UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA

FACULTAD DE INGENIERÍA, ARQUITECTURA Y DISEÑO

Proveedor de identidades federadas con autenticación biométrica por huella dactilar

Tesis que para obtener el grado de

Maestro en Ingeniería

Presenta

Abraham Abiud Jasmín Lomelí

Co-Directora: M.C. Jetzabel Maritza Serna Olvera

Co-Director: Dr. Juan Ivan Nieto Hipólito

Ensenada B.C. Febrero 2012

UNIVERSIDAD AUTONOMA DE BAJA CALIFORNIA

FACULTAD DE INGENIERÍA, ARQUITECTURA Y DISEÑO

MAESTRÍA Y DOCTORADO EN CIENCIAS E INGENIERÍA

ACTA DE REVISIÓN DE TESIS

TESIS DE GRADO DE MAESTRÍA

"Proveedor de identidades federadas con autenticación biométrica por huella dactilar"

Presentada por:

ABRAHAM ABIUD JASMIN LOMELI

APROBADA por:

Co-Directora: M.C. Jetzabel Maritza Serna Olvera

Co-Director: Dr. Juan Ivan Nieto Hipólito

Sinodal: Dra. Mabel Vázquez Briseño

Sinodal: M.I. Luz Evelia López Chico

Febrero de 2012

DEDICATORIA

A mi esposa e hija

Gabriela Huerta Pérez y Valeria Jasmín Huerta, por ser parte importante de mi vida y sobre todo por brindarme inspiración cada día. Alentandome a ser mejor en todos los aspectos. Por brindarme siempre su amor, comprensión y compañía, para así corresponderles con el mismo amor, esfuerzo y dedicación que se merecen.

A mis padres

Luis Benito Jasmín Sánchez, Noemí Mendoza Campero y Maria Hildelisa Lomelí Covarrubias, por haber forjado en mi persona desde el inicio de mi vida y educación, valores sólidos, y sobre todo por haberme brindado confianza y el amor como padres exelentes que son.

A mis hermanos

Desnisse Jasmín Lomelí, Diana Laura Jasmín Mendoza, Aarón Andres Jasmín Lomelí, por ser apoyo incondicional, y sobre parte importante en la vida.

A mi hermana

Jeanine Jasmín Mendoza D.E.P, quien recientemente terminó su carrera de enfermería, pero lamentablemente le toco marcharse de nuestras vidas, le agradesco su apoyo y tomo de ella un ejemplo para terminar y llegar al final de lo que se empezó con dedicación.

A mis abuelos

Delfino Jasmín Catillo y Maria del Rosario Sánchez de Jasmín, pilares de nuestra familia y ejemplo a seguir.

A mi familia

Por estar siempre unida y darme siempre su apoyo, ejemplo de honestidad y buenos valores.

A mis amigos

Luis Ángel Monge, Luis Adrián Lechuga, Juan Carlos Leñero, Rafael Ruíz, Ricardo Aldan, Jorge Vargas, Oscar Agúndez, Jesús Solaiza, Gabriela Solaiza, René Expinoza, Alberto Es-

pinoza, Ma. de los Ángeles Cosio, David Solis, Andrés Camacho, Arturo Laflor, Eduardo Lerma. Quienes también los considero parte de mi familia, por darme su confianza, amistad y apoyo en todo momento.

AGRADECIMIENTOS

A mis directores de tesis

M.C. Jetzabel Maritza Serna Olvera y Dr. Juan Ivan Nieto Hipólito, por su fuerte apoyo, guía, confianza y valioso tiempo brindado durante la maestría. Por la enseñanza que me aportarón para que fuera posible la realización de este trabajo.

A mis sinodales

M.I Luz Evelia López Chico y Dra. Mabel Vázquez Briseño, por los conocimientos aportados, críticas, comentarios y consejos brindados.

A mis maestros

Dr. Jesús Zamarripa, Dr. José Ángel González Fraga, M.I Juan Pablo Torres Herrera, M.C Christian Xavier Navarro Cota, M.C Elitania Jiménez García, M.I Haydee Meléndez Guillen, M.I Víctor Velázquez Mejía, Dr. Cesar Cruz Hernández y Carlos Gonzales Sánchez, por los conocimientos aportados durante la maestría.

A CONACYT

Por su apoyo económico brindado durante la realización de la maestría

RESUMEN

Algunas de nuestras actividades realizadas cada día requieren de seguridad y privacidad; estas van desde acceso a correos electrónicos, transacciones bancarias en línea, hasta accesos a aéreas restringidas y cuentas en cajeros automáticos. Tomando en cuenta que la tecnología avanza continuamente, se busca la mejora en mantener seguridad y privacidad en estas actividades, empleando diversos métodos. Entre ellos podemos contar con el uso de tarjetas, llaves, contraseñas y números secretos. Sin importar lo mucho que nos pueda costar memorizar siempre tantos numeros o el espacio que requieren las tarjetas y llaves en nuestras carteras o bolsas, seguimos haciéndolo, porque queremos tener la seguridad de que nadie más podrá revisar nuestros correos, hacer transacciones bancarias indebidas con nuestras tarjetas o acceder a áreas restringidas sin autorización. Al hacer esto tenemos la seguridad hasta cierto punto, pero nos complica la situación cuando olvidamos las contraseñas y números secretos o cuando extraviamos las tarjetas y llaves.

Hoy en día existe un creciente uso de servicios en Internet, muchos de ellos contienen datos o información personal o restringida muy importante (información bancaria, correo electrónico, datos personales, etc.), debido a ello, se buscan sistemas más seguros para contener esta información. Sin embargo, esta seguridad no estaría completa sin un método de acceso seguro o la cooperación de los usuarios al mantener en secreto u oculto de los demás el elemento de acceso (contraseña, tarjeta, etc.), siendo el nombre de usuario y contraseña el método más utilizado.

El uso de este método suele tener poco nivel de seguridad, debido a que puede ser adivinado, robado o forzado por otros sistemas. Es por eso que, en esta investigación se sugiere el uso de huella dactilar como método de acceso, el cual presenta buen nivel se seguridad ya que no puede ser adivinado o robado puesto que es un elemento único de acceso.

Los módulos de acceso por huella dactilar están al alcance de cualquier empresa, desarrollador o institución, tanto en costo como en variedad de herramientas y fácilmente puede ser agregado a un servicio de Internet, ya que existe una amplia variedad de elementos que permiten desarrollar dichos módulos. Basta con tener un sensor (lector de huella dactilar) y una herramienta para el desarrollo de la misma.

En nuestra investigación, como se verá más adelante, se ha elegido un lector de huellas dactilares comercial y de bajo costo además de sencillo de manejar y una herramienta de

desarrollo completa y segura, además de mantener un precio accesible en el mercado, dando la opción de prueba por tiempo limitado, lo cual nos beneficia para la investigación.

Otro punto importante abordado en este documento, son las identidades de los usuarios y como estos crean una identidad para casa servicio, además de contar con un elemento de acceso diferente para cada uno de ellos. Es decir, un usuario puede tener un nombre de usuario y contraseña para cada servicio (además de datos personales diferentes), los cuales por ser mas de unos pueden ser olvidados más fácilmente o puede resultar tedioso tener que recordar cada unos de ellos. Para ello se presenta la alternativa de utilizar el concepto de federación de identidades, con lo cual se logra tener un acceso y elementos únicos para todos los servicios en donde el usuario este registrado. En consecuencia, se puede acceder a más de un servicio dando sus elementos de acceso una sola vez y más seguro, aún cuando estos elementos de acceso sean el nombre de usuario y la huella dactilar empleada como llave biométrica.

