Manual de Arquitectura

@Firma Versión 4.0

Documento nº:	TI-20-1074-ARQ-001
Revisión:	01
Fecha:	29-07-2004
Período de retención:	Permanente durante su período de vigencia + 3 años después de su anulación

CONTROL DE COMPROBACIÓN Y APROBACIÓN

Documento nº: TI-20-1074-ARQ-001

Revisión: 1

Fecha: 29/07/2004

REALIZADO

29/07/2004

Javier

Cerceda

García

Analista

COMPROBADO

29/07/2004

Jose Antonio

Márquez

Contreras

Director @firma

APROBADO

29/07/2004

Jose Antonio

Márquez

Contreras

Director @firma

CONTROL DE MODIFICACIONES

Documento nº: TI-20-1074-ARQ-001

Revisión: 1

Fecha: 29/07/2004

Rev. 1

Fecha 29/07/2004

Autor/es JCG

Descripción Documentación inicial

CONTROL DE DISTRIBUCIÓN

Documento nº: TI-20-1074-ARQ-001

Revisión: 1

Fecha: 29/07/2004

Copias Electrónicas:

La distribución de este documento ha sido controlada a través del sistema de información.

Copias en Papel:

La vigencia de las copias impresas en papel está condicionada a la coincidencia de su estado de revisión con el que aparece en el sistema electrónico de distribución de documentos.

El control de distribución de copias en papel para su uso en proyectos u otras aplicaciones es responsabilidad de los usuarios del sistema electrónico de información.

Fecha de impresión 23/08/2004 17:32

Distribución en Papel:

Nombre o Cargo y (Organización)	Nº de Ejemplares	Referencia de la carta de transmisión y fecha

Índice

1 Objeto

Es objeto del presente documento es describir los elementos que intervienen en la plataforma de autenticación y firma digital, @firma, indicando:

- El papel que desempeña cada uno de ellos.
- Las comunicaciones y relaciones que se establecen entre los mismos.
- Los requisitos mínimos necesarios para cada uno.

2 Alcance

El presente documento recoge la relación entre los distintos elementos que intervienen en la plataforma de autenticación y firma digital.

3 Siglas

AC	Autoridad de Certificación
CPD	CRL Distribution Point
CRL	Lista de Revocación de Certificados
DES	Data Encryption Standard
FNMT-RCM	Fábrica Nacional de Moneda y Timbre, Real Casa de la Moneda
LDAP	Lightweight Directory Access Protocol
PC	Ordenador Personal
RMI	Remote Method Invocation
RSA	Rivest Shamir Adleman
SID	Signer Identification
SSL	Secure Socket Layer
IIOP	Inter-Orb Protocol
EJB	Enterprise Java Bean
DMZ	Zona Desmilitarizada
JDK	Java Develoment Kit
TI	Telvent Interactiva

4 Documentos de Referencia

- Documento TI-20-1074-ADM-001, Manual de Administración de la Plataforma @Firma
- Documento TI-20-1074-INS-001, Manual de Instalación de la Plataforma @Firma.

5 Arquitectura completa del sistema

El presente documento recoge la arquitectura de la plataforma de Autenticación y Firma Digital @firma Versión 4.0 contemplando los elementos internos y externos a la misma.

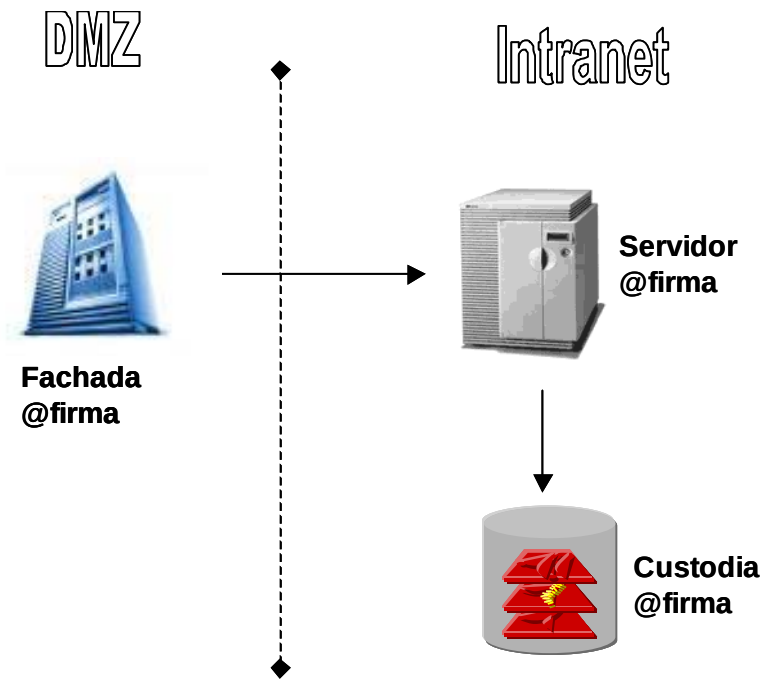
Básicamente, la plataforma @firma Versión 4.0 esta compuesta internamente por tres elementos que se presentan a continuación:

