UNIVERSIDAD CENTRAL DE VENEZUELA
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA ELÉCTRICA

ESPECIALIZACIÓN EN COMUNICACIONES
Y REDES DE COMUNICACIÓN DE DATOS

Diseño e implantación de una plataforma segura para gestionar los procesos de distribución y ventas en una empresa de consumo masivo a través de dispositivos móviles

Caracas, Julio de 2018

Hecho el Depósito de Ley

Depósito Legal DC2018001929

TRABAJO ESPECIAL DE GRADO

Diseño e implantación de una plataforma segura para gestionar los procesos de distribución y ventas en una empresa de consumo masivo a través de dispositivos móviles

Tutor Académico: Prof. Vincenzo Mendillo

Presentado ante la Ilustre
Universidad Central de Venezuela
para optar al Título de Especialista en
Comunicaciones y Redes de
Comunicación de Datos

Por la Lic.: Jenny Dos Reis

Caracas, Julio de 2018

RESUMEN

Por una variedad de razones de costos, flexibilidad, simplicidad y facilidades de administración, las corporaciones (y en especial las empresas de consumo masivo), están incrementando el uso de mecanismos a través de los cuales los trabajadores y el personal de ventas se puedan conectar en forma remota, a través de dispositivos móviles, desde oficinas y/o localizaciones a distancia.

El presente trabajo expone una solución para el área de distribución y ventas de una empresa de consumo masivo, que por razones de confidencialidad se llamará Empresa XYZ.

El tomo consta de nueve capítulos: el primero se refiere a la introducción y el segundo al planteamiento del problema, estableciendo de forma clara y precisa las causas del problema y los objetivos generales y específicos.

En los capítulos tres y cuatro se definen las bases de marco referencial y teórico que sustenta esta investigación. En el marco referencial se exponen los detalles, tanto de la empresa de productos masivos que es objeto este estudio, como todo lo referente a la logística de las operaciones de venta y distribución de dicha empresa. Se analizan las necesidades de seguridad de la información y cómo afrontar las amenazas, vulnerabilidades y riesgos que presentan. Se hace un estudio de los mecanismos criptográficos más usados y se hace énfasis en las facilidades y ventajas de los certificados y firmas digitales.

En el capítulo cinco se discute la factibilidad de este trabajo, a nivel económico, técnico y operativo. En el capítulo seis se propone la solución, dando explicaciones detalladas de las configuraciones e implementaciones otorgadas por las herramientas de software usadas.

En el capítulo siete se analizan los resultados obtenidos, discutiendo los logros y ventajas de la solución propuesta. Por último, los capítulos ocho y nueve exponen las conclusiones y recomendaciones.

DEDICATORIA

A mis padres, Jaime y Lucinda, por ser siempre el ejemplo y los pilares que me guían y sostienen día a día.

A mis hermanos, Jaime y Elena, por ser mis compañeros de vida, por todo su cariño y por estar a mi lado en cada momento.

A mis abuelos, Romana y Manuel, aunque físicamente ya no estén entre nosotros, por haberme inspirado con su espíritu de lucha y trabajo honesto.

A mis sobrinos, Román y Camila, por ser la energía y chispa que alegra mis días.

A toda mi familia, mis primos y tíos, por su cariño incondicional y por estar siempre a mi lado enseñándome el valor del trabajo y ayudándome a mejorar continuamente.

AGRADECIMIENTOS

Al profesor Vincenzo Mendillo por haberme brindado su experiencia y conocimientos durante el curso de la especialización y por su asesoría en la realización de este trabajo de grado.

A Gipsy Azuaje, por toda su ayuda incondicional en cada trámite requerido y por impulsarme a lograr la culminación de este trabajo de grado.

A Alejandro Ferrer y Vicente Sánchez, por haber sido más que mis compañeros de trabajo, mis mentores y amigos. A Kevin Sanabria por su dedicación y trabajo.

A Sandra Cusati y Winstom Ortega por ser mis compañeros y aliados en el transcurrir de toda la especialización.

A Pedro González por sus palabras de aliento y a Jorge Alves por apoyarme en la metodología. A Ignacio Izquierdo y Elkinomar Romero por sus gestiones en la aprobación de este tema de estudio.

A Janette Pereira, Aneliz Godoy y Anna Alloggia por estar siempre allí.

A todos mis amigos, a quienes no voy a enumerar por no querer dejar a ninguno sin mencionar, por sus palabras de aliento y por sus muestras de cariño.

A todo el que de alguna manera me apoyó y estimuló a cerrar este hito en mi carrera.

A Dios por siempre estar junto a mí, dejando una huella al lado de cada paso que doy en mi vida.

INDICE GENERAL

INTRODUCCIÓN

Debido a la alta competitividad las empresas de consumo masivo cada vez se ven más interesadas en lograr una atención directa con sus clientes, que les permita diferenciarse y lograr ventajas competitivas respecto a otras empresas del mercado.

Es por ello, que más allá de la calidad de los productos que ofrecen, es vital que se enfoquen en incrementar la efectividad de las ventas y distribución de los productos marcando la diferenciación con sus competidores, por lo que basan sus estrategias en mejorar la clase de servicio y el tipo de atención que otorguen los vendedores y despachadores de la empresa.

Para soportar las actividades de venta y obtener los resultados esperados es de vital importancia que ellas cuenten con una plataforma la cual les permita manejar de manera integrada, dinámica y segura los datos empresariales, tales como toma de pedidos, detalles de transporte de productos, manejo de almacén, generación de facturas, retorno de mercancía, re cálculo de precios, procesos de liquidación, etc.

La empresa de consumo masivo, que por razones de confidencialidad se llamará Empresa XYZ, posee ya una solución que gestiona estas actividades pero, fortaleciéndose en el auge de la tecnología, ha emprendido un proyecto a fin de evaluar, analizar, diseñar e implantar una nueva solución, la cual debe suministrar un medio seguro, confiable y a menor costo, por medio del cual se pueda compartir información relevante de las operaciones de venta y distribución, entre trabajadores, oficinas a distancia, usuarios móviles y clientes.

Adicionalmente la empresa busca posicionarse en una plataforma más dinámica que permita incorporar cambios en las operaciones de venta de manera eficiente, rápida y sencilla, así como también mayor flexibilidad en el manejo de distintos tipos de dispositivos móviles (Hand-Held, IPhone, Android, etc.) que soporten dichas operaciones.

Actualmente y cada vez más se buscan aplicaciones ligeras y granulares que sean capaces de funcionar en cualquier dispositivo móvil y no sólo en los puntos de venta (Personal Digital Assistant - PDA) actuales.

Con este mundo tecnológico tan cambiante y con la incorporación de nuevos dispositivos inteligentes en el mercado, las necesidades de resguardar la información en la Empresa XYZ son cada vez mayores, por lo cual los esquemas de seguridad que garanticen las operaciones y datos corporativos

deben ser mucho más robustos y se busca que incluyan, entre otros aspectos, aplicaciones criptográficas y en especial facilidades de certificados y firmas digitales.

La criptografía es el arte y ciencia de hacer que un sistema (“criptosistema”) sea capaz de manejar la información de forma segura. Entre los servicios más comunes que provee la criptografía están la confidencialidad, integridad y autenticación de los datos [Tutorials Point, 2015].

Para suministrar estas funcionalidades es necesario “certificar” la información. La certificación es el proceso de ligar una clave pública a los datos de su propietario. Esta actividad la realiza una entidad llamada Autoridad de Certificación (CA “Certification Authority”). Una CA, por lo tanto, es un tercer ente de confianza que acepta y reconoce los dos entes implicados en la comunicación [Mendillo, 2016].

Un certificado digital (también llamado identificador digital o en inglés digital ID) es un documento electrónico que contiene datos de identificación de una persona o entidad (empresa, servidor Web, etc.) y la clave pública de la misma, haciéndose la Autoridad de Certificación responsable de la autenticidad de los datos que figuran en el certificado [Mendillo, 2016].

La mayoría de los certificados digitales que se usan hoy día en las transacciones electrónicas seguras son del tipo X.509, el cual es un estándar de la Unión Internacional de Comunicaciones (UIT) para la infraestructura de clave pública (Public Key Infrastructure o PKI). X.509 es la pieza central de la PKI ya que enlaza la clave pública con los datos que permiten identificar al titular [Palomeque, 2015].

La firma digital consiste en la transformación de un mensaje utilizando un sistema de cifrado asimétrico de manera que la persona que posee el mensaje original y la clave pública del firmante, pueda establecer de forma segura que dicha transformación se efectuó utilizando la clave privada correspondiente a la clave pública del firmante y si el mensaje es el original o fue alterado desde su concepción [Palomeque, 2015].

La alternativa planteada como solución en este proyecto, se basa en dos plataformas de software de SAP [https://www.sap-ag.de, 2016]. La primera de ellas se denomina SAP AFARIA, que es un producto de software para gestión de dispositivos móviles, que ayuda en el manejo de políticas de seguridad y mantenimiento de los mismos [https://support.sap.com, 2016].

La segunda herramienta también es un producto de software de intercambio (middleware), llamada SMP (SAP Mobile Platform) [https://www.sap-ag.de, 2016]. Básicamente esta herramienta SMP facilita la tarea de diseñar, crear y proporcionar aplicaciones (apps), que manejen el flujo de datos empresariales, desde y hacia los dispositivos móviles, garantizando tanto las operaciones transaccionales como la integración con otras plataformas empresariales de forma segura.

En base a lo antes expuesto, en el presente trabajo de grado se cubrirán los fundamentos y bases teóricas sobre políticas de seguridad de la información de sistemas. Se ahondará especialmente en el manejo de certificados y firmas digitales, que son suministradas en la alternativa de SAP planteada y que constituyen un medio para garantizar la seguridad en el flujo de las operaciones.

Por otra parte, y no menos importante, existe la necesidad de la empresa de contar con herramientas de monitoreo que garanticen la correcta transmisión de la información de las operaciones y de proveer mecanismos de auditoría y detección de ataques que eviten posibles fraudes o robos.

CAPITULO II. PLANTEAMIENTO DEL PROBLEMA Y OBJETIVOS

2.1- Planteamiento del Problema

Para dar mayor efectividad a sus actividades de venta y distribución la empresa de consumo masivo, la Empresa XYZ, necesita incorporar cambios en sus procesos de Despacho Directo a Tiendas (DSD por sus siglas en inglés - Direct Store Delivery) de forma rápida, fácil y dinámica. Esto permitirá entre otras cosas, satisfacer las necesidades cambiantes del mercado, que los productos sean entregados directamente a los clientes de forma más eficiente y que se incremente la interacción de los despachadores con esos clientes, lo que se traduce en otorgar un mejor servicio.

Actualmente dicha empresa tiene la necesidad de garantizar que sus trabajadores del área de ventas, cuenten con la información necesaria para soportar las operaciones de ventas con sus clientes, de una forma más rápida, segura, confiable y a un menor costo. Esta corporación posee ya una plataforma que brinda soporte a sus operaciones de venta y distribución.

Esta plataforma se basa en soluciones de software de la empresa SAP AG (System, Applications and Products), una empresa multinacional alemana con sede en Walldorf). [https://www.sap-ag.de, 2016]

La aplicación SAP Mobile Direct Store Delivery (SAP mDSD 3.0) de la solución Consumer Product de la empresa SAP AG funciona bajo el sistema SAP ERP (SAP Enterprise Resource Planning) y permite a la fuerza de ventas realizar toma de pedidos y despacho, directamente de los puntos de venta (Personal Digital Assistant PDA) a través del uso de dispositivos móviles (DM), soportando así el trabajo de la fuerza de venta de la empresa [https://help.sap.com, 2016].

El proceso de DSD de SAP comprende actividades tanto a nivel de “Backend” (sobre SAP ERP en servidores empresariales) así como a nivel del dispositivo móvil (DM). [Szabo, 2006].

Principalmente a nivel de “Backend” se tienen funciones como toma de pedidos, planificación de rutas, planificación de recargas, re cálculo de precios, etc. Al mismo tiempo el dispositivo móvil es utilizado para soportar la gestión en el punto de venta e intercambiar información con el sistema SAP ERP mediante sincronización en línea [Szabo, 2006].

El intercambio de información entre el “Backend” y el dispositivo móvil DM es realizado a través de una aplicación que permite dicha transferencia de información entre las diferentes plataformas involucradas. Esta herramienta “middleware” es otorgada a través del componente de software SAP Mobile Engine (MI) que también es de la plataforma de productos de software SAP [https://www.sap-ag.de, SAP 2016].

La plataforma MI tiene algunas limitantes en las facilidades del manejo y control del software que va hacia los dispositivos móviles, así como también presenta cierta “rigidez” al querer incorporar nuevos modelos de dispositivos móviles (actualmente, solo se manejan Hand Helds (HH) con Windows Mobile).

La rápida penetración de los teléfonos inteligentes multi-funcionales (“smart phones”) en el mercado (iPhone, Android, Blackberry, Nokia, Windows 7 mobile devices, etc.) y las mejoras en la velocidad de conexión de datos 3G (Tercera Generación) ha hecho necesario replantearse las primeras estrategias que se adoptaron, las cuales estaban orientas a aplicaciones móviles que trabajarán sobre dispositivos industriales (tales como los Hand Held antes mencionados).

Por todas estas razones se ubicó como alternativa una solución más flexible y robusta que se basa en inclusión de nuevos componentes de software en el “ Backend”, en adecuaciones (“customizing”) para reflejar los requerimientos propios de las operaciones de la empresa y en sustitución de la plataforma “middleware” MI por dos herramientas con mayor versatilidad de la plataforma de productos de SAP [https://www.sap-ag.de, SAP 2016].

La primera de ellas se denomina SAP AFARIA. Es un producto de software para gestión de dispositivos móviles que ayuda en el manejo de políticas de seguridad y mantenimiento de los mismos [https://help.sap.com, 2016].

La segunda herramienta también es un producto de software de intercambio “middleware” llamada SMP (SAP Mobile Platform). Básicamente esta herramienta SMP facilita la tarea de diseñar, crear y proporcionar aplicaciones (App) que manejan el flujo de datos empresariales (“Backend”) hacia los dispositivos móviles (DM), garantizando así el flujo de trabajo y la integración con otras plataformas empresariales de forma segura [https://help.sap.com, 2016].

En este trabajo de grado propone una solución para garantizar el intercambio seguro entre los datos empresariales del “Backend” (SAP ERP), el middleware (SMP) y los dispositivos móviles (DM).

Un aspecto importante de esta solución es que se enriquece la solución actual pues se facilita y flexibiliza la comunicación para la corporación apoyando a la gestión de ventas, la toma de decisiones y minimizando los costos.

2.2- Objetivo General

Diseñar e Implantar una solución segura que soporte las actividades de venta (DSD) de la empresa de consumo masivo Empresa XYZ a través de las herramientas AFARIA y SMP de SAP, garantizando el acceso a la información y el correcto flujo de las actividades de venta y usando diferentes mecanismos de seguridad de datos entre los cuales se destacan el uso de certificados y firmas digitales. De este modo se satisfarán las necesidades de intercambio de información y de datos transaccionales entre sus trabajadores, oficinas, localidades remotas y clientes a través de dispositivos móviles de forma segura y confiable.

2.3.- Objetivos Específicos

- Estudiar la plataforma instalada en la empresa de consumo masivo Empresa XYZ para plantear necesidades de una mejor solución.

- Analizar las tecnologías de seguridad de sistemas, las políticas de seguridad y en especial el uso y manejo de certificados y firmas digitales.

- Determinar qué información confidencial se desea proteger, e implantar el mecanismo para llevar a cabo dicha tarea y la posibilidad de manejar documentos a través de firmas digitales.

- Ofrecer de una manera efectiva una solución que aporte la información requerida al área de ventas y que facilite las operaciones entre los vendedores y sus clientes a través de dispositivos móviles.

- Contar con herramientas de monitoreo y generación de reportes, que permitan hacer seguimiento del flujo correcto de las operaciones y se brinden mecanismos para auditorias y prevención de ataques, fraudes o robos.

CAPITULO III. MARCO REFERENCIAL

3.1 Sistema SAP ERP

El sistema de información ERP (Enterprise Resource Planning) es un sistema de gestión de recursos empresariales que suministra un conjunto de aplicaciones que de forma interactiva integra las funciones de una empresa [https://help.sap.com, 2017].

Las siglas SAP (System, Applications and Products) identifican a una compañía de sistemas informáticos en Alemania, con sede en Walldorf, Baden-Württemberg, dedicada al diseño de productos de software para la gestión empresarial. [https://www.sap-ag.de, 2017]

Entre las ventajas del sistema de información SAP ERP se encuentran, incorporar procesos más eficientes al negocio, control de costos más ajustados y un buen servicio al cliente.

El sistema SAP ERP se basa en el concepto de combinar todas las actividades de negocio y los procesos técnicos de una empresa en una solución informática simple, integrada, robusta y confiable.

Algunas de las ventajas más resaltantes que se pueden mencionar es que las transacciones y consultas se realizan en tiempo real, integra las funciones claves y los procesos de negocio, permite un manejo uniforme y consistente de la información, otorga flexibilidad, etc.

En cuanto a las desventajas podemos mencionar los altos precios de adquisición de hardware y licenciamiento del software, los largos tiempos que involucran una implantación, el costo elevado que implica llevar a cabo tanto las tareas de mantenimiento, así como también el entrenamiento del personal especializado para llevar a cabo dichas tareas.

El sistema SAP ERP está organizado en una arquitectura cliente/servidor a tres capas o niveles (Presentación, Aplicación y Base de Datos). Se caracteriza por tener un sistema centralizado con una base de datos común [https://help.sap.com, 2017].

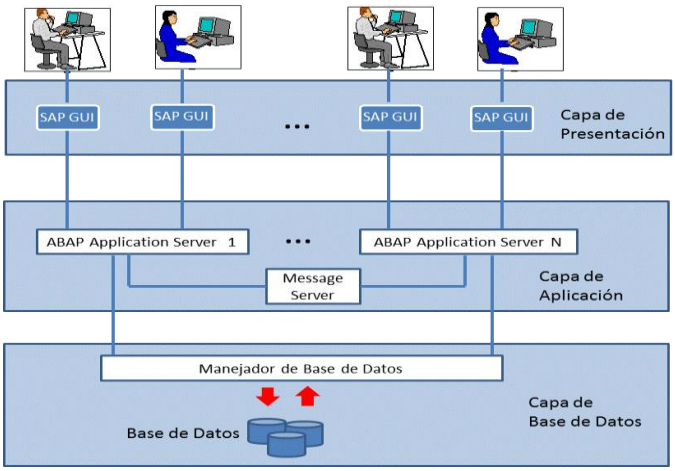


Figura 3.1.1. Arquitectura de tres capas de SAP ERP

Entre los sistemas operativos con los que es compatible podemos mencionar HP-UX, AIX, Linux, Open VMS, Windows Server, IBM OS/400, IBM S/390, etc. [https://support.sap.com, 2017]

Así mismo a nivel de base de datos puede ser instalado sobre SAP HANA, MAX DB, Sybase ASE, Informix, Oracle, Microsoft SQL Server, etc. [https://support.sap.com, 2017]

Los módulos de aplicación tienen una arquitectura común y la misma interfaz con el usuario. Entre las interfaces tipo “front-end” más comunes podemos mencionar SAPGui, Windows, Java mulltiplataforma, Macintosh, etc. [https://support.sap.com, 2017]

Estos módulos de aplicación soportan todas las transacciones de negocios de la empresa y están integrados en forma interactiva.

En consecuencia, un cambio en un módulo de aplicación automáticamente modificará los datos en los otros módulos involucrados.

Los componentes o módulos más comunes de éste sistema de información SAP ERP incluyen las funciones de finanzas, planificación, costos, comercial, mercadeo, manufactura, logística, mantenimiento, control de calidad y recursos humanos. [https://www.sap-ag.de, 2017]

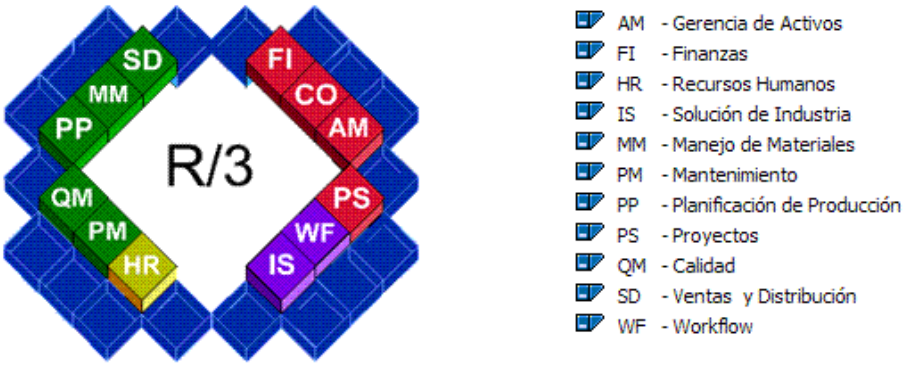


Figura 3.1.2. Módulos de SAP ERP

3.2 La solución de Direct Store Delivery (DSD) para la industria de consumo masivo

Direct Store Delivery (DSD) es un proceso de negocio empleado en la industria de productos de consumo masivo para distribuir bienes directamente al cliente. En un proceso de DSD la distribución no involucra mayoristas, distribuidores o centros de distribución de clientes [Szabo, 2006]. La implementación de un sistema DSD permite a las empresas:

- Rápido despacho de materiales a tiendas y clientes en general (Por ejemplo: productos de alimentos y bebidas)
- Contacto directo con los clientes al momento del pedido y despacho
- Integración de una solución móvil de la gestión de despacho
- Optimizar el proceso de liquidación en ventas y distribución
- Optimizar los costos logísticos por medio de la planificación efectiva de visitas a los clientes.

SAP ofrece una solución para dar soporte al proceso de ventas usa una aplicación DSD basada en la entrega directa a los clientes, permitiendo el intercambio de información entre el sistema central empresarial y un dispositivo móvil. [SAP Help DSD, 2016].

La solución comprende tres componentes básicos: en el “Backend” como parte del sistema SAP ERP (sistema de gestión empresarial) en donde se ejecutan todos los procesos básicos del negocio como son: ventas, movimiento de inventario, mantenimiento, contabilidad, etc. El otro componente es una aplicación móvil también referida como “frontend” que brinda soporte a los Representantes De Venta (RDV) en su gestión de ventas. El “Backend” y el dispositivo móvil trabajan en conjunto para cubrir todas

las áreas involucradas en la gestión de ventas y distribución incluyendo las etapas de antes, durante y después de la gestión de ventas. El tercer componente trabaja como un habilitador o plataforma de intercambio “Middleware” que es quién finalmente permite la transferencia de datos entre el “ Backend” y el dispositivo móvil DM. [https://help.sap.com, 2017].

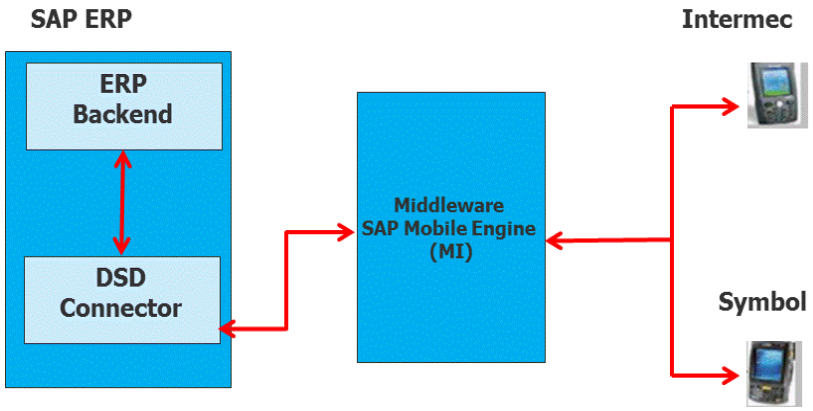


Figura 3.2.1 Arquitectura de solución SAP Mobile DSD

Como se mencionó anteriormente en el “Backend” se mantienen y administran todos los datos correspondientes a la operación comercial y solamente se envía al dispositivo móvil los datos pertinentes a la ruta de ventas que se tenga planificada para un día en particular. A este intercambio de información se le conoce con el nombre de “sincronización” y se lleva a cabo conectando el dispositivo móvil al “Backend” a través de la red nacional de Empresa XYZ. Esta conexión puede hacerse a través de una “cuna”, con módem vía VPN (Virtual Private Network) o de forma inalámbrica. La sincronización tiene dos etapas:

- **Download:** Proceso de transmisión de información del “Backend” hacia el dispositivo móvil.
- **Upload:** Proceso de transmisión de información desde el dispositivo móvil hacia el “Backend”.

Figura 3.2.2. Procesos de sincronización SAP Mobile DSD

Al igual que en los demás módulos de SAP ERP en la aplicación DSD se tienen componentes que son propios de éste módulo, pero interactúan constantemente con los componentes de los módulos de ventas, logística, finanzas, etc., lográndose una integración completa a lo largo de todos los procesos de la empresa bajo una misma plataforma tecnológica. [Szabo, 2006].

3.2.1 Datos Maestros

En los datos maestros para el componente de DSD “Backend” se mantienen datos específicos que permanecen inalterados por períodos considerables y que a su vez contienen información que se necesita constantemente para control.

3.2.2 Control de Visitas

El control de visitas del “Backend” de DSD es utilizado para planificar la periodicidad de las visitas recurrentes de los clientes por parte de la fuerza de ventas. El control de visitas presenta dos componentes: uno táctico (planificación de visitas) y uno operacional (lista de visitas).

La planificación de visitas a los clientes consiste en determinar los clientes que deben ser despachados un día específico de la semana, el orden o la secuencia en que se deben visitar, y los conductores y vehículos que se usarán para tal fin.

La lista de visitas se usa para determinar el total de clientes pertenecientes a una ruta que serán visitados en una fecha específica. Esta lista es de gran importancia, pues determina la información que será bajada al dispositivo móvil.

3.2.3 Planificación Dinámica de transporte

En este componente se consolidan en transportes de despacho las entregas provenientes de pedidos hechos por clientes. Se le llama dinámica ya que al crear los transportes se toman en consideración: las listas de visitas, datos maestros de la ruta y la capacidad de los vehículos, y basado en esta información, se crean transportes de despacho optimizados que pueden atender clientes diferentes con despachadores y vehículos diferentes en cada oportunidad.

3.2.4 Contabilidad de Rutas (Route Accounting)

Una vez que los vehículos han sido cargados y la fuerza de ventas empieza su gestión comercial, todos los materiales montados en el camión deben mantenerse contados y contabilizados, todas las

salidas y entradas de mercancía al camión deben registrarse en el dispositivo móvil. De manera tal que se pueda dar seguimiento a los inventarios y cobranzas de las rutas y tener un manejo efectivo de las pérdidas.

El proceso de contabilidad de rutas termina cuando todas las transacciones de la ruta han sido completadas. La contabilidad de las rutas de DSD soporta despachos y ventas de ruta utilizando:

- Documentos e información específica de cada ruta
- Entrada de datos de control salientes y entrantes
- Entrada de documentos e información que los vendedores (con distintos roles) entregan a la oficina de liquidación después de su ruta.
- Liquidación de documentos y datos ya disponibles en SAP ERP
- Liquidación de documentos y con datos que pueden ser introducidos en SAP ERP

La contabilidad de rutas es una solución off-line, lo que quiere decir que el intercambio de información solo ocurre al final del procesamiento de la ruta, no es posible el intercambio de datos durante la ruta. Por lo cual, al regresar de sus respectivas rutas, la fuerza de ventas entrega todos los documentos referentes a la misma a la oficina de liquidación y en este momento se registran los pedidos de los clientes, cobranzas realizadas, devoluciones, etc.

En Empresa XYZ sólo los vendedores están dotados con dispositivos móviles, por lo cual solo deben realizar una sincronización del dispositivo móvil (DM) para subir los datos de la ruta al “Backend” y se reflejará en la transacción de liquidación (conocida como “cockpit de liquidación” o “settlement cockpit”). Los despachadores realizan su gestión de manera “manual”, es decir los datos de su ruta son introducidos manualmente en la transacción de liquidación en el “Backend”.

En el “cockpit” de liquidación, de ser necesario, se modifican los datos que suben desde el dispositivo móvil, y una vez conforme se liquida la ruta. En este momento se crea todo el flujo de documentos correspondiente a la ejecución de la ruta y los demás módulos reciben la información necesaria para generar los documentos que corresponda. Por ejemplo, en el módulo de ventas se crean los pedidos, facturas, etc., en el módulo de logística, se contabilizan las entradas y salidas de mercancía, inventario, etc.

3.3 La aplicación SAP Mobile Engine (MI)

SAP introdujo a comienzos de los años 2000 una aplicación denominada SAP Mobile Engine (MI), que es una plataforma abierta para aplicaciones empresariales móviles. Está diseñada para soportar las

operaciones SAP Mobile de la organización, pero puede también ser usada para soluciones móviles distintas de las soluciones móviles de SAP.

SAP MI es una plataforma que provee un componente que es instalado localmente en el dispositivo móvil, incluye un Web Server, una capa de base de datos y su propia lógica del negocio. El dispositivo puede operar de manera "offline" y no tiene que esperar por una conexión de red para completar las aplicaciones críticas del negocio.

Tiene inmerso un modelo de datos denominado "SyncBo" ("Syncronizer Business Object") donde se replican los datos almacenados en la base de datos del "Backend" hacia los dispositivos móviles.