En este documento se presenta un sistema de gestión de identidades para acceso a diversos servicios en Internet, empleando el uso de usuario y huella dactilar como método de autenticación biométrica.

Índice general

1. Introducción **8**

1.1. Antecedentes 8

1.1.1. Ubicación geográfica 8

1.1.2. Antecedentes históricos 8

1.2. Justificación 11

1.3. Planteamiento del problema 12

1.3.1. Descripción del problema 12

1.3.2. Interrogantes del estudio 12

1.4. Delimitaciones del estudio 12

1.4.1. Delimitación geográfica 12

1.4.2. Delimitación tecnológica 13

1.4.3. Sistema propuesto 13

1.5. Objetivos 14

1.5.1. Objetivo general 14

1.5.2. Objetivos específicos 14

2. Estado del Arte **16**

2.1. Autenticación como servicio de seguridad 16

2.2. Biometría 17

2.3. Sistemas biométricos 17

2.3.1. Características 17

2.3.2. Modos de operación 19

2.3.3. Rendimientos de los sistemas biométricos 22

2.4. Sistemas de reconocimiento mediante huella dactilar 23

2.4.1. Características de la huella 23
2.4.2. Clasificación de las huellas dactilares 24
2.4.3. Adquisición de datos biométricos y procesamiento de la huella 25
2.4.4. Determinación de minucias y marcado de decisión 27
2.4.5. Aplicación de los sistemas biométricos por huella 27
2.4.6. Herramientas para desarrollo de sistemas para gestión de huellas . . . 29
2.5. Gestión de identidades 30
2.5.1. Protección de identidades en Internet 30
2.5.2. Enfoques para la gestión de identidades 31
2.6. Federación de Identidades 32
2.6.1. Proyecto Liberty Alliance 32
2.7. OpenSSO 35
2.8. Comparativa entre OpenSSO y OpenID 37
2.9. Proveedor de identidades por huella dactilar 38

3. Requerimientos y Metodología **39**
3.1. Requerimientos 39
3.2. Plan de trabajo 40

4. Implantación del servidor de directorios **42**
4.1. Servidores de directorios 42
4.2. Recursos para el Servidor de directorios 43

5. Implantación del proveedor de identidades **45**
5.1. Servidor de aplicaciones 45
5.2. Proveedor del identidades 46

6. Módulo de autenticación biométrico **49**
6.1. Herramientas y requerimientos 49
6.1.1. Lectores de huellas dactilares 50
6.1.2. Selección del lector de huellas 52
6.1.3. Software de desarrollo para huellas dactilares 52
6.2. Diseño del módulo biométrico 54

6.3. Desarrollo del módulo biométrico 59

7. Proveedor de identidades federadas con autenticación por huella dactilar 61

7.1. Integración del módulo proveedor de identidades al módulo biométrico 61

7.1.1. Arquitectura de comunicación 61

7.1.2. Ventajas 62

7.1.3. Desventajas 63

8. Pruebas y Resultados 67

8.1. Registro de huella y perfil en el IDP 68

8.2. Acceso a un servicio de Web 70

8.3. Acceso a un servicio por huella dactilar 74

8.4. Interacción entre servicios Web sin federación de identidades 77

8.5. Federación de identidades 81

8.6. Inicio de sesión único (SSO, Single Sign On) 85

8.7. Cierre de sesión único (SLO, Single Log Out) 89

8.8. Terminando federación de cuentas 92

8.9. Conclusiones 94

Índice de figuras

1.1. Proveedor de identidades con autenticación por huella dactilar 14

2.1. Diagrama de bloques del sistema de inscripción biométrica 20
2.2. Diagrama de bloques del sistema de verificación biométrica 20
2.3. Diagrama de bloques del sistema de identificación biométrica 21
2.4. Tasas de errores del sistema biométrico 23
2.5. Algunas de las minucias principales 25
2.6. Clases de huellas dactilares 26
2.7. Procesamiento de la huella dactilar 26
2.8. Diagrama de bloques del Círculo de Confianza 35

3.1. Proveedor de identidades con autenticación por huella dactilar 40

4.1. Módulo LDAP 43

5.1. Módulo servidor de aplicaciones 46
5.2. Arquitectura de comunicación entre el proveedor de identidades y el servidor de directorios OpenDS 47
5.3. Diagrama de bloques del proveedor de identidades y el servidor de directorios 47

6.1. Imagen de huella dactilar 51
6.2. Diagrama del sensor de huellas capacitivo 51
6.3. Arquitectura de comunicación entre el módulo de captura biométrico y el Web Service de verificación de huellas 55
6.4. Arquitectura de comunicación entre el módulo de captura biométrico y el Web Service de verificación de huellas 56
6.5. Interfaz gráfica del módulo de registro con huella dactilar 57

6.6. Interfaz gráfica del módulo de acceso por huella dactilar 57
6.7. Diagrama de bloques del módulo de registro 57
6.8. Diagrama de bloques del módulo de autenticación 58
6.9. Diagrama de bloques del módulo biométrico 60

7.1. Arquitectura de comunicación entre el proveedor de identidades y el módulo biométrico en el acceso a un servicio A 64
7.2. Arquitectura de comunicación entre el proveedor de identidades y el módulo biométrico en el acceso a un servicio B 65
7.3. Diagrama de bloques del proveedor de identidades con autenticación por huella dactilar 66

8.1. Enlace de acceso a registro de proveedor de identidades con huella dactilar . 69
8.2. Página de ingreso de información de registro al proveedor de identidades por huella dactilar 69
8.3. Página de acceso al servicio Web de reservación de autos 71
8.4. Autenticación del usuario 71
8.5. Negación de acceso 72
8.6. Autorización de acceso 72
8.7. Servicio Web de prueba 73
8.8. Página de acceso al Servicio Web de reservación de vuelos 75
8.9. Autenticación del usuario por huella 75
8.10. Negación de acceso por huella 76
8.11. Autorización de acceso por huella 76
8.12. Página de acceso al servicio Web de reservación de vuelos 78
8.13. Autenticación de usuario por huella 78
8.14. Servicio autorizado 79
8.15. Accediendo al servicio Web de reservación de autos 79
8.16. Servicio sin autorización de acceso 80
8.17. Selección de acceso seguro por medio del IDP 82
8.18. Autenticación en el IDP 82
8.19. Autenticación en el servicio Web 83

8.20. Servicio Web de reservación de autos 83
8.21. Servicio Web de reservación de vuelos 84
8.22. Selección de acceso seguro por medio del IDP dentro del servicio reserva de vuelos 86
8.23. Autenticación por huella 86
8.24. Servicio reserva de vuelos 87
8.25. Acceso al servicio reserva de autos 87
8.26. Servicio reserva de autos 88
8.27. Servicio Web reserva de vuelos 90
8.28. Servicio Web reserva de autos 90
8.29. Cierre de sesión en reserva de autos 91
8.30. Cierre de sesión en reserva de vuelos 91
8.31. Terminando federación de cuentas 93
8.32. Federación de cuentas terminada 93

Índice de tablas

2.1. Comparativa entre las características biométricas 18
2.2. Comparativa entre OpenSSO y OpenID 37

3.1. Plan de trabajo 41

6.1. Comparativa entre lectores de huella dactilar 52
6.2. Lectores de huella dactilar 54

8.1. Caso de prueba: Registro de usuario por huella dactilar 68
8.2. Caso de prueba: Acceso a un servicio Web 70
8.3. Caso de prueba: Acceso por huella 74
8.4. Caso de prueba: Interacción entre servicios Web sin federación de identidades 77
8.5. Caso de prueba: Federación de identidades 81
8.6. Caso de prueba: Inicio de sesión único 85
8.7. Caso de prueba: Cierre de sesión único 89
8.8. Caso de prueba: Termino de federación 92

Capítulo 1

Introducción

En este capítulo se abordan los antecedentes del tema de investigación, asi como la justificación e importancia del estudio, para despues plantear la problemática del tema con las herramientas y objetivos a cumplir para resolverla.

