



Paperless  
digital concepts | Chile



Paperless  
digital concepts | Chile

# Cómo Firmar un TED y no morir en el intento

## Capacitación Conceptual

**V 9.9.3**



- Contexto
- Antecedentes
- ¿Cómo se aplica?
- ¿Dónde están las llaves?
- Proceso Final



Paperless  
digital concepts | Chile

# CONTEXTO

# ¿Qué es el TED?

## <DTE>

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<DTE version="1.0"
  - <Documento ID="520050706611025413"
  - <Encabezado>
    - <IdDoc>
      - TipoDTE=61 </TipoDTE>
      - Folio=1025413 </Folio>
      - Fecha=2005-07-06 </Fecha>
      - Mensajes=1 </Mensajes>
    </IdDoc>
  - <Emisor>
    - RUTEmisor=90299000-3 </RUTEmisor>
    - RznSoc=Cia. Nacional de Telefonos Telefonica del Sur S.A. </RznSoc>
    - GiroEmis=Telecomunicaciones </GiroEmis>
    - Acceso=7001 </Acceso>
    - Sucursal=Casa Matriz </Sucursal>
    - DirOrigen=San Carlos 107 </DirOrigen>
    - CmaOrigen=Valdivia </CmaOrigen>
    - CiudadOrigen=Valdivia </CiudadOrigen>
  - <Emisor>
  - <Receptor>
    - RUTRecep=76186240-5 </RUTRecep>
    - RznSocRecep=MOLINA GALLARDO Y CIA LTDA. </RznSocRecep>
    - GiroRecep=SERVICIOS TECNICOS </GiroRecep>
    - DirRecep=VOLCAN HORNOPIREN 1733 </DirRecep>
    - CmaRecep=PTO. MONTT </CmaRecep>
    - CiudadRecep=PTO. MONTT </CiudadRecep>
  - <Metadatos>
    - <MetNeto>
      - MetNeto=135827 </MetNeto>
      - MetExe=0 </MetExe>
      - TasaIVA=19 </TasaIVA>
      - IVA=25807 </IVA>
      - MetTotal=161634 </MetTotal>
    </Metadatos>
  - <Encabezado>
  - <Detalle>
    - NroLinDet=1 </NroLinDet>
    - NroItem=1. RECLAMO/IMPUGNACION/ </NroItem>
    - NroItem=10995 </NroItem>
  - <Detalle>
  - <Referencia>
  - <ID version="1.0"
  - <Comentarios>
  - <Signature xmlns="http://www.w3.org/2000/09/xmldsig#"
  - <SignedInfo>
    - CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315/"
    - SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"
    - Reference URI="#S20050706611025413"
  - <DigestValue>
  - </Reference>
  - </SignedInfo>
  - <SignatureValue>
  - <KeyInfo>
  - <KeyValue>
  - <RSAKeyValue>
  - </RSAKeyValue>
  - </KeyValue>
  - <X509Data>
  - <X509Certificate>
  - </X509Certificate>
  - </KeyInfo>
  - <Signature>
  - </Personalizados>
  - </DTE>
```

## <TED>

```
- <TED version="1.0"
- <DD>
  <RE>90299000-3 </RE>
  <TD>61 </TD>
  <F>1025413 </F>
  <FE>2005-07-06 </FE>
  <RR>76186240-5 </RR>
  <RSR>MOLINA GALLARDO Y CIA </RSR>
  <MNT>161634 </MNT>
  <IT1>1. RECLAMO/IMPUGNACION/ </IT1>
- <CAF version="1.0"
- <DA>
  <RE>90299000-3 </RE>
  <RS>CIA NACIONAL DE TELEFONOS TELEFONICA DEL </RS>
  <TD>61 </TD>
- <RNG>
  <D>1000000 </D>
  <H>1119999 </H>
  </RNG>
  <FA>2005-01-06 </FA>
- <RSAPK>
  <M>1FHUBpcwtrWQI0KhFSV9gBxPaIlgKSQpLdz0u6/xTGnxkgCBsPI
  <E>Aw== </E>
  </RSAPK>
  <IDK>300 </IDK>
  </DA>
  <FRMA algoritmo="SHA1withRSA">GnEyTlLiamX/9j4kLZSVJW7a0dXQlCg
  </CAF>
  <TSTED>2005-08-05T17:39:12 </TSTED>
  </DD>
  <FRMT algoritmo="SHA1withRSA">aBwcVr4Yn3mfCUJOU9xUZ07pZ19wzIIo
  </TED>
```



Timbre Electrónico SII  
Res. 12345 del 2005. - Verifique documento: www.sii.cl



# TED - Timbre Electrónico del DTE