SAP NetWeaver Application Server es una solución que funciona como un servidor de aplicaciones Web para las soluciones SAP. Estos servidores de aplicaciones ejecutan aplicaciones ABAP (Advanced Business Application Programming) y se comunican con los componentes de presentación, la base de datos y también entre sí, utilizando un servicio de mensajes.

El MI es parte de la solución de SAP NetWeaver Application Server que usa tanto una plataforma java J2EE[1] (Java 2 Platform Enterprise Edition) y un "stack" ABAP (Advanced Business Application Programming). Funciona como una plataforma de intercambio "Middleware", que permite la transferencia de datos desde el "Backend" al dispositivo móvil y viceversa, para lo cual usa unos "mapas" basados en los SyncBo. SAP MI ofrece herramientas para la sincronización y replicación de los datos que garantizan la consistencia de los datos desde el dispositivo al "Backend" y viceversa.

SAP MI está basada en dos estándares abiertos de la industria que son Java[2] y XML[3] (eXtensible Markup Language)

A través de la máquina virtual de Java provee un modelo de programación abierto sobre el cual se pueden desarrollar aplicaciones móviles en el dispositivo.

Esta arquitectura hace la plataforma independiente tanto para dispositivos móviles como para la red. Soporta dispositivos tales como PDAs (Personal Digital Assistants), laptops y Smart Phones [https://help.sap.com/, 2016].

[1] Java Platform, Enterprise Edition o Java EE: es una plataforma de programación para desarrollar y ejecutar software de aplicaciones en el lenguaje de programación Java.

[2] Java es un lenguaje de programación orientado a objetos que fue diseñado para tener pocas dependencias de implementación

[3] XML eXtensible Markup Language es un lenguaje que permite almacenar datos de forma legible y se propone como un como un estándar para el intercambio de información entre diferentes plataformas.

3.4. La aplicación móvil SAP mDSD

La aplicación móvil dentro de la solución de DSD lleva el nombre de SAP mDSD (por sus siglas en inglés de Mobile Direct Store Delivery). Esta aplicación cubre las necesidades de los vendedores y despachadores en las situaciones de despacho directo en tienda y soporta todas las operaciones que se deben hacer en el punto de venta, brindándole a los RDV (Representantes de Venta) las herramientas necesarias para poder prestar un mejor servicio a los clientes. [Szabo, 2006].

La aplicación mDSD se ejecuta en un dispositivo móvil de tipo PDA (Personal Digital Assistant), de manera desconectada o "off-line". Esto quiere decir que no hay un intercambio de datos entre el dispositivo móvil y el "Backend" durante el procesamiento de la ruta. Este intercambio solo ocurre al inicio y al final del día mediante el mecanismo de sincronización contra SAP Mobile Infrastructure (MI). [Szabo, 2006].

Estas son algunas funcionalidades de la aplicación móvil:

- "Check out": los supervisores de almacén pueden validar las cantidades de productos cargadas en el camión previo a su salida en ruta y reportar diferencias respecto a la carga planificada.
- "Check in": los supervisores de almacén pueden registrar en el dispositivo móvil las cantidades de productos y dinero presentes en el camión a su regreso de la ruta.
- Procesamiento de órdenes, facturas y entregas.
- Cobros a clientes y gastos al conductor.
- Ventas directas desde el camión (auto ventas).
- Toma de órdenes para entregas futuras (preventa).
- Toma de devoluciones.
- Reportes de rendimiento y procesamiento de rutas.
- Intercambio de datos hacia el "Backend".

Con la aplicación móvil SAP mDSD, se cubren todos los pasos de los procesos de ventas y distribución DSD en el sistema SAP ERP, obteniéndose una visión completa de todos los eventos que se llevan a cabo desde la toma de pedidos hasta la cobranza del cliente (order-to-cash process).

3.5 Proceso de venta y distribución

Como se mencionó anteriormente en Empresa XYZ, se opera bajo dos esquemas de venta y distribución: auto venta y preventa. [Szabo, 2006].

3.5.1 Auto venta

El proceso de auto venta describe el trabajo diario de los Representantes de Venta (RDV) en el que salen de ruta para visitar una lista de clientes previamente determinada por el negocio. Estos clientes, según sus características y por el volumen de ventas que generan, se pueden clasificar en bodegas, abastos, charcuterías, kioskos y en general, tiendas detallistas, cuyos pedidos de venta sean menores en volumen a 400 Kg.

A los clientes se les venden productos contenidos en el camión llevando a cabo la negociación, facturación, cobranza y despacho, manejo de devoluciones y gestión del material POP (Point of Purchase). Este material POP, literalmente “punto de compra”, corresponde a los implementos destinados a promocionar la empresa y se entregan como regalos a los clientes. [Szabo, 2006].

Por otro lado, es su responsabilidad chequear el inventario del cliente al igual que el precio de venta sugerido y ordenar los productos en el anaquel siguiendo la táctica de FIFO (first in-first-out) basados en la fecha de vencimiento. El RDV de Auto venta, cuenta también con un ayudante (Mercaderista) quien se encarga del despacho de los productos, su colocación en los anaqueles y en el almacén del cliente, el manejo de material POP y que la carga de los camiones sea la adecuada para la ruta de ventas.

La gestión de auto ventas se compone a su vez de varios subprocesos: Preparar Auto venta, Ejecutar Auto venta y Liquidar Auto venta.

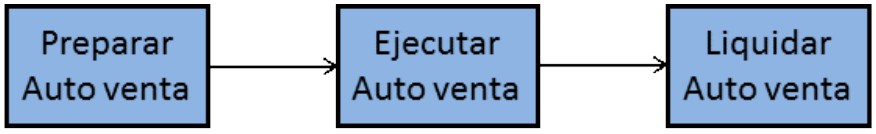


Figura 3.5.1.1 Subprocesos de Auto venta [Szabo, 2006].

3.5.1.1 Preparar auto venta

Este subproceso describe los pasos que se deben llevar a cabo para preparar la ruta diaria de visita de los representantes de venta. Estos pasos son necesarios para generar los documentos que serán utilizados, por la aplicación móvil durante el recorrido de ventas. [Szabo, 2006].

Los procesos relacionados con preparación de auto venta son:

- Generar y ajustar inventario meta por cliente
- Calcular carga planificada
- Verificar disponibilidad de inventario y generar guía de carga
- Preparar mercancía y cargar
- Preparar Kit de “Merchandandising” para la Ruta
- Sincronizar dispositivo móvil (“Download”)

3.5.1.2 Ejecutar auto venta

La ejecución de la auto venta describe las actividades que deben llevar a cabo los RDV una vez que están en el PDV (Punto de Venta). Todas las actividades se realizan en el dispositivo móvil. [Szabo, 2006].

Estas actividades están representadas en una secuencia de procesos que el RDV sigue durante la ejecución de la negociación en el PDV. Ellos son:

- Seleccionar clientes de la ruta
- Analizar situación del cliente
- Analizar documentos pendientes
- Tomar inventario del cliente
- Generar pedido sugerido
- Registrar pedido definitivo
- Generar devolución de productos en mal estado
- Generar devolución de productos en buen estado
- Crear notas de débito/crédito
- Registrar cobranza/emitir recibo
- Emitir factura
- Despachar producto

3.5.1.3 Liquidar auto venta

Este subproceso describe todos los pasos que deben ser llevados a cabo de una vez que el RDV retoma a la sucursal al final de la jornada de ventas. [Szabo, 2006]. En la Liquidación de auto venta se contemplan las siguientes actividades:

- Registrar ingreso al camión

- Registrar información de cierre de ruta
- Registrar cobranza
- Registrar inventario final
- Sincronización del dispositivo móvil
- Contabilización de la ruta
- Entrega documentación de venta

3.5.2 Preventa

Bajo este esquema de ventas, el RDV visita a una lista de clientes previamente establecida por el negocio, por lo general tiendas y establecimientos que realizan pedidos de mayor volumen como es el caso de las cadenas de supermercados, los hipermercados, tiendas mayoristas, etc. [Szabo, 2006].

A los clientes atendidos bajo esta modalidad se les toman pedidos que serán despachados en una visita posterior. En el PDV el RDV lleva a cabo la negociación con el cliente, la cual parte de un pedido sugerido que le hace éste al cliente y modifica de acorde con las necesidades del cliente. De esta manera, el RDV registra los pedidos de los clientes que visita, así como también registra los pedidos de devolución y las cobranzas, que posteriormente son cargados al "Backend" donde son procesados y convertidos en entregas, que son luego despachadas a los clientes mediante el uso de transporte contratados a terceros. En este caso, los camiones de despacho van cargados con la mercancía exacta a despachar para cada cliente y deben recoger los pedidos de devolución que registró el RDV en la visita anterior. Como se mencionó anteriormente, el RDV de preventa, al igual que el de auto venta, hace uso de un dispositivo móvil, en el que registra toda la información asociada a los procesos ya descritos, la cual es luego intercambiada con el sistema "Backend". [Szabo, 2006].

La gestión de preventa se compone a su vez de varios subprocesos: Preparar Preventa, Ejecutar Preventa, Liquidar Preventa, Preparar Despacho de Preventa y Liquidar Despacho de Preventa.

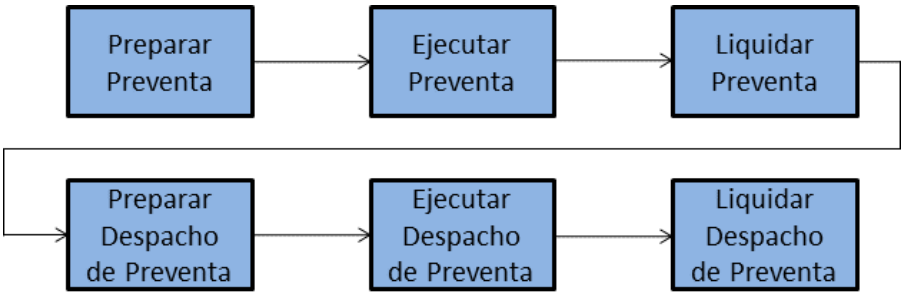


Figura 3.5.2.1 Subprocesos de Preventa [Szabo, 2006].

A continuación, se dará una breve descripción de cada uno de ellos:

3.5.2.1 Preparar preventa

Este subproceso describe los pasos que se deben llevar a cabo para preparar la ruta diaria de visita de los representantes de venta. Estos pasos son necesarios para generar los documentos que serán utilizados por la aplicación móvil durante el recorrido de ventas. [Szabo, 2006].

Los procesos relacionados con Preparación de Preventa son:

- Generar y ajustar inventario meta por cliente
- Sincronizar dispositivo móvil (“Download”)

3.5.2.2 Ejecutar preventa

La ejecución de la preventa describe las actividades que deben llevar a cabo los RDV una vez en el PDV. Todas estas actividades se realizan en el dispositivo móvil. [Szabo, 2006].

Estas actividades están representadas en una secuencia de procesos que el RDV sigue durante la ejecución de la negociación en el PDV. Ellos son:

- Seleccionar de clientes según la ruta
- Analizar situación del cliente
- Analizar documentos pendientes
- Tomar inventario del cliente
- Generar pedido sugerido
- Registrar pedido definitivo
- Registrar pedido de devolución de productos en mal estado
- Registrar pedido de devolución de productos en buen estado
- Crear notas de débito/crédito
- Registrar cobranza/emitir recibo
- Emitir documento de pedido

3.5.2.3 Liquidar preventa

Este subproceso describe todos los pasos que deben ser llevados a cabo una vez que el RDV retorna a la sucursal al final de la jornada de ventas. [Szabo, 2006].
En la liquidación de Preventa se contemplan las siguientes actividades:

- Registrar información de cierre de ruta
- Registrar cobranza
- Sincronización del dispositivo móvil
- Contabilización de ruta

3.5.2.4 Preparar despacho de preventa

Este subproceso describe los pasos que se deben llevar cabo una vez tomados los pedidos y procesados al "Backend". [Szabo, 2006].

En este subproceso se contemplan las siguientes actividades:

- Planificación de rutas de despacho mediante planificación dinámica
- Generación de guías de despacho
- Generación de guía de despacho (entregas y devoluciones)
- Carga de camión

3.5.2.5 Ejecutar despacho de preventa

Este subproceso describe precisamente el despacho de los pedidos realizados por los clientes durante la ejecución de la preventa. [Szabo, 2006].

En este subproceso se contemplan las siguientes actividades:

- Seleccionar cliente de la ruta
- Entrega de productos ordenados durante la ejecución de la preventa
- Recepción de productos devueltos por el cliente y registrados por el RDV durante la ejecución de la preventa

3.5.2.6 Liquidar despacho de preventa

Este subproceso describe las actividades que deben realizar los despachadores, una vez que hayan vuelto a la sucursal después de la ejecución de la ruta de despachos del día. [Szabo, 2006].

Como se mencionó anteriormente, los despachadores no llevan consigo un dispositivo móvil para la ejecución de la ruta por lo tanto las actividades de liquidación que se mencionan a continuación, son diferentes a las mencionadas en los otros procesos:

- Registrar ingreso de camión
- Registrar información de cierre de ruta
- Registrar inventario final
- Copia manual del transporte al cockpit de liquidación
- Contabilización de ruta

3.6 SAP AFARIA

SAP Afaria es un sistema de gestión de dispositivos móviles (Mobile Device Managenent MDM) que permite proteger y administrar los dispositivos móviles, las aplicaciones móviles y los datos de la organización [https://help.sap.com/, Afaria Overview, 2013].

SAP Afaria permite conectarse remotamente a dispositivos móviles registrados con Afaria para configurar el dispositivo e instalar las aplicaciones requeridas.

Entre sus principales funciones están:

- **Puede proteger los dispositivos y los datos del dispositivo.**

Afaria incluye una serie de características y tecnologías para asegurar dispositivos registrados. Por ejemplo, Afaria aprovecha las infraestructuras de seguridad existentes en la red empresarial, como Active Directory[4] y LDAP[5], para garantizar que sólo los usuarios conocidos por la red puedan acceder a la red. También utiliza certificados para asegurar conexiones entre el servidor de Afaria y el dispositivo. Por último, Afaria puede aprovechar las funciones de seguridad del dispositivo, por ejemplo, para reforzar una contraseña o cifrar un dispositivo que almacena datos corporativos confidenciales. También se puede utilizar Afaria para bloquear de forma remota dispositivos perdidos o robados e incluso "limpiar" el dispositivo de datos corporativos. [https://help.sap.com/, Afaria Overview, 2013].

- **Configurar los dispositivos para que cumplan con los estándares corporativos.**

[4] Active Directory (AD) o Directorio Activo son los términos que utiliza Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadores.
[5] Lightweight Directory Access Protocol (LDAP) es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido

A través de Afaria se pueden definir y mantener atributos y configuraciones de dispositivos para asegurar que los dispositivos móviles están configurados correctamente para la red empresarial. Por ejemplo, Afaria puede administrar la configuración de ActiveSync[6], incluida la configuración de conexión y las opciones de sincronización. También se puede utilizar para configurar remotamente configuraciones de conexión, como detalles sobre el servicio de red, las direcciones de servidor y el inicio de sesión. Las opciones de sincronización para la información de correo electrónico, calendario e información de contacto se pueden configurar de forma centralizada y se aplican en los dispositivos cliente. [https://help.sap.com/, Afaria Overview, 2013].

- **Administrar aplicaciones móviles.**

Puede asegurar que todos los dispositivos cuentan con las últimas versiones del software necesario. Afaria facilita la distribución, instalación y mantenimiento de aplicaciones móviles, aplicaciones internas y disponibles públicamente en una tienda de aplicaciones como la Apple Store App[7] o Google Play Store[8]. La capacidad de Afaria para instalar aplicaciones, suministrar archivos perdidos o dañados y desinstalar o revertir aplicaciones significa que todos los empleados tendrán las versiones correctas, las últimas actualizaciones y la configuración adecuada en todo momento. [https://help.sap.com/, Afaria Overview, 2013].

- **Controlar los activos corporativos e informar sobre el uso de dispositivos móviles.**

Con Afaria, se puede ver el inventario de dispositivos, incluyendo quién está utilizando el dispositivo, qué software está instalado y qué configuraciones están configuradas. Soporta los sistemas operativos Android, iOS, Windows, Windows CE, Windows Mobile, Windows Phone y Windows en los dispositivos del cliente. [https://help.sap.com/, Afaria Overview, 2013].

3.6.1 Arquitectura de SAP AFARIA

Afaria es un sistema de gestión de dispositivos móviles distribuido que consiste en una serie de componentes de software separados.

Los componentes principales son el Servidor Afaria, la Consola de Administración Afaria, el Servidor de Inscripción, el Servidor de Paquetes y la base de datos Afaria. [https://help.sap.com/, Afaria Overview, 2013].

6 ActiveSync es un programa de sincronización de datos desarrollado por Microsoft
7 Apple Store App es un servicio para iPhone que permite a los usuarios buscar y descargas aplicaciones de Apple
8 Google Play Store es una plataforma de distribución de aplicaciones móviles para dispositivos con Android

La solución Afaria es altamente escalable y puede soportar instalaciones muy grandes. Puede instalar Afaria en un único servidor (“standalone" o autónomo) para instalaciones pequeñas o distribuir Afaria a través de varios servidores para instalaciones más grandes.

Para grandes instalaciones, se pueden instalar varios Servidores Afaria en un escenario de granja. En este escenario el primer Afaria Server que instale es el servidor "maestro". Servidores adicionales de Afaria se denominan servidores de “granjas” o “farms”. El servidor maestro puede hablar con varios servidores de la granja de servidores para gestionar el equilibrio de carga y admitir cientos de miles de conexiones remotas con los dispositivos gestionados. En este entorno, Afaria puede sincronizar contenido a través de servidores distribuidos, que pueden estar ubicados en diferentes ubicaciones. Cualquier servidor con el que el cliente se comunica tiene la misma funcionalidad. [https://help.sap.com/, Afaria Overview, 2013].

En un escenario “Afaria Server Farm”, el Servidor de origen (Source Server o maestro) es el servidor donde se crean, editan y administran todos los canales. Estos canales se replican a los servidores de destino (o esclavos) en la granja de servidores. Los clientes de Afaria pueden conectarse a cualquier servidor de la comunidad y ejecutar los canales asignados. Esto proporciona un tipo de solución de equilibrio de carga si tiene muchos clientes programados para conectarse al mismo tiempo. Los grupos de clientes pueden conectarse a cualquier servidor de la comunidad para ejecutar los canales necesarios.

Un entorno de Servidor Distribuido (Distributed Server) está compuesto por un grupo de servidores que funcionan de forma independiente y generalmente en diferentes ubicaciones físicas cuya funcionalidad es impulsada total o parcialmente por un único servidor maestro. Los servidores Afaria Server distribuidos admiten el uso local de una base de datos Afaria independiente, que contiene información sobre registros, inventarios y datos de alertas sólo para el servidor que soportan. Una máquina elegida dinámicamente en la comunidad de servidores ejecuta el motor de reglas de alertas y la notificación de alertas, así como la detección de cambios para todos los servidores, pero sólo para la funcionalidad compartida. [https://help.sap.com/, Afaria Overview, 2013].

En un escenario Servidor Distribuido de Afaria (Distributed Server), el Servidor de origen (o maestro) es el servidor donde se crean, editan y administran todas las tareas de administración. Estas directivas se replican en los servidores de destino. Los clientes pueden conectarse a cualquier servidor de la comunidad y ejecutar las directivas asignadas. Esto proporciona un tipo de solución de equilibrio de carga si tiene muchos clientes ubicados en distintas geografías heterogéneas. Los grupos de clientes pueden conectarse a un servidor local, evitando así retrasos en la comunicación y la congestión inherentes a un entorno WAN[9].

[9] WAN Wide Area Network es una red que se utiliza para tarnsmitir datos a través de largas distancias

Afaria soporta una base de datos Microsoft SQL Server o SAP SQL Anywhere. El software del servidor de base de datos no se envía con Afaria.

Una granja de servidores de Afaria ("Afaria Server Farm") admite el uso compartido de una base de datos Afaria centralizada, que contiene información sobre registros, inventario y datos de alertas en todos los servidores Afaria que son miembros de la granja. Una máquina elegida dinámicamente en la comunidad de servidores ejecuta el motor de reglas de alertas y la notificación de alertas, así como la detección de cambios de inventario para todos los servidores. [https://help.sap.com/, Afaria Overview, 2013].

El servidor de retransmisión (Relay Server) es un servidor proxy inverso[10] (Reverse Proxy) y se incluye con Afaria para gestionar las conexiones entrantes desde dispositivos remotos. El servidor de retransmisión también se puede configurar en un escenario de granja. [https://help.sap.com/, Afaria Overview, 2013].

3.6.2 Componentes de SAP AFARIA

Los principales componentes de Afaria son:

- **Afaria Server (Servidor Afaria)**: Comunica y controla los dispositivos aplicando políticas de configuración y recopilando datos de inventario.
- **Afaria Administration Console (Consola de administración Afaria):** Una interfaz de usuario basada en web para configurar Afaria, administrar dispositivos e inventario.
- **Enrollment Server (Servidor de inscripción):** gestiona la inscripción de dispositivos con Afaria y también proporciona información útil para la administración de dispositivos iOS. El servidor de inscripción debe instalarse en el mismo servidor que el Servidor Afaria.
- **Self-Service Portal (Portal de autoservicio):** permite que los usuarios finales inscriban su dispositivo en Afaria, y además facilita a los usuarios, ver la información de su dispositivo y emitir comandos, tales como restablecer una contraseña. El portal es opcional para la inscripción y permite a los usuarios instalar políticas de la aplicación desde el servidor de paquetes (Packages Server). El portal de autoservicio está destinado a la implementación dentro del firewall[11] empresarial [https://help.sap.com/, Afaria Overview, 2013].

Afaria también incluye varios componentes opcionales y paquetes de software:

[10] Proxy Inverso (Relay Proxy) es un tipo de servidor Proxy que recupera un recurso en nombre de un cliente de uno o más servidores
11 Firewall: cortafuegos, es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas

- **SMS Gateway:** Maneja mensajes SMS como notificaciones salientes y comandos de borrado remoto. El Gateway SMS no es necesario para la operación de Afaria. Afaria utiliza la pasarela SMS (para los dispositivos y los clientes Afaria que soportan mensajería SMS) para entregar notificaciones salientes, comandos de borrado remoto, aprovisionamiento de Open Mobile Alliance[12] (OMA) y mensajes de notificación de servidores, y cualquier otra comunicación de Afaria destinada al enrutamiento de SMS.

- **Relay Server (Servidor de retransmisión):** Un proxy para las conexiones HTTP y HTTPS[13] desde Internet a un servidor de componentes, como el Afaria Server o el Enrollment Server. El Relay Server es opcional, pero es recomendable para incrementar la seguridad de la red empresarial.

- **Access Control for E: Mail (control de acceso para el correo electrónico):** Los componentes de control de acceso le permiten restringir el acceso al correo electrónico de la empresa.

- **Network Access Control (Control de acceso a la red):** el control de acceso a la red (NAC) le permite restringir el acceso a la red empresarial. [https://help.sap.com/, Afaria Overview, 2013].

Afaria también se conecta con los siguientes componentes de la red empresarial:

- **Base de datos Afaria (Afaria Data Base):** Base de datos SAP SQL Anywhere[14] o Microsoft SQL[15] que almacena los procedimientos, propiedades de configuración, datos de dispositivo, grupos, política y todo el registro de mensajes y actividades. Para los componentes del servidor Afaria el acceso a la base de datos es directo a la base de datos o indirecto a través del servidor Afaria

- **Certificate Authority[16] (Autoridad de certificación):** las definiciones de autoridad de certificado se asignan a la inscripción y al servidor de paquetes “Packages Server”, para admitir la inscripción la inscripción o “enroll” de dispositivos o facilitar el aprovisionamiento de certificados para aplicaciones.

---

12 Open Mobile Alliance (OAM) es una organización de estándares abiertos para la industria de telefonía móvil.

13 Hypertext Transfer Protocol (HTTP) y Hypertext Transfer Protocol Secure (HTTPS) son protocolos de comunicación que permiten la transferencia de información en la World Wide Web

14 SAP SQL Anywhere es una base de datos relacional propiedad de SAP

15 Microsoft SQL es una base de datos relacional desarrollada por Microsoft

16 Certification Authority CA es una entidad de confianza, responsable de emitir y revocar los certificados digitales o certificados

- **E-Mail Server (Servidor de correo electrónico):** para el control de acceso para el correo electrónico corporativo, como una función opcional, el servidor puede alojar el servicio PowerShell de control de acceso (Windows PowerShell es una interfaz de consola), que realiza sondeos en el servidor Afaria para las políticas de control de acceso actuales y entrega esa información al proxy de correo electrónico en la DMZ[17] (zona desmilitarizada o Demilitarized Zone). Es usado para el control de acceso para correo electrónico, cuando el correo electrónico se encuentra en Internet y no incluye un servidor de correo electrónico en la empresa. [https://help.sap.com/, Afaria Overview, 2013].

3.7 SAP Mobile Platform (SMP)

SAP Mobile Platform (SMP) proporciona una solución integrada para facilitar y ampliar las aplicaciones de la empresa a los trabajadores móviles.

SAP Mobile Platform actúa como el medio ("Hub") que conecta los sistemas de información corporativos de la empresa a los dispositivos móviles. Otorgando características para el desarrollo de aplicaciones móviles, despliegue, seguridad y administración continua de dispositivos móviles y aplicaciones móviles (Mobile Device Management MDM / Mobile Application Management MAM), proporcionando una solución completa de extremo a extremo. [https://help.sap.com/, smp_fundamentals.pdf, 2013].

Esta plataforma tecnológica provee:

- Conectividad de múltiples tipos de dispositivos y de sistemas operativos, para clientes móviles
- Soporte para clientes nativos de objetos API[18] (Application Programming Interface) basados en el lenguaje del dispositivo
- Soporte para clientes basados en Web dentro de la seguridad de la empresa
- Herramientas de desarrollo y construcción basadas en Eclipse[19] para servicios de datos móviles y generación de datos persistentes del lado del dispositivo.
- Provee una arquitectura móvil empresarial que usa los estándares e interfaces propios para soportar una variedad de recursos de los datos empresariales
- Seguridad punto a punto ("end to end") desde la empresa a los dispositivos

17 DMZ (Demilitarized Zone) es una zona segura que se ubica entre la red interna de una organización y una red externa, generalmente en Internet
18 API Application Programming Interface es un conjunto de subrutinas, funciones y procedimientos que ofrece la interfaz de programación de aplicaciones
19 Eclipse es un conjunto de herramientas de programación de código abierto multiplataforma para entornos de desarrollo integrados

- Soporte para usuarios móviles quienes ocasionalmente se conectan o cuyo trabajo es enteramente en línea (online)
- Dar notificaciones que alerten a los usuarios que deben refrescar la vista de los datos en su dispositivo
- Unificar la administración y monitoreo de la plataforma [https://es.slideshare.net/SyambabuAllu/sap-mobile-platform-version-23-architecture, 2013].

La plataforma se compone de:

- **SAP Mobile SDK (Software Development Kit):** conjunto de herramientas de desarrollo de plataformas utilizadas para crear aplicaciones móviles que satisfagan las necesidades de movilidad.

- **SAP Mobile WorkSpace:** proporciona un desarrollo integrado basado en Eclipse para modelado, diseño e implementación de aplicaciones móviles.

- **Agentry Editor (Editor de Agente):** ofrece un mecanismo basado en Eclipse para el desarrollo de aplicaciones en Agentry.

- **Librerías:** proporciona librerías para apoyar el desarrollo de objetos API[20], HTML5[21] / JS Hybrid[22] y aplicaciones móviles OData[23] SDK.

- **SAP Mobile Platform Runtime**: la arquitectura de implementación, gestión y de otorgamiento de servicios, para ejecutar y administrar aplicaciones móviles. SAP Mobile Server es una plataforma que proporciona servicios tales como seguridad, almacenamiento en caché y sincronización para dispositivos móviles y además permite la integración con el EIS (Executive Information System). [https://help.sap.com/, smp_fundamentals.pdf, 2013].

- **SAP Control Center**: un componente clave de "Runtime", es la consola Web que proporciona una plataforma de gestión y control, que incluye el manejo y monitoreo de dispositivos móviles y la administración de aplicaciones. [https://help.sap.com/, smp_fundamentals.pdf, 2013].

[20] APIs (Application Programming Interface) La interfaz de programación de aplicaciones, es un conjunto de subrutinas, funciones y procedimientos (o métodos, en la programación orientada a objetos) que pueden ser utilizado por otro software.
21 HTML5 (HyperText Markup Language, versión 5) es la quinta revisión importante del lenguaje básico de la World Wide Web, HTML
22 JS Hybrid (Java Script) es un lenguaje de programación de alto nivel orientado a objetos, dinámico e interpretado. Comúnmente usado en ambientes Web
23 Open Data Protocol (OData) es un protocolo abierto que permite la creación y uso de APIs (Application Programming Interface) interoperables de una manera simple y estándar. Microsoft inició OData en 2007

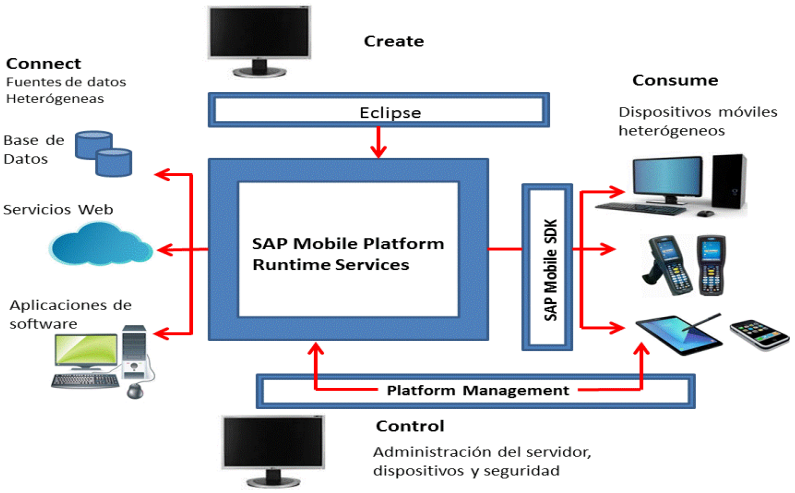


Figura 3.7.1. Plataforma SAP Mobile.

