personal.

SEGURIDAD FÍSICA

La descripción de la seguridad física se encuentra descripta en la Declaración de Prácticas de Certificación de VITSA en el punto 5.1.

GESTIÓN DE LAS OPERACIONES

La descripción de la gestión de las operaciones se encuentra descripta en la Declaración de Prácticas de Certificación de VITSA en el punto 5.2.

GESTIÓN DE ACCESO A SISTEMAS

Los sistemas de la Autoridad de Validación se encuentran con las mismas medidas de seguridad de acceso que la autoridad certificadora CA VIT SA.
Esto implica la protección las 24 hs los 365 días del año.

COMPROMISO DE LOS SERVICIOS DE VALIDACIÓN DE CERTIFICADOS

En caso de compromiso de los servicios la autoridad de certificación procederá a la revocación del certificado de la Autoridad de Validación y la inmediata emisión de la CRL.
Al mismo tiempo se comunicará a los suscriptores y terceros verificadores la naturaleza del compromiso y las herramientas o procedimientos necesarios para la comprobación de las respuestas OCSP.
La Autoridad dejara de operar inmediatamente.

CESE DE LA AUTORIDAD DE VALIDACIÓN

La Autoridad de Validación garantiza la minimización del impacto en caso de cese del servicio de validación de certificados mediante protocolo OCSP. En particular, asegura la continuidad de la información requerida para verificar la corrección de las respuestas OCSP.
En caso de cese de actividad voluntaria, VITSA, como Autoridad de Validación, realizara con una antelación mínima de dos meses las siguientes acciones:

- Informar a todos los subscriptores y partes confiantes del cese de actividad y los mecanismos habilitados para garantizar la validez de los sellos existentes.
- Comunicar a los organismos de control pertinentes del cese de actividad y los mecanismos habilitados para garantizar la validez de los sellos existentes.

CUMPLIMIENTO DE LOS REQUISITOS LEGALES

VITSA como Autoridad de Validación cumple con todos los requisitos en cuanto a la protección de datos personales y a la gestión y operación de servicios y sistemas informáticos.
En los casos en que no haya legislación se siguen buenas prácticas y estándares como ETSI.

REGISTRO DE INFORMACIÓN RELATIVA A LA OPERACIÓN

VITSA como Autoridad de Validación cuenta con los mecanismos necesarios para el correcto registro de la operación y cumpliendo con la normativa vigente.