1.1. Antecedentes

1.1.1. Ubicación geográfica

El proyecto "Proveedor de identidades federadas con autenticación biométrica"surge en la Universidad Politécnica de Cataluña en España, ante la necesidad de implantar una solución que implementara el proceso de gestión de identidades y que permitiese a los usuarios acceder a diversas aplicaciones web utilizando las mismas credenciales de acceso.

1.1.2. Antecedentes históricos

Desde hace ya tiempo como solución a dar soporte al manejo de información de usuarios para el acceso a servicios, surgió la gestión de identidades, que se encarga de resolver todos y cada uno de los pasos de la secuencia de generación, asignación de privilegios, modificación de los mismos, suspensión y eliminación de perfiles de usuario para el acceso a sistemas y servicios. Las herramientas de gestión de identidad concentran gran parte del interés tecnológico existente en el mercado de la seguridad en TI (tecnologías de información). En este caso, confluyen la madurez de las soluciones que los diversos fabricantes presentan, la concietización y necesidad de los potenciales usuarios. Por un lado, se asiste a ciertos cambios regulatorios en Estados Unidos y la Unión Europea que introducen exigencias a los acce-

sos al procesamiento, custodia y transmisión de ciertos tipos de datos, especialmente por los requisítos impuestos en la auditoría posterior del cumplimiento de dichas normas. Por otro lado, la cada vez más problemática gestión del ciclo de vida de las autorizaciones de acceso de usuarios ha forzado a las grandes corporaciones a interesarse por herramientas que habiliten, faciliten y demuestren una correcta gestión tanto de la identidad como permisos de sus usuarios, proveedores, colaboradores y demás roles asociados a su objeto de negocio. Ciertos problemas de la gestión de identidades digitales han sido abordados desde hace bastante tiempo como la validación de las identidades, el acceso remoto a las credenciales de autenticación o la unificación de identificadores y contraseñas. No obstante, es ahora cuando los productos de identidad tratan de abordar el problema de forma global, para ello añaden el control y la automatización de táreas que hasta ahora era necesario realizar con técnicas propias de cada organización o de una forma poco eficiente [21].

Se ha utilizado mucho la Gestión de Identidades para diferentes áreas (compra/ventas, servicios bancarios, comercio, educación, etc.) y existen diversos medios de identidad para acceder a estos servicios. Entre estos se pueden mencionar el uso de usuario y contraseña, pasaporte, dirección IP, tarjetas inteligentes o Smartcards (cualquier tarjeta del tamaño de un bolsillo con circuitos integrados incluidos que permitan la ejecución de cierta lógica programada), foto y parámetros biométricos (iris del ojo humano, huella digital) y datos proporcionados por usuarios (dirección, teléfono, correo electrónico, etc.).

La **autenticación** es un proceso de identificación para acceder a servicios, que se hace numerosas veces cada día por los humanos y las computadoras por igual. Cuando hablamos acerca de la autenticación humana básicamente tenemos tres opciones: la utilización de algo que sabemos (como el uso de contraseñas y claves), algo que tenemos (como el uso de fichas de acceso, tarjetas inteligentes, etc.) o algo de lo que somos (biometría). No existe "un mejor"método de autenticación; cada uno tiene sus ventajas y limitaciones dependiendo de la aplicación, los usuarios, y el ambiente en el cual se emplean. Sea cual sea el método de autenticación que se use, se puede reforzar mediante la combinación de uno o más métodos. Un ejemplo de autenticación fuerte, sería un sistema que exige la posesión de una tarjeta inteligente, el conocimiento de una contraseña o número de identificación personal (PIN),

y verificación biométrica. Obviamente, para robar o falsificar los tres, sería más difícil que robar o falsificar solo uno de estos, sin embargo, esto resultaría más costoso y complicado de operar [9].

La autenticación es un mecanismo fundamental, representa la base de protección de un sistema, el cual consiste en comprobar que un usuario es quien dice ser, y comúnmente se basa en el conocido par nombre de usuario y contraseña. Pero una autenticación tan simple deja mucho que desear, pues si alguien conoce ambos datos podría entrar en el sistema por nosotros falseando nuestra identidad, y tendría acceso a todas las aplicaciones para las que estemos autorizados.

Actualmente, el método de acceso más usual a algún servicio de Internet, es por medio de usuario y contraseña; además lo más común es que cada usuario tenga un identificador único para cada servicio ofrecido.

La utilización de claves secretas o tarjetas de identificación no es suficiente en algunos casos. Lo que se necesita es algo que pueda verificar sin lugar a dudas que uno es quién dice ser, justo lo que ofrece la biometría.

Las técnicas de autenticación biométrica se han asociado con algo muy complejo y costoso, pero eso hoy en día no es así. La evolución tecnológica permite construir equipos sencillos y económicos, con un alto poder de procesamiento, que se pueden utilizar, por ejemplo, para leer las huellas dactilares, identificar la voz o escanear el iris. De esta manera, algunas aplicaciones biométricas para la identificación resultan muy eficientes y, una vez rota la barrera del precio, su extensión empieza a dispararse por todos los ámbitos, desde el profesional al doméstico [20].

El uso de la **biometría** representa una solución fuerte en la protección de datos e identificación, es un tema muy joven, pero ha resultado efectivo hasta el momento, debido a la gran seguridad que este ofrece. En este método de autenticación y reconocimiento, los elementos consisten o están basados en características fisiológicas o de comportamiento de un humano que los distingue de otras personas y que teóricamente puede ser utilizada para identificación o verificación de identidad.

Como elemento biométrico podemos encontrar la huella digital o dactilar, que es utilizado

comúnmente para autenticación y es posiblemente la más utilizada de todas las tecnologías biométricas, y ha sido cuidadosamente verificada a través de diversas aplicaciones. En particular ha demostrado su alta eficiencia y ha mejorado la tecnología en la investigación penal durante más de un siglo [9]. Es también una de las formas más seguras y accesibles de control de acceso al personal que labora en una empresa o institución. La demanda de equipos que capturen huellas digitales ha propiciado una producción masiva y por tanto una significativa reducción del precio final del equipo al consumidor.

1.2. Justificación

Actualmente los métodos de acceso más usual para los servicios de Web o servicios de Internet, se basan en el empleo de usuario como identificador y su respectiva contraseña; además, lo más común es que cada usuario posea un identificador y contraseña distintos para cada servicio, lo cual suele ser cansado, por el hecho de tener que estar recordándolos y la solución para ello, generalmente es anotar esta información, algo que puede ser una grave falta de seguridad.