```
- <TED version="1.0">  
- <DD>  
  <RE>96915310-6</RE>  
  <TD>33</TD>  
  <F>9</F>  
  <FE>2004-03-01</FE>  
  <RR>92580000-7</RR>  
  <RSR>ENTEL S.A.</RSR>  
  <MNT>19992756</MNT>  
  <IT1>40% Proyecto de Plataforma de Recepcion,</IT1>
```

```
- <CAF version="1.0">  
- <DA>  
  <RE>96915310-6</RE>  
  <RS>E-PARTNERS S A</RS>  
  <TD>33</TD>  
- <RNG>  
  <D>1</D>  
  <H>200</H>  
</RNG>  
  <FA>2003-10-23</FA>  
- <RSAPK>  
  <M>5kqVT7QIegkAVyMLwc2aVkJMI+6je6hxBnEc2q5YUyTGVm+Skl  
  <E>Aw==</E>  
</RSAPK>  
  <IDK>300</IDK>  
</DA>  
  <FRMA algoritmo="SHA1withRSA">c545rqV52qd5kGtO/7UDvIHEwi9hcLql  
</CAF>
```

**NODO - TED**

**RE - RUT EMISOR**

**TD - TIPO DE DOCUMENTO**

**F - FOLIO**

**FE - FECHA EMISION**

**RR - RUT RECEPTOR**

**RSR - RAZON SOCIAL RECEPTOR**

**MNT - MONTO NETO**

**IT1 - GLOSA DETALLE 1**

**CAF**

**TSTED - TimeStamp TED**

**FRMT - Firma TED**

```
<TSTED>2004-03-17T17:41:00</TSTED>
```

```
</DD>
```

```
<FRMT algoritmo="SHA1withRSA">vdeP8CkpQW9pGS7KA65+8SkOOPKEOllEl
```

```
</TED>
```

**VOLVER**





# CAF – Código de Autorización de Folios

```
<?xml version="1.0" ?>
- <AUTORIZACION>
- <CAF version="1.0">
- <DA>
  <RE>96915310-6</RE>
  <RS>E-PARTNERS S A</RS>
  <TD>110</TD>
- <RNG>
  <D>1</D>
  <H>100</H>
</RNG>
  <FA>2008-01-15</FA>
- <RSAPK>
  <M>2lVT8m0M/vuYsrJFuM+cxXc77Wh7n54Mqlc7n4/A1zXL7tn80FT5Nkt3y
  <E>Aw==</E>
</RSAPK>
  <IDK>100</IDK>
</DA>
<FRMA
  algoritmo="SHA1withRSA">sYU2w5Hn9S0KC+/SWgxNprxwAM/iW9TxBNSa3U
</CAF>
<RSASK>-----BEGIN RSA PRIVATE KEY----- MIIBOgIBAAJBANpVU/JtDP77mLKyRI
+TZLecvfJmTWbxBSe6VvsnlSJnvBEuYU+LsCAQMCQQCRjff2813/UmXMdtkl37:
+ifzmv0VFAhW5NJqX9XkzUyigc4eBwrIkfIwQo/+p8OWfpBhyZkXNq9gaSWEhH
AiEA8lq9zZZnS199+K4ow4PqsaqHPK40WIttWfgWiZjwHUcCIQDmoFl6DOMdqfk
1VKK4vAYBA1mZIZ0SxLFcwzRBI4y7QIhAKGR095kRNzqU/sexdetRyEcWih0IuW
SOalZFu7Sr4vAiEAmcA7prNCE8ahuTjhseygEAKzmZhd+DIMg6Ii1mUIfMCIDHE
PRIVATE KEY-----</RSASK>
<RSAPUBK>-----BEGIN PUBLIC KEY----- MFowDQYJKoZIhvcNAQEBBQADSQAwrG.
DIJX05+PwNc1y+7Z/NBU+TZLecvfJmTWbxBSe6VvsnlSJnvBEuYU+LsCAQM=
</AUTORIZACION>
```

RUT EMISOR

RAZON SOCIAL

TIPO DE DOCUMENTO

RANGO - DESDE

RANGO - HASTA

FECHA DE AUTORIZACION

FIRMA CAF

LLAVE PRIVADA

LLAVE PUBLICA

VOLVER



# ¿Por qué tiene validez el TED?