La solución permite:

- **Conectar (Connect):** durante el desarrollo y la implementación, permite conectar fuentes de datos heterogéneas y sistemas empresariales de "Backend". [https://help.sap.com/, smp_fundamentals.pdf, 2013].

- **Create (Crear):** utiliza las herramientas de desarrollo incluidas con SAP Mobile SDK (Software Development Kit), para crear y probar las aplicaciones móviles que satisfagan las necesidades de movilidad de la empresa. [https://help.sap.com/, smp_fundamentals.pdf, 2013].

- **Control:** para implementar y administrar SAP Mobile Platform Runtime, incluido el entorno en tiempo de ejecución, seguridad de extremo a extremo y aplicaciones de dispositivo. [https://help.sap.com/, smp_fundamentals.pdf, 2013].

- **Consume (uso):** Las aplicaciones móviles se instalan en dispositivos que permiten a los usuarios de dispositivos trabajar en línea y fuera de línea. Se accede a los datos empresariales desde una variedad de dispositivos móviles. [https://help.sap.com/, smp_fundamentals.pdf, 2013].

3.7.1 Elementos de la plataforma SAP SMP

A continuación, los componentes en una plataforma SAP SMP

3.7.1.1 Topología de red

Los componentes de mensajería y replicación en la arquitectura de SAP Mobile Platform típicamente son instalados junto a otro servidor Web. Un balanceador de carga y uno o más servidores Reverse Proxy son instalados en la DMZ para aislar el servidor Web y el "Mobile Middleware", del tráfico directo de Internet. Cuando un "Cluster Mobile Middleware" es usado, el SAP Mobile Platform puede ser posicionado en una zona, junto a otros servidores de base de datos empresariales. Un balanceador de carga, puede también ser ubicado entre los servidores de "Backend" y los nodos del servidor Web de SAP Mobile Platform, para cuando las notificaciones de cambios de datos necesiten ser enviadas, para ambos nodos en el "cluster" de SAP Mobile Platform. [https://help.sap.com/, smp_fundamentals.pdf, 2013].

SAP Afaria despliega y configura aplicaciones en los dispositivos y ayuda en tareas de administración y seguridad de los datos empresariales en los dispositivos. Afaria interactúa con las facilidades de la plataforma de administración local del dispositivo para asegurar las políticas empresariales. Para algunas plataformas, Afaria también ofrece un almacenamiento empresarial de las aplicaciones, así como también provee facilidades de cara a los clientes. [https://help.sap.com/, smp_fundamentals.pdf, 2013].

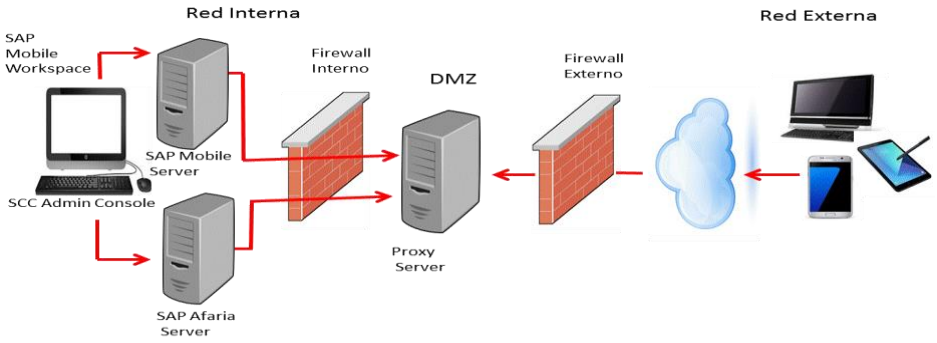


Figura 3.7.1.1.1 Topología de red.

Las siguientes sesiones describen algunos de los patrones de uso de la tecnología de SAP Mobile Platform y provee una visión general de la arquitectura.

3.7.1.2 Administración y monitoreo

El servicio SAP Control Service (SCC) actúa como un facilitador de control de la tecnología SAP Mobile Server. Este agente basado en Java, tiene incluido un servidor Web que habilita la comunicación, y tiene asociada una base de datos para su propio control y manejo de alertas.

Desde el punto de vista de administración y despliegue hay varias jerarquías:

- Un host administrador tiene control global sobre toda la infraestructura móvil
- Un dominio (“Domain”) es asociado a un contexto de configuración de seguridad y puede ser usado para aislar aplicaciones dentro de un solo servidor. Un administrador del dominio puede configurar elementos únicamente dentro del dominio sobre el cual tiene permisos
- Una aplicación es asociada a un contexto de seguridad y a un conjunto de “paquetes” (“Packages”).
- Los paquetes son desplegados desde el servidor dentro de un dominio de administración como una aplicación
- Las políticas pueden ser aplicadas de forma separada, a nivel de dominio y a nivel de paquete

Los procesos de monitoreo dentro del servidor, registran el comportamiento de las aplicaciones, incluyendo requerimientos de los dispositivos y estadísticas de las aplicaciones. Estos registros son escritos de forma asíncrona para la base de datos de monitoreo. SAP recomienda aislar la base de datos de monitoreo en su propio hardware si se ejecuta una cantidad considerable de datos. [https://help.sap.com/, smp_fundamentals.pdf, 2013]. Existe una herramienta de SAP denominada SAP Solution Manager que puede ser integrada con el SAP Plaform para monitoreo técnico, alertas, análisis de causa raíz, diagnóstico de cambios y análisis de la carga de trabajo.

3.7.1.3 Servicios de dispositivos

Hay dos tipos de enfoque de aplicaciones para dispositivos, Hybrid Web Container y aplicaciones nativas.

Cada una de estas aplicaciones utilizan varios servicios SDK,[24] algunas son aplicaciones tipo y algunas otras son aplicaciones inter tipos (“across type"). Varios protocolos son soportados para las

[24] SDK Un kit de desarrollo de software es generalmente un conjunto de herramientas de desarrollo de software que le permite al programador o desarrollador de software crear una aplicación informática para un sistema concreto, por ejemplo ciertos paquetes de software, frameworks, plataformas de hardware, computadoras, videoconsolas, sistemas operativos, etcétera.plataformas de hardware, computadoras, videoconsolas, sistemas operativos, etcétera.

aplicaciones. The Hybrid Web Container utiliza un protocolo de mensajería que interactúa con la capa de MBO´s (Mobile Business Objects).

Las aplicaciones nativas sincronizan directamente con SAP Mobile Plaform utilizando una capa de cache y una eficiente tecnología de replicación para mover datos, desde el cache del servidor y la base de datos del dispositivo. Aplicaciones nativas OData usan llamadas de mensajería síncrona para interactuar con el SAP Online Data Proxy y el SAP NetWeaver Gateway. Los servicios de OData usan comandos (GET, PUT, POST and MERGE) para habilitar operaciones contra el dispositivo [https://help.sap.com/, smp_fundamentals.pdf, 2013].

Las facilidades de seguridad son incluidas en el SDK para almacenar certificados de seguridad y habilitar mecanismos de autenticación tales como SSO (X.509 y "logon[25]" tickets SSO2) y otras facilidades relacionadas a encriptación de los datos.

Hay APIs usadas para almacenar certificados, certificados de "logon", y almacenar datos, que son usados para habilitar la seguridad requerida. Cualquier tipo de aplicación para el dispositivo, hace uso del mismo conjunto de herramientas de seguridad.

El Agentry soporta características de seguridad, incluyendo autenticación anónima y autenticación SSL (Secure Sockets Layer). Estas son parte de una funcionalidad, que requiere la configuración de certificados y reglas de manejo de certificados. [https://help.sap.com/, smp_fundamentals.pdf, 2013].

3.7.1.4 Servicios de mensajería

El flujo de trabajo de la arquitectura, las Hybrid App, DOE, y los mecanismos de notificación a los dispositivos, están apalancados sobre un mecanismo de servicio de mensaje asíncrono para mover los datos entre los dispositivos y el servidor. Este servicio de mensajería es basado en el protocolo HTTP, pero usa una "carga" binaria propia que es comprimida y encriptada. Los mensajes asíncronos en tránsito, son almacenados en las colas de cache de la base de datos del servidor hasta que una notificación es enviada al dispositivo con instrucciones para colocar la carga, desde el servicio de mensajería hacia el servidor. Una vez tomado por la capa de cliente SDK, el mensaje reside en la base de datos hasta que es procesado por la capa de aplicación del dispositivo. Los mensajes son encriptados en el dispositivo. [https://help.sap.com/, smp_fundamentals.pdf, 2013].

Las aplicaciones OData SDK usan la misma infraestructura de mensajería, pero usan el modo de mensajería síncrona para el tráfico de requerimiento/replica. Estas aplicaciones deben asegurar que un

25 Logon: inicio de sesión. El acto de conectarse a la computadora, que generalmente requiere la entrada de una identificación de usuario y contraseña en una terminal de computadora.

requerimiento sea completado, por pruebas con condiciones de error. Las notificaciones se envían desde las aplicaciones OData SDK mientras están en línea y garantizan que sean entregadas. Si el dispositivo esta off-line y la aplicación no es capaz de mantener la conexión con el servidor, el servidor envía una notificación específica a la plataforma del dispositivo (APNS, BES, etc.) informando que la aplicación que tiene los datos está esperando en el servidor. [https://help.sap.com/, smp_fundamentals.pdf, 2013].

Para recibir las notificaciones y mensajes, los dispositivos deben ser registrados en el servidor vía un proceso llamado "on-boarding". Un dispositivo puede estar "on-board" a través de un proceso manual o a través de un proceso automatizado basado en la seguridad del dominio que es asociado a las credenciales de "login" del usuario del dispositivo.

Las aplicaciones Agentry usan TCP/IP [26]y SSL[27] a través de un tipo de conexión denominado ANGEL (Agentry Next Generation Encryptation Layer). Tanto las comunicaciones síncronas como las asíncronas son soportadas. Los Agentry Clients pueden operar en modo online u offline, con todos los datos almacenados localmente en el cliente, y soporta una sincronización delta (Exchange data model). El modo (online u offline) es manejado por la definición de la lógica de la aplicación empresarial. [https://help.sap.com/, smp_fundamentals.pdf, 2013].

3.7.1.5 Servicios de seguridad

SAP Mobile Platform provee el Common Security Infrastructure (CSI) que es una facilidad para garantizar las operaciones de autenticación, autorización y auditoría. Los usuarios pueden autenticarse contra un conjunto de autorizaciones incluyendo el LDAP y el Active Directory. Las conexiones seguras pueden ser establecidas con Secure Sockets Layer (SSL) entre el dispositivo y el canal de replicación. Las bases de datos de los dispositivos pueden también ser encriptadas con una clave suplida por el usuario. [https://help.sap.com/, smp_fundamentals.pdf, 2013].

3.7.1.6 Aplicaciones Hybrid Web Container

Hybrid Web Container hace un puente entre las deficiencias de los Web browsers de hoy, con el poder de los servicios de sistema operativo del dispositivo, tales como GeoLocation. Permite a los

[26] TCP/IP: es un protocolo de red desarrollado para comunicaciones en redes. Describe un conjunto de guías generales de operación para permitir que un equipo pueda comunicarse en una red. TCP/IP provee conectividad de extremo a extremo especificando cómo los datos deberían ser formateados, direccionados, transmitidos, enrutados y recibidos por el destinatario.

27 SSL Secure Sockets Layer: es un protocolo criptográficos que proporciona comunicación segura por una red, comúnmente Internet. Se usan certificados X.509 y por lo tanto criptografía asimétrica para autentificar a la contraparte con quien se están comunicando y para intercambiar una llave simétrica. Esta sesión es luego usada para cifrar el flujo de datos entre las partes.

desarrolladores construir aplicaciones usando tecnologías Web y añadir funcionalidad similar a las ya contempladas en las aplicaciones nativas.

La integración con Apache Cordova (formalmente Adobe PhoneGap) permite el enlace con el código nativo del cliente con el Hybrid Web Container y llama este código nativo desde el JavaScript, también provee acceso a funcionalidad nativa del dispositivo usando el marco de referencia ("framework") Cordova.

La tecnología de Hybric Web Container típicamente es usada para mantener el flujo de trabajo ("workflow") del dispositivo y para aplicaciones ligeras. También incluye características, tales como:

- Bajo volumen de datos
- Experiencia de usuario simple
- Transacciones en estado offline sin larga duración
- Lógica simple del negocio

El Hybric Web Container soporta tres patrones. En muchas aplicaciones, la combinación de estos patrones es aplicada para implementar casos específicos:

- Simple requerimiento/respuesta o una aplicación de búsqueda usando la mensajeria SDK de API´s o basada en invocaciones REST
- Notificaciones Hybric Web Container que son el resultado de una operación de cambio de datos MBO (Mobile Business Object), enviada desde el "Backend" vía el "Middleware", en el contexto de un proceso de negocio que envía información para los usuarios móviles
- Formas de Acción/Decisión (Action/Decision Forms) que incorpora requerimientos SDK, respuestas y notificaciones. Los usuarios toman acciones sobre los dispositivos para emitir un formato, tomar una decisión, y también, como el resultado en el proceso de transición de algunos procesos empresariales.

El Hybric Web Container está presente en el tiempo de ejecución del dispositivo, sobre el cual estos servicios son ejecutados. El Hybric Web Container es una aplicación nativa con un browser embebido que permite a los desarrolladores construir aplicaciones con la simplicidad de un desarrollo Web, combinada con el poder de los servicios nativos del dispositivo. SAP Mobile Platform desarrolla una aplicación nativa para plataformas iOS, Android, Windows Mobile y Black Berry.

Adicional a las capacidades de los Web browser de código estándar HTML/CSS/JS, el Hybric Web Container también provee estos servicios adicionales:

- Cache offline
- Mensajería de confianza (no para OData)
- Almacenamiento seguro para herramientas de seguridad (certificados, etc.)
- Aprovisionamiento de aplicaciones de una instancia HTML
- Integración con el middleware SAP Mobile Platform para intercambio de datos MBO

3.7.2 Aplicaciones de sincronización móviles

Las aplicaciones de sincronización proveen consistencia en las transacciones entre el dispositivo móvil, el middleware y el sistema "Backend". Estas aplicaciones de clientes son diseñadas y construidas para ciertos escenarios específicos de negocio, o puede iniciarse como una solución a la medida que es adaptada con un gran grado de personalización ("customizing"). Existen varios requerimientos de aplicación a considerar en la escogencia de la mejor tecnología de SAP Mobile Platform a emplear. Las aplicaciones diseñadas que no toman en cuenta estos criterios pueden tener serios problemas de performance. [https://help.sap.com/, smp_fundamentals.pdf, 2013].

3.7.2.1 Sincronización cache

La sincronización cache permite "mapear" los datos del dispositivo móvil y los objetos SAP "Backend" de manera remota (usando un conector, Java Connector JCO[28]), y también contra otros objetos no SAP, tales como base de datos y servicios Web. Cuando SAP Mobile Platform es usada en forma estándar para sincronizar datos, esta usa una forma eficiente de transferencia y de inserción de datos entre el cache del servidor y las bases de datos de los dispositivos. La aplicación móvil es diseñada tal cual el desarrollador especificó como sería la carga de datos desde el "Backend" al cache, y entonces filtra y baja los datos del cache, usando los parámetros especificados en el dispositivo. El modelo contenido en el dispositivo y el "mapeo" al "Backend" está directamente integrado. [https://help.sap.com/, smp_fundamentals.pdf, 2013].

El estilo de "acoplamiento" entre el "Backend" y los dispositivos, implica que el "Backend" debe ser capaz de responder a los requerimientos desde el "middleware" basado en los parámetros especificados por el usuario, y proveer así, los datos móviles de forma apropiada. En otras palabras, el "Backend" debe ser capaz de retornar la respuesta de un requerimiento particular de un usuario supliendo la interfaz apropiada. Normalmente, algunas adaptaciones móviles son requeridas dentro de SAP Business Application Programming Interface (BAPI). [https://help.sap.com/, smp_fundamentals.pdf, 2013].

28 JCO Connection o SAP Java Connector es un componente de middleware que permite que una aplicación JAVA llame o se comunique con cualquier sistema SAP y viceversa.

Dado la naturaleza directa de mapear parámetros de la aplicación y la eficiencia en los protocolos de replicación, el cache de despliegue de SAP Mobile Platform es ideal para:

- Para grandes y reiterados despliegues (“Deployment”) de carga a los dispositivos, en donde el tiempo es critico
- Donde el uso “ad hoc” de dispositivos puede generar grandes transferencias de datos o de carga inicial
- Para SAP y no SAP “Backend” con servicios Web o interfaces JDBC[29]

3.8 SAP Direct Store Delivery 1.0

SAP Direct Store Delivery es una aplicación móvil SAP que soporta el proceso de venta y distribución de mercancías directamente en la tienda del cliente sin pasar por el almacén del minorista.

La aplicación móvil proporciona una solución que integra la capacidad móvil DSD con funciones ampliadas de SAP Mobile Direct Store Delivery (SAP mDSD) incluidas en SAP ERP y poniendo a disposición algunas actividades de ventas disponibles de SAP Customer Relationship Management (SAP CRM).

La aplicación móvil permite a sus usuarios de dispositivo móvil, es decir, su servicio externo y encargados de entregas responder rápidamente a las necesidades de clientes y órdenes revisadas mientras se reducen las pérdidas de material. SAP Direct Store Delivery se puede utilizar en dispositivos móviles basados en Windows Mobile y en dispositivos Android.

SAP Direct Store Delivery es una aplicación móvil diseñada para soportar procesos empresariales de ventas, marketing y logística, por ejemplo, visitas de clientes, pedidos, actividades de ventas y entregas para permitir a los usuarios del dispositivo móvil vender y distribuir mercancías directamente al punto de venta.

Los roles de usuario de dispositivo móvil se pueden definir de manera flexible para permitir a estos usuarios proporcionar servicios para preventas, ventas de mercancía, así como una combinación de estos roles.

Las actividades de usuario de dispositivo móvil comunes en las rutas incluyen, la planificación de visitas, venta, entrega, determinación de precio offline, recaudaciones de pago, encuestas en vivo y una

29 JDBC es una API que permite la ejecución de operaciones sobre bases de datos desde el lenguaje de programación Java, independientemente del sistema operativo donde se ejecute o de la base de datos a la cual se accede

variedad de auditorías para determinación de precios, promociones y distribución. SAP Direct StoreDelivery proporciona a los usuarios de dispositivo móvil datos actuales, por ejemplo, en sus itinerarios diarios, visitas a clientes, actividades, determinación de precios, gastos para llevar a cabo sus actividades

La interfaz de usuario (IU) de la aplicación móvil ofrece una rica experiencia de usuario con pantallas que incluyen procesos estandarizados, procedimientos y mejores prácticas. La IU está estructurada de manera que los usuarios del dispositivo móvil puedan navegar de manera intuitiva.

SAP Direct Store Delivery puede ser usado en:

- Dispositivos móviles basados en Windows Mobile
- Ciertas funciones solo están disponibles en dispositivos móviles basados en Windows Mobile
- Dispositivos móviles basados en Android
- Ciertas funciones, por ejemplo, la generación y carga de informes PDF solo están disponibles en dispositivos móviles basados en Android.

SAP Direct Store Delivery ofrece nuevas ampliaciones importantes, así como mejoras funcionales a las funciones SAP mDSD incluidas en SAP ERP. Puesto que las actividades de los usuarios de dispositivo móvil se ejecutan en el punto de venta con clientes, SAP Direct Store Delivery proporciona una aplicación móvil flexible, rápida y fiable que es la clave para soportar el proceso empresarial de DSD en curso.

3.8.1 Infraestructura del sistema

A continuación, se encontrará la arquitectura básica de SAP y los componentes opcionales para SAP Direct Store Delivery:

- **Módulos SAP ERP:** Logistics Execution System (LE), Comercial (SD), Gestión de materiales (MM), Contabilidad financiera (FI) incluyendo la configuración base.

- **Middleware SMP** (para dispositivos basados en Windows Mobile)

Componentes Adicionales:

- **SAP CRM Customer Relationship Management** (recomendado)

- **Módulo SAP ERP**, por ejemplo, Gestión de almacenes (WM), Planificación y control de producción (PP), Servicio al cliente (CS), Mantenimiento(PM)

- **Afaria** (recomendado)

3.8.2 Integración con SMP

Para utilizar la aplicación móvil primero se tiene que instalar los sistemas “Backend” y middleware para realizar todas las opciones de “Customizing” relevantes (adecuaciones o “personalización”). Las siguientes figuras presentan un resumen de la arquitectura de SAP Direct Store Delivery y la infraestructura del sistema:

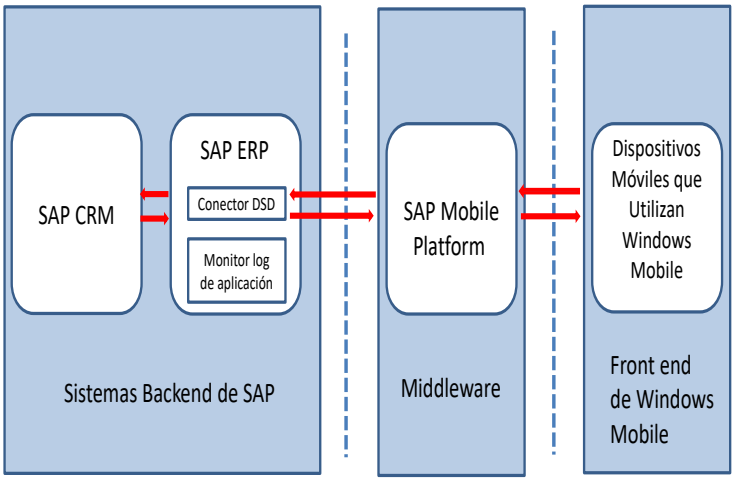


Figura 3.8.2.1 Arquitectura de SAP Direct Store Delivery para dispositivos móviles basados en Windows Mobile

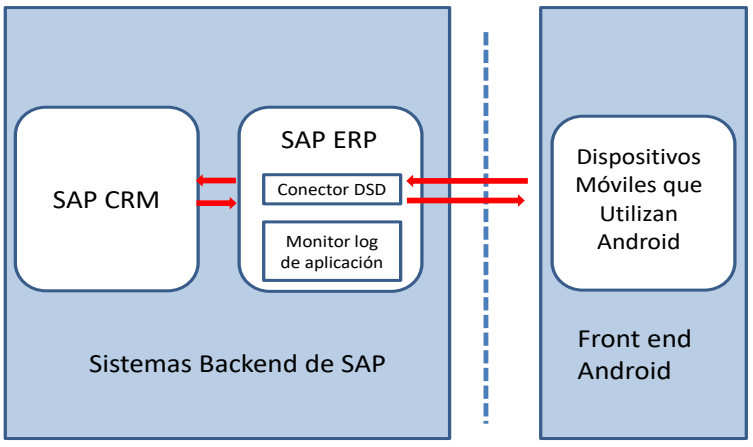


Figura 3.8.2.2 Arquitectura de SAP Direct Store Delivery para dispositivos móviles basados en Android

En los sistemas “Backend” de SAP, se pueden intercambiar datos entre SAP ERP y SAP CRM.

El conector DSD, localizado en SAP ERP, es un área de fase para descargar, cargar y tratar status de datos relevantes para las actividades de los usuarios de dispositivos móviles. Abarca un conjunto de tablas de base de datos en el esquema del dispositivo móvil.

El conector DSD actúa como interfaz entre sistemas SAP y dispositivos móviles:

- **SAP Direct Store Delivery para Windows Mobile**

  El conector DSD actúa como interfaz entre sistemas SAP y el middleware. Los datos del conector DSD se intercambian con el middleware SAP Mobile Platform. Los datos de SAP Mobile Platform se intercambian con dispositivos móviles front end.

- **SAP Direct Store Delivery para Android**

  El conector DSD actúa como interfaz directa entre los sistemas SAP y los dispositivos móviles “front end”.

Al final de las rutas, los datos cargados en sistemas SAP “Backend” desencadenan lo siguiente:

- En SAP ERP, las facturas y pagos cobrados se liquidan en el cockpit de liquidación y contabilización de rutas; se actualizan/crean documentos de ventas, contabilizaciones financieras y movimientos de materiales. Una vez completados estos procesos, se puede procesar la facturación final.

- Si se integra con SAP CRM, los datos de la actividad de ventas se cargan desde el conector DSD en SAP ERP a SAP CRM

- En el Monitor de log de la aplicación en SAP ERP, los status de ruta y mensajes de log de aplicación de los dispositivos móviles se ponen a disposición para la supervisión.

3.8.3 Características de SAP DSD

SAP Direct Store Delivery permite a los usuarios del dispositivo móvil grabar en log todas las actividades relacionadas con la ruta utilizando dispositivos móviles.

Durante una ruta, los usuarios de dispositivo móvil normalmente hacen lo siguiente:

- Realizar actividades de inicio de la jornada, por ejemplo, verificaciones de seguridad del vehículo
- Visualizar una lista de todas las vistas, reorganizar el orden de las visitas y, si es necesario, crear nuevas visitas no planificadas
- Ejecutar actividades que son necesarias para cada visita, por ejemplo, tomar pedidos o entregar mercancías
- Actualizar datos de cliente, actualizar status de cliente con una clave de motivo que indica por qué no se ha podido realizar una visita
- Tomar pedidos utilizando propuestas de posición y capturando stock en almacén
- Entregar mercancías y ajustar cantidades durante el proceso de entrega real si es necesario; recoger devoluciones y envases.
- Llevar a cabo actividades de ventas de una ruta
- Usar escenarios conectados ocasionalmente
- Usar determinación de precios
- Emitir facturas; cobrar pagos y emitir recibos de pago
- Transferir stock en caso necesario
- Registrar gastos
- Informar en la ruta

3.8.4 Proceso SAP Direct Store Delivery

El gráfico siguiente ofrece un resumen de las actividades que se llevan a cabo en los dispositivos móviles en un proceso Direct Store Delivery:

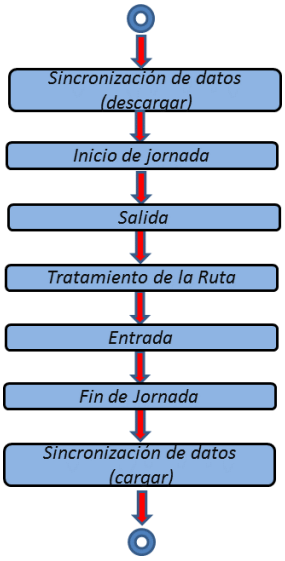


Figura 3.8.4.1 Resumen del proceso de Direct Store Delivery

3.8.4.1. Sincronización de datos (Descargar)

Los datos de transacción y los datos maestros se descargan desde los sistemas “Backend” a dispositivos móviles.

3.8.4.2. Actividad de inicio de jornada

Al inicio de la jornada los usuarios del dispositivo móvil registran y verifican datos de ruta básicos, por ejemplo, ID[30] de conductor, ID de vehículo, verificaciones de seguridad del vehículo y la lectura del odómetro.

3.8.4.3. Salida (Check out)

Los usuarios del dispositivo móvil verifican qué se ha cargado en sus vehículos. Esto puede incluir tanto materiales como efectivo. Uno o más supervisores confirman un check out utilizando una captura de firma en el dispositivo móvil.

3.8.4.4. Tratamiento de la ruta

Los usuarios del dispositivo móvil visualizan una lista de todas las visitas. Para cada visita efectúan actividades asociadas o actualizan el status de visita con una clave de motivo para indicar por qué no han podido visitar un cliente (por ejemplo, el cliente estaba cerrado o se agotó el tiempo del conductor). Los usuarios de dispositivo móvil pueden reorganizar el orden de sus visitas y crear nuevas visitas no planificadas.

Las actividades principales efectuadas por parte del cliente son las siguientes:

- **Tomar pedidos para entregas futuras:** los usuarios de dispositivos móviles son pre vendedores, o tienen un rol mixto, toman pedidos de los clientes en la ruta. Las firmas de clientes se pueden capturar en el dispositivo móvil, por ejemplo, para la confirmación de pedidos. Estos pedidos se entregan en rutas posteriores por usuarios de dispositivos móviles que son conductores de entregas.

- **Entregar pedidos de artículos vendidos previamente:** los usuarios de dispositivo móvil que son conductores de entregas o tienen un rol mixto, entregan material vendido previamente de su camión e imprimen una nota de entrega o factura. Si es necesario, pueden añadir artículos y modificar cantidades. La aplicación móvil soporta la devolución de mercancías (por ejemplo,

[30] ID: identificador que permite la certificación del conductor, vehículo, etc.

mercancías deterioradas, artículos incorrectos) y la devolución de envases, que se añade a las entregas.