Otro aspecto que molesta al usuario, es el hecho de tener que esta autenticándose en cada servicio, lo cual le resta fluidez a la navegación. Además de todo, el hecho de emplear contraseña para conseguir el acceso a cada servicio, ofrece muy poca seguridad, ya que por lo generar, pocas veces se crean contraseñas fuertes, y aun cuando esto se consigue, pueden ser adivinadas, fácilmente robadas o existen algoritmos que pueden generarlas.

Los proveedores de identidades tienen las características de encargarse directamente de la gestión de identidades dando privacidad a los datos de usuarios y seguridad de acceso a los servicios de internet, además de fluidez a la navegación del usuario, evitando la autenticación repetitiva; aunado a esto el implementar un módulo de autenticación biométrica por medio de huella dactilar que es un método de autentificación confiable, a un proveedor de identidades, daría como resultado un método de acceso cómodo y con un alto nivel de seguridad y confianza.

1.3. Planteamiento del problema

1.3.1. Descripción del problema

Muchos de los servicios ofrecidos en Internet, requieren de autenticación previa, esto provee cierto grado de seguridad de acceso. Este depende del método de autenticación que se emplee y por lo general suele usarse nombre de usuario y contraseña, presentando poco grado de seguridad además de tener que memorizar la contraseña. Además, sí se tiene que acceder a más de un servicio, hay que autenticarse igual de veces y tener tantas contraseñas como servicios se tengan, volviendo muy pausada la navegación.

Un método de autenticación más seguro y en el que no hay que memorizar palabras claves, es empleando huella dactilar acompañada de nombre de usuario. Por otro lado, también existe el concepto de **Single Sign On**, que presenta un método de acceso único para varios servicios, haciendo más fluida la navegación.

Estos dos elementos se encuentran por separado, y son bien aceptados entre los usuarios y prestadores de servicios. Sin embargo, aún no se cuenta con sistema alguno en el cual se involucren ambos.

1.3.2. Interrogantes del estudio

¿Cómo se puede generar e incorporar un módulo de acceso por huella dactilar al proveedor de identidades?
¿Qué nivel de eficiencia y fluidez en la navegación entre servicios Web ofrecerá un proveedor de indetidades federadas con el modulo biométrico?

1.4. Delimitaciones del estudio

1.4.1. Delimitación geográfica

Se trabajó en la Universidad Autónoma de Baja California, en un ambiente favorable para los servidores, empleando direcciones IP y dominios para poder ser probado y desarrollado con apoyo de la Universidad Politécnica de Cataluña, en España.

1.4.2. Delimitación tecnológica

- Uso del código abierto OpenSSO para Gestión de Identidades.
- Servidor de directorio LDAP.
- Utilización de un lector de huella digital para puerto USB para autenticación biométrica.
- Librerías para la gestión de huellas dactilares.
- Lenguaje de programación Java.
- Sistema operativo Fedora 8.
- Sistema Operativo Windows.

1.4.3. Sistema propuesto

Consiste básicamente en la implementación e integración de un módulo de autenticación biométrica por huella dactilar, a un sistema de proveedor de identidades.
Como se observa en la figura 1.1, el módulo de autenticación biométrica puede ser empleado por otros Proveedores de Servicios(SP) afiliados al Proveedor de Identidades; IDP, por sus siglas en inglés Identity Provider.

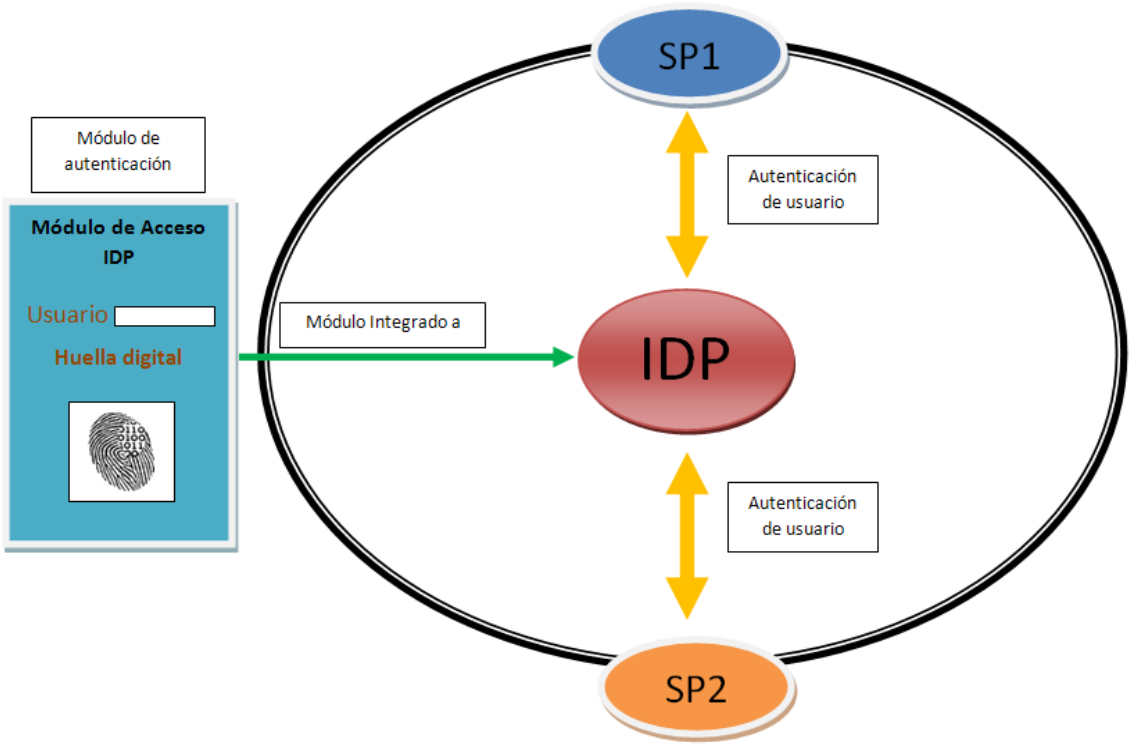

Figura 1.1: Proveedor de identidades federadas con autenticación por huella dactilar

1.5. Objetivos

1.5.1. Objetivo general

Diseñar e implementar, un sistema proveedor de identidades federadas que utilice autentificación biométrica por huella dactilar.

1.5.2. Objetivos específicos

- Analizar las características y funcionamiento de los sistemas biométricos por huella dactilar.
- Analizar las características y funcionamiento del modelo proveedor de identidades.
- Implantar un proveedor de identidades empleando OpenSSO que es un software libre de código fuente abierto.
- Diseñar e implementar, un módulo de autenticación por huella dactilar.
- Integrar el módulo de huella dactilar al proveedor de identidades.

- Realizar pruebas de acceso por autenticación de huella dactilar a servicios afiliados al proveedor de identidades.

Capítulo 2

Estado del Arte

Se analizan los elementos que intervienen en el proyecto, dejando en claro la importancia y funcionalidad que cada uno de estos tiene. Así mismo, se presenta una comparación entre dos sistemas proveedores de identidades y elementos biométricos.