```
- <TED version="1.0">
- <DD>
  <RE>96915310-6</RE>
  <TD>33</TD>
  <F>9</F>
  <FE>2004-03-01</FE>
  <RR>92580000-7</RR>
  <RSR>ENTEL S.A.</RSR>
  <MNT>19992756</MNT>
  <IT1>40% Proyecto de Plataforma de Recepción,</IT1>
- <CAF version="1.0">
- <DA>
  <RE>96915310-6</RE>
  <RS>E-PARTNERS S A</RS>
  <TD>33</TD>
- <RNG>
  <D>1</D>
  <H>200</H>
</RNG>
  <FA>2003-10-23</FA>
- <RSAPK>
  <M>5kqVT7QIegkAVyMLwc2aVvMI+6je6hxTBnEc2q5YUyTGVm+Skl
  <E>Aw==</E>
</RSAPK>
  <IDK>300</IDK>
</DA>
  <FRMA algoritmo="SHA1withRSA">c545rqV52qd5kGtO/7UDvIHEwi9hcLqI
</CAF>
  <TSTED>2004-03-17T17:41:00</TSTED>
</DD>
  <FRMT algoritmo="SHA1withRSA">vdeP8CkpQW9pGS7RA65+8SkOOPKEOILeI
</TED>
```

1. Permite validar que la información del TED no ha sido intervenida
2. No permite regenerarlo a partir de la información provista

**FRMT – Firma del TED**



Paperless  
digital concepts | Chile

# ANTECEDENTES





# Fundamentos de Llaves Públicas

- RSA = Algoritmo matemático permite determinar tres números que satisfacen la siguiente condición:

- $\beta = T \text{ } \overset{\text{PR}}{\circ} \text{ mod } K$

- $T = \beta \text{ } \overset{\text{PU}}{\circ} \text{ mod } K$

Llave Privada

Módulo

Llave Pública



# Ejemplo – Encriptar 123

CONSIDERANDO > PRIVADA = 17 | PUBLICA = 2753 | MODULO = 3233

## ENCRYPTAR

- CYPHER = RSA(123)
- CYPHER =  $(123^{17}) \bmod 3233$
- CYPHER = 337587917446653715596592958817679803 mod 3233
- CYPHER = 855

## DESENCRIPTAR

- VALOR =  $(855^{2753}) \bmod 3233$
- VALOR = 555658809385189881181290561427408580916876  
546209789056.....00812354234523  
3562528362829324776927492484375 mod 3233
- VALOR = 123



# Aspectos Importantes

- No funciona al revés, es decir, dada la llave pública no se puede aplicar el proceso inverso para reconstruir el valor cifrado

$$T^{PU} \text{ mod } K \neq C^{PU} \text{ mod } K$$

- Se requieren operaciones matemáticas con grandes números para poder hacer las operaciones de exponente y módulo

$$(855^{2753}) \text{ mod } 3233 = ?$$



Paperless  
digital concepts | Chile

## ¿COMO SE APLICA?



# RSA - Proceso de Firma

- Dado un texto (TEXTO), el cálculo de la firma comprende el siguiente algoritmo:
  - $A \leftarrow \text{SHA1}(\text{TEXTO})$
  - $B \leftarrow \text{PaddingPKCS1}(A)$
  - $C \leftarrow \text{RSA}(B, \text{PRIVADA}, \text{MODULO})$
  - $D \leftarrow \text{Base64}(C)$
- **IMPORTANTE:**
  - *El resultado D corresponde a la firma del hash SHA1 del texto*
  - *Si se envía el TEXTO + D + PUBLICA + MODULO, receptor puede validar aplicando el proceso inverso*

# RSA - Proceso de Validación



Paperless  
digital concepts | Chile

- Usuario recibe TEXTO + FIRMA + PUBLICA + MODULO.
- Proceso de validación comprende:
  - **CALCULO**
    - $A \leftarrow \text{SHA1}(\text{TEXTO})$
  - **COMPARACION**
    - $B \leftarrow \text{UNBASE64}(\text{ FIRMA } )$
    - $C \leftarrow \text{RSA}( B, \text{ PUBLICA}, \text{ MODULO } )$
    - $D \leftarrow \text{SINPADDINGPKCS1}( C )$
    - $\text{¿}A = D\text{?}$







Paperless  
digital concepts | Chile

¿DONDE ESTAN LAS LLAVES?



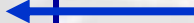
# Las Llaves del CAF

