CERTIFICADOS FNMT DE COMPONENTE:

- ✓ **SSL/TLS**
- ✓ **WILDCARD**
- ✓ **MULTIDOMINIO SAN/UCC**
- ✓ **SELLO DE ENTIDAD**

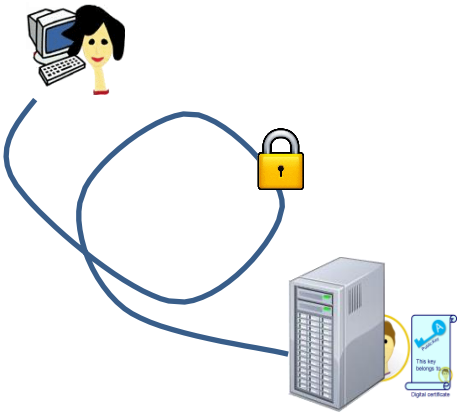
Contenido

0. TIPOS DE CERTIFICADOS FNMT DE COMPONENTE

La FNMT – RCM emite diferentes tipos de certificados de componente para cubrir distintos propósitos, según la siguiente relación:

1. Certificado de servidor web:
   - 1.1 Certificado SSL/TLS
   - 1.2 Certificado wildcard
   - 1.3 Certificado multidominio SAN/UCC
2. Certificado de sello de Entidad

1. CERTIFICADO FNMT DE SERVIDOR WEB



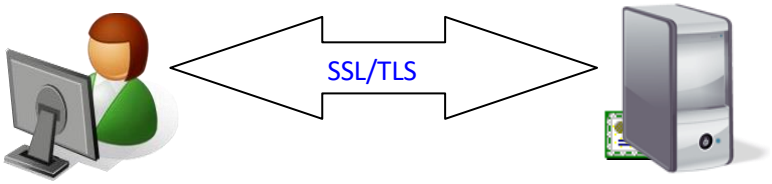
El objetivo de un certificado de servidor web es garantizar la verdadera identidad de un sitio web (nombre del dominio) y establecer un "canal seguro" de comunicación entre éste y el navegador del usuario de Internet, es decir, un canal cifrado que garantice la confidencialidad de la comunicación. Para el establecimiento de dicho canal seguro se utilizan protocolos de seguridad SSL/TLS.

Utilizando SSL o TLS se consiguen los siguientes servicios de seguridad:

- Confidencialidad en la conexión: la información se cifra utilizando criptografía de clave simétrica.
- Autenticación de cliente y servidor: usando criptografía de clave pública.
- Integridad de la información intercambiada: la integridad de los mensajes se asegura usando firma

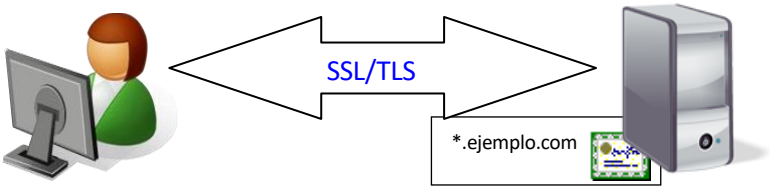
1.1 Certificado SSL/TLS

Los certificados FNMT de servidor SSL/TLS incluyen la configuración estándar para autenticar el dominio del servidor y establecer comunicaciones seguras con los clientes web con protocolos SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1 y el más reciente TLS 1.2, capaz de establecer conexiones protegidas criptográficamente con claves de sesión de hasta 256 bits.



1.2 Certificado wildcard

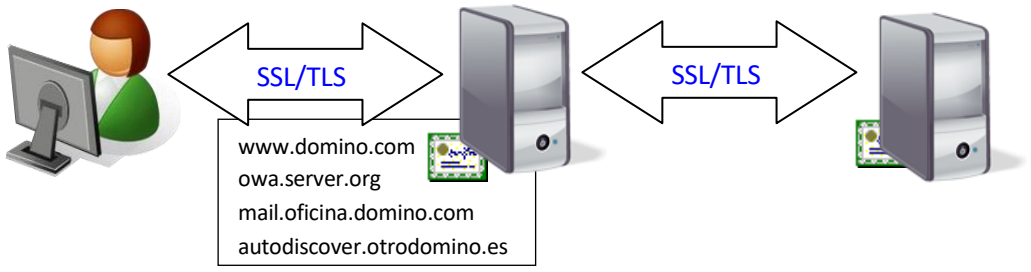
Los certificados wildcard permiten, con un solo certificado, securizar todos los subdominios de nivel inmediatamente inferior a un domino dado. Es decir, con un solo certificado de tipo *.ejemplo.com es posible proteger www.ejemplo.com, mail.ejemplo.com, y cualquier otro subdominio de ejemplo.com. Podrá instalar el certificado en tantas máquinas como necesite sin coste adicional.



Si requiere proteger con un solo certificado dominios con diferentes niveles de profundidad o diferente dominio base, como por ejemplo www.subdominio.ejemplo.com y mail.otrodominio.es, deberá solicitar un certificado de tipo SAN.