2.1. Autenticación como servicio de seguridad

El manejo de identidades para la autenticación en servicios de Internet, utiliza diferentes elementos que sirven para permitir acceso a un usuario en aquellas áreas o sitios que se encuentren restringidos. Entre estos elementos se pueden mencionar, las SmartCards; usuario y contraseña; dirección IP y los elementos biométricos (huella digital, iris del ojo, etc.).
Una amplia variedad de sistemas requieren de esquemas fiables de reconocimiento de personas para confirmar o determinar la identidad de un individuo que solicita sus servicios. El propósito de tales esquemas es asegurar que el acceso a los servicios que se prestan, sea sólo por un usuario legítimo y nadie más. Ejemplos de tales aplicaciones incluyen el acceso seguro a los edificios, sistemas de computadoras (servicios de internet, programas, etc.), computadoras portátiles, teléfonos celulares, y los cajeros automáticos. En la ausencia de un esquema robusto de reconocimiento de personas, estos sistemas son vulnerables a la astucia de un impostor. El reconocimiento biométrico o, simplemente, la biometría se refiere al reconocimiento automático de los individuos sobre la base de sus rasgos fisiológicos y / o características de comportamiento.
Mediante el uso de la biometría, es posible confirmar o establecer la identidad de un individuo basada en “lo que el individuo es”, en lugar de “lo que posee”(por ejemplo, un ID

tarjeta) o "lo que recuerda o sabe"(por ejemplo, una contraseña) [6].

2.2. Biometría

El termino biometría proviene de la palabra griega *bios* (vida) y *metrikos* (medida). Es bien sabido que los seres humanos usan de manera intuitiva algunas características del cuerpo, tales como el rostro, la manera de andar o la voz, para reconocerse entre ellos. Tradicionalmente, las contraseñas y tarjetas de identificación se han utilizado para restringir el acceso a sistemas de seguridad, pero esto métodos pueden ser fácilmente burlados o no son fiables.
Los elementos biométricos no pueden ser prestados, robados u olvidados, y su recreación es prácticamente imposible [10].

2.3. Sistemas biométricos

Un sistema biométrico es esencialmente un sistema de reconocimiento de patrones que reconoce o confirma la identidad una persona, basándose en un conjunto de características (vector característico) derivadas de características fisiológicas o conductuales que la persona posee [10], [24].

El vector característico es usualmente almacenado en una base de datos (o en una tarjeta inteligente dada a la persona) después de ser extraído. Un sistema biométrico basado en características fisiológicas, es generalmente más fiable que uno que adopta características conductuales, aunque este último puede ser más fácil de integrar en ciertas aplicaciones especificas [10].

2.3.1. Características

Para poder formar parte de un sistema biométrico, las características físicas y conductuales, deben satisfacer las siguientes condiciones [27]:

- **Universalidad**: toda persona debe poseer la característica.
- **Unicidad**: que una persona pueda distinguirse de la otra a partir de la característica.
- **Permanencia**: no se modifica o no cambia significativamente con el paso del tiempo o con el medio ambiente.
- **Medible o cuantificable (Collectability)**: que el identificador biométrico se pueda medir cuantitativamente.
- **Desempeño**: precisión de la identificación.
- **Aceptabilidad**: que el sistema biométrico sea aceptado por la mayor parte de la gente.
- **Elusión (Circumvention)**: debe ser suficientemente robusta, para diversos métodos fraudulentos.

En la tabla 2.1 se muestra una breve comparación obtenida de la fuente [24] de quince características biométricas empleadas en sistemas.

Características biométricas	Universalidad	Unicidad	Permanencia	Cuantificable	Desempeño	Aceptabilidad	Elusión
Termograma facial	H	H	L	H	M	H	L
Venas de las manos	M	M	M	M	M	M	L
Modo de andar	M	L	L	H	L	H	M
Tecleo	L	L	L	M	L	M	M
Olor	H	H	H	L	L	M	L
Oreja	M	M	H	M	M	H	M
Geometría de la mano	M	M	M	H	M	M	M
Huella dactilar	M	H	H	M	H	M	M
Rostro	H	L	M	H	L	H	H
Retina	H	H	M	L	H	L	L
Iris	H	H	H	M	H	L	L
Palma de la mano	M	H	H	M	H	M	M
Voz	M	L	L	M	L	H	H
Firma	L	L	L	H	L	H	H
ADN	H	H	H	L	H	L	L

Tabla 2.1: Donde **H** denota un valor alto, **M** un valor medio y **L** valor bajo

2.3.2. Modos de operación

Dependiendo en el contexto de aplicación, un sistema biométrico puede funcionar bien en el modo de verificación o modo de identificación [6].

En el modo de verificación (Figura 2.2), el sistema realiza la validación de identidad de la persona mediante la comparación de los datos biométricos capturados contra los de su propia plantilla o plantillas almacenadas en la base de datos del sistema. En tal sistema, un individuo que desea o pide ser reconocido hace una petición (reclamación) de identidad, usualmente a través de un número de identificación personal (NIP), un nombre de usuario, o una tarjeta inteligente, y el sistema realiza una comparación de uno a uno para determinar sí la reclamación de identidad es cierta o no (p. ej. "¿Estos datos biométricos pertenecerán a Juan?"). La verificación de la identidad es típicamente utilizada para el reconocimiento positivo, donde el objetivo es evitar que varias personas utilicen la misma identidad [26].

En el modo de identificación (Figura 2.3), el sistema reconoce a un individuo mediante la búsqueda de entre las plantillas de todos los usuarios de la base de datos. Por lo tanto el sistema realiza una comparación de uno a muchos para establecer la identidad de un individuo (o no si el sujeto no está inscrito en la base de datos del sistema), sin algún objeto al tener que reclamar una identidad (p. ej. "¿A quién pertenecen estos datos biométricos?"). La identificación es un componente crítico en aplicaciones de reconocimiento negativo en donde el sistema determina que la persona es quién es y niega que sea. El propósito del reconocimiento negativo es prevenir que una sola persona use múltiples identidades [26]. Si bien los métodos tradicionales de reconocimiento personal, como contraseñas, números de identificación, llaves, y las fichas pueden trabajar para el reconocimiento positivo, el reconocimiento negativo sólo puede establecerse a través de la biometría [6].

Para que estos dos modos puedan operar correctamente, previamente se debe hacer un proceso de inscripción (Figura 2.1) para la captura de las características de una muestra biométrica dada por un individuo y convertirla en una plantilla. La eficiencia de la inscripción depende estrictamente de la calidad de los datos presentados junto con los datos biométricos. Por lo tanto, el proceso de inscripción ha de garantizar que la verificación de los documentos (como los pasaportes y licencias de los conductores, etc.) sea digna de confianza, de modo que una

falsificación o una falsa identidad no están ligadas a un elemento biométrico. Además no se almacenan registros duplicados en la base de datos para la misma identidad. Tal mecanismo de inscripción es un aspecto clave de la autenticación biométrica por lo que es muy fiable. La inscripción es la primera interacción del usuario con el sistema biométrico, y el mal uso de dicha operación puede afectar a la calidad de la muestra proporcionada por el usuario, que a su vez afecta el rendimiento global del sistema. Una primera experiencia incómoda después podrían afectar a las interacciones del usuario con el sistema, y eso afecta al rendimiento global del sistema. Una vez que el proceso de registro es completado con éxito, la persona puede utilizar el sistema biométrico para la autentificación [3].