- **Entregar sin pedido artículos vendidos previamente:** los usuarios de dispositivo móvil que son vendedores de mercancías o que tienen un rol mixto, entregan material que no se ha pedido. Venden material directamente de su vehículo, creando entregas nuevas. Esto incluye tanto entregas de salida normales como entregas entrantes de devolución. El tratamiento físico de la entrega es parecido al de las entregas de pedidos vendidos previamente.

- **Actividades de ventas:** si se integra SAP CRM los usuarios de dispositivos móviles pueden efectuar actividades de ventas, como hacer encuestas, escribir diarios y notas y crear anexos.

- **Escenarios conectados ocasionalmente:** los usuarios de dispositivo móvil pueden añadir clientes, entregas, pedidos o actividades adicionales durante la ejecución de una ruta conectándose a la ubicación central. Pueden cargar datos de ruta, por ejemplo, para visitas.

- **Emitir facturas:** Los usuarios de dispositivo móvil pueden estar habilitados para emitir facturas legales. Los clientes que no reciben una factura, reciben en su lugar una nota de entrega.

- **Cobro del pago:** los usuarios de dispositivo móvil pueden estar habilitados para cobrar pagos de entregas actuales, así como otras partidas abiertas pendientes. Los métodos y condiciones de pago se pueden modificar en el dispositivo. Los clientes emiten recibos de pago.

También se soportan las siguientes actividades generales relacionadas con la ruta.

- **Registro de ajustes de "stocks[31]" o inventarios:** los usuarios de dispositivo móvil pueden registrar ajustes de "stocks", por ejemplo, en el caso de rupturas o transferencias de camión a camión de "stock" no reservado.

- **Registrar gastos de conductor**: los usuarios de dispositivo móvil pueden registrar varios gastos, como, peajes, aparcamiento y combustible.

- **Informes:** los usuarios de dispositivos móviles que utilizan SAP Direct Store Delivery puede visualizar e imprimir informes, por ejemplo, un Informe de liquidación preliminar o un informe de rendimiento de ruta.

[31] Stock: inventario, registro documental de los bienes y demás cosas pertenecientes a una persona, empresa o comunidad.

3.8.4.5. Entrada (Check in)

Los materiales y envases devueltos al almacén se validan. En este caso, los usuarios de dispositivo móvil introducen las cantidades devueltas, que los supervisores pueden verificar y confirmar.

3.8.4.6. Actividad de fin de jornada

La actividad de fin de jornada consiste en registrar datos de fin de ruta, por ejemplo, la lectura del odómetro final y el efectivo/pagos devueltos.

3.8.4.7. Sincronización de datos (Cargar)

Los datos de transacción se cargan desde los dispositivos móviles a los sistemas “Backend”.

3.9 SAP Web Dispatcher

El SAP Web Dispatcher es un software de SAP que se encuentra entre Internet y un sistema SAP. Es el punto de entrada para las solicitudes HTTP (s) en el sistema, que consiste en uno o más servidores de aplicaciones SAP NetWeaver. Como un "conmutador web de software", el SAP Web Dispatcher puede rechazar o aceptar conexiones. Cuando acepta una conexión, equilibra la carga para garantizar una distribución homogénea o pareja entre todos los servidores de SAP R/3. Por lo tanto, SAP Web Dispatcher contribuye a la seguridad y también equilibra la carga en un sistema SAP. Puede utilizar el SAP Web Dispacther en sistemas solo ABAP, así como en sistemas ABAP / Java combinados (sistemas de "doble stack”[32]) y en sistemas solo Java.

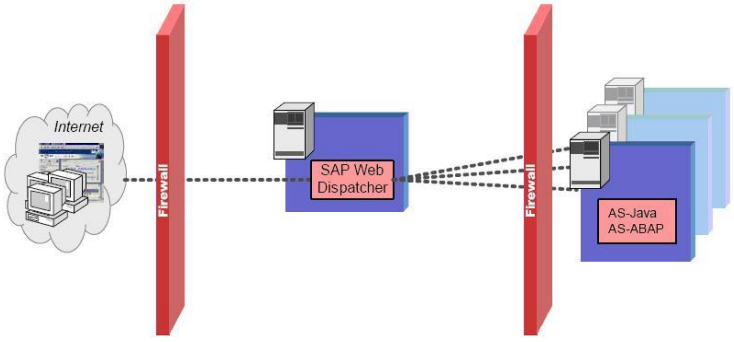


Figura 3.9.1 SAP Web Dispatcher

[32] “Dual stack” o “Doble stack”: sistema SAP que contiene instalaciones de Application Server ABAP y Application Server Java.

3.10 Network Load Balancing Services (NLBS)

Network Load Balancing Services (NLBS) es una implementación de Microsoft de “cluster[33]” y balanceo de carga que está diseñada para proporcionar alta disponibilidad y alta confiabilidad, así como una alta escalabilidad.

NLBS está destinado a aplicaciones con conjuntos de datos relativamente pequeños que rara vez cambian (un ejemplo sería páginas web) y no tienen estados en memoria de larga ejecución. Este tipo de aplicaciones se denominan aplicaciones “stateless” (sin estado), y generalmente incluyen servidores Web, Protocolo de transferencia de archivos (FTP) y redes privadas virtuales (VPN).

Cada solicitud de cliente a una aplicación sin estado es una transacción separada, por lo que es posible distribuir las solicitudes entre varios servidores para equilibrar la carga. Una característica atractiva de NLBS es que todos los servidores de un clúster se controlan entre sí con una señal, por lo que no existe un solo punto de falla.

En la versión en Windows Server 2003 , NLBS no admite la eliminación automática de un servidor fallido desde un clúster a menos que el servidor esté completamente fuera de línea o si su servicio NLBS está detenido. Por ejemplo, si un servidor web devuelve una página de error en lugar del contenido correcto, NLBS todavía la percibe como "viva". Como tal, normalmente se requiere una secuencia de comandos de supervisión en cada nodo participante, que verifica la corrección de la entrega de la página web local y llama a un ejecutable (nlb.exe) para agregarla o eliminarla del clúster según sea necesario.

[33] Cluster es un conjunto de dos o más máquinas que se caracterizan por mantener una serie de servicios compartidos y por estar constantemente monitorizándose entre sí.

CAPITULO IV. ALCANCE Y FACTIBILIDAD DEL PROYECTO

Como ya se mencionó, la presente investigación consiste en el análisis, diseño e implantación de una solución que brinde una plataforma segura y confiable para soportar las actividades de venta de una empresa de consumo masivo, Empresa XYZ, a través de dispositivos móviles.

Este proyecto abarcará las siguientes etapas:

- Análisis, en la que se estudia y verifica la situación actual y se determinan los requerimientos.
- Diseño y propuesta, la cual consiste en el establecimiento de alternativas a través del análisis y la evaluación técnica de las facilidades aportadas por las soluciones de SAP AFARIA y SMP
- Implantación, donde se llevará a cabo la instalación de un prototipo de pruebas y se dejarán las bases para expandir la solución propuesta a todas las operaciones de venta de la empresa.

La solución propuesta por este proyecto pretende cubrir las necesidades actuales y futuras de los servicios de conexión de los dispositivos móviles de los trabajadores de la fuerza de ventas desde y hacia sus clientes y la empresa.

4.1 Análisis de Factibilidad

Para lograr desarrollar este trabajo se consideraron tres estudios de factibilidad, que se encuentran enfocados hacia la búsqueda de una solución óptima al problema planteado.

4.1.1 Factibilidad técnica

Las plataformas e infraestructura que posee la empresa de consumo masivo de esta investigación, se ajustan fácilmente a los requerimientos del proyecto.

Por otra parte, gracias a los avances tecnológicos, en el área de seguridad de datos de las herramientas de AFARIA/SMP, existen alternativas que cubren las necesidades y expectativas de la empresa, entre las cuales cabe destacar el requerimiento del uso y manejo de certificados y firmas digitales, como medios de protección de la información.

Además, la solución que se instalará, estará en la capacidad de soportar un plan de expansión o crecimiento de la empresa en cualquier momento.

Se aprovechan muchos de los avances de la solución ya existente, pero se incorporarán facilidades, que permitirán cubrir los requerimientos de flexibilidad, seguridad y monitoreo que se plantean. Se cuentan con herramientas de monitoreo que pueden ser acondicionadas para llevar controles que garanticen la confiablidad y seguridad de la información.

4.2.1 Factibilidad económica

Esta investigación es de mucha relevancia para la corporación porque afianzará la seguridad sobre los servicios de dispositivos móviles y está dispuesta a cubrir los costos del mismo, ya que se estima que con su implantación se logren muchos beneficios, tanto en la reducción de costos de operación como en mayor efectividad en las ventas.

El hecho de implementar esta solución, garantiza que los servicios tengan un esquema de alta disponibilidad, lo que se traduce en un tiempo muy pequeño en la interrupción de los mismos, y esto implica minimizar los riesgos que paralicen parcial o totalmente el negocio. De esta forma se garantizará el rendimiento económico y además se ganará la aceptación y confianza de sus clientes, que en consecuencia se convertirá en beneficio para la corporación.

Por otro lado, el manejo de información será más seguro, autentico e integral, esto por supuesto disminuirá o eliminará, los intentos de ataques informáticos. Esto permitirá que los trabajadores de la fuerza de ventas, puedan entrar a los sistemas internos con la seguridad, de que no exista riesgo alguno de ser intervenidos por un ente malicioso, pudiendo descifrar los datos capturados y en consecuencia poder realizar cualquier tipo de ataque o fraude.

Todo lo anterior, se traduce en mejoras en términos económicos, tanto en las operaciones, como en el control de los datos y activos (por ejemplo, el dispositivo móvil DM).

4.3.1 Factibilidad operativa

El presente proyecto brindará a los usuarios y clientes de la corporación mayor seguridad en el desempeño de sus funciones, tareas y servicios, reduce los tiempos de procesos y disminuye el margen de error, garantizando así la eficiencia de las operaciones.

Además, la solución a implementar es concebida para adaptarse al escenario ya existente con lo cual, el entrenamiento al personal de ventas será mucho más expedito. Igualmente, facilitará el mantenimiento y control de la solución, lo cual redundará en actividades más rápidas, sencillas y a menor costo.

La información tendrá un alto grado de seguridad y confiabilidad, ya que la solución podrá supervisar todo lo que es el proceso de ventas, esto redunda en que la información pueda llegar a su destino en forma oportuna, en cualquier momento, logrando así un rendimiento más eficiente en las operaciones de la empresa.

CAPITULO V. SOLUCION PLANTEADA

Las actividades de venta y distribución de la empresa de consumo masivo, Empresa XYZ, cuenta ya con una plataforma que soporta los procesos de Despacho Directo a Tiendas (DSD), sin embargo, esta presenta algunas limitaciones tanto en el manejo de las operaciones, como en la adaptabilidad y seguridad. Por ello, este trabajo plantea el diseño e implantación de una nueva solución que permita gestionar las actividades de venta de una forma rápida, fácil, dinámica y segura. Esto permitirá que los productos sean entregados directamente a los clientes de forma más eficiente, y que se incremente la interacción de los despachadores con esos clientes, lo que se traduce en otorgar un mejor servicio.

5.1 Situación actual

En la actualidad la plataforma instalada está basada en los componentes de SAP NetWeaver ERP con la solución de DSD (en el "Backend") y en el "Middleware" de SAP NetWeaver Mobile (MI) para manejo de las operaciones HTTP desde los dispositivos móviles. También se cuenta con un SAP Web Dispatcher para manejar el balanceo de carga de las solicitudes de HTTP hacia el servidor de SAP Netweaver de Mobile (MI). La interacción de estos componentes puede verse en la siguiente figura:

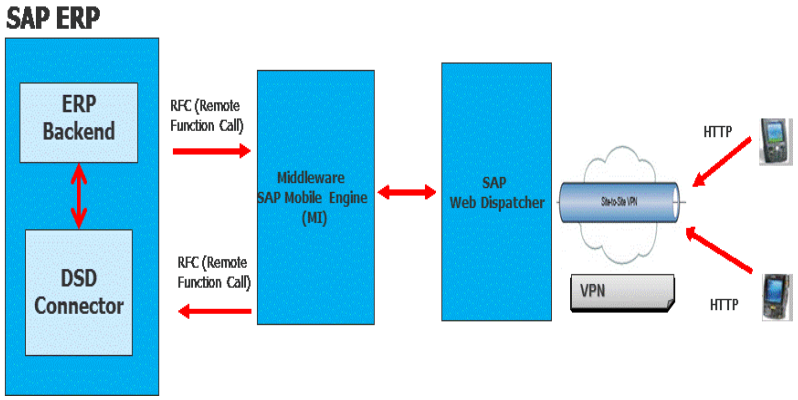


Figura 5.1.1 Plataforma actual de SAP DSD con Mobile (MI)

5.1.1 Limitantes de la plataforma actual

A pesar de que la solución actual soporta las actividades de venta de la empresa, presenta algunas limitaciones:

- Complejidad en adecuar requerimientos nuevos del negocio de ventas, tanto en el "Backend" como en los clientes en los dispositivos móviles.

- La actualización de los dispositivos móviles no es “amigable”, requiere intervención de un equipo de desarrollo para actualizar los clientes en los dispositivos móviles. Adicional, la actualización debe hacerse de manera masiva en todos los dispositivos. Si una actualización es requerida, se debe invertir largos períodos de tiempo para realizarla, y esto se traduce, en no contar con la plataforma, y suspender las actividades de venta hasta su culminación.

- No existe diversidad en el manejo de modelos de dispositivos. Solo se tienen modelos de dispositivos móviles Intermec y Symbol.

- Vulnerabilidad en la seguridad. Al inicio de la implantación las sincronizaciones de los dispositivos móviles se hacían vía HTTP y a través de “cunas”, esto permitía que las operaciones se llevarán en forma segura dentro de las instalaciones de la empresa. Sin embargo, debido a requerimientos de flexibilidad y movilidad, se han expandido las operaciones a través de redes VPN[34] y con antenas, pero este esquema tiene vulnerabilidades en el ámbito de seguridad.

- Imposibilidad de actualización tecnológica. SAP ya no generará nuevas versiones de SAP NetWeaver Mobile (MI) ni actualizaciones del cliente que va en el dispositivo móvil, lo que obliga a moverse a nueva solución.

5.2 Nueva solución planteada

La nueva plataforma instalada está basada en los componentes de SAP NetWeaver ERP con la solución de DSD (en el “Backend”) y en las soluciones de SAP Mobile Platform SMP, Afaria y Relay Server para manejo de las operaciones HTTP(s) desde los dispositivos móviles. La interacción de estos componentes puede verse en la siguiente figura:

34 VPN: Virtual Private Network es una tecnología de red de computadoras que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet

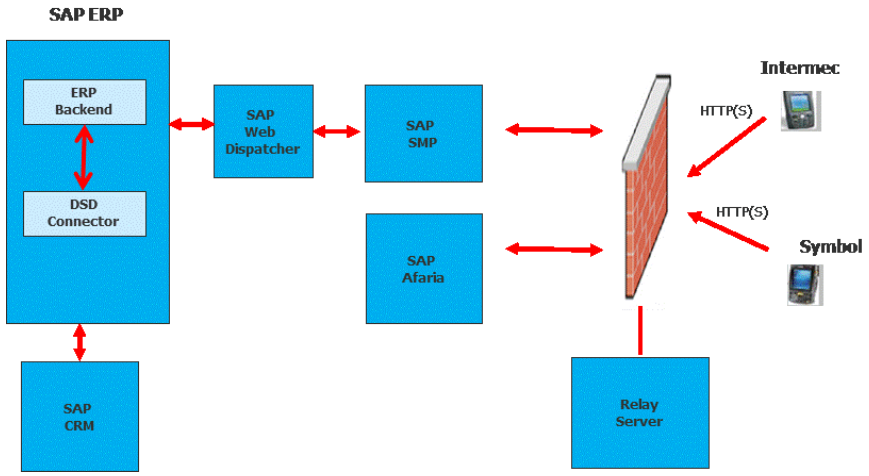


Figura 5.2.1 Plataforma nueva solución de SAP DSD con SAP SMP

5.2.1 Ventajas de la nueva plataforma

La nueva solución soporta las actividades de venta de la empresa, pero con varias ventajas con respecto a la solución anterior:

- Los requerimientos nuevos del negocio de ventas, tanto en el “Backend” como en los clientes de los dispositivos móviles es mucho más fácil y amigable. No se requiere inversión de desarrollos largos y costosos.

- La actualización de los dispositivos móviles puede manejarse de manera centralizada a través de AFARIA. Se establecen políticas de actualización y seguridad, que son llevadas a cabo por la operación de “enrolar” el dispositivo.

- Permite diversidad en el manejo de modelos de dispositivos. Actualmente se tienen modelos de dispositivos móviles Intermec y Symbol, para aprovechar la inversión hecha en la solución anterior, pero da la posibilidad de incluir dispositivos de nuevas tecnologías tales como IPhone y Android.

- Mayor esquema de seguridad. Se cuenta con una solución que permite operaciones HTTP´s a través de Internet con esquema de certificados y manejo seguro a través del Relay Server. Adicionalmente soporta un mecanismo de encriptación de datos suministrado por SAP SMP.

- Mayor flexibilidad y dinamismo, pues los vendedores no dependen de la red interna VPN para conectarse a los servidores de la empresa. Pueden usar las nuevas tecnologías del

mercado y usar las conexiones otorgadas por las operadoras de telefonía de manera segura (3G).

- Posicionamiento en la última tecnología de SAP para manejo y actualizaciones, tanto para los clientes que van en el dispositivo móvil, como en la solución de DSD para manejo de ventas.

5.2.2 Flujo de información a través de la nueva solución de SAP SMP

Tal y como se muestra en la siguiente figura, el dispositivo se conecta a través de una operación segura HTTPs desde la DMZ con el servidor de Relay Server (1). En el Relay Server se encuentran definidas las “farms” o “granjas” de servidores lo que habilita la conexión a SAP SMP (2). Desde SAP SMP se cuenta con dos tipos de conexiones hacia el “Backend” SAP ERP, una conexión tipo “Proxy” y otra “Web Service” (3 y 4). Internamente, el “Backend” SAP ERP maneja una conexión a otro “Backend” con la solución de SAP CRM. El “Backend” SAP ERP posee un esquema de autenticación del usuario hacia SAP SMP (5). Finalmente, SAP SMP envía la información segura al dispositivo (6). El servidor de SAP AFARIA habilita tanto las políticas de autenticación como la actualización del cliente que va a cada dispositivo móvil. Los usuarios y “password” se autentican a través del directorio activo de la solución Microsoft Windows (7).

Cabe resaltar, que entre SMP y el “Backend” SAP ERP existen dos servidores SAP Web Dispatcher, que permiten balancear la carga de trabajo HTTP y HTTPs hacia los distintos servidores de ERP. Igualmente, para balancear la carga entre ambos Web Dispatchers, se ha instalado una solución Network Load Balancing Services (NLBS) que es una implementación de Microsoft de “cluster” y balanceo de carga que está diseñada para proporcionar alta disponibilidad, confiabilidad y escalabilidad.

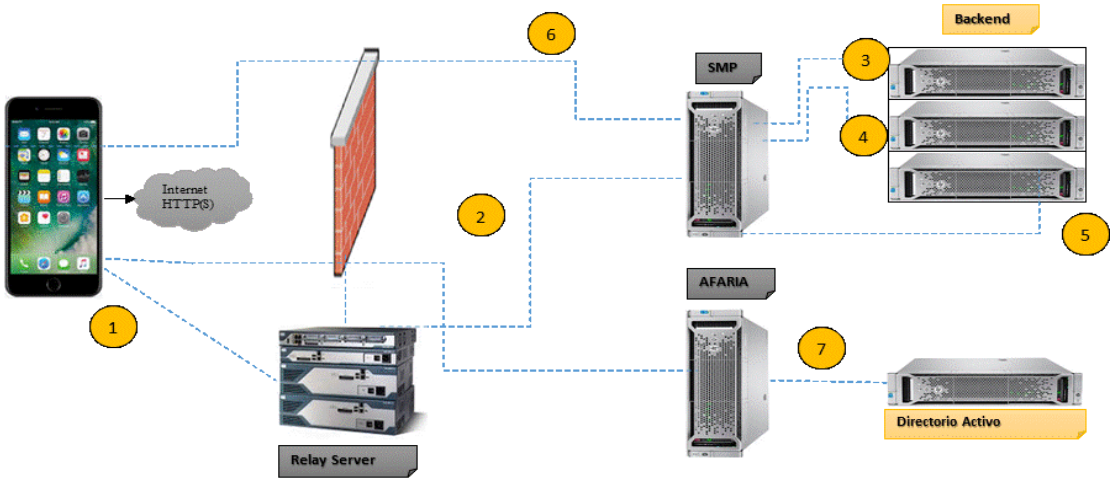


Figura 5.2.2.1 Flujo de información a través de nueva solución con SAP SMP

5.2.3 Conexiones y configuraciones entre los diferentes componentes de la solución SAP ERP/SMP

Desde la consola de SAP SMP (SCC) se crea un esquema de seguridad y se crean los usuarios de administración y los roles necesarios para establecer tanto la conexión, como las operaciones contra el "Backend" de ERP.

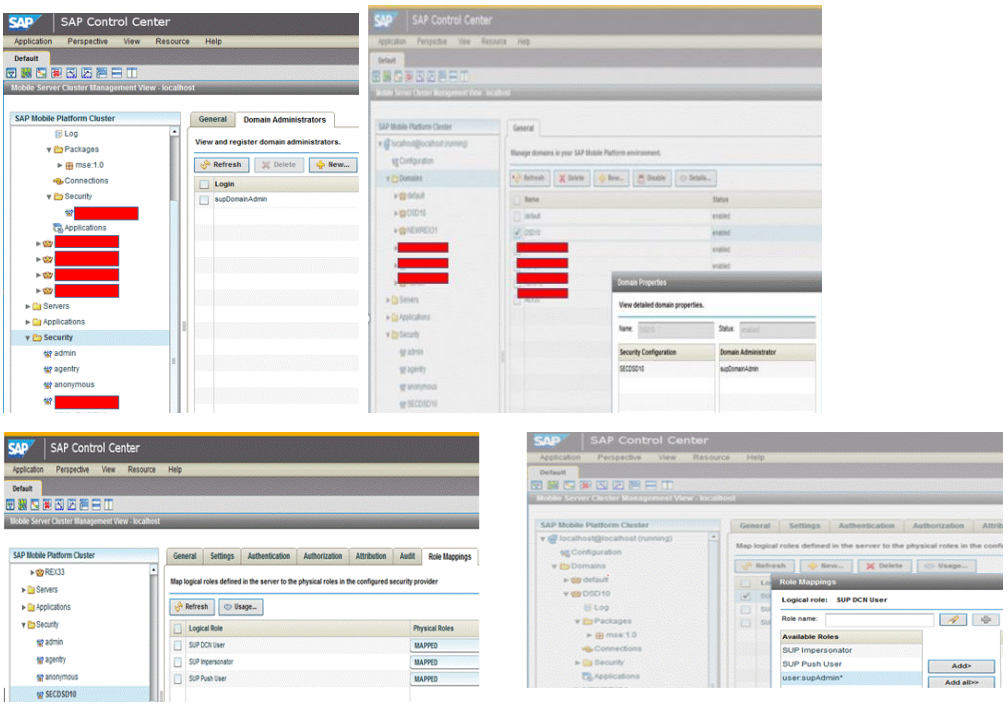


Figura 5.2.3.1 Esquema de seguridad desde consola de SAP SMP

Cada aplicación es manejada dentro de un domino o "Domain" dentro de la consola de SAP SMP (SCC) y es allí donde se hace una carga del paquete de software de la aplicación DSD ("Deploy" del paquete).

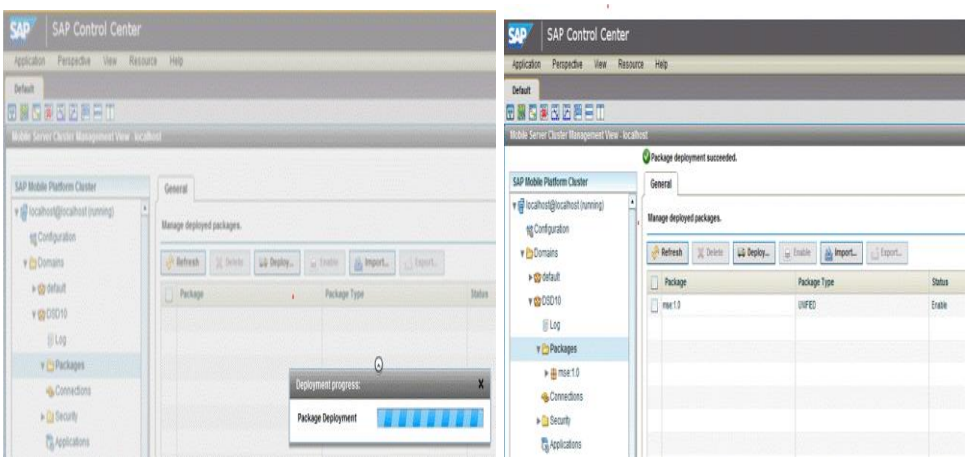


Figura 5.2.3.2 Carga de la aplicación DSD en SAP SMP

En cada “Domain” se deben definir dos conexiones, la primera tipo “Proxy” y la segunda tipo “Webservice”. Se especifican las direcciones URL[35] para conectar a los servidores de SAP ERP.

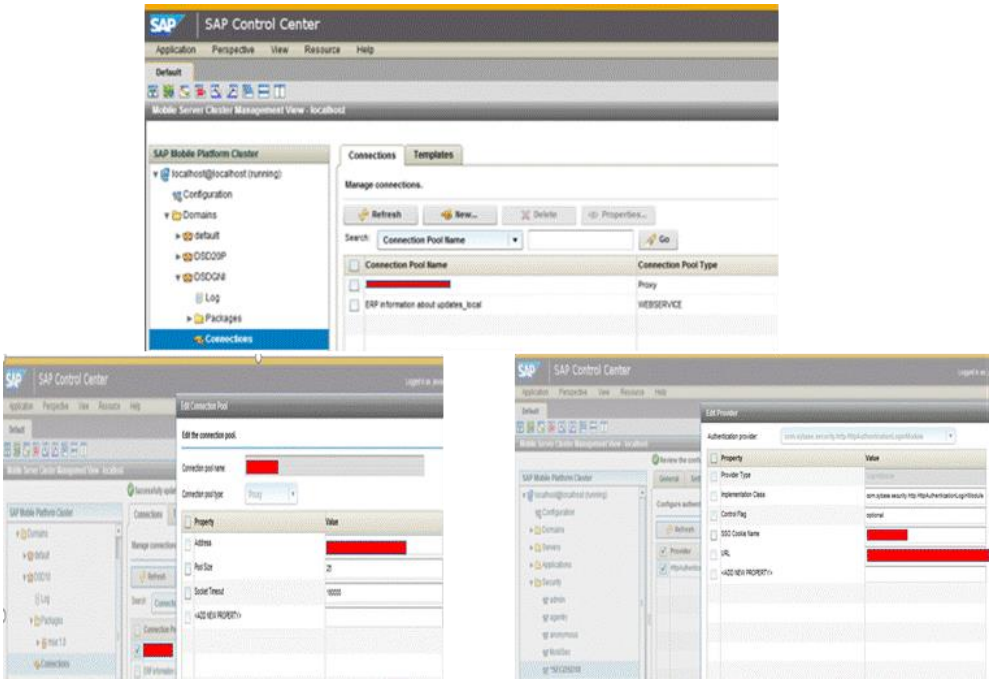


Figura 5.2.3.3 Conexiones de SMP hacia “Backend” ERP

Desde SAP ERP, también se define una conexión hacia el servidor de SAP SMP. Se debe especificar usuario y clave (“password”) con él que se autenticará.

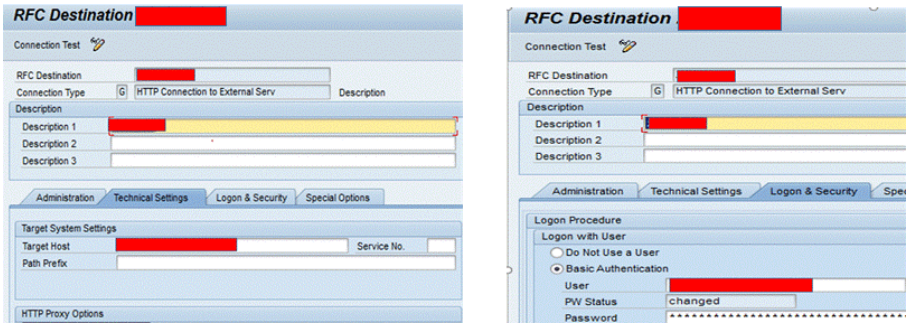


Figura 5.2.3.4 Conexiones de “Backend” ERP hacia SMP

[35] URL es la ruta que se encuentra ubicada en la barra de navegación del navegador, sirve para ubicar de manera precisa en un servidor, cualquier recurso: una imagen, un video o una página web.

Finalmente, cada “paquete” o aplicación tiene asociado un “Domain” y un esquema de seguridad.

