POLÍTICA ÚNICA DE CERTIFICACIÓN

LISTA DE CERTIFICADOS REVOCADOS

CERTIFICADOR LICENCIADO

DIGILOGIX S.A.

Versión 1.0 (diciembre 2014)

PERFILES DE CERTIFICADOS Y DE LISTAS DE CERTIFICADOS REVOCADOS.

Perfil del certificado.

Los certificados emitidos por la **AC – DIGILOGIX** respaldados por la Política Única de Certificación cumplen con lo establecido en la especificación ITU X509 versión 3.

La **AC – DIGILOGIX** adhiere a las recomendaciones de los siguientes documentos en relación al perfil de los certificados:

a) RFC 3739 “Internet X.509 Public Key Infrastructure Qualified Certificates Profile” [RFC3739].

b) RFC 3280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile” [RFC3280].

Perfil del certificado de la persona física.

Los siguientes campos se encuentran presentes en los certificados emitidos a personas físicas por la **AC – DIGILOGIX**:

Campos Atributos Extensiones	Valor/OID	Observaciones
Versión (Version)	2	Corresponde a versión 3
Número de serie (SerialNumber)	hasta 20 octetos 2.5.4.5	Entero positivo asignado unívocamente por la AC-DIGILOGIX a cada certificado
Algoritmo de Firma (SignatureAlgoritm)	sha1RSA 1.2.840.113549.1.1.5	Algoritmo usado por el certificador para firmar
Nombre distintivo del emisor (Issuer)		
commonName	AC-DIGILOGIX 2.5.4.3	Identificación de la Autoridad Certificante
serialNumber	30714128716 2.5.4.5	CUIT del Certificador
organizationName	DIGILOGIX S.A. 2.5.4.10	Denominación del Certificador Licenciado
stateOrProvinceName	Ciudad Autónoma de Buenos Aires 2.5.4.8	Ciudad en la que se encuentra el Certificador
countryName	AR 2.5.4.6	País del Certificador Licenciado
Validez (desde, hasta) (Validity (Not before, not after))		
notBefore	<fecha y hora de emisión UTC>	Fecha y hora en que el período de vigencia del certificado comienza

	yyyy/mm/dd hh:mm:ss huso-horario	
notAfter	<fecha y hora de emisión UTC+ 1 año> yyyy/mm/dd hh:mm:ss huso-horario	Fecha y hora en que el periodo de vigencia del certificado termina
Nombre distintivo del suscriptor (Subject)		
commonName	<Nombres y Apellidos> 2.5.4.3	Datos que surgen del Documento Nacional de Identidad presentado por el titular
serialNumber	<Tipo> <Número de documento> 2.5.4.5	Datos que surgen del Documento presentado por el titular
title	<Nombre de la función> 2.5.4.12	Cargo o título del suscriptor dentro de la organización, debe corresponder con la certificación aportada en el proceso de autenticación
organizationName	<Nombre de la empresa u organismo> 2.5.4.10	Nombre que surge de la certificación aportada en el proceso de autenticación
localityName	<Nombre de localidad> 2.5.4.7	Nombre que surge de la certificación aportada en el proceso de autenticación
stateOrProvinceName	<Nombre de la provincia> 2.5.4.8	Nombre que surge de la certificación aportada en el proceso de autenticación
countryName	AR 2.5.4.6	Código de País de acuerdo a ISO3166
Clave pública del suscriptor (Subject Public Key Info)		
public key algorithm	RSA 1.2.840.11.35.49.1.1.1	Tipo de algoritmo de clave pública utilizado
Public key length	1024 bits	Longitud de la clave pública del suscriptor
Clave pública del suscriptor (Subject Public Key Info)	<Clave pública del suscriptor>	Valor de la clave pública del suscriptor
Extensiones del certificado (Extensions)		
Restricciones básicas (Basic Constraints)	Tipo de asunto = Entidad final pathLenghtConstraint = Null 2.5.29.19	Define el certificado como de entidad final
Usos de clave (Key Usage)	digitalSignature = 1 nonRepudiation = 1 keyEncipherment = 0 dataEncipherment = 0 keyAgreement = 0 keyCertSign = 0 cRLSign = 0 encipherOnly = 0 decipherOnly = 0 2.5.29.15	Propósito para el cual será utiliza la clave contenida en el certificado. Sin repudio, firma digital