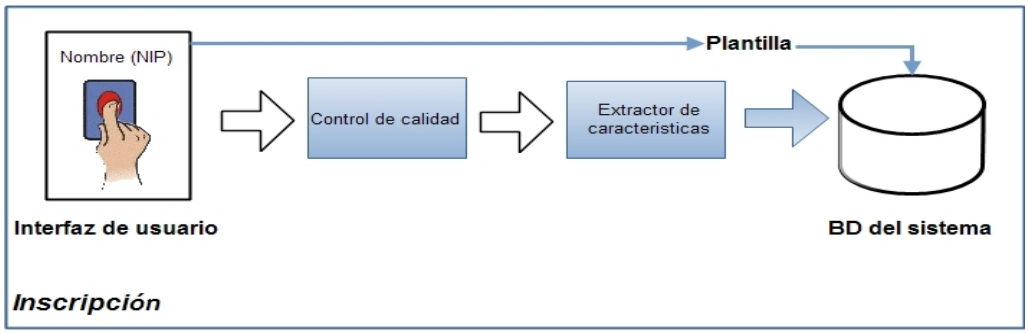

Figura 2.1: Diagrama de bloques del sistema de inscripción biométrica [6]

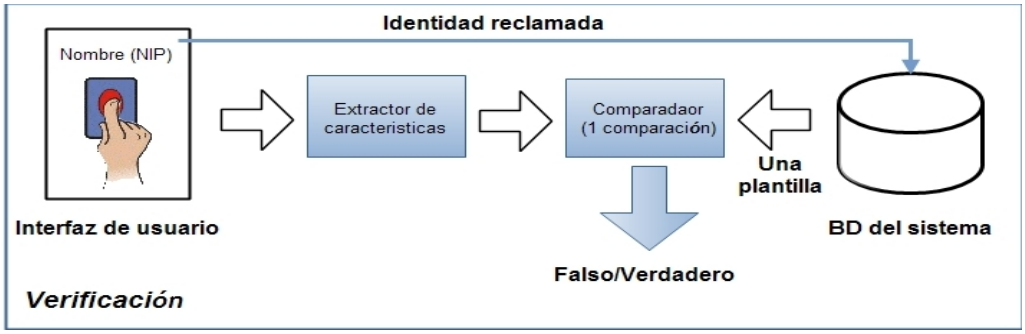

Figura 2.2: Diagrama de bloques del sistema de verificación biométrica [6]

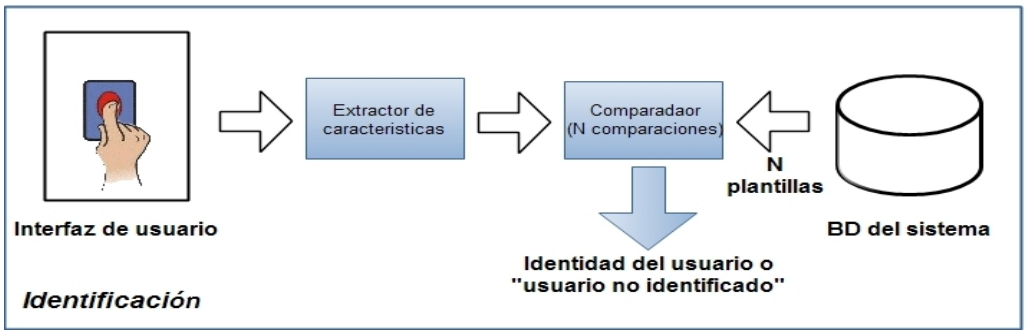

Figura 2.3: Diagrama de bloques del sistema de identificación biométrica [6]

Como se muestró en las figuras anteriores, un sistema biométrico es diseñado con cuatro principales módulos [6]:

Módulo del sensor: captura los datos biométricos de cada individuo. Un ejemplo es un sensor de huella dactilar que toma la imagen de la estructura de las crestas y valles de la huella dactilar.

Módulo de extracción de características: en este módulo los datos biométricos adquiridos se procesan para extraer una serie de características salientes o características discriminatorias. Por ejemplo, la posición y orientación de los puntos de las minucias (singularidades de crestas y valles). En una imagen de huella dactilar se extraen en el módulo de extracción de características de un sistema biométrico basado en huella dactilar.

Módulo de comparación: en este módulo las características extraídas se comparan con los de las plantillas guardadas para generar resultados de coincidencias. Por ejemplo, en un módulo de comparación de un sistema biométrico basado en huella dactilar, se determina el número de minucias coincidentes entre las entradas y las plantilla de imágenes de las huellas dactilares y se reporta la puntuación de coincidencias. Este módulo también encapsula o contiene un modulo de toma de decisiones, en el cual la identidad reclamada por el usuario es confirmada (verificación) o se establece la identidad del usuario (identificación) basando se en los resultados de la comparación.

Módulo de sistema de base de datos: éste es utilizado por el sistema biométrico para almacenar las plantillas biométricas de los usuarios inscritos. El módulo de inscripción es responsable de inscribir a las personas en la base de datos del sistema biométrico. Durante la fase de inscripción, la característica biométrica de una persona por primera vez es escaneada

por un lector biométrico para producir una representación digital de la característica. Durante el proceso de inscripción puede o no ser supervisada la captura de los datos por un humano, según la aplicación. Generalmente es realizado un control de calidad, para garantizar que la muestra adquirida pueda ser fiablemente procesada por las siguientes etapas. Con el fin de facilitar la comparación, la representación digital de entrada es procesada por un extractor de características para generar una representación compacta, pero expresiva, llamada plantilla. Dependiendo de la aplicación, la plantilla puede ser almacenada en la base de datos central del sistema biométrico o ser grabada en una tarjeta inteligente emitida al individuo. Usualmente se almacenan múltiples plantillas de una persona para dar cuenta de las variaciones observadas en los rasgos biométricos y las plantillas de la base de datos pueden ser almacenadas a lo largo del tiempo.

2.3.3. Rendimientos de los sistemas biométricos

Debido a las diferentes posiciones sobre el sensor de adquisición, condiciones de imperfección de imágenes, cambios ambientales, deformaciones, ruido y mala interacción de los usuarios con el sensor, es imposible que dos muestras de una misma característica biométrica, adquiridas en diferentes sesiones, coincidan exactamente. Por esta razón la respuesta de la comparación de los sistemas biométricos es típicamente una puntuación de comparación denominada "s"(normalmente un numero único) que cuantifica la similitud entre la representación de la plantilla de entrada y la de la base de datos. Cuanto más alto sea el puntaje, es más seguro que en el sistema las dos muestras coincidan [24]. Una puntuación similar "s"se compara con un umbral de aceptación denominado "t" y sí "s" es mayor o igual que "t", las muestras comparadas pertenecen a una misma persona. Los pares de muestras con puntuaciones más bajas que "t"pertenecen a diferentes personas. La distribución de los resultados generados a partir de pares de muestras de diferentes personas se llama "distribución de impostor", y la puntuación de distribución generada a partir de pares de muestras de la misma persona que se llama "distribución genuina"(Ver Figura 2.4) [24].