- Sistema de Custodia: Representa la Base de Datos donde se almacenan las transacciones de firma realizadas y se custodian los documentos firmados. El Sistema Gestor de Base de Datos permitido es ORACLE 8/9i. Por regla general el Servidor de Base de Datos es independiente del Servidor de firma y dedicado únicamente a BD. Este elemento debe colocarse en la Intranet corporativa.

- Servidor Centralizado @firma: Representa el núcleo de la plataforma, es decir el Servidor de Autenticación y Firma Digital. Publica las interfaces necesarias para la comunicación con el mismo (RMI-IIOP, WEBSERVICES). Este elemento debe colocarse en la Intranet corporativa.

- Fachada de Comunicación @firma: Representa la parte de la plataforma encargada de atender las peticiones de Autenticación y Firma Digital externas / internas y redirigirlas al Servidor de Firma. A su vez publica las interfaces adecuadas (WEBSERVICES), los applets necesarios y componentes descargables. Este elemento debe colocarse en la DMZ corporativa.

La siguiente figura muestra los elementos citados anteriormente y la relación entre los mismos.



El resto de elementos que intervienen en la arquitectura son los siguientes:

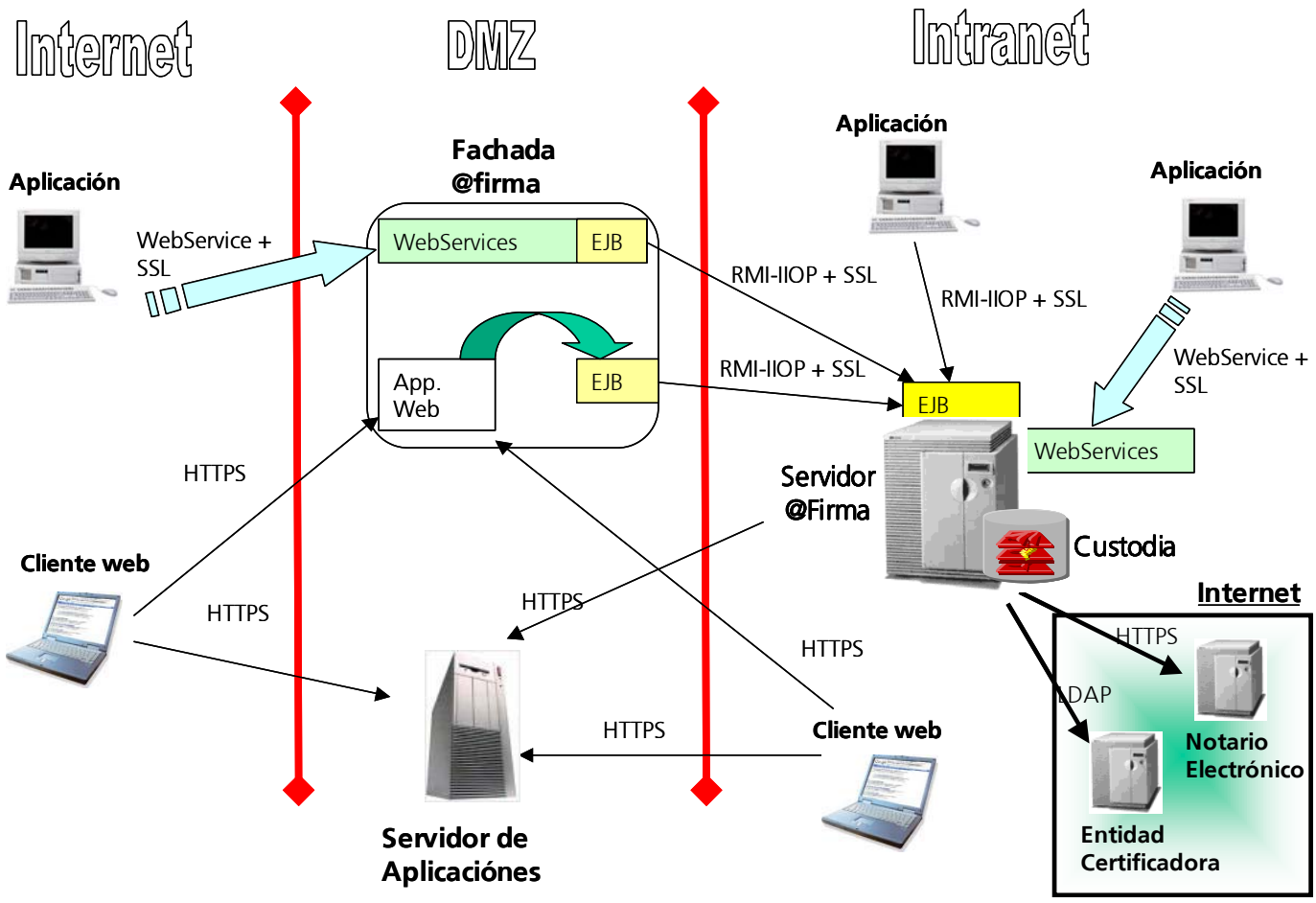
- **Cliente (Web, Aplicación)**: Son los clientes de la plataforma, tanto navegadores Webs como Aplicaciones de diferentes tecnologías, que mediante las interfaces securizadas de @firma (RMI-IIOP, WebServices) hacen uso de Autenticación, Firma Electrónica Avanzada, Verificación de Firmas, Acceso Sistema de Custodia, etc. Este elemento se ubica en Intranet corporativa o Internet.