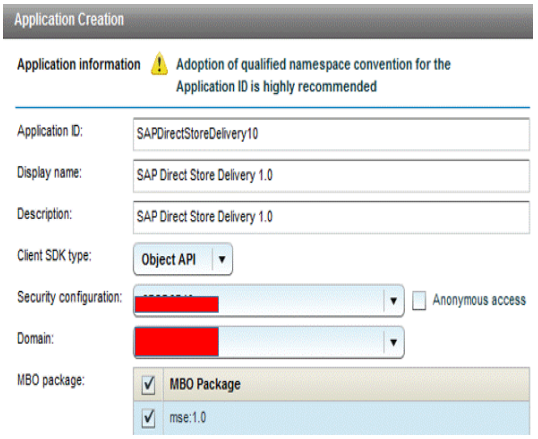


Figura 5.2.3.5 Paquete de DSD: especificación de Dominio y de esquema de Seguridad hacia SMP

Cada “paquete” tiene un “Connection Template” que no es más que un conjunto de especificaciones, en donde se suministra el nombre de la “granja” de servidores, los puertos usados y el URL con la dirección del servidor de Relay Server. La solución suministra “logs” donde se pueden ver los detalles de la “autenticación” de cada dispositivo, usuario, hora, etc.

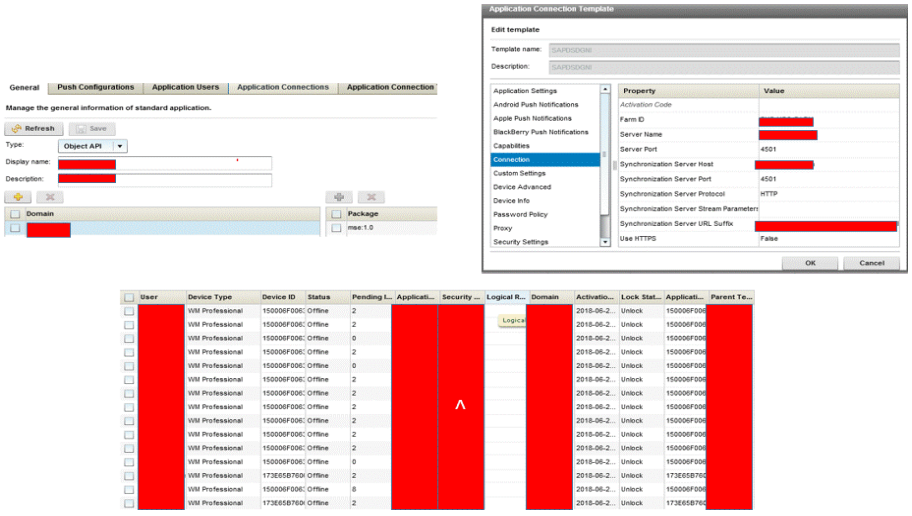


Figura 5.2.3.6 Definición de conexiones al Relay Server y detalles de autenticación de cada dispositivo móvil hacia SMP

5.2.4 Certificados digitales en la nueva solución de SAP SMP

El servidor SMP es el centralizador de los certificados que van a permitir las conexiones seguras desde y hasta los dispositivos móviles. Posee un área de “SSL[36] configuration” en donde se almacenan

36 SSL: Secure Sockets Layer: en español capa de puertos seguros) son protocolos criptográficos, que proporcionan comunicaciones seguras por una red, comúnmente Internet

los certificados. La solución incluye dos certificados tipo PKCS12[37]. Uno propio del servidor SMP y otro que permite la encriptación de los datos que viajan al dispositivo (MySelfSigned). Los otros certificados son tipo X.509[38], hay uno por cada uno de los servidores involucrados en la solución, esto incluye tanto los Web Dispatcher como cada servidor de la plataforma de SAP ERP.

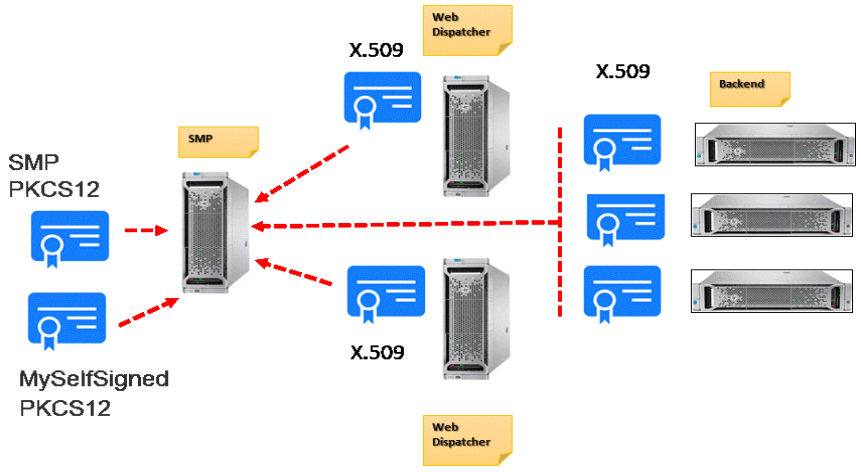


Figura 5.2.4.1 Certificados en solución SAP SMP

5.2.5 Solicitud, generación e importación de certificados en SAP ERP y SMP

Como se expuso anteriormente, es necesario que cada servidor SAP ERP cuente con un certificado. Dichos certificados son solicitados desde cada servidor SAP ERP y son de tipo SHA-2:

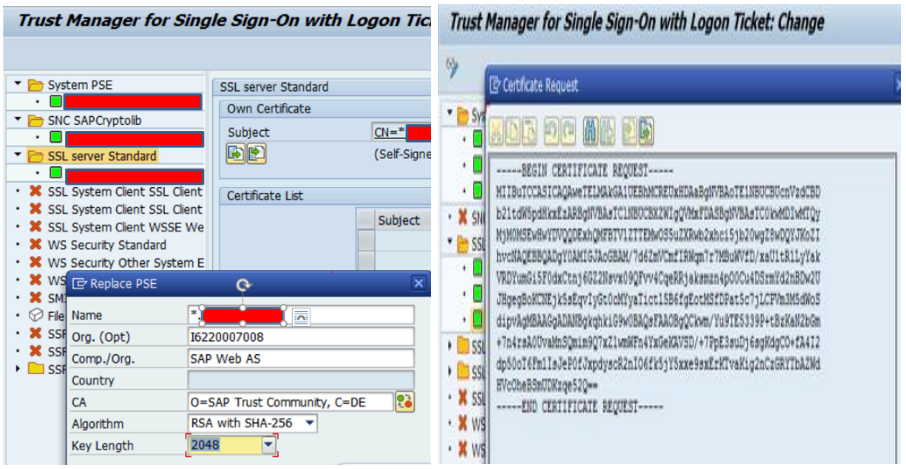


Figura 5.2.5.1 Solicitud y cuerpo de la solicitud de certificado desde SAP ERP

37 PKCS12: define un formato de fichero usado comúnmente para almacenar claves privadas con su certificado de clave pública protegido mediante clave simétrica.

38 X.509 es un estándar UIT-T para infraestructuras de claves públicas (en inglés, Public Key Infrastructure o PKI). X.509 especifica, entre otras cosas, formatos estándar para certificados de claves públicas y un algoritmo de validación de la ruta de certificación

Los requerimientos se envían a la entidad certificadora (CA). El archivo del certificado contiene la llave privada del mismo, y debe estar protegido por una contraseña, la contraseña de este certificado debe ser la misma del "keystore[39]" del servidor que lo solicita. SMP también debe contar con un certificado propio. A partir de la versión 3.3 de SMP 3.3, se genera una clave aleatoria que se almacena en un archivo plano.

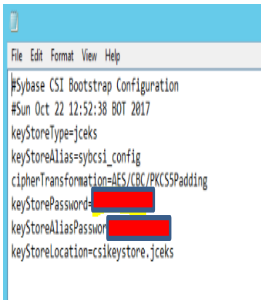


Figura 5.2.5.2 Archivo con la clave privada de certificado de SAP SMP

Para la emisión de cada certificado, se siguen varios pasos a través de la consola de la CA

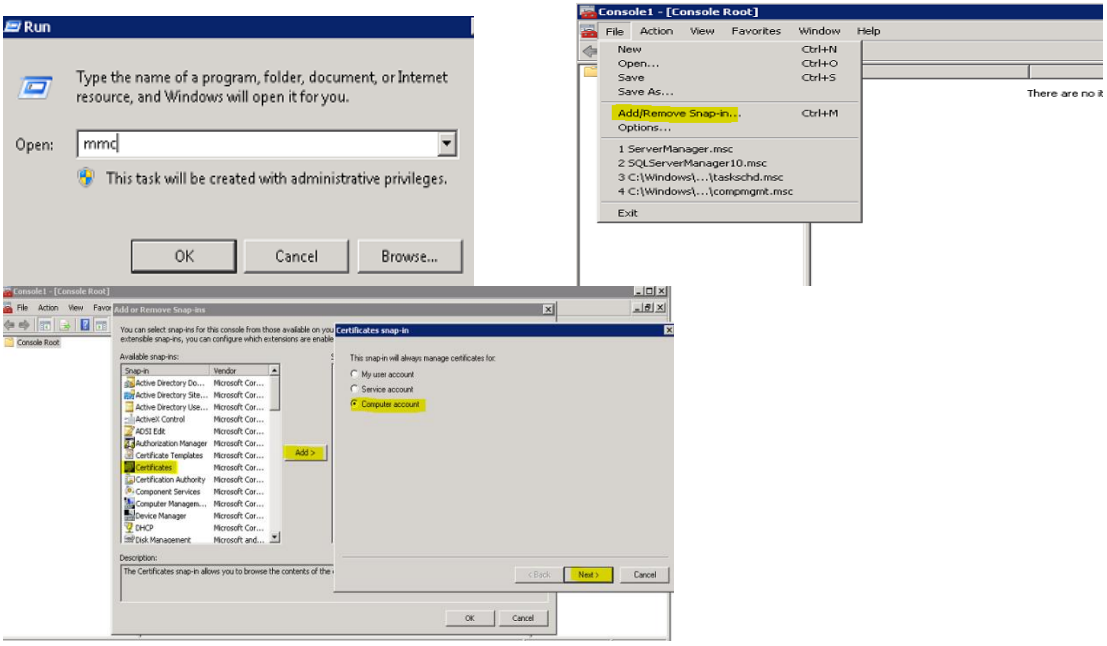


Figura 5.2.5.3 Consola de manejo de certificados en CA

[39] Keystore: es un repositorio de certificados de seguridad, ya sean certificados de autorización o certificados de clave pública, más las claves privadas correspondientes, que se utilizan, por ejemplo, en el cifrado SSL.

Se debe elegir la opción de “Request New Certificate” y el tipo de “Web server certificate”, incluyendo la opción de permitir exportar la clave privada.

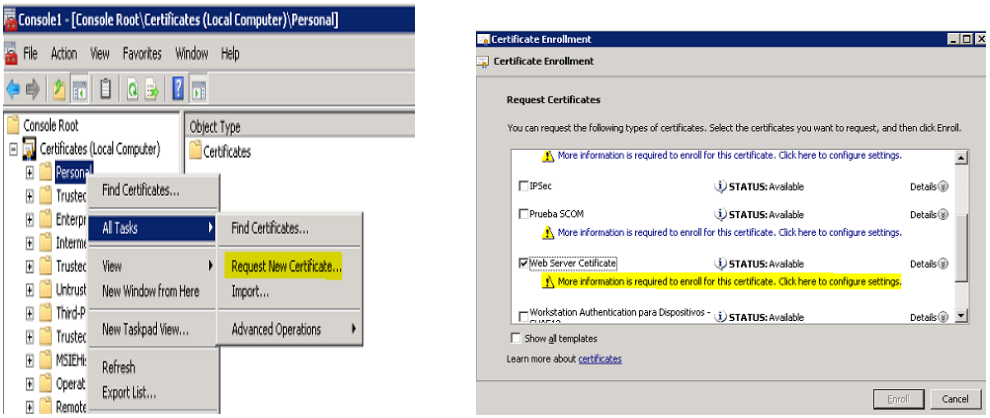


Figura 5.2.5.4 Consola de manejo de certificados en CA

Se agregan los “Common Names (CN)” que tendrá el certificado, generalmente se coloca el nombre del servidor y el nombre con el sufijo con el nombre del dominio de red. Luego se debe seleccionar “enroll”.

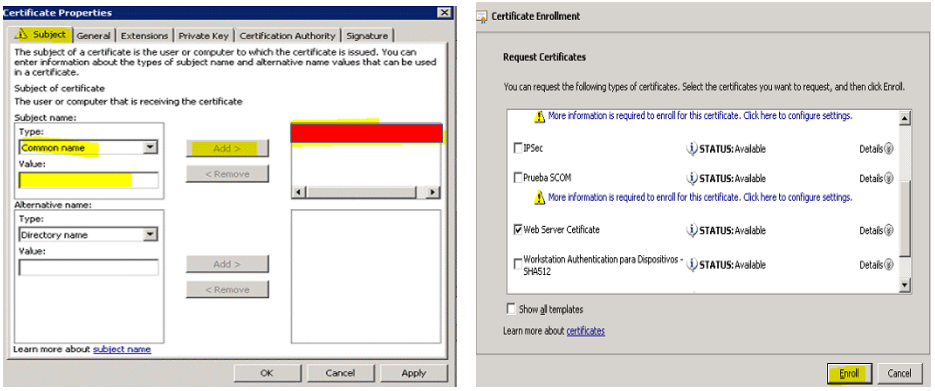


Figura 5.2.5.5 Generación de Web Service Certificate

Una vez que la CA genere el certificado este debe ser exportado.

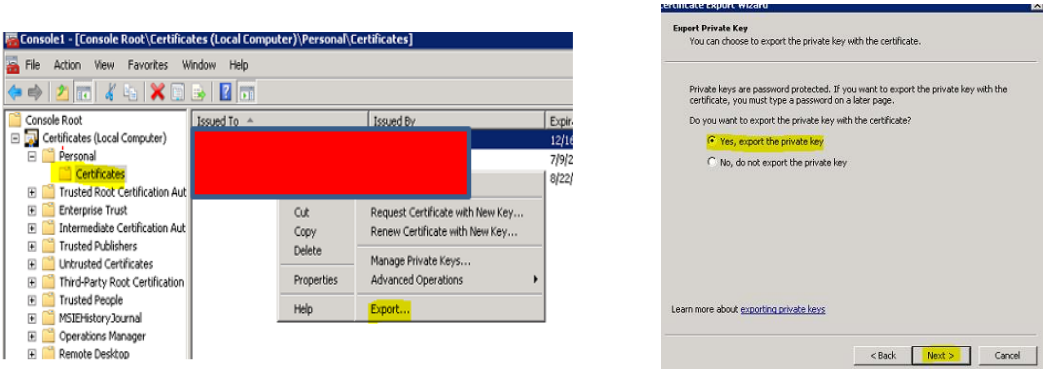


Figura 5.2.5.6 Exportar el certificado desde CA

Se coloca la clave privada que se tiene almacenada (en el “keystore”) y se exporta el certificado.

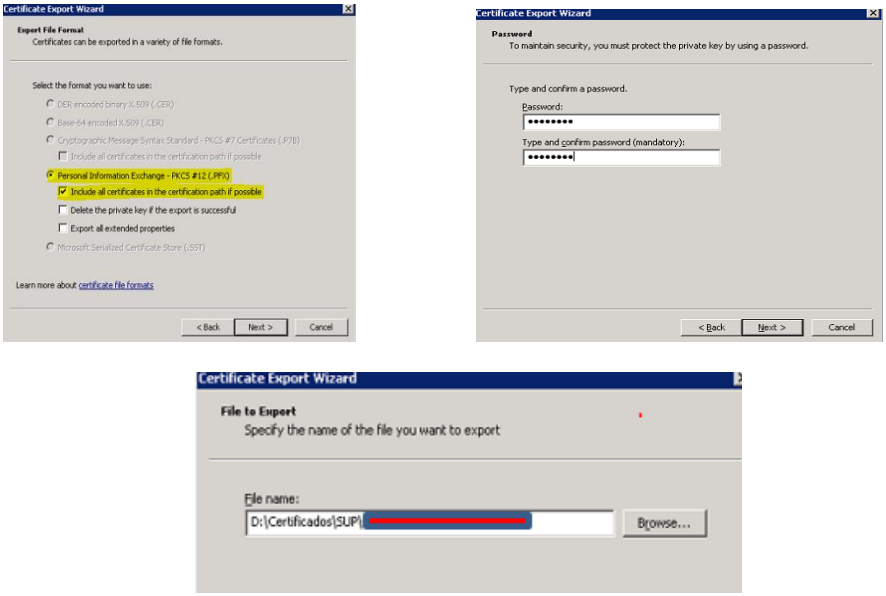
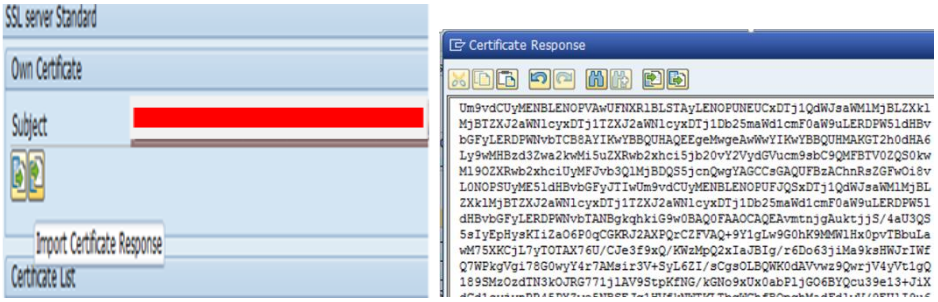


Figura 5.2.5.7 Clave privada en el “Keystore” y exportación del certificado

Dentro de SAP ERP se procede a importar la respuesta de cada certificado



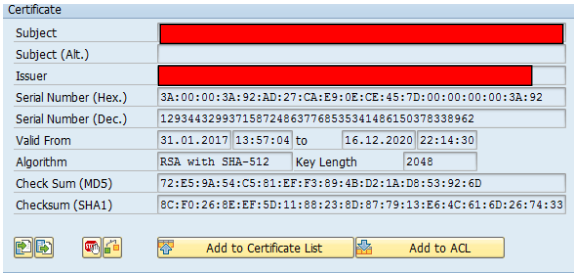


Figura 5.2.5.8 Importación de la respuesta de certificado en SAP ERP

Desde la consola de SAP SMP (SCC) se deben importar todos los certificados. Tanto los propios de SMP como el de encriptado de datos, que son tipo PKCS#12.

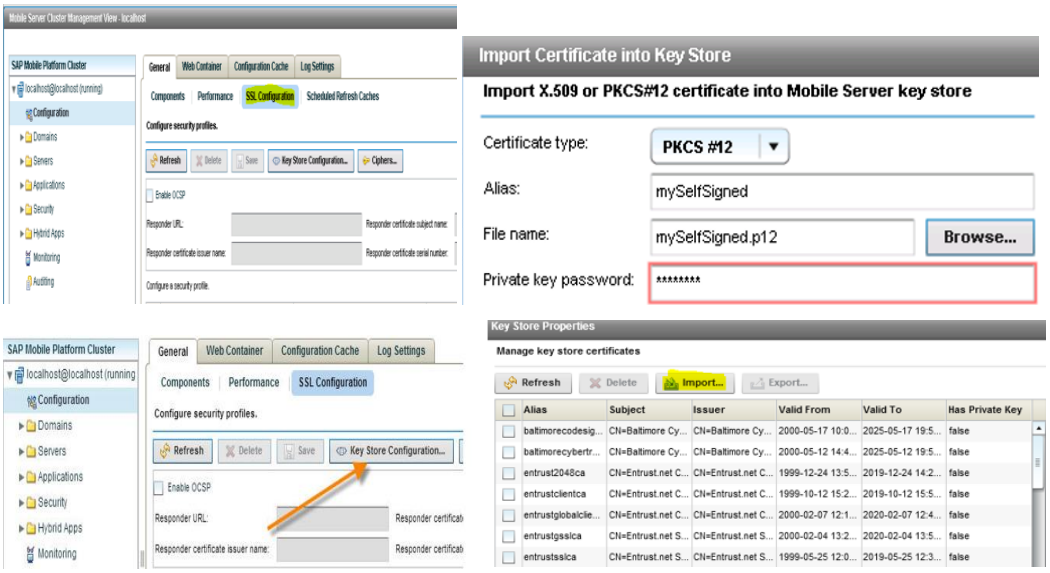


Figura 5.2.5.9 Importación de los certificados PKCS#12 en SAP SMP

También se deben importar los certificados X.509, de cada servidor de SAP ERP y Web Dispatchers dentro de la consola de SAP SMP (SCC):

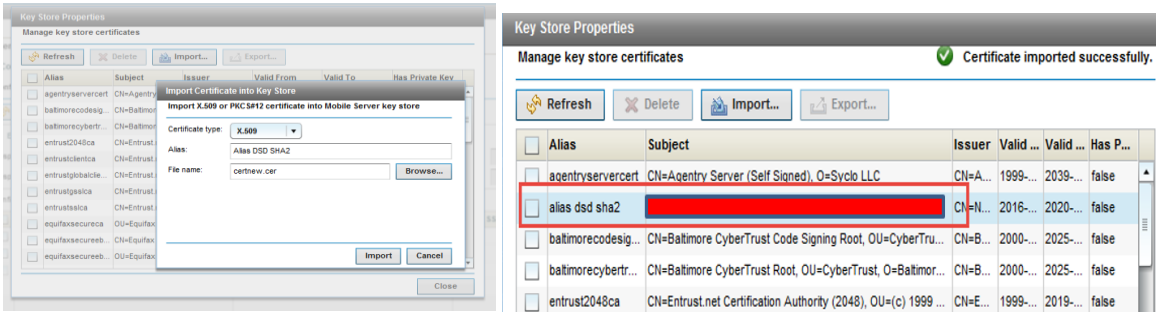


Figura 5.2.5.10 Importación de los certificados X.509 en SAP SMP

5.2.6 Utilización de firmas digitales en SAP DSD

Con la firma digital, el sistema SAP ERP proporciona una herramienta para firmar y aprobar datos digitales. La firma digital garantiza que el firmante de un documento digital, se puede identificar sin ambigüedades y su nombre se documenta junto con el documento firmado, la fecha y la hora. Puede usar la firma digital para aprobar documentos u objetos en todas las aplicaciones configuradas para su uso.

El objetivo de la herramienta de firma es proporcionar un diálogo de usuario para la firma de documentos. El usuario puede mostrar el documento que se va a firmar. El usuario verifica el documento. Si no hay problemas, él o ella proporciona una firma o cancela la firma digital si los chequeos que se ejecutan cuando se proporciona una firma producen resultados que indican errores. Los datos relacionados con la firma proporcionada se guardan y pueden evaluarse en un momento posterior.

Desde la solución de SAP DSD en el “Backend” de ERP, se configuran los tipos de documentos que requerirán firma digital. Particularmente, para la solución que está siendo implantada, se usará para los pedidos de venta.

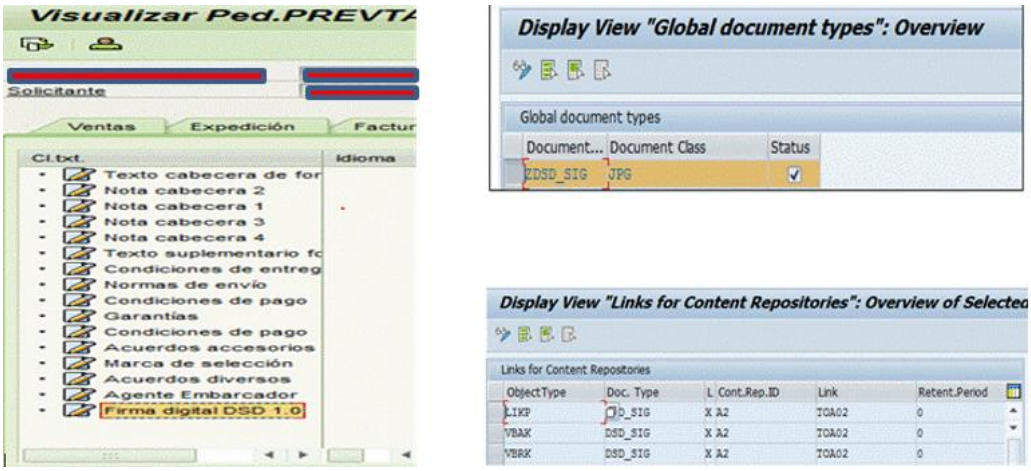


Figura 5.2.6.1 Parte de la configuración en la solución SAP DSD para firma digital

Es importante definir los servidores y directorios donde se almacenarán estos documentos.

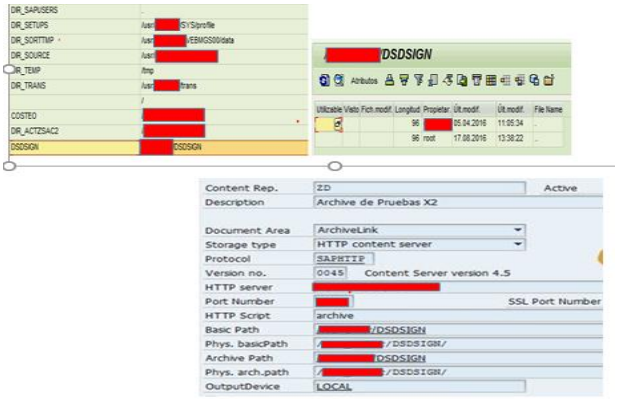


Figura 5.2.6.2 Configuración de los repositorios en SAP DSD de los documentos con firma digital

5.2.7 Registro del dispositivo móvil en el inventario (SAP AFARIA)

A continuación, se exponen las acciones requeridas para registrar un dispositivo en el inventario, a través de la herramienta de SAP AFARIA.

Se debe seleccionar la aplicación “Afaria” desde el dispositivo móvil (1) y luego se debe elegir la opción “Connect” (2), tal como se muestra en la figura.

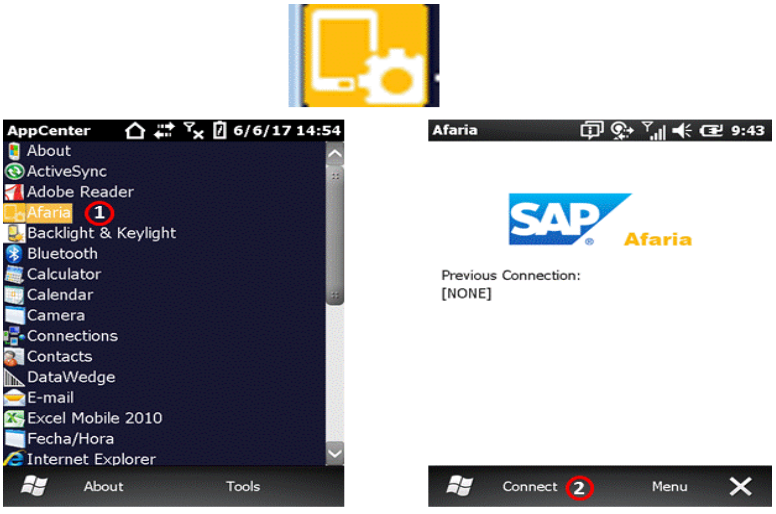


Figura 5.2.7.1 Dispositivo móvil con Afaria

A continuación, se realizan una cantidad de pasos desde el dispositivo móvil (DM) a través de Afaria:

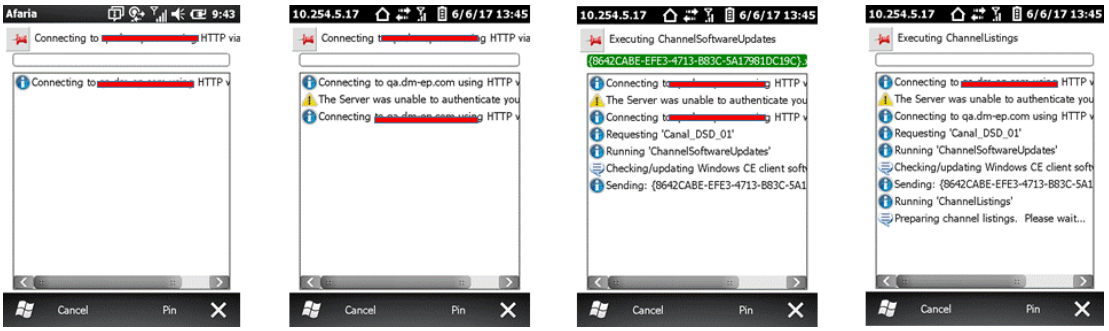


Figura 5.2.7.2 Pasos del DM en SAP Afaria

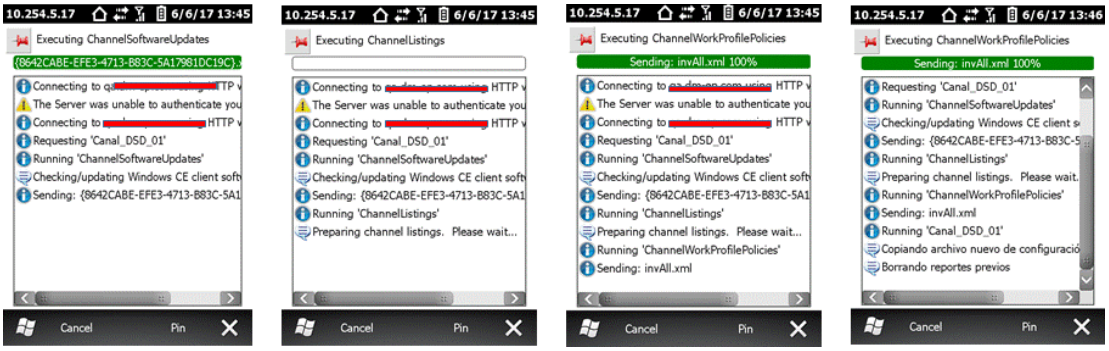


Figura 5.2.7.3 Pasos del DM en SAP Afaria

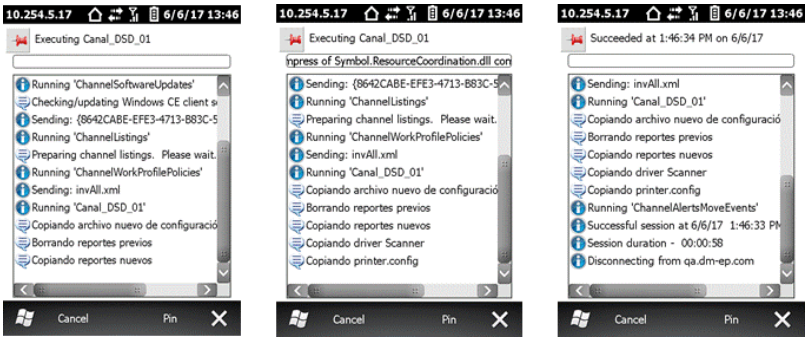


Figura 5.2.7.4 Pasos del DM en SAP Afaria

Para confirmar la comunicación con servidor de Afaria se debe elegir el botón de “Afaria”, luego “Menú” y presionar “Log”.