```

<?xml version="1.0" ?>
-<AUTORIZACION>
- <CAF version="1.0">
- <DA>
  <RE>96915310-6</RE>
  <RS>E-PARTNERS S A</RS>
  <TD>110</TD>
- <RNG>
  <D>1</D>
  <H>100</H>
</RNG>
  <FA>2008-01-15</FA>
- <RSAPK>
  <M>2lVT8m0M/vuYsrJFuM+cXxc77Wh7n54Mglc7n4/A1zXL7tn80FT5Nkt5y
  <E>Aw==</E>
</RSAPK>
  <IDK>100</IDK>
</DA>
<FRMA
  algoritmo="SHA1withRSA">sYU2w5Hn9S0KC+/SWgxNprxwAM/iW9TxBNSa3U
</CAF>
<RSASK>-----BEGIN RSA PRIVATE KEY----- MIIBOgIBAAJBANpVU/JtDP77mLKyRI
+TZLecvfJmTWbxBSe6VvsnlSjnvBEuYU+LsCAQMCQQRjff2813/UmXMdtkl37:
+ifzmv0VFAhW5NJqX9XkzUyigc4eBwrIkIwQo/+p8OWfpBhyZkXNq9gaSWEhH
AiEA8lq9zZZnS199+K4ow4PqsaqHPK40WIttWfgWiZjwHUcCIQDmoFl6DOMdqfK
1VKK4vAYBA1mZIZ0SxLfcwzRBI4y7QIhAKGR095kRNzqU/sexdetRyEcWih0IuW
SOalZFu7Sr4vAiEAmcA7prNCE8ahuTjhseygEAKzmZhd+DIMg6Ii1mUIfMCIDHE
PRIVATE KEY-----</RSASK>
<RSAPUBK>-----BEGIN PUBLIC KEY----- MFowDQYJKoZIhvcNAQEBBQADSQAwrG.
DIJXO5+PwNc1y+7Z/NBU+TZLecvfJmTWbxBSe6VvsnlSjnvBEuYU+LsCAQM=
</AUTORIZACION>

```

**SOLO SE  
INCORPORA ESTA  
SECCION EN EL TED  
ELIMINANDO LA  
LLAVE PRIVADA  
(RSASK) Y LA  
LLAVE PUBLICA  
(RSAPUBK)**



**LLAVE PRIVADA**



**LLAVE PUBLICA**



# ¿Cómo leer las llaves?