En [10] se hace mención que los principales errores de los sistemas, usualmente se miden en términos de:

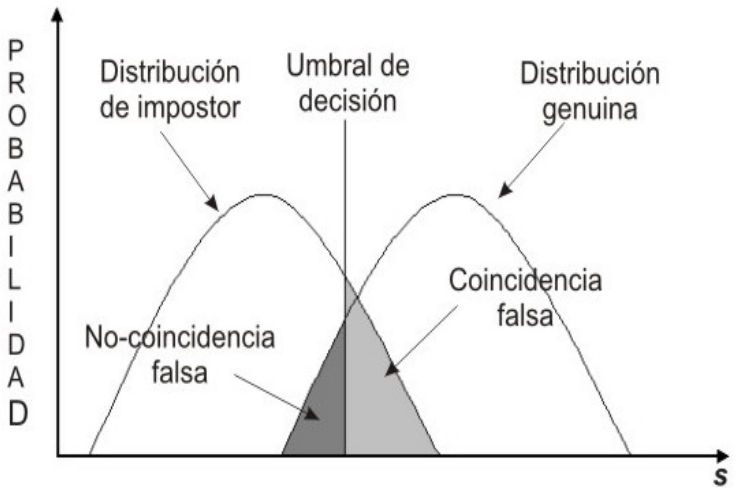

Figura 2.4: Tasas de errores del sistema biométrico [24]

(a) Tasa de no-coincidencia falsa, en ingles **FNMR** (**false nonmatch rate**), en el cual se confunden dos mediciones biométricas de la misma persona, como si fueran de personas diferentes.

(b) Tasa de coincidencia falsa, en ingles **FMR** (**false match rate**), en la cual se confunden dos mediciones biométricas de diferentes personas como si fueran de la misma.

2.4. Sistemas de reconocimiento mediante huella dactilar

Sin duda alguna, los sistemas de reconocimiento por huella dactilar como sistemas biométricos son hoy en día son mayormente aceptados y empleados para control de acceso a recintos, identificación y seguridad en medios electrónicos e informáticos. No obstante, para poder ser empleado como tal, debe tener características únicas que lo hacen infalsificable y diferente para cada individuo, además de poder ser fácilmente almacenados y tratados para propósitos de accesos e identificación.

2.4.1. Características de la huella

La huella dactilar es un patrón de crestas y surcos localizados en la punta de cada dedo. Han sido utilizadas para identificación dactilar, por muchos siglos y la comparación ha sido de muy alta precisión [8].

Los patrones han sido extraídos creando una impresión en tinta de huella dactilar sobre un papel. Hoy en día existen sensores compactos que proveen de imágenes digitales de estos patrones. El reconocimiento de huella dactilar para identificación adquiere la imagen inicial en vivo, a través de la exploración del dedo de la mano por el contacto directo con un dispositivo lector que puede verificar también atributos como la temperatura y el pulso. Desde que el dedo realmente toca el dispositivo de escaneo, la superficie puede hacerse grasa y turbia después de un uso repetido, lo cual puede reducir la sensibilidad y fiabilidad de un escáner óptico. Los sensores de estado sólido pueden superar esta y otras dificultades técnicas debido a que el chip de silicio recubierto es el sensor. Los dispositivos de estado sólido usan capacitancias eléctricas para detectar las crestas de una huella dactilar y crear una imagen digital compacta. Hoy en día, un escáner de huellas dactilares cuesta alrededor de 20 USD y se han convertido en accesibles para un gran número de aplicaciones. En sistemas de verificación en tiempo real, la imagen adquirida por sensores es usada por el módulo de extracción de características para calcular los valores característicos. Los valores característicos típicamente corresponden a la posición y orientación de algunos puntos críticos conocidos como puntos de minucias [2] (Ver Figura 2.5).

2.4.2. Clasificación de las huellas dactilares

Para fines de un mejor análisis, las huellas dactilares se clasifican en 6 clases principales (Ver Figura 2.6) [27]:

(a) Arco.

(b) Arco tendido.

(c) Lazo a la izquierda.

(d) Lazo a la derecha.

(e) Espiral.

(f) Doble lazo.

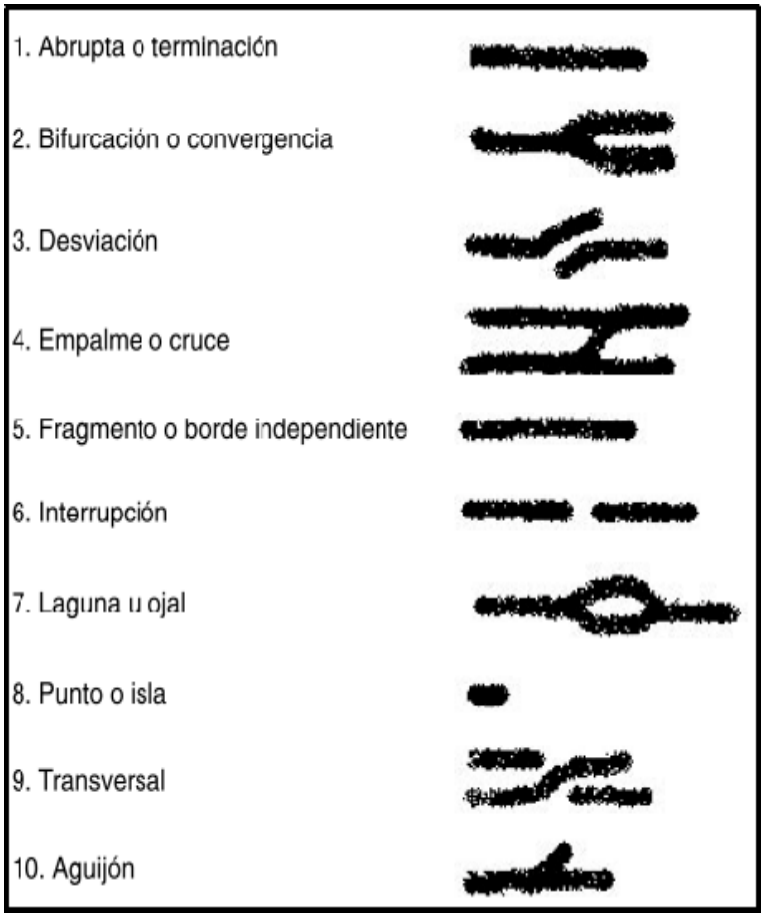

Figura 2.5: Algunas de las minucias principales [5]

2.4.3. Adquisición de datos biométricos y procesamiento de la huella

La adquisición del dato, es la recopilación de la información biométrica, en este caso sería la huella dactilar de la persona. La adquisición de la información es extremadamente importante. Sí no se obtienen imágenes de alta calidad, las siguientes fases no pueden operar con fiabilidad [22]. Para extraer las minucias de la imagen a escala de grises, el procesamiento de la imagen de la huella dactilar es una operación clave en los sistemas actuales de identificación. Principalmente consiste en tres etapas [27], [14], [18]:

1. Un pre-procesamiento: Una vez que se obtuvo la imagen, se mejorara la calidad, mediante el uso de filtros y algoritmos.