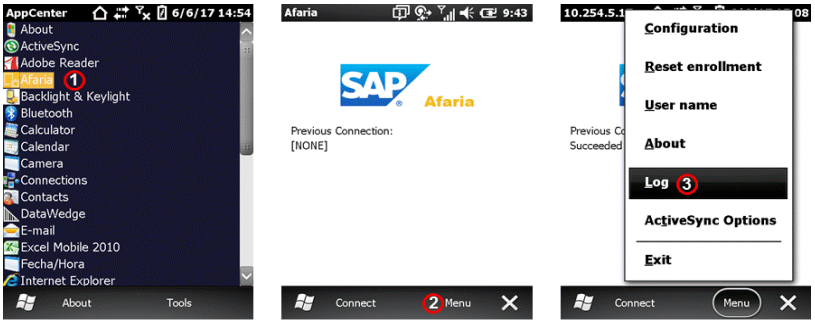


Figura 5.2.7.5 Pasos de comunicación con servidor Afaria y revisión de “logs”

Se visualiza la secuencia de los pasos realizados por el dispositivo móvil (DM) durante la ejecución de AFARIA.

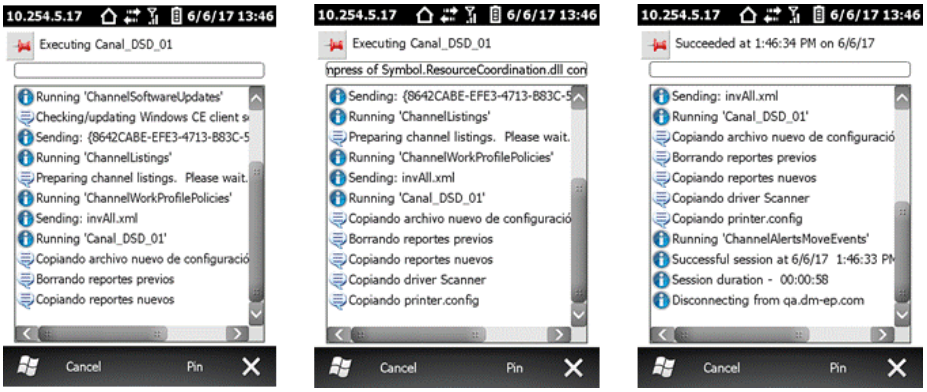


Figura 5.2.7.6 Secuencia de pasos en DM durante ejecución Afaria.

5.2.8 Configuración del dispositivo móvil (DM) o Hand Held (HH)

En cada dispositivo móvil o Hand Held, existe un archivo de configuración en donde se especifican datos propios de conexión como dirección del URL del Relay Server, Dominio de SMP, conexión Proxy hacia ERP, puertos, nombre del paquete, etc. También se especifican parámetros de configuración tales como tamaños de los “logs”, tiempos de conexión, etc.

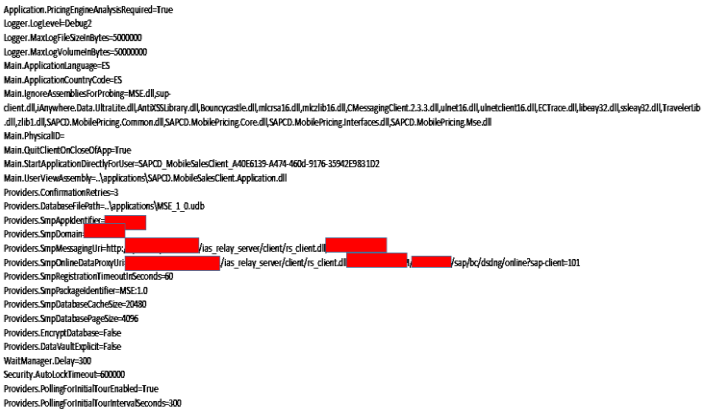


Figura 5.2.8.1 Parámetros de configuración en el HH.

5.2.9 Sincronización desde el dispositivo móvil (DM) o Hand Held (HH)

Esta sesión muestra las operaciones a realizar dentro del Hand Held (HH) para una ejecución de ventas. Primero se debe actualizar los datos de la ruta (“Download”) y luego subir los datos de la venta (“Upload”). Para obtener los datos de la ruta, se debe seleccionar el icono de sincronizar (1) y luego optar por “Sinc” (2) para iniciar la sincronización.

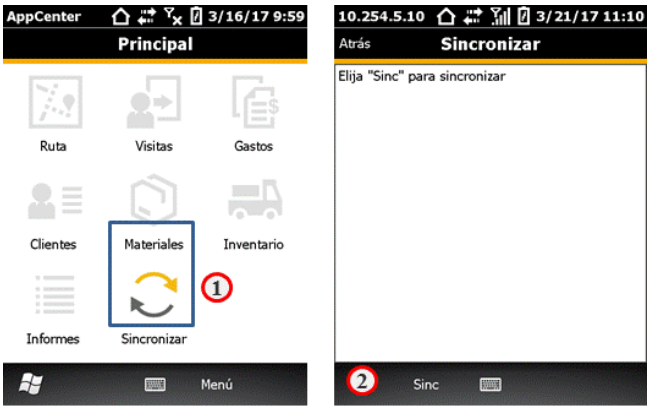


Figura 5.2.9.1 Sincronización de HH

El dispositivo móvil DM se conecta al servidor de SAP SMP y desde allí se extraen los datos del de la ruta correspondiente desde el “Backend” SAP ERP.

Figura 5.2.9.2 Descarga de datos de la ruta al HH

Una vez culminada la sincronización, se selecciona “Atrás” (3) para ir al menú principal

Figura 5.2.9.3 Finalización de descarga de datos

Una vez se culminan las operaciones de venta, es necesario hacer el “upload” de los datos para que se registren en el “Backend” SAP ERP. Este proceso también es denominado sincronización final. Se debe elegir el icono de ruta (1). Seleccionar “Fin” (2) para finalizar la ruta, registrar el kilometraje final ingresando en “Odométro[40]” y luego “Siguiente” (3).

[40] Odómetro: aparato en forma de reloj de bolsillo que sirve para contar el número de pasos que da la persona que lo lleva y medir la distancia que ha recorrido.

Figura 5.2.9.4 Sincronización final

Elegir “Sincronizar” (5), luego “Sinc” (6) para iniciar la sincronización. Este proceso tarda unos minutos. Una vez concluido el proceso se presiona “Atrás” (7) para ir a la pantalla inicial.

Figura 5.2.9.5 Fin de sincronización de los datos de venta

5.2.10 Herramientas de monitoreo y “logs”

La solución provee de varias herramientas de monitoreo y “logs”. Existen monitores técnicos tanto en SAP ERP como en AFARIA y SMP, que permiten determinar los tiempos de respuesta de cada operación, suministrar alertas sobre umbrales que ajustar como memoria, espacio en disco, tiempos de cancelación, etc.

También provee “logs” que ayudan a determinar problemas de autenticación con los usuarios y claves (“passwords”), si el dispositivo móvil logró conexión, si se culminó la sincronización, problemas con los certificados, vencimientos de los mismos, etc. Todas estas herramientas son útiles tanto en la

administración de la plataforma, como en el soporte de las operaciones del negocio, así como también son medios para facilitar tareas de auditoría a la hora de algún requerimiento o problema.

User	# Steps	T Response Time	Ø Time	Process.	Avg. Proc. Time	T CPU~	Ø CPU~	T DB Time	Ø DB Time	T Time	Ø Time	T Roll Wait Time
[redacted]	3	1.113	371.082,0	24	8.021,3	21	6.901,0	427	142.298,7	0,0	0,0	662
[redacted]	3	786	262.057,7	12	3.950,7	8	2.578,0	462	153.845,0	0,0	0,0	313
[redacted]	2	771	385.349,0	11	5.654,0	8	4.070,5	385	192.482,5	0,0	0,0	374
[redacted]	2	766	382.881,5	15	7.486,5	15	7.500,0	442	220.931,5	0,0	0,0	309
[redacted]	1	737	736.666,0	10	9.745,0	7	6.766,0	423	422.879,0	0,0	0,0	304
[redacted]	1	719	718.557,0	0	0,0	7	6.672,0	469	468.931,0	0,0	0,0	237
[redacted]	1	700	700.266,0	9	8.829,0	6	6.484,0	393	392.759,0	0,0	0,0	299
[redacted]	1	672	672.307,0	10	9.762,0	8	7.563,0	331	330.896,0	0,0	0,0	332
[redacted]	1	657	656.507,0	7	7.216,0	6	5.828,0	449	449.297,0	0,0	0,0	200
[redacted]	1	655	654.530,0	8	8.108,0	6	5.938,0	343	342.545,0	0,0	0,0	304
[redacted]	3	650	216.763,7	11	3.661,7	7	2.442,7	252	83.995,3	0,0	0,0	387
[redacted]	1	623	623.058,0	9	9.442,0	8	7.672,0	370	370.376,0	0,0	0,0	243

Report or Transaction name	# Steps	T Response Time	Ø Time	Process.	Avg. Proc. Time	T CPU~	Ø CPU~	T DB Time
/DSD/SAPLME_STATUS_CONTROL	13.250	91.933	6.938,4	38.181	2.881,6	46.070	3.477,0	42.953
SAPLME_GEN_DSD	940	91.707	97.560,9	38.662	41.129,3	50.006	53.198,2	51.668
/SDF/IS_PROXY	65.292	83.091	1.272,6	81.266	1.244,6	45.375	695,0	30
/DSD/SAPLME_DE_ADDON	836	71.832	85.923,1	37.648	45.033,0	58.889	70.441,1	34.121
CL_BGRFC_SUPERVISOR_START=====CP	3.452	69.600	20.162,1	330	95,7	128	37,0	29
/DSD/SAPLME_STATDAT	762	63.697	83.592,1	1.890	2.481,0	491	644,0	3.783
/EMSE/SAPLME_DE_ADDON	64	31.994	499.912,8	15.192	237.369,1	21.088	329.498,8	16.457

Figura 5.2.10.1 Fin de sincronización de los datos de venta

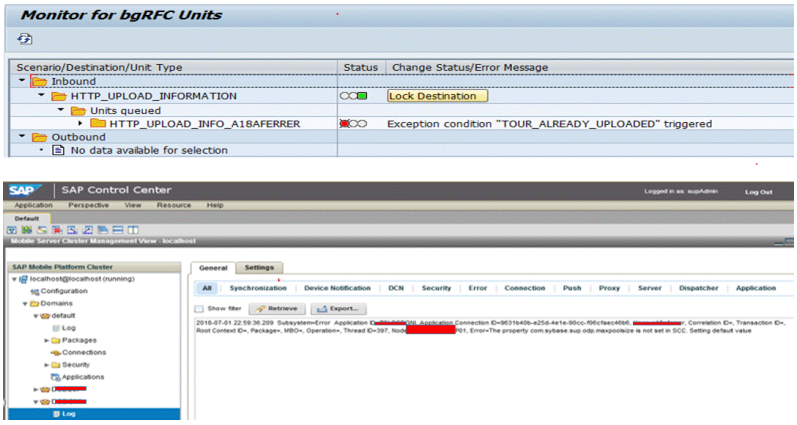


Figura 5.2.10.2 Los de SAP ERP y “logs” de SMP con errores y resultados de operaciones

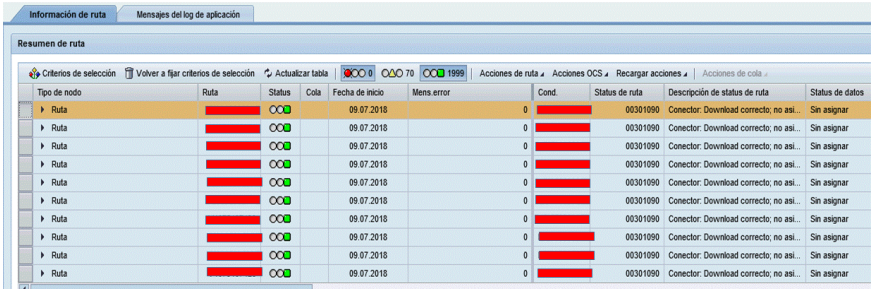


Figura 5.2.10.3 Log Monitor para ver el estado de las rutas

CAPITULO VI. ANALISIS DE RESULTADOS

Para hacer un análisis de los resultados es conveniente enfocarse en los objetivos planteados y en los logros obtenidos:

- La solución satisface las necesidades de intercambio de información y de datos transaccionales entre los trabajadores, oficinas, localidades remotas y clientes a través de dispositivos móviles de forma segura y confiable. Cumple a cabalidad con el objetivo planteado empleando el algoritmo de hash SHA256 con RSA, pues permite generar valores apropiados para el par de clave pública y privada (SAP SMP y SAP ERP). Mantiene el acceso externo restringido y resguardado a través de claves de protección (Relay Server y SAP SMP). Se garantiza el encriptado de los datos de las operaciones (SAP SMP). Se establecen políticas de actualización y seguridad de los dispositivos (AFARIA). Se brinda confidencialidad, integridad de la información y no repudio. Puede haber vulnerabilidades de seguridad ante futuras explotaciones de los protocolos de cifrado, por lo cual se debe trabajar en proceso de mejoras y actualización continuo.

- Beneficia a los usuarios en la operación de ventas y distribución de los productos. Hay un menor esfuerzo en la labor operativa. Las actividades de los vendedores para ejecutar el proceso de pre venta, se realizaba de manera manual por limitantes de la cantidad de dispositivos móviles. Esta solución suministra más herramientas para apoyar su trabajo. Hay un incremento en los indicadores de venta y de atención a los clientes, lo que se traduce en mayores beneficios para la empresa. Como posible desventaja, se requiere de una inducción en el uso de las herramientas tecnológicas y hay dependencia de la tecnología para realizar las operaciones.

- Habilita el manejo de documentos transaccionales mediante registro de firmas digitales (SAP ERP DSD). La configuración solo se realizó para las operaciones de pedidos y aún se encuentra en fase de pruebas. Puede que sea necesario la extensión de la solución para otros documentos. Cambios tecnológicos o innovaciones modernas pueden presentar vulnerabilidades que impliquen una oportunidad de mejora, por ejemplo, incluir firma digital con la huella dactilar del empleado, pero actualmente suministra confiabilidad, seguridad en la realización del pedido y elementos de auditoría.

- Otorga mayor flexibilidad y dinamismo en las operaciones de venta. Los vendedores no dependen de la red interna VPN para conectarse a los servidores de la empresa. Pueden usar las nuevas tecnologías del mercado y usar las conexiones otorgadas por las operadoras de telefonía (3G) de manera segura a través del Relay Server. Los requerimientos nuevos del negocio de ventas, tanto en el “Backend” como en los clientes de los dispositivos móviles es mucho más fácil y amigable.

No se requiere inversión de desarrollos largos y costosos para hacer adecuaciones a las necesidades cambiantes del negocio.

- Suministra mayor información sobre el flujo de datos, para seguimiento y control. Se cuenta con herramientas de monitoreo y generación de reportes, que permitan hacer seguimiento del flujo correcto de las operaciones y se brindan mecanismos para auditorias y prevención de ataques, fraudes o robos (SAP SMP y SAP ERP). También apoya al área de negocio, pues puede determinarse que realizó el vendedor y se cuentan con mecanismos de auditoría y control de inventario (SAP ERP DSD)

- Mejora el posicionamiento tecnológico. Se cuenta con la última tecnología de SAP disponible, lo que garantiza mayor seguridad, soporte y mejoras en general para las operaciones de venta y distribución. Permite habilitar dispositivos de nuevos modelos como IPhone y Android. Esto tiene una desventaja, que es la dependencia en los desarrollos y versiones nuevas que realice SAP. Sin embargo, es resaltante que esta solución da mayor flexibilidad y dinamismo. Los requerimientos nuevos del negocio de ventas, tanto en el “Backend” como en los clientes de los dispositivos móviles, es mucho más fácil y amigable. Los cambios de versión del software a nivel de dispositivos, puede manejarse de manera escalonada y no implica un cambio masivo de todos los dispositivos a la vez, lo que hace más viable actualizarlos en las nuevas versiones.

CAPITULO VII. CONCLUSIONES

- Este trabajo de grado satisface las necesidades de intercambio de información y de datos transaccionales para la Empresa XYZ, entre sus trabajadores y clientes, a través de dispositivos móviles de forma segura y confiable. La solución cumple a cabalidad con el objetivo planteado, empleando mecanismos de seguridad a través de manejo de certificados, encriptación de datos y manejos de firmas digitales. La solución brinda confidencialidad, integridad de la información y no repudio.

- Se logran mejoras en la integridad, disponibilidad y prestación de servicios de técnicos e información, pues hay disminución de problemas operacionales, mayor conocimiento por parte del personal técnico especializado, reducción de los costos relacionados con pérdidas de información por incidentes de seguridad y reducción de la manipulación de información confidencial por personas no autorizadas.

- También se otorgan políticas y mecanismos de actualización de los dispositivos móviles, lo que se traduce en mayor control de las versiones de software implicadas en cada dispositivo y por ende del mayor control y manejo del inventario de los activos de la empresa (dispositivos móviles).

- Suministra herramientas de control, monitoreo y “logs” para el soporte, mantenimiento y auditoría de las operaciones. Esto se traduce en mejoras en las operaciones de venta, pues el tiempo de resolución de problemas es menor. Se facilitan las labores de auditoría de los equipos ante casos de pérdida, fraude o robo. Adicional, hay un incremento de habilidades técnicas relacionadas con la detección, prevención y corrección de incidentes que pudieran atentar contra la información de las operaciones de venta y distribución de la organización.

- La implantación de la solución de SAP DSD en todas las sucursales de la empresa ayudará a disminuir los costos de mantenimiento de los sistemas, pues se minimiza la dependencia de adecuaciones hechas en casa y se cuenta con único sistema robusto estándar para soportar las operaciones comerciales.

- Al tener todos los datos del negocio en una misma aplicación se tiene una visión completa del proceso de ventas y distribución y esto facilita también la toma de decisiones, tanto a nivel de la alta gerencia como a nivel de la gerencia operativa.

- A nivel de los procesos es de vital importancia que los autores involucrados se les brinde entrenamiento para comprender tanto el nuevo proceso de ventas, las responsabilidades definidas en cada rol y en el uso de las nuevas herramientas tecnológicas que deben ser usadas. Es

importante que los usuarios sean entrenados para comprender el flujo continuo de los procesos de la operación comercial.

- Se solicitaron varios cambios al proveedor de las aplicaciones para que se incluyeran características propias de la Empresa XYZ. Algunos de los cambios fueron implantados en la aplicación estándar SAP DSD, mientras otros son adecuaciones propias para la empresa. La entrega oportuna de estas adecuaciones fue un factor crítico de éxito para el proyecto.

- Se beneficia a los usuarios en la operación de ventas y distribución de los productos, pues se simplifica, y por tanto hay un menor esfuerzo en la labor operativa. Hay una mejoría considerable en el esquema anterior, pues hay un incremento en los indicadores de venta y de atención a los clientes, lo que se traduce en mayores beneficios para la empresa.

- El adecuado uso de las herramientas propuestas se fundamenta en el conocimiento que de ellas tiene la fuerza de ventas. El factor humano es de vital importancia para lograr sinergias, al involucrar, capacitar y actualizar a los trabajadores en las herramientas y procesos de forma constante.

CAPITULO VIII. RECOMENDACIONES

- Dado que los temas de criptografía y seguridad son muy cambiantes, y que pueden existir futuras explotaciones de los protocolos de cifrado, se debe trabajar de manera continua en mejoras y actualización de la solución, tratando de mantener en la medida de lo posible las últimas versiones en cada uno de los componentes. Por ello es importante mantener una constante revisión de las nuevas facilidades que anuncie SAP sobre hallazgos de vulnerabilidades y/o soluciones (SAP SMP, SAP AFARIA, SAP DSD, SAP ERP, etc.).

- Dada la dependencia de las operaciones del negocio con esta solución tecnológica es prioritario mantener un plan de contingencia ante riesgos de pérdida de conexión, perdida de servicio, perdida de servidores, etc. Se tienen equipos y estrategias que garantizan la alta disponibilidad de los equipos y las conexiones internas, pero hay ciertos elementos externos o de terceros que no dependen de la empresa, por ejemplo, las comunicaciones otorgadas por las empresas de telefonía, por lo cual es vital que se cuenten con dichos planes de contingencia.

- Ampliar y explotar las herramientas de monitoreo y “logs” de cada componente de la solución a fin de contar con mayores indicadores, tanto para agilizar las transacciones, como para garantizar la seguridad y mecanismos de auditoría de las operaciones de venta.

- Con esta solución se mejoran los procesos y procedimientos en la cadena logística, pero estos se deben auditar constantemente para mantener la calidad del servicio.

- Continuar con el manejo de documentos transaccionales mediante registro de firmas digitales para el caso de los pedidos y evaluar si puede extenderse la solución a otro tipo de documentos. Cambios tecnológicos o innovaciones modernas pueden presentar vulnerabilidades que impliquen una oportunidad de mejora, por ejemplo, incluir firma digital con la huella dactilar del empleado.

- En caso de que se requieran adecuaciones, cambios o mejoras de la plataforma, es importante que los usuarios finales entiendan las bondades que estas actualizaciones representarán y como influirán positivamente en sus labores, de manera de crear expectativas positivas y se evite en lo posible la resistencia al cambio. Igualmente, es importante que cuenten con el adiestramiento adecuado para el uso de las nuevas herramientas tecnológicas.

- Por ser una solución bastante nueva, al inicio de este proyecto no se contaba con mayor información ni documentación sobre los pasos a seguir. SAP suministró algunas guías y manuales, pero las adecuaciones y configuraciones de la solución, fueron plasmadas en

documentos propios de Empresa XYZ los cuales deben ser revisados en caso de requerirse cambios o mejoras en la plataforma.

- Un proyecto de esta índole es justificable en la medida que presente beneficios tangibles para la empresa, es por ello que se le debe dar seguimiento a todos los indicadores claves de gestión una vez implantadas las futuras mejoras en el sistema.

- El presente trabajo demostró que el uso de firmas y certificados digitales mejora los niveles de seguridad de la información, por lo tanto, es importante que estos mecanismos sean tomados en cuenta para otras soluciones similares.

- La concientización en seguridad de información empresarial es una necesidad vital de las empresas pues tiene como objeto el resguardo de la información y de los activos, contra amenazas y vulnerabilidades tecnológicas. Es importante que Empresa XYZ, cuente con un enfoque de entrenamiento y educación apropiada que conduzca al desarrollo de una cultura de seguridad de la información; donde el personal adopte la política de seguridad de la organización, la respalde durante la ejecución de sus tareas normales y tenga la sensibilización para responder segura e intuitivamente a la acción de agentes que pongan en riesgo la seguridad de la información, en cualquiera de sus dimensiones: confidencialidad, disponibilidad e integridad.

- Se recomienda realizar una auditoría de sistemas externa una vez al año y realizar una auditoría de sistemas interna dos veces al año para certificar el mantenimiento de niveles de riesgo o identificar nuevas debilidades en la solución implantada.

CAPITULO IX. GLOSARIO DE TERMINOS

3G: 3G es la abreviación de tercera generación de transmisión de voz y datos a través de telefonía móvil.

Active Directory (AD) o Directorio Activo: son los términos que utiliza Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadores.

ActiveSync: es un programa de sincronización de datos desarrollado por Microsoft.

Android: es un sistema operativo basado en el núcleo Linux. Fue diseñado principalmente para dispositivos móviles con pantalla táctil, como teléfonos inteligentes, “tablets” o teléfonos; y también para relojes inteligentes, televisores y automóviles.

APIs (Application Programming Interface): la interfaz de programación de aplicaciones, es un conjunto de subrutinas, funciones y procedimientos (o métodos, en la programación orientada a objetos) que pueden ser utilizado por otro software.

App: aplicaciones que pueden ser cargadas y descargadas a los dispositivos móviles.

Apple Store App: es un servicio para iPhone que permite a los usuarios buscar y descargas aplicaciones de Apple.

Backend: Sistema de gestión empresarial de una empresa en donde se llevan a cabo los procesos medulares de gestión de la empresa.

CA: Certification Authority. En criptografía una autoridad de certificación, certificadora o certificante (AC o CA por sus siglas en inglés Certification Authority) es una entidad de confianza, responsable de emitir y revocar los certificados digitales o certificados, utilizados en la firma electrónica, para lo cual se emplea la criptografía de clave pública.

Cluster: es un conjunto de dos o más máquinas que se caracterizan por mantener una serie de servicios compartidos y por estar constantemente monitorizándose entre sí.

DSD: Direct Store Delivery, proceso usado en la industria de consumo masivo para vender y distribuir productos de manera directa al cliente.

DM: Dispositivo Móvil. Dispositivo manual con capacidad de interactuar contra otros equipos y con algunas funcionalidades de equipos de escritorio.

DMZ (Demilitarized Zone): es una zona segura que se ubica entre la red interna de una organización y una red externa, generalmente en Internet.

"**Dual stack" o "Doble stack":** sistema SAP que contiene instalaciones de Application Server ABAP y Application Server Java.

Empresa XYZ: siglas que por motivo de confidencialidad se refieren a la Empresa de consumo masivo en la cual se llevará a cabo el proyecto.

ERP: Enterprise Resource Planning. Sistema diseñado para integrar las operaciones y procesos de negocio, usando una base de datos común.

Firewall: un corta fuegos es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Google Play Store: es una plataforma de distribución de aplicaciones móviles para dispositivos con Android.

Hand Held: el término handheld, hand-held computer o hand-held device, es un anglicismo que traducido al español significa "de mano" (computadora o dispositivo de mano) y describe al tipo de computadora portátil que se puede llevar en una mano mientras se utiliza.

Hypertext Transfer Protocol (HTTP) y Hypertext Transfer Protocol Secure (HTTPS): son protocolos de comunicación que permiten la transferencia de información en la World Wide Web.

HTML5 (HyperText Markup Language, versión 5): es la quinta revisión importante del lenguaje básico de la World Wide Web, HTML.

IPhone: es una línea de teléfonos inteligentes de alta gama diseñada y comercializada por Apple Inc. Ejecuta el sistema operativo móvil iOS.

J2EE (Java Platform, Enterprise Edition o Java EE): es una plataforma de programación para desarrollar y ejecutar software de aplicaciones en el lenguaje de programación Java.

Java: es un lenguaje de programación orientado a objetos que fue diseñado para tener pocas dependencias de implementación.

JCO Connection o SAP Java Connector: es un componente de middleware que permite que una aplicación JAVA llame o se comunique con cualquier sistema SAP y viceversa.

JS Hybrid (Java Script): es un lenguaje de programación de alto nivel orientado a objetos, dinámico e interpretado. Comúnmente usado en ambientes Web.

Kerberos: es un protocolo de autenticación de redes de ordenador creado por el MIT que permite a dos ordenadores en una red insegura demostrar su identidad mutuamente de manera segura.

Keystore: es un repositorio de certificados de seguridad, ya sean certificados de autorización o certificados de clave pública, más las claves privadas correspondientes, que se utilizan, por ejemplo, en el cifrado SSL.

Log: archivo de trazas. Para registrar detalles de información o eventos en un sistema organizado de mantenimiento de registros, generalmente secuenciados en el orden en que ocurrieron.

Logon: inicio de sesión. El acto de conectarse a la computadora, que generalmente requiere la entrada de una identificación de usuario y contraseña en una terminal de computadora.

Lightweight Directory Access Protocol (LDAP): es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido.

Microsoft: empresa multinacional de origen estadounidense, fundada por Bill Gates y Paul Allen. Dedicada al sector del software y el hardware, tiene su sede en Redmond, Washington, Estados Unidos. Microsoft desarrolla, fabrica, licencia y produce software y equipos electrónicos, siendo sus productos más usados el sistema operativo Microsoft Windows y la suite Microsoft Office.