```
-----BEGIN RSA PRIVATE KEY-----  
MIIBOgIBAAJBALocJF/TtxJOoYdweX0+AhnMcALqVcsSmiiyL2W5JAmH4o6LxN  
gTkvdYiPlRU1y53md1vrNJc9dU6KpCH7ZPNTMCAQMCQHwSwuqNJLbfFlpK+6jU  
AWaISqycOTIMZsXMH5kmGAZZcqsXSeFdhbY7qXSgnChP7A5ABMETADS/1lCzcm  
YsrvsCIQDwNq3281T5DuiXfmeppkjfpSTSAUKRSWCH6uHzAHg75wIhAMZXot8S  
s1FQlnNL+L95+Rys8OWQamHW1P9GUwEck/LVAiEAoCRz+feN+19FulRFG8Qw1R  
jDNquBtnZAWpyWogBQJ+8CIQCEOic/Ycw2NbmiMqXU+/toc0tDtZxBoeNU2Yyr  
aGKh4wIhANI1qNouzu5cAKn3vqgAWsXRy6+H9aEX/k1Efc3ik2Dv  
-----END RSA PRIVATE KEY-----
```

- Formato PEM (Privacy-Enhanced Mail)
- Permite el transporte seguro de las llaves
- Utiliza el estándar ASN.1 (Abstract Syntax Notation 1)



# TED - Timbre Electrónico del DTE

```
- <TED version="1.0">  
- <DD>  
  <RE>96915310-6</RE>  
  <TD>33</TD>  
  <F>9</F>  
  <FE>2004-03-01</FE>  
  <RR>92580000-7</RR>  
  <RSR>ENTEL S.A.</RSR>  
  <MNT>19992756</MNT>  
  <IT1>40% Proyecto de Plataforma de Recepcion,</IT1>
```

```
- <CAF version="1.0">  
- <DA>  
  <RE>96915310-6</RE>  
  <RS>E-PARTNERS S A</RS>  
  <TD>33</TD>  
- <RNG>  
  <D>1</D>  
  <H>200</H>  
  </RNG>  
  <FA>2003-10-23</FA>  
- <RSAPK>  
  <M>5kqVT7QIegkAVyMLwc2aVvMI+6je6hxTBnEc2q5YUyTGVm+Skl  
  <E>Aw==</E>  
  </RSAPK>  
  <IDK>300</IDK>  
  </DA>  
  <FRMA algoritmo="SHA1withRSA">c545rqV52qd5kGtO/7UDvIHEwi9hcLql  
</CAF>
```