Identificador de clave del Suscriptor (Subject Key Identifier)	Valor de hash de 20 bytes 2.5.29.14	Contiene un hash de 20 bytes del atributo clave pública del suscriptor
Puntos de Distribución de la Lista de Certificados Revocados (CRLDistributionPoints)	[1]Punto de distribución CRL Dirección URL=http://www.digilogix.com.ar/crl/digilogix.crl [2]Punto de distribución CRL Dirección URL= http://backup.digilogix.com.ar/crl/digilogix.crl 2.5.29.31	URI del punto de distribución
Política de Certificación (Certificate Policies)	OID de la Política de Certificación de DIGILOGIX S.A, URI de la Política: http://www.digilogix.com.ar /documentos/cps.pdf Texto de aviso=certificado emitido por un certificador licenciado en el marco de la Ley 25.506	OID de la Política de Certificación de DIGILOGIX S.A, otorgado por la ONTI, URI de la Política de Certificación y texto obligatorio para los certificados de la IFDRA
Identificador de la Clave de la Autoridad Certificante (AuthorityKeyIdentifier)	Valor de hash de 20 bytes 2.5.29.35	Contiene un hash de 20 bytes del atributo clave pública del DIGILOGIX AC que emitió el certificado.
Uso Extendido de Clave (Extended Key Usage)	Autenticación del cliente (1.3.6.1.5.5.7.3.2) Correo seguro (1.3.6.1.5.5.7.3.4) 2.5.29.37	Usos adicionales de la clave pública a los enumerados en el campo keyUsage
Nombres Alternativos del Suscriptor (Subject Alternative Name)	<Dirección de correo electrónico> 2.5.29.17	Dirección de mail del suscriptor verificada por circuito seguro compatible con RFC 822

Perfil del certificado de la persona jurídica.

Los siguientes campos se encuentran presentes en los certificados de personas jurídicas emitidos por la **AC – DIGILOGIX**:

Campos Atributos Extensiones	Valor/OID	Observaciones
Versión (Version)	2	Corresponde a versión 3
Número de serie (SerialNumber)	hasta 20 octetos 2.5.4.5	Entero positivo asignado unívocamente por la AC-DIGILOGIX a cada certificado
Algoritmo de Firma (Signature)	sha1RSA 1.2.840.113549.1.1.5	Algoritmo usado por el certificador para firmar
Nombre distintivo del emisor (Issuer)		
commonName	AC-DIGILOGIX 2.5.4.3	Identificación de la Entidad Certificante
serialNumber	30714128716 2.5.4.5	CUIT del Certificador
organizationName	DIGILOGIX S.A. 2.5.4.10	Denominación del Certificador Licenciado
stateOrProvinceName	Ciudad Autónoma de Buenos Aires 2.5.4.8	Ciudad en la que se encuentra el Certificador
countryName	AR 2.5.4.6	País del Certificador Licenciado
Validez (desde, hasta) (Validity (Not before, not after))		
notBefore	<fecha y hora de emisión UTC> yyyy/mm/dd hh:mm:ss huso-horario	Fecha y hora en que el período de vigencia del certificado comienza
notAfter	<fecha y hora de emisión UTC+3 años> yyyy/mm/dd hh:mm:ss huso-horario	Fecha y hora en que el periodo de vigencia del certificado termina
Nombre distintivo del suscriptor (Subject)		
commonName	Unidad Operativa del Suscriptor 2.5.4.3	Denominación de la Unidad Operativa del Suscriptor
serialNumber	CUIT <Número de CUIT> 2.5.4.5	CUIT de la Persona Jurídica
organizationName	<Nombre de la empresa u organismo> 2.5.4.10	Nombre que surge de la certificación aportada por el representante autorizado durante el proceso de autenticación
localityName	<Nombre de localidad> 2.5.4.7	Nombre que surge de la certificación aportada en el proceso de autenticación
stateOrProvinceName	<Nombre de la provincia> 2.5.4.8	Nombre que surge de la certificación aportada en el proceso de autenticación

countryName	AR 2.5.4.6	
Clave pública del suscriptor (Subject Public Key Info)		
public key algorithm	RSA 1.2.840.11.35.49.1.1 .1	Tipo de algoritmo de clave pública utilizado
Public key length	1024 bits	Longitud de la clave pública del suscriptor
Subject Public Key Info	<Clave pública del suscriptor>	Valor de la clave pública del suscriptor
Extensiones del certificado (Extensions)		
Restricciones básicas (Basic Constraints)	Tipo de asunto = Entidad final pathLenghtConstraint = Null 2.5.29.19	Define el certificado como de entidad final
Usos de clave (Key Usage)	digitalSignature = 1 nonRepudiation = 1 keyEncipherment = 0 dataEncipherment = 0 keyAgreement = 0 keyCertSign = 0 cRLSign = 0 encipherOnly = 0 decipherOnly = 0 2.5.29.15	Sin repudio, firma digital
Identificador de clave del Suscriptor (Subject Key Identifier)	Valor de hash de 20 bytes 2.5.29.14	Contiene un hash de 20 bytes del atributo clave pública del suscriptor
Puntos de Distribución de la Lista de Certificados Revocados (CRLDistributionPoints)	[1]Punto de distribución CRL Dirección URL=http://www.digilogix.com.ar/crl/digilogix.crl [2]Punto de distribución CRL Dirección URL= http://backup.digilogix.com.ar/crl/digilogix.crl 2.5.29.31	URI del punto de distribución
Política de Certificación (Certification Policies)	OID de la Política de Certificación de DIGILOGIX S.A, URI de la Política: http://www.digilogix.com.ar/documentos/cps.pdf Texto de aviso=certificado emitido por un certificador licenciado en el marco de la Ley 25.506	OID de la Política de Certificación de DIGILOGIX S.A, otorgado por la ONTI, URI de la Política de Certificación y texto obligatorio para los certificados de la IFDRA