- **Servidor de Aplicaciones:** corresponde al servidor que contiene la aplicación que se integra con la plataforma de autenticación y firma digital @firma. Este elemento se encuentra en DMZ o Intranet corporativas.

- **Notario Electrónico:** corresponde al servidor externo al cual la plataforma de firma solicita sellados de tiempo y acuses de recibo. Este elemento se encuentra en Internet.

- **Autoridad Certificadora:** Autoridad que emite certificados digitales de confianza y permite comprobar el estado de un certificado en un momento determinado. La plataforma admite múltiples Autoridades Certificadoras. Este elemento se encuentra en Internet.

La siguiente figura muestra la arquitectura completa del sistema, reflejando las relación entre todos los elementos citados anteriormente:



Consideraciones importantes:

- Las Interfaces WebServices se pueden publicar en el Servidor @firma, en la Fachada @firma o en los dos sitios a la vez, esto dependerá de las necesidades de cada organización.

- El **cliente Web** ha de tener acceso HTTPS con el **Servidor de Aplicaciones** donde se encuentra la aplicación a la que necesita acceder y con la **Fachada @firma.**

- El **Servidor @firma** ha de tener acceso HTTPS con los **Servidores de Aplicaciones** que utilizan los servicios de Firma Web. El Certificado Digital del Servidor de Aplicaciones para comunicación HTTPS debe ser incluido en el keystore de Certificados de Aplicaciones del Servidor de @firma.

- El **Servidor @firma** tiene que tener conexión directa a través del puerto LDAP (389 u otro definido) con la **Autoridad de Certificación**, en este caso la FNMT-RCM para descargarse la lista de CRL's.

- El **Servidor @firma** ha de tener acceso HTTP/S al Servidor de **Notario Electrónico**.

- La **Fachada @firma** publica los puertos necesarios para acceder a los módulos de la plataforma. Ésta debe disponer de un Certificado Digital de Servidor para el protocolo de comunicación HTTPS y para la comunicación SSL. Este certificado debe tener en el campo Nombre/Apellidos el nombre de la Fachada @firma. En caso de no ser así, se mostraría una alerta al usuario advirtiendo de la no coincidencia de nombres.

    - Autenticación Web (HTTPS Puerto 443)

    - Firma Web e interfaces WebServices (HTTPS Puerto 444).