Microsoft SQL: es una base de datos relacional desarrollada por Microsoft.

Middleware: middleware o lógica de intercambio de información entre aplicaciones ("interlogical") es un software que asiste a una aplicación para interactuar o comunicarse con otras aplicaciones, o paquetes de programas, redes, hardware y/o sistemas operativos.

Network Load Balancing Services (NLBS): es una implementación de Microsoft de “cluster” y balanceo de carga que está diseñada para proporcionar alta disponibilidad y alta confiabilidad, así como una alta escalabilidad.

Nokia: es una línea de teléfonos inteligentes de la empresa Nokia, la cual es una empresa multinacional de comunicaciones y tecnología con sede en Finlandia.

Odómetro: aparato en forma de reloj de bolsillo que sirve para contar el número de pasos que da la persona que lo lleva y medir la distancia que ha recorrido.

Open Data Protocol (OData): es un protocolo abierto que permite la creación y uso de APIs (Application Programming Interface) interoperables de una manera simple y estándar. Microsoft inició OData en 2007.

Open Mobile Alliance (OAM): es una organización de estándares abiertos para la industria de telefonía móvil.

PDA: Personal Digital Assistant. Del inglés Personal Digital Assistant, asistente digital personal, computadora de bolsillo, organizador personal o agenda electrónica de bolsillo, es una computadora de mano, originalmente diseñada como agenda personal electrónica (para tener uso de calendario, lista de contactos, bloc de notas, recordatorios, dibujar, etc.) con un sistema de reconocimiento de escritura.

PDV: Punto de Venta. Lugar donde los clientes de una empresa de consumo masivo comercializan los productos.

Proxy Inverso (Relay Proxy): es un tipo de servidor Proxy que recupera un recurso en nombre de un cliente de uno o más servidores.

PKCS12: define un formato de fichero usado comúnmente para almacenar claves privadas con su certificado de clave pública protegido mediante clave simétrica.

PKI: en criptografía, una infraestructura de clave pública (o, en inglés, PKI, Public Key Infrastructure) es una combinación de hardware y software, políticas y procedimientos de seguridad, que permiten la ejecución con garantías de operaciones criptográficas como el cifrado, la firma digital o el no repudio de transacciones electrónicas.

SAP AFARIA: SAP Afaria es un producto de software de gestión de dispositivos móviles. Ayuda a las grandes organizaciones a conectar dispositivos móviles como teléfonos inteligentes y tabletas a la red de la empresa y a simplificar las tareas de tecnología de la información asociadas con la compra, implantación, seguridad y mantenimiento de dichos dispositivos.

SAP AG: es una empresa multinacional alemana dedicada al diseño de productos informáticos de gestión empresarial, tanto para empresas como para organizaciones y organismos públicos.

SAP CRM: SAP Customer Relationship Management es un software integrado de gestión de relaciones con los clientes fabricado por SAP, que se dirige a los requisitos de software empresarial de las medianas y grandes organizaciones en todas las industrias y sectores.

SAP ERP: SAP Enterprise Resource Planning. Sistema de SAP diseñado para soportar todas las áreas de gestión de una empresa, con alto grado de flexibilidad y efectividad.

SAP Direct Store Delivery (DSD): SAP Direct Store Delivery es una aplicación móvil de SAP, que soporta el proceso de venta y distribución de mercancías directamente en la tienda del cliente sin pasar por el almacén del minorista.

SAP Mobile Engine (MI): es una herramienta "middleware" de SAP que habilita la transmisión de información entre los servidores y los dispositivos móviles.

SAP Mobile Platform (SMP): es una plataforma de aplicaciones empresariales móviles diseñada para simplificar la tarea de crear aplicaciones que conectan datos empresariales a dispositivos móviles para la gestión del flujo de trabajo y la integración de "Backend".

SAP SQL Anywhere: es una base de datos relacional propiedad de SAP.

SAP Web Dispatcher: es un software de SAP que se encuentra entre Internet y un sistema SAP. Es el punto de entrada para las solicitudes HTTP (s) en el sistema.

SDK Un kit de desarrollo de software es generalmente un conjunto de herramientas de desarrollo de software que le permite al programador o desarrollador de software crear una aplicación informática para un sistema concreto, por ejemplo ciertos paquetes de software, frameworks, plataformas de hardware, computadoras, videoconsolas, sistemas operativos, etcétera.
SMART PHONE: el teléfono inteligente (smartphone en inglés) es un tipo de teléfono móvil construido sobre una plataforma informática móvil, con mayor capacidad de almacenar datos y realizar actividades, semejante a la de una minicomputadora, y con una mayor conectividad que un teléfono móvil convencional.

SSH (Secure Shell): es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder servidores privados a través de una puerta trasera (también llamada backdoor).

SSL Secure Sockets Layer: es un protocolo criptográfico que proporciona comunicación segura por una red, comúnmente Internet. Se usan certificados X.509 y por lo tanto criptografía asimétrica para autentificar a la

contraparte con quien se están comunicando y para intercambiar una llave simétrica. Esta sesión es luego usada para cifrar el flujo de datos entre las partes.

Stock: inventario, registro documental de los bienes y demás cosas pertenecientes a una persona, empresa o comunidad.

Tablet: tableta o tablet es una computadora portátil de mayor tamaño que un teléfono inteligente o un PDA, integrada en una pantalla táctil (sencilla o multitáctil) con la que se interactúa primariamente con los dedos o un estilete (pasivo o activo), sin necesidad de teclado físico ni ratón**.**

TCP/IP: es un protocolo de red desarrollado para comunicaciones en redes. Describe un conjunto de guías generales de operación para permitir que un equipo pueda comunicarse en una red. TCP/IP provee conectividad de extremo a extremo especificando cómo los datos deberían ser formateados, direccionados, transmitidos, enrutados y recibidos por el destinatario.

UIT: Unión Internacional de Comunicaciones es el organismo especializado en telecomunicaciones de la Organización de las Naciones Unidas (ONU), encargado de regular las telecomunicaciones a nivel internacional entre las distintas administraciones y empresas operadoras. La sede de la UIT se encuentra en la ciudad de Ginebra, Suiza.

URL es la ruta que se encuentra ubicada en la barra de navegación del navegador, sirve para ubicar de manera precisa en un servidor, cualquier recurso: una imagen, un video o una página web.

WAN Wide Area Network: es una red que se utiliza para transmitir datos a través de largas distancias.

Windows Mobile: es un sistema operativo móvil compacto desarrollado por Microsoft, y diseñado para su uso en teléfonos inteligentes y otros dispositivos móviles.

X.509: es un estándar UIT-T para infraestructuras de claves públicas (en inglés, Public Key Infrastructure o PKI).

XML eXtensible Markup Language: es un lenguaje que permite almacenar datos de forma legible y se propone como un como un estándar para el intercambio de información entre diferentes plataformas.

CAPITULO X. BIBLIOGRAFIA

ARTICULOS Y GUIAS

[Aertzen, 2016] AERTZEN, Maarten. KORCZY´NSKI, Maciej. C.M. MOURA, Giovane. TAJALIZADEHKHOOB, Samaneh. NO DOMAIN LEFT BEHIND: IS LET´S ENCRYPT DEMOCRATIZING ENCRYPTION? Cornell University Library. Diciembre 2016.

[Mendillo, 2016] MENDILLO, Vincenzo. CERTIFICADOS DIGITALES E INFRAESTRUCTURA DE CLAVE PUBLICA (PKI). Diciembre 2016

[SAP – AG, 2006] SAP-AG. DIRECT STORE DELIVERY. Sap Technical Brief. Enero, 2006.

[SAP E2E100, 2008] E2E100. EN-TO-END ROOT CAUSE ANALYSIS. SAP, 2008

[SAP DSD, 2015] SAP. SAP DIRECT STORE DELIVERY 1.0 CONFIGURATION GUIDE. SAP 2015

[NIST, 1995]. AN INTRODUCTION TO COMPUTER SECURITY: THE NIST HANDBOOK, Special Publication 800-12, WS, USA. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY NIST, 1995. http://www.csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf

*[*Swanson, 2001] SWANSON, Marianne*. NIST SPECIAL PUBLICATION SP 800-26: SECURITY SELF ASSESSMENT GUIDE FOR INFORMATION TECHNOLOGY SYSTEMS. WS, USA, 2001.* http:// csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf

[Noguera KRB, 2017] NOGUERA, Ignacio. GESTION DE PROYECTOS. Preparación en Modelos de Gestión de Proyectos. Noguera KRB, 2017.

LIBROS

[Balestrini Acuña, 2002] BALESTRINI ACUÑA, Miriam. COMO SE ELABORA EL PROYECTO DE INVESTIGACION. BL Consultores Asociados, Servicio Editorial. 2002

[Barrios, 2005] BARRIOS YASELLI, Maritza. MANUAL de TRABAJOS DE GRADO DE ESPECIALIZACION Y MAESTRIA Y TESIS DOCTORALES.

[Forndron, 2005] FORNDRON, Frank. MY SAP ERP ROADMAP. Galileo Press. Bonn, Alemania 2005

[Easttom, 2015]. EASTTOM, Chuck. MODERN CRYPTOGRAPHY: APPLIED MATHEMATICS FOR ENCRYPTION AND INFORMATION. Security, McGraw-Hill, 2015

[Hankerson, 2004] HANKERSON, Darrel. MENEZES, Alfred. VANSTONE, Scott. GUIDE TO ELLIPTIC CURVE SRYPTOGRAPHY. Springer-Verlag, 2004

[Karch, 2005] KARCH, Steffen. SAP NETWEAVER ROADMAP. Galileo Press. Bonn, Alemania 2005

[Mall, 2012] MALL, Sanjeer. STEFANOV, Tzanko. STADELMAN, Stanley. MOBILIZING YOUR ENTERPRISE WITH SAP. EBook, SAP 2012

[Montero, 1996] MONTERO, Maritza. HOCHMAN, Elena. INVESTIGACION DOCUMENTAL. TECNICAS Y PROCEDIMIENTOS. Editorial Panapo, 1996

[Ramírez, 1999] RAMIREZ, Tulio. COMO HACER UN PROYECTO DE INVESTIGACION. Editorial Panapo de Venezuela, C.A, 1999

[Stallings, 2011] STALLINGS, William. CRYPTOGRAPHY AND NETWORK SECURITY Prentice-Hall, 2011

[Tutorials, 2015] TUTORIALS, Point. CRYTOGRAPHY FOR BEGINNERS, 2015

PAGINAS WEB

[GOOGLE, 2018] TRADUCTOR DE GOOGLE. https://translate.google.com/?hl=es

[ISACA, 2018] INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION. www.isaca.org.

[MICROSOFT, 2018]. MICROSOFT APPLICATION OF DIGITAL SIGNATURE https://technet.microsoft.com/en-us/library/cc962021.aspx

[REAL ACADEMIA DE LA LENGUA ESPANOLA, 2018] REAL ACADEMIA ESPAÑOLA http://www.rae.es/.

[SAP AFARIA, 2018] http://help.sap.com/afaria7sp5?current=afaria-cloud

[SAP HELP, 2018]. https://help.sap.com

[SAP HELP DSD, 2018]. https://help.sap.com/dsd

[SAP MARKETPLACE, 2018]. https://www.sap-ag.de/

[SAP MOBILE PLATFORM, 2018]. https://es.slideshare.net/SyambabuAllu/sap-mobile-platform-version-23-architecture

[SAP ENTERPRISE TECHINICAL SUPPORT, 2018] http://frontline.sybase.com/support/

[SAP SUPPORT, 2018]. https://support.sap.com

TESIS

[Brito, 2007]. BRITO S, Zaira C. LA SEGURIDAD DE INFORMACIÓN EN VENEZUELA. Universidad Metropolitana, 2007

[Palomeque, 2015]. PALOMEQUE, John. IMPLEMENTACION DE CERTIFICADOS Y FIRMAS DIGITALES PARA SISTEMAS DE INFORMACION TRANSACCIONALES EN UNA EMPRESA GUBERNAMENTAL. Escuela Superior Politécnica del Litoral 2015

[Szabo, 2006] SZABO, Jorge. DISEÑO DE LOS PROCESOS DE VENTA Y DISTRIBUCION DE UNA EMPRESA DE CONSUMO MASIVO BAJO LA PLATAFORMA TECNOLOGICA SAP. Universidad Simón Bolívar 2006

ANEXOS

ANEXO A. SEGURIDAD DE LA INFORMACION

A.1 ¿Qué es la seguridad de la información?

La seguridad de la información es el conjunto de medidas preventivas y reactivas, de las organizaciones y de los sistemas tecnológicos, que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de los datos.

La Seguridad de la Información, según ISO 27001, se refiere a la confidencialidad, la integridad y la disponibilidad de la información y los datos importantes para la organización, independientemente del formato que tengan, estos pueden ser: electrónicos, en papel, audio y vídeo, etc.

A.2 Objetivos de la seguridad de la información

Realizar correctamente la Gestión de la Seguridad de la Información requiere establecer y mantener los programas, los controles y las políticas de seguridad que tienen la obligación de conservar la confidencialidad, la integridad y la disponibilidad de la información de la empresa.

De estas definiciones podemos deducir que los principales objetivos de la seguridad informática son:

- **Confidencialidad**: consiste en la capacidad de garantizar que la información, almacenada en el sistema informático o transmitida por la red, solamente va a estar disponible para aquellas personas autorizadas a acceder a dicha información, es decir, si los contenidos cayesen en manos ajenas, estas no podrían acceder a la información o a su interpretación. Este es uno de los principales problemas a los que se enfrentan muchas empresas; en los últimos años se ha incrementado el robo de los portátiles con la consecuente pérdida de información confidencial, de clientes, líneas de negocio, etc.

- **Disponibilidad:** se define como la capacidad de garantizar que tanto el sistema como los datos van a estar disponibles al usuario en todo momento. Pensemos, por ejemplo, en la importancia que tiene este objetivo para una empresa encargada de impartir ciclos formativos a distancia. Constantemente está recibiendo consultas, descargas a su sitio web, etc., por lo que siempre deberá estar disponible para sus usuarios.

- **Integridad:** es la capacidad de garantizar que los datos no han sido modificados desde su creación sin autorización. La información que disponemos es válida y consistente. Este objetivo es muy importante cuando estamos realizando trámites bancarios por Internet. Se deberá garantizar que ningún intruso pueda capturar y modificar los datos en tránsito.

A.3 Tipos de Amenazas y vulnerabilidades

Las amenazas están relacionadas con causas que representan riesgos, las cuales pueden ser causas naturales o no naturales y causas internas o externas.

Las amenazas son constantes y pueden ocurrir en cualquier momento. Esta relación de frecuencia-tiempo, se basa en el concepto de riesgo, lo cual representa la probabilidad de que una amenaza se concrete por medio de una vulnerabilidad o punto débil. Las vulnerabilidades o las amenazas, por separado, no representan un peligro. Pero si se juntan, se convierten en un riesgo, o sea, en la probabilidad de que ocurra un desastre. Las amenazas se podrán dividir en tres grandes grupos:

- **Amenazas naturales**: condiciones de la naturaleza y la intemperie que podrán causar daños a los activos, tales como fuego, inundación, terremotos.

- **Intencionales:** son amenazas deliberadas, fraudes, vandalismo, sabotajes, espionaje y ataques, robos y hurtos de información, entre otras.

- **Involuntarias:** son amenazas resultantes de acciones inconscientes de usuarios, por virus electrónicos, muchas veces causadas por la falta de conocimiento en el uso de los activos, tales como errores, imprudencia y accidentes.

Por otra parte, teniendo en cuenta que los puntos débiles o vulnerabilidades son los elementos que, al ser explotados por amenazas, afectan la confidencialidad, disponibilidad e integridad de la información de un individuo o empresa, estos dependen de la forma en que se organizó el ambiente en que se maneja la información. La existencia de puntos débiles está relacionada con la presencia de elementos que perjudican el uso adecuado de la información y del medio en que la misma se está utilizando o transmitiendo. Lo cual representa otro objetivo de la seguridad de la información: la corrección de puntos débiles o vulnerabilidades existentes en el ambiente en que se usa la información, con el objeto de reducir los riesgos a que está sometida, evitando así la concretización de una amenaza.

Las vulnerabilidades a las cuales los activos están expuestos pueden ser:

- Físicas
- Naturales
- De hardware
- De software
- De medios de almacenamiento
- De comunicación
- Humanas

Las vulnerabilidades son fallas en diseño, configuración o funcionamiento que pueden ser aprovechadas por entidades maliciosas de manera que se obtengan privilegios de acceso mayores a los dispuestos por los responsables de los servicios de información. En cuanto a la tecnología de información se refiere, muchas organizaciones están fuertemente enfocadas en hacer inversiones que sean efectivas y minimalistas en cuanto al costo. Los profesionales de tecnología de información tienen la responsabilidad de balancear los dos hechos anteriores. La gestión de vulnerabilidades debe ser un proceso de prevención, en comparación con la naturaleza reactiva con la que en muchas ocasiones se procede. Las vulnerabilidades pueden ser mitigadas mediante diversos mecanismos: instalación de correcciones o "parches", creación de políticas, mecanismos de hardware, mecanismos de software, ajuste de privilegios, ajustes de configuración. La decisión debe estar basada en un análisis de riesgos.

A.4 Mecanismos para garantizar la seguridad de la información

Los mecanismos de seguridad se dividen en tres grupos:

- **Prevención:** evitan desviaciones respecto a la política de seguridad. Ejemplo: utilizar el cifrado en la transmisión de la información evita que un posible atacante capture (y entienda) información de un sistema en la red.

- **Detección:** detectan las desviaciones si se producen, violaciones o intentos de violación de la seguridad del sistema. Ejemplo: una herramienta "Tripwire" para la seguridad de los archivos.
- **Recuperación:** se aplican cuando se ha detectado una violación de la seguridad del sistema para recuperar su normal funcionamiento. Ejemplo: las copias de seguridad.

Dentro del grupo de mecanismos de prevención tenemos:

- **Mecanismos de identificación y autenticación:** permiten identificar de forma única “entidades” del sistema. El proceso siguiente es la autenticación, es decir, comprobar que la entidad es quien dice ser. Pasados estos dos filtros, la entidad puede acceder a un objeto del sistema. En concreto los sistemas de identificación y autenticación de los usuarios son los mecanismos más utilizados.

- **Mecanismos de control de acceso:** los objetos del sistema deben estar protegidos mediante mecanismos de control de acceso que establecen los tipos de acceso al objeto por parte de cualquier entidad del sistema.

- **Mecanismos de separación:** si el sistema dispone de diferentes niveles de seguridad se deben implementar mecanismos que permitan separar los objetos dentro de cada nivel. Los mecanismos de separación, en función de cómo separan los objetos, se dividen en los grupos siguientes: separación física, temporal, lógica, criptográfica y fragmentación.

- **Mecanismos de seguridad en las comunicaciones:** la protección de la información (integridad y privacidad) cuando viaja por la red es especialmente importante. Clásicamente se utilizan protocolos seguros, tipo SSH[41] o Kerberos[42], que cifran el tráfico por la red.

ANEXO B. CRIPTOGRAFIA

B.1 Origen de la criptografía

El arte y la ciencia de ocultar los mensajes para introducir el secreto en la seguridad de la información se reconoce como criptografía. La palabra "criptografía" fue acuñada por la combinación de dos palabras griegas, "Krypto" significa oculto y "graphene" que significa escribir.

El arte de la criptografía se considera que nace junto con el arte de la escritura. A medida que las civilizaciones evolucionaban, los seres humanos se organizaban en tribus, grupos y reinos. Esto llevó a la aparición de ideas como el poder, las batallas, la supremacía y la política. Estas ideas alimentaron aún más la necesidad natural de las personas de comunicarse secretamente con el receptor selectivo, lo que a su vez aseguraba la continua evolución de la criptografía.

41 SSH: (Secure SHell, en español: intérprete de órdenes seguro) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder servidores privados a través de una puerta trasera (también llamada backdoor).

42 Kerberos es un protocolo de autenticación de redes de ordenador creado por el MIT que permite a dos ordenadores en una red insegura demostrar su identidad mutuamente de manera segura.

B.2 Servicios de seguridad de criptografía

El principal objetivo de usar criptografía es proveer los siguientes cuatro servicios fundamentales de seguridad:

- **Confidencialidad:** es el servicio de seguridad fundamental que provee la criptografía. Este es el servicio que guarda la información de una persona no autorizada. Algunas veces es llamado como "privado" o "secreto". La confidencialidad puede ser alcanzada a través de muchos medios, comenzando por la seguridad física hasta usar algoritmos matemáticos para encriptar los datos.

- **Integridad de los datos:** este es el servicio que identifica cualquier alteración de los datos. Los datos pueden ser modificados por una entidad no autorizada intencional o accidentalmente. El servicio de integridad confirma si los datos están intactos o no ya que estos fueron creados, transmitidos o almacenados por un usuario autorizado. La integridad de los datos, no puede prevenir la alteración de los datos, pero provee un medio para detectar si los datos han sido manipulados de manera no autorizada.

- **Autenticación:** provee la identificación del emisor. Este confirma al receptor que los datos recibidos han sido enviados únicamente por un emisor identificado y verificado.

  El servicio de autenticación tiene dos variantes:

  - **Autenticación del mensaje**: identifica el origen del mensaje sin ningún enrutador o sistema que haya enviado el mensaje.

  - **Entidad de autenticación**: esta asegura que los datos han sido recibidos desde una entidad específica, tales como un sitio Web específico.

  Aparte del emisor, la autenticación también puede proveer certeza sobre otros parámetros relacionados a los datos, tales como la fecha y hora de creación/transmisión.

- **No Repudio:** este es un servicio de seguridad que asegura que una entidad no puede rechazar al dueño de una confirmación previa o de una acción. Este asegura, que el creador original de los datos no puede denegar la creación o transmisión de los datos desde un receptor o de una tercera parte. No-repudio es una propiedad que es muy deseable en situaciones donde existen oportunidades de disputar sobre le intercambio de datos. Por ejemplo, una vez que una orden es localizada

electrónicamente, un vendedor no puede denegar la orden de compra, si el servicio de no repudio fue habilitado en la transacción.

B.3 Primitivas de criptografía

Las primitivas de criptografía no son otra cosa que las herramientas y técnicas de criptografía que pueden utilizarse selectivamente para proporcionar un conjunto de servicios de seguridad:

- Cifrado
- Funciones de Hash
- Códigos de Autenticación de mensajes (Message Authentication codes MAC)
- Firmas digitales

La siguiente tabla muestra una comparación entre las primitivas de seguridad:

Primitivas de Servicio	**Cifrado**	**Funciones Hash**	**MAC**	**Firmas Digitales**
Confidencialidad	Si	No	No	No
Integridad	No	Algunas veces	Si	Si
Autenticación	No	No	Si	Si
No Repudio	No	No	Algunas veces	Si

Las primitivas de criptografía están relacionadas y a menudo se combinan para proveer los servicios de seguridad en un criptosistema. Un criptosistema es una implementación de técnicas criptográficas, junto con la infraestructura necesaria, proporciona servicios de seguridad de la información. Un criptosistema también se conoce como un sistema de cifrado. [Cryptography for Beginners. Tutorials Point, 2015].

A continuación, se presentará un modelo simple de un criptosistema que proporciona confidencialidad a la información que se está transmitiendo abajo:

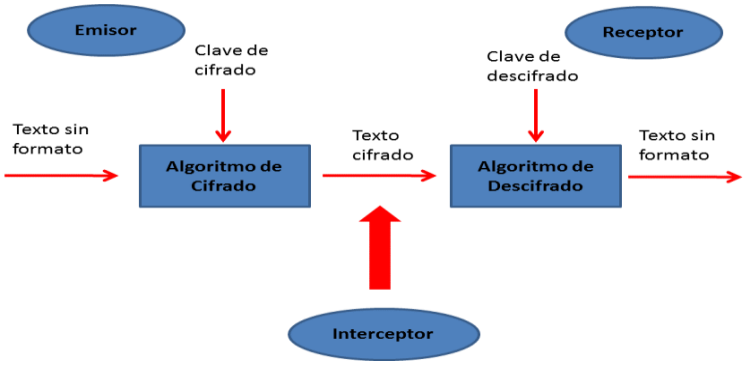


Figura B.3.1 Modelo Simple de Criptosistema

La figura muestra un remitente que desea transferir algunos datos confidenciales a un receptor, de tal manera, que cualquier parte que intercepte o escuche por el canal de comunicación no puede extraer los datos. El objetivo de este criptosistema simple es que al final del proceso, sólo el remitente y el receptor conocerán el texto sin formato.

B.4 Componentes de un criptosistema

Los diversos componentes de un criptosistema básico son los siguientes:

- **Texto sin formato o texto plano (Plaintext).** Son los datos a proteger durante la transmisión.

- **Algoritmo de cifrado**. Es un proceso matemático que produce un texto cifrado, a partir de cualquier texto sin formato y con una clave de cifrado.

- **Texto cifrado**. Es la versión codificada del texto plano producido por el algoritmo de cifrado usando una clave de cifrado específica. El texto cifrado no está protegido. Fluye en el canal público. Puede ser interceptado o comprometido por cualquiera que tenga acceso al canal de comunicación.

- **Algoritmo de descifrado**. Es un proceso matemático, que produce un texto plano único para cualquier cifrado y clave de cifrado. Es un algoritmo criptográfico que toma un texto cifrado y una clave de descifrado como entrada, y genera un texto plano. El algoritmo de descifrado invierte esencialmente el algoritmo de cifrado y, por lo tanto, está estrechamente relacionado con él.

- **Clave de cifrado.** Es un valor que es conocido por el remitente. El remitente introduce la clave de cifrado en el algoritmo de cifrado junto con el texto plano para obtener el texto cifrado.

• **Clave de descifrado**. Es un valor que es conocido por el receptor. La clave de descifrado está relacionada con la clave de cifrado, pero no siempre es idéntica a ella. El receptor introduce la clave de descifrado en el algoritmo de descifrado junto con el texto cifrado para obtener el texto plano. [Cryptography for Beginners. Tutorials Point, 2015]

B.5 Tipos de criptosistemas

Fundamentalmente, existen dos tipos de criptosistemas basados en la manera en que se realiza el cifrado-descifrado en el sistema cifrado con clave simétrica y cifrado con claves asimétricas. La principal diferencia entre estos criptosistemas es la relación entre el cifrado y la clave de descifrado. Lógicamente, en cualquier criptosistema, ambas claves están estrechamente asociadas. Es prácticamente imposible descifrar el texto cifrado con la clave que no está relacionada con la clave de cifrado. [Cryptography for Beginners. Tutorials Point, 2015]

B.5.1 Cifrado de clave simétrica

El proceso de cifrado en el que se utilizan las mismas claves para cifrar y descifrar la información se conoce como cifrado de clave simétrica. El estudio de criptosistemas simétricos se denomina criptografía simétrica. Los criptosistemas simétricos también se denominan a veces criptosistemas de clave secreta.

Algunos ejemplos bien conocidos de métodos de cifrado de clave simétrica son: Digital Encryption Standard (DES), Triple-DES (3DES), IDEA y BLOWFISH. [Cryptography for Beginners. Tutorials Point, 2015]

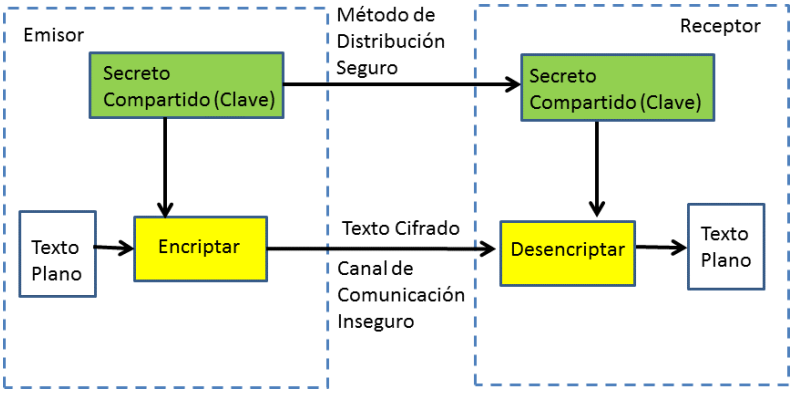


Figura B.5.1.1 Cifrado de Clave Simétrica

Las características principales del criptosistema basado en cifrado de clave simétrica son:

- Las personas que utilizan cifrado de clave simétrica deben compartir una clave común antes del intercambio de información.

- Se recomienda cambiar las claves regularmente para evitar cualquier ataque al sistema.

- Debe existir un mecanismo robusto para intercambiar la clave entre las partes que se comunican. Como las claves se requieren para ser cambiado regularmente, este mecanismo se vuelve costoso y engorroso.

- En un grupo de n personas, para permitir la comunicación entre dos personas, el número de claves requeridas para el grupo es n × (n - 1) / 2.

- La longitud de la clave (número de bits) en este cifrado es menor, por lo tanto, el proceso de cifrado-descifrado es más rápido que el cifrado de clave asimétrica.

- El poder de procesamiento del sistema informático requerido para ejecutar el algoritmo simétrico es menor.

B.5.2 Cifrado de clave asimétrica

El proceso de cifrado en el que se utilizan diferentes claves para cifrar y descifrar la información se conoce como cifrado de clave asimétrica. Aunque las claves son diferentes, están relacionadas matemáticamente y, por lo tanto, recuperar el texto sin formato a partir de descifrar el texto cifrado es factible.