Identificador de la Clave de la Autoridad Certificante (AuthorityKeyIdentifier)	Valor de hash de 20 bytes 2.5.29.35	Contiene un hash de 20 bytes del atributo clave pública del DIGILOGIX AC que emitió el certificado.
Uso Extendido de Clave (Extended Key Usage)	Autenticación del cliente (1.3.6.1.5.5.7.3.2) Correo seguro (1.3.6.1.5.5.7.3.4) 2.5.29.37	Usos adicionales de la clave pública a los enumerados en el campo keyUsage
Nombres Alternativos del Suscriptor (Subject Alternative Name)		
commonName	Nombres y Apellidos 2.5.4.3	Datos que surgen del Documento Nacional de Identidad presentado por el titular
serialNumber	<Tipo> <Número de documento> 2.5.4.5	Datos que surgen del Documento Nacional de Identidad presentado por el titular
title	<Nombre de la función> 2.5.4.12	Cargo o título del suscriptor dentro de la organización, debe corresponder con la certificación aportada en el proceso de autenticación
email	<Dirección de correo electrónico> 2.5.29.17	Dirección de mail del titular verificada por circuito seguro compatible con RFC 822

Perfil de la lista de certificados revocados.

En lo referente a CRLs la **AC – DIGILOGIX** adhiere a las recomendaciones del documento:

- RFC 3280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile” [RFC3280]

Los siguientes campos se encuentran presentes en la Lista de Certificados Revocados, emitida por la **AC – DIGILOGIX**:

Campos Atributos Extensiones	Valor/OID	Observaciones
Versión (Version)	1	Corresponde a versión 2
Algoritmo de Firma (Signature)	sha1RSA 1.2.840.113549.1.1.5	Algoritmo usado por el certificador para firmar
Nombre distintivo del emisor (Issuer)		
commonName	AC-DIGILOGIX 2.5.4.3	Identificación de la Entidad Certificante
serialNumber	30714128716 2.5.4.5	CUIT del Certificador
organizationName	DIGILOGIX S.A. 2.5.4.10	Denominación del Certificador Licenciado

stateOrProvinceName	Ciudad Autónoma de Buenos Aires 2.5.4.8	Ciudad en la que se encuentra el Certificador
countryName	AR 2.5.4.6	País del Certificador Licenciado
Día y hora de vigencia (thisUpdate)	<fecha y hora UTC> yyyy/mm/dd hh:mm:ss huso-horario	Fecha y hora efectivas de emisión, a partir de la cual entre en vigencia
Próxima Actualización (nextUpdate)	<fecha y hora UTC> yyyy/mm/dd hh:mm:ss huso-horario	Fecha y hora de emisión de la próxima Lista de Certificados Revocados
Identificador de la Clave de la Autoridad Certificante (AuthorityKeyIdentifier)	Valor de hash de 20 bytes 2.5.29.35	Contiene un hash de 20 bytes del atributo clave pública del DIGILOGIX AC que emitió la Lista de Certificados Revocados.
Número de CRL (CRL Number)	Número de la CRL OID - 2.5.29.20	Número incremental que identifica la CRL emitida
Indicador Delta CRL (Delta CRL Indicator)	Número de Delta CRL 2.5.29.27	Número que se incrementa cada vez que se emite una Delta CRL
Certificados Revocados (Revoked Certificates)		
Fecha de Revocación	<fecha y hora UTC> yyyy/mm/dd hh:mm:ss huso-horario	Fecha y hora en que se revocó el certificado
Número de Serie del Certificado revocado (Serial Number)	hasta 20 octetos 2.5.4.5	Número de Serie del Certificado revocado
Motivo de la Revocación (ReasonCode) 2.5.29.21	Motivo de acuerdo al RFC 5280	Motivo de la Revocación
Versión de CA	V0.0	Versión de CA