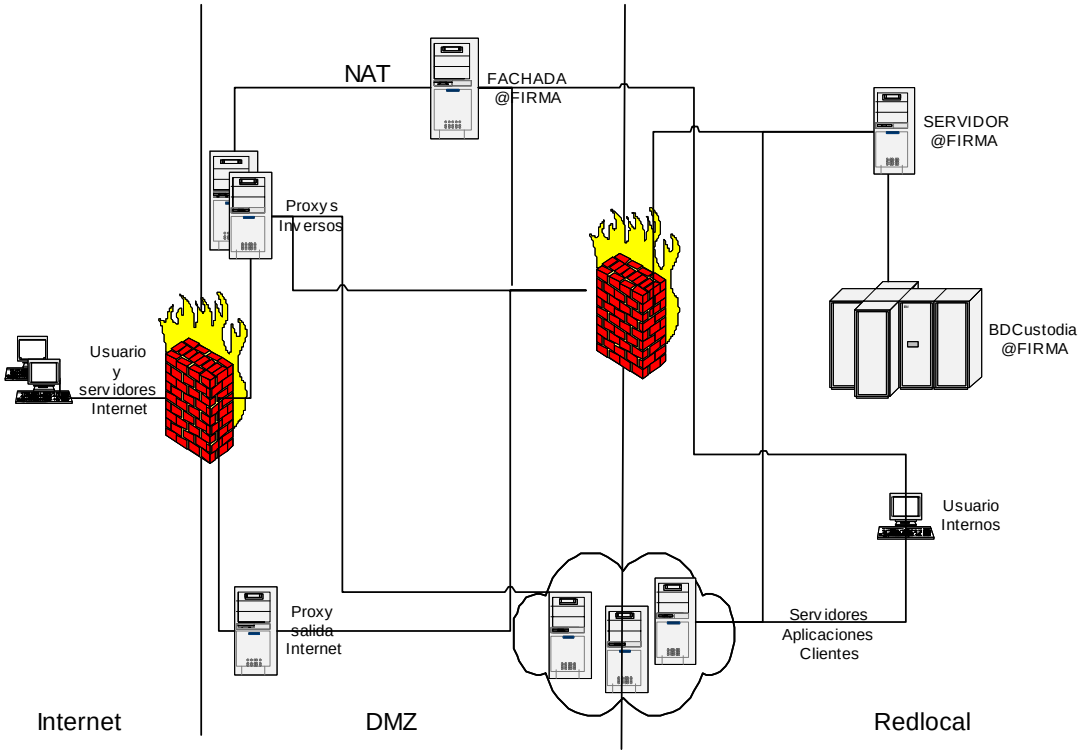
- El **Servidor @firma** publica los puertos necesarios para acceder a los módulos de la plataforma. Esta debe disponer de un Certificado Digital de Servidor para el protocolo de comunicación HTTPS y para la comunicación SSL. Este certificado debe tener en el campo Nombre/Apellidos el nombre del Servidor @firma. En caso de no ser así, se mostraría una alerta al usuario advirtiendo de la no coincidencia de nombres.

    - RMI-IIOP

    - WebServices (HTTPS Puerto 443)

6 Arquitectura a nivel de red del sistema

La siguiente figura muestra la arquitectura del sistema a nivel de red considerando los elementos de interconexión: Proxys, Firewalls, etc..



En esta arquitectura se determinan tres zonas o subredes independientes e interconectadas: Internet, la DMZ (zona desmilitarizada) y la red local. El acceso a las redes DMZ y local suelen estar protegidas por sus correspondientes firewalls, aunque en determinados sistemas un solo firewall puede separar las tres redes.

En Internet se localizan los usuarios remotos y servidores externos de otras entidades. En la DMZ, se sitúan los elementos de red de la organización que son accesibles desde internet, como por ejemplo, los servidores webs, proxys inversos, firewalls, proxys para el acceso a internet, Fachada @firma, etc. Esta subred supone la parte más propensa a ataques dentro de la organización, dada su exposición al exterior, por lo que suele ser la subred más protegida y auditada de toda la entidad.

En la red local se sitúan los servidores internos, BDs, etc. Dado su aislamiento del exterior corresponde con la red más segura, por lo que será el lugar indicado para situar tanto el servidor @firma como el sistema de custodia.

7 Requsitos mínimos

1. Cliente Web:

- *En Sistema Operativo Windows*:
  - *Firma Web*: Navegador Internet Explorer 5.0 o superior con JVM de Microsoft 1.1.4 presente por defecto o JRE de Sun 1.4.0 o superior. También se admite navegador Netscape 4.78 o superior con JRE de Sun 1.4.0 o superior.
  - *Firma Ficheros*: Navegador Internet Explorer 5.0 o superior. También se admite navegador Mozilla 1.3 o superior con JRE de Sun 1.4.1 o superior. NOTA: IE no necesita JRE ni JVM.
- *En Sistema Operativo Linux:* Navegador Mozilla 1.3 o superior con JRE de Sun 1.4.0 o superior y librería JSS33.

2. Cliente Aplicación.

- Sistema Operativo Windows (9x, NT, 2000, XP) y JDK 1.4.0 o superior para aplicaciones Java.

3. Servidor de Aplicaciones.

- Para Servidores de Aplicaciones Java, el contenedor de Servlets/JSP ha de cumplir con las especificaciones Servlet 2.3 y JSP 1.2 de Sun Microsystems, y disponer de una Máquina Virtual Java 1.4.0 o superior.

4. Servidor @firma.

- Sistema Operativo: Windows 2000 (professional/Server) con el Service pack 2 instalado ó Sistemas Operativos UNIX, Linux (RedHat 7.2, Debian), Solaris, etc ...
- Memoria RAM: Para un rendimiento óptimo del servidor es aconsejable tener un mínimo de 1 GB de memoria. Recomendable 2 GB.
- Máquina virtual de Java: Java Development Kit 1.4.x, de Sun Microsystems.

5. Sistema de Custodia.

- Bases de datos Soportadas: Oracle (Versiones 8.1.7 y 9i).