El proceso se representa en la siguiente ilustración:

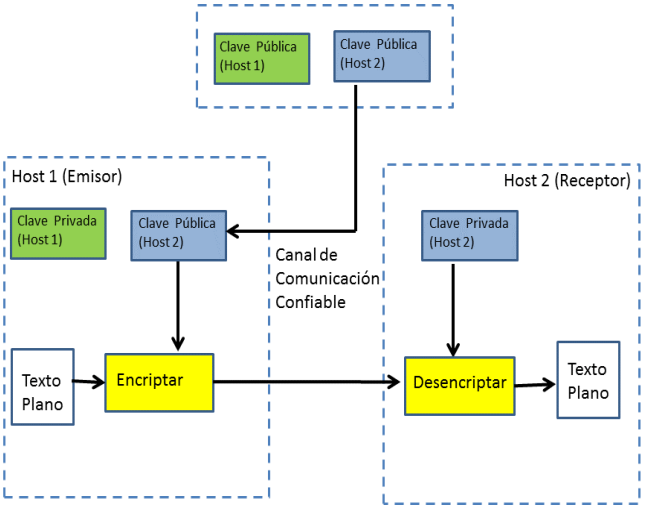


Figura B.5.2.1 Cifrado de Clave Asimétrica

El cifrado de clave asimétrica fue inventado en el siglo 20 para cubrir la necesidad de clave secreta pre-compartida entre las personas que se comunican.

Las características más destacadas de este esquema de cifrado son las siguientes:

- Cada usuario en este sistema necesita tener un par de claves diferentes, clave privada y clave pública. Estas claves están matemáticamente relacionadas, cuando una clave se utiliza para el cifrado, el otro puede descifrar el texto cifrado y volver al texto original.

- Requiere poner la clave pública en el repositorio público y la clave privada como un secreto bien guardado. Por lo tanto, este esquema de cifrado también se denomina cifrado de clave pública.

- Aunque las claves públicas y privadas del usuario están relacionadas, es computacionalmente imposible encontrar una de otra. Esta es una fuerza de este esquema.

- Cuando el Host1 necesita enviar datos al Host2, obtiene la clave pública de Host2 desde el repositorio, cifra los datos y los transmite.

- El Host2 utiliza su clave privada para extraer el texto sin formato.

- La longitud de claves (número de bits) en este cifrado es grande, por lo tanto, el proceso de cifrado-descifrado es más lento que el cifrado de clave simétrica.

- El poder de procesamiento del sistema informático requerido para ejecutar el algoritmo asimétrico es mayor. [Cryptography for Beginners. Tutorials Point, 2015]

B.5.3 Cifrado de clave pública

Con la expansión de más redes informáticas inseguras en las últimas décadas, se sintió una verdadera necesidad de utilizar la criptografía a mayor escala. Se descubrió que la clave simétrica no era práctica debido a los desafíos que enfrentaba para la administración de claves. Esto dio lugar a los criptosistemas de clave pública.

El proceso de cifrado y descifrado se muestra en la siguiente figura:

Figura B.5.3.1 Cifrado de Clave Pública

Las propiedades más importantes del esquema de cifrado de clave pública son:

- Se usan diferentes claves para cifrado y descifrado. Esta es una propiedad que establece este esquema diferente al esquema de cifrado simétrico.

- Cada receptor posee una clave de descifrado única, generalmente conocida como su clave privada.

- El receptor necesita publicar una clave de cifrado, conocida como su clave pública.

- Se necesita cierta seguridad de la autenticidad de una clave pública en este esquema para evitar falsificaciones por parte del adversario como receptor. En general, este tipo de criptosistema involucra a un tercero de confianza que certifica que una clave pública en particular pertenece únicamente a una persona o entidad específica.

- El algoritmo de encriptación es lo suficientemente complejo como para prohibir al atacante deducir el texto plano del texto cifrado y la clave de encriptación (pública).

- Aunque las claves privadas y públicas están relacionadas matemáticamente, no es factible calcular la clave privada a partir de la clave pública. De hecho, la parte inteligente de cualquier criptosistema de clave pública está en el diseño de una relación entre dos claves.

  Hay tres tipos de esquemas de cifrado de clave pública:

- **Criptosistema RSA:** este criptosistema es uno del sistema inicial. Sigue siendo el criptosistema más utilizado incluso hoy en día. El sistema fue inventado por tres estudiosos Ron Rivest, Adi Shamir y Len Adleman y, por lo tanto, se lo denomina criptosistema RSA.

- **Criptosistema ElGammal:** hay otros criptosistemas de clave pública aparte del RSA, y muchos de ellos se basan en diferentes versiones del Problema del Logaritmo Discreto.

- **Criptografía de curva elíptica (Elliptic Curve Cryptography ECC):** criptografía de curva elíptica (Elliptic Curve Cryptography ECC) es un término utilizado para describir un conjunto de herramientas criptográficas y protocolos cuya seguridad se basa en versiones especiales del problema del logaritmo discreto.

ANEXO C. FUNCIONES HASH

C.1 Funciones Hash

Una función Hash es una función matemática que convierte un valor numérico de entrada en otro valor numérico comprimido. La entrada a la función Hash es de longitud arbitraria, pero la salida siempre es de longitud fija. Los valores devueltos por una función Hash se denominan mensaje resumen o simplemente valores Hash. La siguiente imagen ilustra la función Hash:

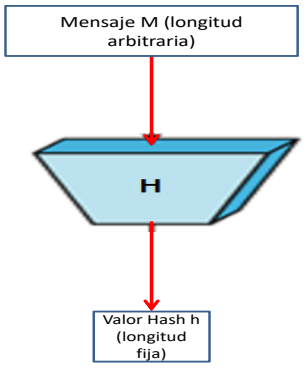


Figura C.1.1 Función Hash

C.1.1 Funciones Hash más populares

A continuación, algunas funciones Hash más populares:

- **Message Digest (MD):** MD5 fue la función Hash más popular y ampliamente utilizada durante algunos años. La familia MD comprende funciones Hash MD2, MD4, MD5 y MD6. Fue adoptado como el estándar de Internet RFC 1321. Es una función Hash de 128 bits. Los resúmenes o "digests" de MD5 se han utilizado ampliamente en el mundo del software para proporcionar seguridad sobre la integridad del archivo transferido. Por ejemplo, los servidores de archivos suelen proporcionar una suma de comprobación MD5 pre calculada para los archivos, de modo que un usuario pueda comparar la suma de comprobación del archivo descargado.

- **Secure Hash Function (SHA):** la familia de SHA se compone de cuatro algoritmos SHA; SHA-0, SHA-1, SHA-2 y SHA-3. La versión original es SHA-0, una función hash de 160 bits, fue publicada por el Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology NIST) en 1993. Tenía pocas debilidades y no se volvió muy popular. Más tarde, en 1995, SHA-1 fue diseñado para corregir presuntas debilidades de SHA-0. SHA-1 es la función de hash SHA más utilizada. Se emplea en varias aplicaciones y protocolos ampliamente utilizados, incluida la seguridad de Secure Socket Layer (SSL). La familia SHA-2 tiene cuatro variantes SHA adicionales, SHA-224, SHA-256, SHA-384 y SHA-512, dependiendo de la cantidad de bits en su valor Hash. Aún no se han reportado ataques exitosos en la función Hash SHA-2.

- **RIPEMD** es el acrónimo de RACE Integrity Primitives Evaluation Message Digest. Este conjunto de funciones Hash fue diseñado por una comunidad de investigación abierta y generalmente conocido como una familia de funciones Hash europeas. El conjunto incluye RIPEND, RIPEMD-128 y RIPEMD-160. También existen versiones de 256 y 320 bits de este algoritmo.

- **Whirlpool:** esta es una función Hash de 512 bits. Se deriva de la versión modificada de Advanced Encryption Standard (AES). Uno de los diseñadores fue Vincent Rijmen, cocreador de AES. Existen tres versiones de Whirlpool; a saber, WHIRLPOOL-0, WHIRLPOOL-T y WHIRLPOOL. [Cryptography for Beginners. Tutorials Point, 2015]

ANEXO D. AUTENTICACION DE MENSAJES

D.1 Autenticación de mensajes

Otro tipo de amenaza que existe para los datos, es la falta de autenticación de mensajes. En esta amenaza, el usuario no está seguro sobre el originador del mensaje. La autenticación de mensajes se puede proporcionar usando las técnicas criptográficas que usan claves secretas como se hace en caso de cifrado. [Cryptography for Beginners. Tutorials Point, 2015]

D.2 Código de autenticación de mensaje (Message Authentication Code MAC)

El algoritmo MAC es una técnica criptográfica de clave simétrica para proporcionar autenticación de mensajes. Para establecer el proceso MAC, el emisor y el receptor comparten una clave simétrica K. Básicamente, un MAC es una suma de verificación encriptada generada en el mensaje subyacente que se envía junto con un mensaje para garantizar la autenticación del mensaje. El proceso de usar MAC para autenticación se muestra en la siguiente figura:

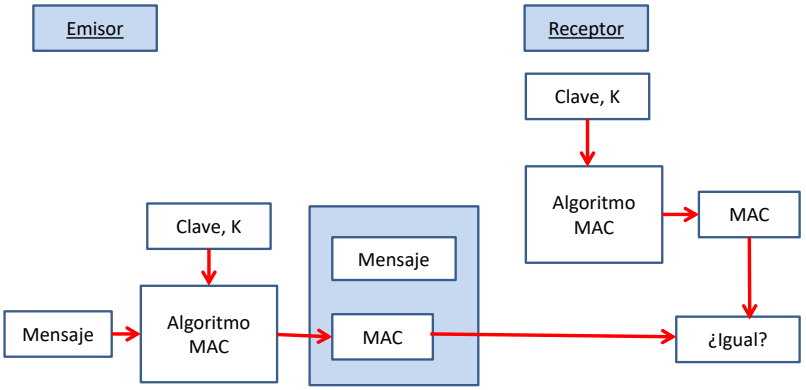


Figura D.2.1 Proceso MAC para Autenticación

ANEXO E. FIRMA DIGITAL

E.1 Firma digital

Las firmas digitales son las primitivas de clave pública de la autenticación de mensajes. En el mundo físico, es común usar firmas manuscritas en mensajes escritos a mano o escritos a máquina. Se usan para unir al signatario al mensaje.

Del mismo modo, una firma digital es una técnica que vincula a una persona / entidad con los datos digitales. Este enlace puede ser verificado independientemente por el receptor y por cualquier tercero.

La firma digital es un valor criptográfico que se calcula a partir de los datos y una clave secreta conocida solo por el firmante.

El concepto de firma digital consiste en la transformación de un mensaje utilizando un sistema de cifrado asimétrico de manera que la persona que posee el mensaje original y la clave pública del firmante, pueda establecer de forma segura, que dicha transformación se efectuó utilizando la clave privada.

En el mundo real, el receptor del mensaje necesita la seguridad de que el mensaje pertenece al remitente y no debería poder rechazar el origen de ese mensaje. Este requisito es muy importante en las aplicaciones comerciales, ya que la probabilidad de una disputa sobre el intercambio de datos es muy alta. [Cryptography for Beginners. Tutorials Point, 2015]

E.2 Modelo de firma digital

Como se mencionó anteriormente, el esquema de firma digital se basa en la criptografía de clave pública. El modelo del esquema de firma digital se muestra en la siguiente figura:

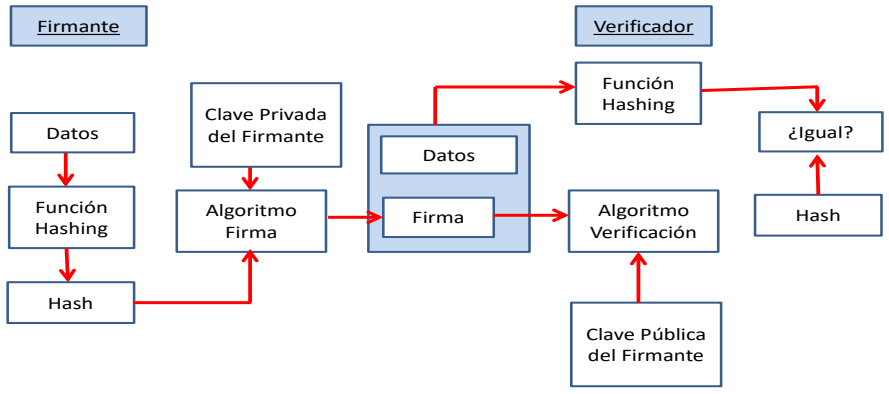


Figura E.2.1 Modelo de Esquema de Firma Digital

A continuación, se explica todo el proceso en detalle:

- Cada persona que adopta este esquema tiene un par de claves público-privadas.

- En general, los pares de claves utilizados para el cifrado / descifrado y la firma / verificación son diferentes. La clave privada utilizada para la firma se conoce como la clave de firma y la clave pública como la clave de verificación.

- El firmante da los datos a la función Hash y genera el Hash de datos.

- El valor de Hash y la clave de firma se envían al algoritmo de firma que produce la firma digital en el Hash dado. La firma se agrega a los datos y luego ambos se envían al verificador.

- El verificador introduce la firma digital y la clave de verificación en el algoritmo de verificación. El algoritmo de verificación da algún valor como salida.

- El verificador también ejecuta la misma función Hash en los datos recibidos para generar el valor Hash.
- Para la verificación, se comparan este valor Hash y el resultado del algoritmo de verificación. En base al resultado de la comparación, el verificador decide si la firma digital es válida.

- Dado que la firma digital se crea con la clave 'privada' del firmante y nadie más puede tener esta clave; el firmante no puede rechazar la firma de los datos en el futuro.

Cabe resaltar, que en lugar de firmar datos directamente mediante el algoritmo de firma, generalmente se crea un Hash de datos. Como el Hash de datos es una representación única de datos, es suficiente firmar el Hash en lugar de los datos. La razón más importante de usar Hash en lugar de datos directamente para la firma es la eficiencia del esquema.

E.3 Importancia de la Firma Digital

De todas las primitivas criptográficas, la firma digital que utiliza la criptografía de clave pública se considera una herramienta muy importante y útil para lograr la seguridad de la información.

Además de la capacidad de proporcionar un mensaje de no repudio, la firma digital también proporciona autenticación de mensajes e integridad de datos. Veamos brevemente cómo se logra esto con la firma digital:

- **Autenticación de mensaje: c**uando el verificador valida la firma digital utilizando la clave pública de un remitente, se le garantiza que la firma ha sido creada solo por el remitente que posee la clave privada secreta correspondiente y nadie más.

- **Integridad de los datos:** en caso de que un atacante tenga acceso a los datos y los modifique, la verificación de la firma digital en el extremo del receptor falla. El Hash de datos modificados y el resultado proporcionado por el algoritmo de verificación no

coincidirán. Por lo tanto, el receptor puede denegar el mensaje de forma segura suponiendo que se ha infringido la integridad de los datos.

- **No repudio:** como se supone que solo el firmante conoce la clave de firma, solo puede crear una firma única en un dato dado. Por lo tanto, el receptor puede presentar datos y la firma digital a un tercero como evidencia si surge una disputa en el futuro.

- **Imposibilidad de suplantación:** el hecho de que la firma haya sido creada por el signatario mediante medios que mantiene bajo su propio control (su clave privada protegida, por ejemplo, por una contraseña, una tarjeta inteligente, etc.) asegura, además, la imposibilidad de su suplantación por otro individuo.

- **Auditable:** permite identificar y rastrear las operaciones llevadas a cabo por el usuario dentro de un sistema informático cuyo acceso se realiza mediante la presentación de certificados**.**

Al agregar el cifrado de clave pública al esquema de firma digital, podemos crear un criptosistema que puede proporcionar los cuatro elementos esenciales de seguridad, a saber: Privacidad, Autenticación, Integridad y No repudio. [Cryptography for Beginners. Tutorials Point, 2015]

E.4 Encriptación con firma digital

En muchas comunicaciones digitales, es deseable intercambiar mensajes cifrados en lugar de texto sin formato para lograr la confidencialidad. En el esquema de cifrado de clave pública, una clave pública (encriptación) del remitente está disponible en dominio abierto, por lo tanto, cualquiera puede falsificar su identidad y enviar cualquier mensaje encriptado al receptor.

Esto hace que sea esencial para los usuarios que utilizan PKC (Public Key Cryptography) para el cifrado, buscar firmas digitales junto con datos cifrados para garantizar la autenticación del mensaje y el no repudio. Esto puede alcanzarse mediante la combinación de firmas digitales con el esquema de cifrado. Para lograr este requisito, hay dos posibilidades, Firma-entonces-encriptar (sign-then-encrypt) y encriptar-entonces-firma (encrypt-then-sign). Sin embargo, el sistema de cifrado basado en Firma-entonces-encriptar puede ser explotado por el receptor para falsificar la identidad del remitente y enviar esa información a un tercero. Por lo tanto, este método no es preferido. El proceso de Cifrar-luego-firmar es más confiable y ampliamente adoptado. [Cryptography for Beginners. Tutorials Point, 2015]

E.5 Funcionalidad de las firmas digitales

La firma digital garantiza que los datos proceden de una parte concreta es única. Este proceso también utiliza funciones de Hash. Por simplificar, las firmas digitales combinan el Hash (para la validación de los datos de firma) con el cifrado asimétrico para codificar los datos de esa firma. [Cryptography for Beginners. Tutorials Point, 2015]

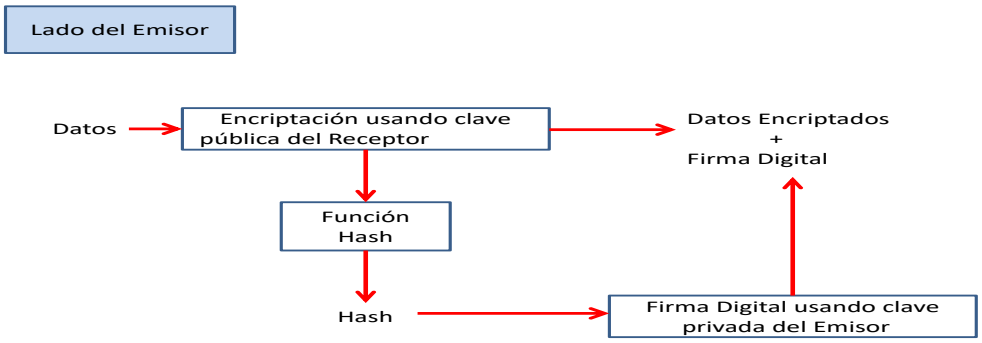


Figura E.5.1 Proceso de Encrypt-then-sign

El receptor después de recibir los datos encriptados y la firma en él, primero verifica la firma usando la clave pública del remitente. Después de garantizar la validez de la firma, luego recupera los datos mediante descifrado usando su clave privada.

Cuando se firman datos con una firma digital ocurre lo siguiente:

- Se aplica un algoritmo de Hash a los datos para crear un valor de Hash.
- Se cifra el valor de Hash con la clave privada del usuario A, creando así la firma digital.
- Se envía al usuario B la firma digital y los datos.
- Cuando se descifran datos firmados digitalmente ocurre lo siguiente:
- El usuario B descifra la firma mediante la clave pública del usuario A y después recupera el valor de Hash. Si la firma se puede descifrar, el usuario B sabe que los datos proceden del usuario A (o del propietario de la clave privada).
- Se aplica el algoritmo de Hash a los datos para crear un segundo valor de Hash.

- Se comparan los dos valores de hash. Si los valores de Hash coinciden, el usuario B sabe que no se han modificado los datos.

Esto se representa en la siguiente figura:

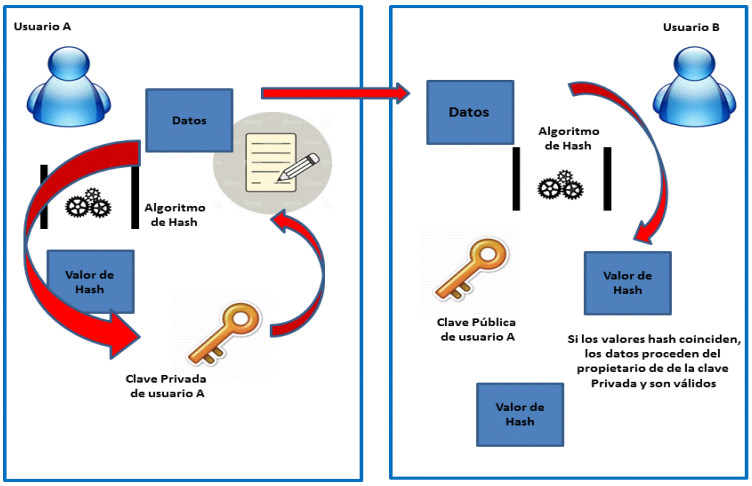


Figura E.5.2 Proceso de Firma Digital

E.6 Aplicaciones de firmas digitales

La firma digital se puede aplicar en las siguientes situaciones:

- Transferencia en sistemas electrónicos, por ejemplo, si se quiere enviar un mensaje para transferir una cantidad X de una cuenta a otra. Si el mensaje se quiere pasar sobre una red no protegida, es muy posible que algún adversario quiera alterar el mensaje tratando de cambiar los valores de la cantidad, con esta información adicional no se podrá verificar la firma lo cual indicará que ha sido alterada y por lo tanto se denegará la transacción
- En aplicaciones de negocios, un ejemplo es el Electronic Data Interchange (EDI) intercambio electrónico de datos de computadora a computadora intercambiando mensajes que representan documentos de negocios

- En sistemas legislativos, es a menudo necesario poner un grupo fecha/hora a un documento para indicar la fecha y la hora en las cuales el documento fue ejecutado o llegó a ser eficaz. Un grupo fecha/hora se podría poner a los documentos en forma electrónica y entonces firmar usando al DSA o al RSA. Aplicando cualquiera de los dos

algoritmos al documento protegería y verificaría la integridad del documento y de su grupo fecha / hora.

- E-mail
- Contratos electrónicos
- Procesos de aplicaciones electrónicos
- Formas de procesamiento automatizado
- Transacciones realizadas desde centros financieros alejados

ANEXO F. CERTIFICADO DIGITAL

F.1 Certificado digital

Por analogía, un certificado se puede considerar como la tarjeta de identificación emitida a la persona. La gente usa tarjetas de identificación, como una licencia de conducir, pasaporte para demostrar su identidad.

Los certificados digitales no solo se emiten a personas, sino que también se pueden emitir a computadoras, paquetes de software o cualquier otra cosa que necesite demostrar su identidad en el mundo electrónico.

- Los certificados digitales se basan en el estándar ITU X.509 que define un formato de certificado estándar para certificados de clave pública y validación de certificación. Por lo tanto, los certificados digitales a veces también se conocen como certificados X.509. La clave pública perteneciente al cliente usuario se almacena en certificados digitales por la Autoridad de Certificación (CA) junto con otra información relevante, como información del cliente, fecha de vencimiento, uso, emisor, etc.

- CA firma digitalmente toda esta información e incluye la firma digital en el certificado.

- Cualquier persona que necesite la seguridad sobre la clave pública y la información asociada del cliente, lleva a cabo el proceso de validación de la firma utilizando la clave pública de CA. La validación exitosa asegura que la clave pública que figura en el certificado pertenece a la persona cuyos detalles se proporcionan en el certificado.

El proceso de obtención de certificado digital por una persona / entidad se muestra en la siguiente figura. [Cryptography for Beginners. Tutorials Point, 2015]

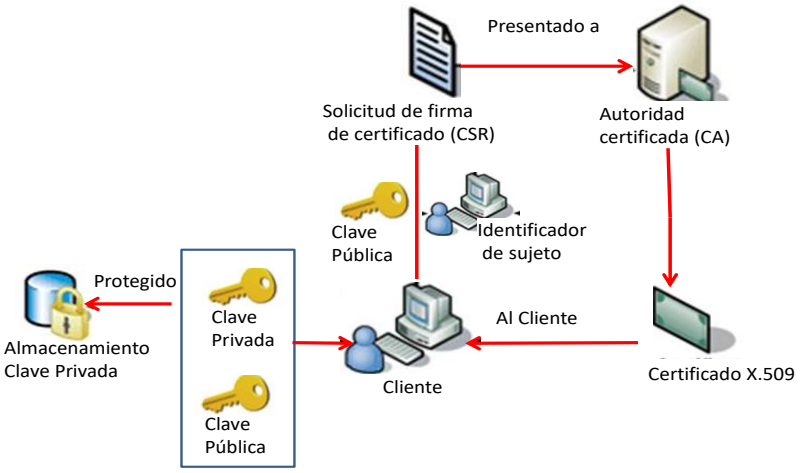


Figura F.1.1 Obtención de Certificado Digital

Como se muestra en la figura, la CA acepta la aplicación de un cliente para certificar su clave pública. La CA, luego de verificar debidamente la identidad del cliente, emite un certificado digital a ese cliente.

F.2 Autoridad de certificación (Certifying Authority CA)

La CA emite un certificado a un cliente y ayuda a otros usuarios a verificar el certificado. La CA se responsabiliza de identificar correctamente la identidad del cliente que solicita la emisión de un certificado y

garantiza que la información contenida en el certificado sea correcta y la firme digitalmente.

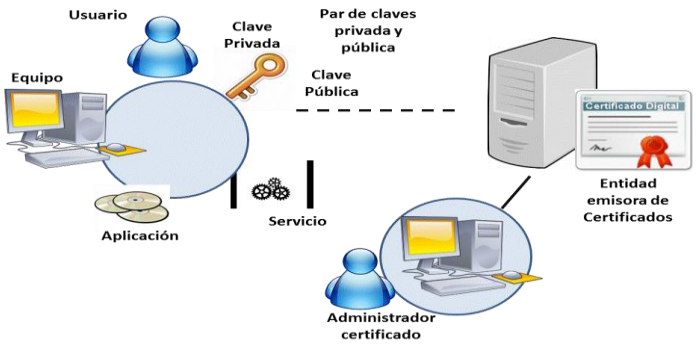


Figura F.2.1 Entidad Emisora de Certificados

F.3 Funciones clave de CA

Las funciones clave de una CA son las siguientes:

- **Generación de pares de claves**: la CA puede generar un par de claves de forma independiente o conjunta con el cliente.

- **Emisión de certificados digitales**: se podría considerar que la CA es el equivalente PKI de una agencia de pasaportes: la CA emite un certificado luego de que el cliente proporciona las credenciales para confirmar su identidad. Luego, la CA firma el certificado para evitar la modificación de los detalles contenidos en el certificado.

- **Publicación de certificados**: la CA debe publicar certificados para que los usuarios puedan encontrarlos. Hay dos formas de lograr esto. Una es publicar certificados en el equivalente de un directorio telefónico electrónico. El otro es enviar su certificado a las personas que cree que podrían necesitarlo de una manera u otra.

- **Verificación de certificados**: la CA pone a disposición su clave pública en el entorno para ayudar a la verificación de su firma en el certificado digital de los clientes.

- **Revocación de certificados: en ocasiones**, CA revoca el certificado emitido debido a alguna razón, como compromiso de clave privada por usuario o pérdida de confianza en el cliente. Después de la revocación, CA mantiene la lista de todos los certificados revocados que están disponibles para el entorno. [Cryptography for Beginners. Tutorials Point, 2015]

F.4 Funcionamiento de los certificados digitales

Si bien las firmas digitales aseguran que los datos proceden de una parte que tiene acceso a una clave privada, no garantizan la identidad de dicha parte. Por ejemplo, un atacante podría haber obtenido una clave privada perteneciente a Microsoft. Entonces podría utilizar esa clave junto con un algoritmo de Hash estándar para firmar unos datos, lo que daría a entender que el origen de los datos es Microsoft. Un certificado digital impide este robo de la identidad electrónica al comprobar que la firma pertenece sin duda alguna al editor. Ahora es posible comprobar los datos y la firma como pertenecientes al editor autorizado porque la entidad emisora de certificados (CA) de confianza ha comprobado que el editor posee tanto la clave pública como la clave privada. [Cryptography for Beginners. Tutorials Point, 2015]

Con los certificados digitales tiene lugar el siguiente proceso:

- Un usuario, equipo, servicio o aplicación crea el par de claves pública y privada.
- La clave pública se transmite a la entidad emisora de certificados (CA) a través de una conexión de red segura.
- El administrador certificado examina la solicitud de certificado para comprobar la información.
- Para la aprobación, el administrador certifica la firma la clave pública con la clave privada de la CA y asegura su autentificación, caso contrario la rechaza y pone en consideración del usuario receptor de la llave que no la utilice.

F.5 ITU X.509

Es la recomendación o norma internacional, encargada de la Interconexión de Sistemas Abiertos y Autentificación de los mismos por certificado digital y tiene como funciones:

- Indica la forma de la información de autenticación contenida por el directorio.
- Describe cómo puede obtenerse la información de autenticación a partir del directorio
- Enuncia los supuestos formulados en cuanto a la formación y al emplazamiento de esa información de autenticación en el directorio
- Define tres modos en los cuales las aplicaciones pueden usar esa información de autenticación para realizar la autenticación, y describe cómo otros servicios de seguridad pueden ser soportados por autenticación.

Esta recomendación describe dos niveles de autenticación: autenticación simple, mediante el uso de una contraseña como verificación de una identidad pretendida, y autenticación fuerte, que implica credenciales formadas usando técnicas criptográficas. Si bien la autenticación simple ofrece cierta protección limitada contra el acceso no autorizado, la autenticación fuerte debe servir de base para ofrecer servicios seguros.