```
<TSTED>2004-03-17T17:41:00</TSTED>  
</DD>  
<FRMT algoritmo="SHA1withRSA">vdeP8CkpQW9pGS7KA65+8SkOOPKEOILel  
</TED>
```

**NODO - TED**

**RE - RUT EMISOR**

**TD - TIPO DE DOCUMENTO**

**F - FOLIO**

**FE - FECHA EMISION**

**RR - RUT RECEPTOR**

**RSR - RAZON SOCIAL RECEPTOR**

**MNT - MONTO NETO**

**IT1 - GLOSA DETALLE 1**

**CAF**

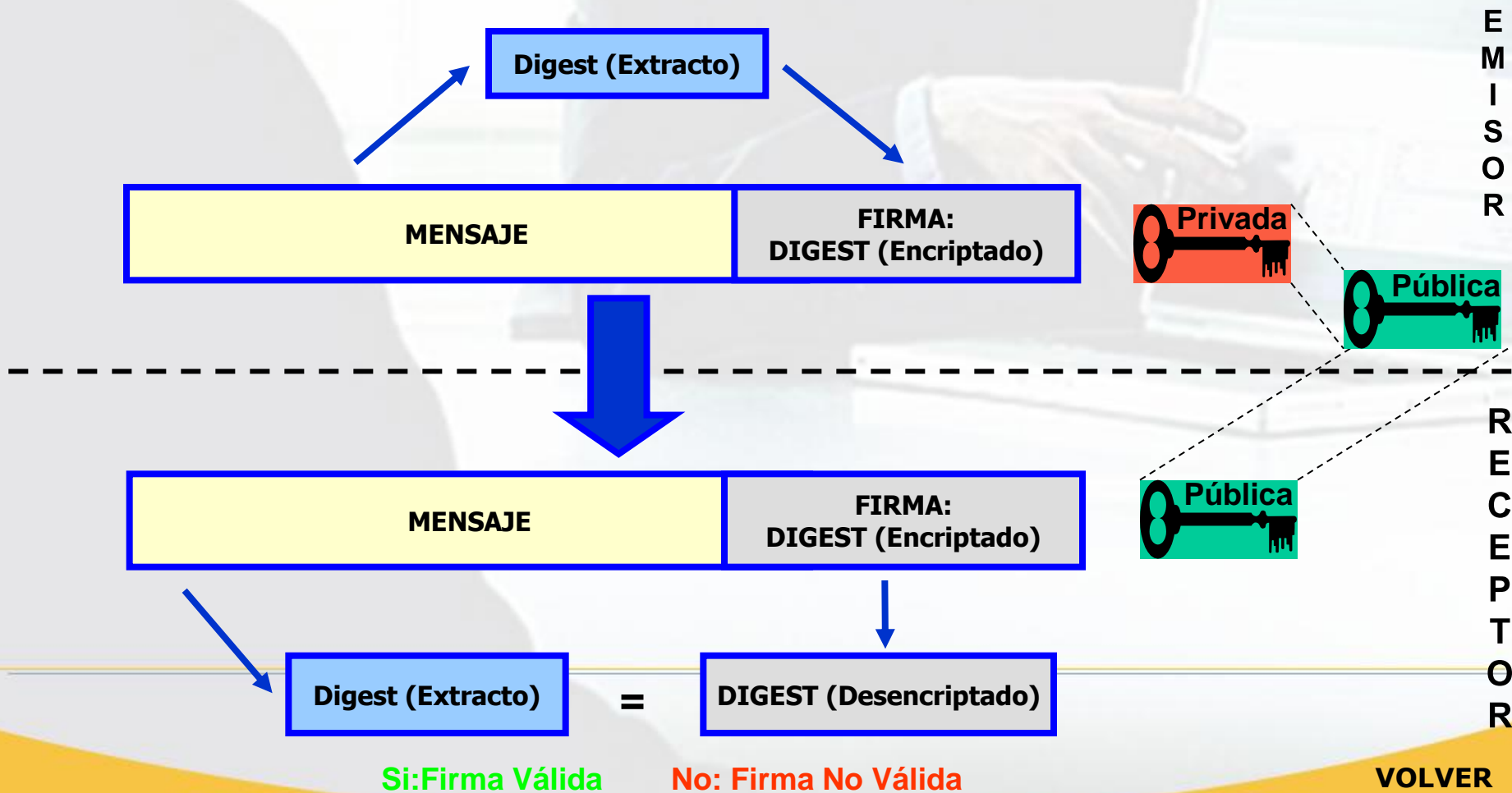
**TSTED - TimeStamp TED**

**FRMT - Firma TED**

**VOLVER**



# Firma Electrónica (1)









# ASN.1 – Abstract Syntax Notation

- Norma que establece cómo representar en modo binario objetos.
- Preeliminar al XML
- Objetos Disponibles:
  - *BOOLEAN*
  - *INTEGER*
  - *BITSTRING*
  - *OCTET*
  - *:*
  - *:*





Paperless  
digital concepts | Chile

# PROCESO FINAL