1.3 Certificado multidominio SAN /UCC

Los certificados multidominio SAN, también conocidos como certificados UCC o *Unified Communications Certificates*, le permiten securizar, con un solo certificado, hasta doce dominios diferentes. Podrá instalarlo en servidores que respondan a diferentes dominios con la misma IP o en tantas máquinas como precise.



2 CERTIFICADO FNMT DE SELLO DE ENTIDAD

El certificado de sello de entidad permite a una persona jurídica identificarse telemáticamente y realizar firmas electrónicas. Su flexible configuración permite dotarle de diferentes usos:

- Creación de sellos electrónicos para garantizar, mediante firma electrónica, la autenticidad e integridad de los documentos electrónicos a los que están vinculados.
- Autenticación de componentes informáticos de una Entidad en su acceso a servicios informáticos, o a otras infraestructuras tecnológicas, con acceso restringido o identificación de cliente.
- Intercambio de mensajes o datos cifrados con garantías de confidencialidad, autenticación e integridad.

Los certificados representan inequívocamente a la Entidad a la que se ha expedido el certificado, incluyendo su denominación, localidad y número de identificación fiscal (N.I.F.).

La configuración por defecto del certificado le permite la realización de firmas electrónicas, cifrado de datos y autenticación como cliente en conexiones SSL. Adicionalmente, usted podrá solicitar que el certificado se emita con el uso extendido de clave 'protección de email'.

Se emite con el uso de clave extendido 'autenticación de cliente' es necesaria en conexiones seguras entre máquinas que requieren que ambos extremos se identifiquen mediante el uso de un certificado y establezcan una conexión TLS. Es decir, permitirá que su componente informático

pueda conectarse como cliente en conexiones hacia otros servidores o servicios.

El propósito de clave extendida de 'protección de email' es utilizado para el intercambio de correo seguro en algunos programas de correo electrónico.

3 COMPARATIVA DE CERTIFICADOS EMITIDOS POR FNMT-RCM

	SSL/TLS	Wildcard	Multidominio SAN/UCC	Sello de Entidad
Clave pública	RSA 2048 bits	RSA 2048 bits	RSA 2048 bits	RSA 2048 bits
Algoritmo de firma	RSA/SHA256	RSA/SHA256	RSA/SHA256	RSA/SHA256
Uso de clave	Autenticación de servidor	Autenticación de servidor	Autenticación de servidor	Firma y cifrado de documentos
Compatible SSL/TLS (hasta 256 bits)	✓	✓	✓	✓[1]
Subdominios ilimitados[2]		✓		
Múltiples dominios (Unified Communications certificate)			✓	
Autovalidación[3]	OCSP público	OCSP público	OCSP público	OCSP público
· Autenticación de cliente				✓
· Protección de correo				✓

[1] Para conexiones TLS se requiere la opción de autenticación de cliente.
[2] Subdominios inmediatamente inferior al dominio certificado (e.g. *.dominio.es).
[3] En navegadores y sistemas que soporten dicha característica.

4 ¿CÓMO SOLICITAR UN CERTIFICADO DE COMPONENTE?

El proceso de emisión de los certificados tiene tres fases:

1. Solicitud: El solicitante deberá rellenar un formulario web y aportar el PKCS#10 o CSR (*certificate signing request*). El suscriptor del certificado, mediante la firma electrónica de un contrato PDF, aceptará las condiciones uso y autorizará a la persona solicitante. La firma del contrato se realizará con un certificado de representante de persona jurídica expedido por la FNMT. En el caso de ser clientes y tener constituida oficina de registro, también puede ser firmado por el Responsable de Operaciones de Registro (ROR), utilizando su certificado de persona física, empleado público o DNIe. que acredite la identidad del solicitante y del suscriptor.
2. Registro: La FNMT-RCM llevará a cabo las verificaciones necesarias para comprobar que los datos consignados son veraces y la solicitud es auténtica. Posteriormente, se autoriza la emisión del certificado y queda listo para su descarga.
3. Pago y descarga del certificado: Previo al proceso de descarga, el suscriptor deberá abonar el importe del certificado a través de los medios de pago concertados con el Área comercial.

El procedimiento de solicitud, así como la documentación a aportar, se encuentran en el siguiente enlace:

https://apus20.cert.fnmt.es/SolicitudCertComp/

5 DATOS DE CONTACTO

Soporte Técnico: Si tuviese problemas técnicos al realizar la petición, disponemos de un servicio que, bien telefónicamente en el Tlf. 915666914 o bien mediante email: soporte_tecnico_ceres@fnmt.es, le resolverá los mismos.

Área de Registro: Si le surgiesen dudas de carácter administrativo al completar los formularios de solicitud o en la interpretación de los propios Procedimientos de Registro, tenemos un servicio especializado de Atención al cliente en los Telf.: 915 666 916/917/912 email: registroceres@fnmt.es

Área Comercial : Para ofertas económicas o cualquier otro tipo de aclaración, estamos en el Telf.: 915 66 6948/7831/6929/7679/7689/6918, email: comercial.ceres@fnmt.es

6 REFERENCIAS

- RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- The Secure Sockets Layer (SSL) Protocol Version 3.0

- The Transport Layer Security (TLS) Protocol Version 1.2
- Wikipedia: Transport Layer Security