2. Binarización de la imagen: la imagen se convierte a binario, es decir, está formada de ceros y unos, donde un “1” significa un píxel blanco y un “0” significa un píxel

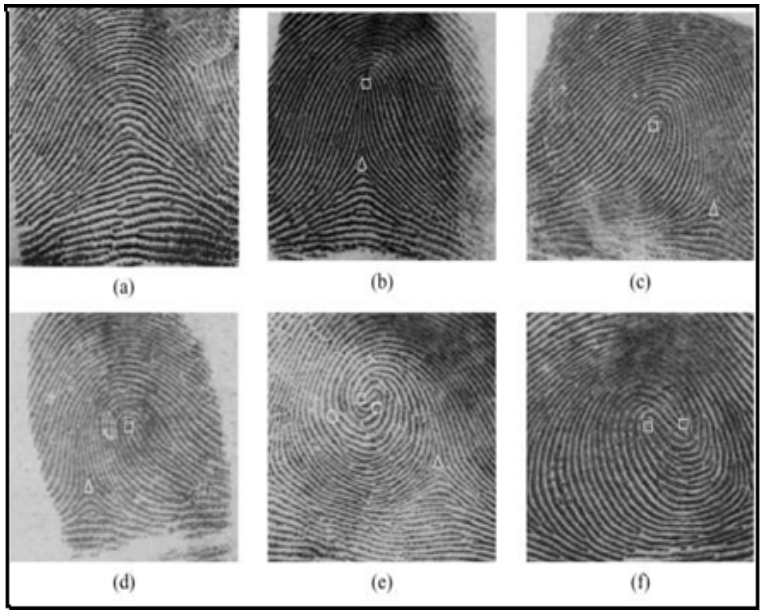

Figura 2.6: Clases de huellas dactilares [27]

negro. Lleva la imagen de escala de grises, (normalmente 256 bits de profundidad) a una imagen en blanco y negro, (2 bits de profundidad).

3. Adelgazamiento de la imagen: Consiste en aplicar algoritmos consecutivos de adelgazamiento de imagen hasta llegar a una forma de esqueleto de huella dactilar.

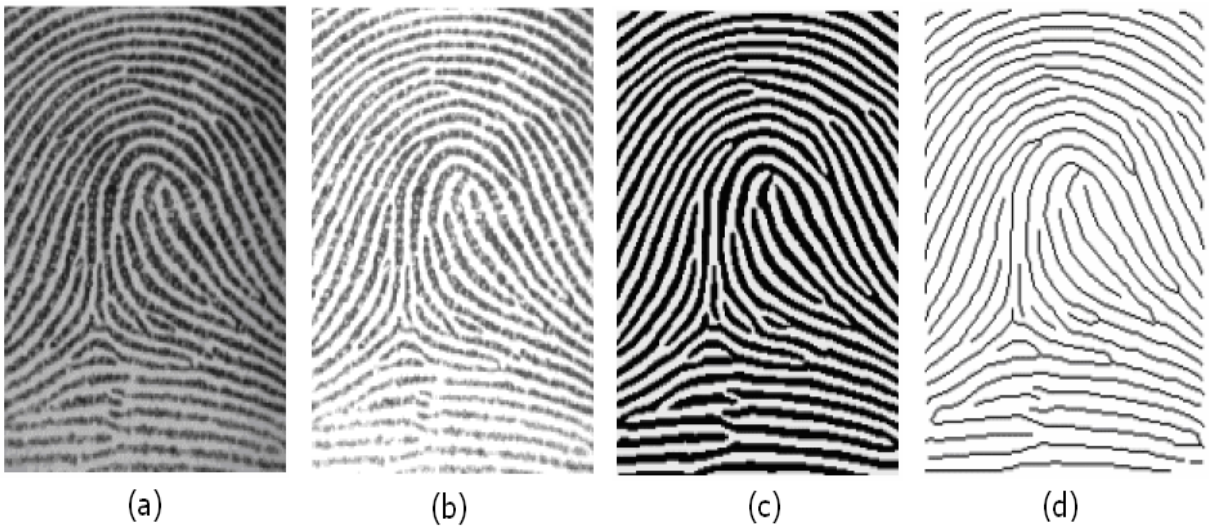

Figura 2.7: Procesamiento de la huella dactilar mostrando la imagen adquirida por el lector (a) , la etapa de pre-procesamiento (b), la etapa de binarización y (c) adelgazamiento, [18]

2.4.4. Determinación de minucias y marcado de decisión

La determinación de minucias también llamada extracción de las características de huella dactilar, extrae información importante de la imagen de huella dactilar obtenida de la fase de adquisición. Esta información es normalmente un patrón de características o marcas que permite que un determinado individuo pueda ser identificado. Para el reconocimiento de huella dactilar estas características son típicamente puntos denominados minucias tales como terminaciones de crestas (ridge endings) que son los puntos de terminación de las crestas de las huellas dactilares y las bifurcaciones de crestas (ridge bifurcations) que son los puntos en donde las crestas se dividen en forma de "Y".

La fase final de un sistema biométrico es el marcado de decisión, en esta fase el patrón de características que fue extraído de la imagen, se compara con un ejemplo conocido previamente. La decisión se hace con respecto a la identidad del individuo. Sí los patrones concuerdan lo suficiente, la identidad del individuo se ha verificado, de lo contrario, la identidad es declarada rechazada [22].

2.4.5. Aplicación de los sistemas biométricos por huella

Algunos de los trabajos sobre reconocimiento de huellas digitales utilizan algoritmos que no se ocupan de la actualización permanente del Banco de Imágenes [19]. A continuación se citan dos ejemplos.

El trabajo "Sistema de reconocimiento de huellas dactilares para el control de acceso a recintos" [15], presenta el desarrollo de un AFAS (Automatic Fingerprint Authentification System), basado en la detección de bifurcaciones y terminaciones dentro de la huella para la verificación de personas. El sistema utiliza los detalles formados en las huellas dactilares. Estos detalles llamados "ridges"son definidos como un segmento de curva simple. La combinación de varios ridges forman un patrón de huella dactilar. Las pequeñas características formadas por el cruce y terminación de ridges son llamadas minucias.

El "Sistema de identificación mediante huella digital" [16], es un mecanismo biométrico que consta de tres partes: un mecanismo de captura, uno de procesamiento y un medio de almacenamiento. La aplicación cliente-servidor detecta huellas digitales usando un sensor térmico

asociado. La información se almacena en un servidor de base de datos y se accede a ella mediante una aplicación desarrollada bajo el entorno Windows, con el software de programación visual Borland Delphi. El proyecto se centra en la reconstrucción de la imagen censada con el lector térmico. La reconstrucción de la imagen de la huella digital requiere: *i)* detectar cuando el dedo toca al sensor: esta es la señal para comenzar el proceso, *ii)* adquirir los pedazos de la imagen de huella, *iii)* detectar cuando el dedo ya no está más sobre el sensor para detener la adquisición, *iv)*calcular la deslocalización relativa de las piezas de imágenes obtenidas y *v)* reconstruir la imagen completa juntando las piezas extraídas.

2.4.6. Herramientas para desarrollo de sistemas para gestión de huellas

Marca	Nitgen	Nitgen	Nitgen	DigitalPersona	DigitalPersona
Modelo	Mouse	Hamster	Hamster II	U.are.U 4000B	U.are.U 4500
Imagen					
Descripción	Mouse óptico con lector de huella dactilar incorporado.	Lector de huella dactilar de sobremesa conexión PC.	Lector de huella dactilar de sobremesa conexión PC.	Lector de huella dactilar de sobremesa conexión PC.	Lector de huella dactilar de sobremesa conexión PC.
Interfaces	USB	USB	USB 2.0	USB 2.0	USB 2.0
Software	Software de seguridad SecuEnterprise: Logon de Windows, Gestor centralizado de usuarios, Protector de pantalla, Encriptación de ficheros y directorios, Listado de eventos. Herramienta de desarrollo de software (SDK) disponible (vendido por separado).	Software de seguridad SecuEnterprise: Logon de Windows, Gestor centralizado de usuarios, Protector de pantalla, Encriptación de ficheros y directorios, Listado de eventos. Herramienta de desarrollo de software (SDK) disponible (vendido por separado).	Software de seguridad SecuEnterprise: Logon de Windows, Gestor centralizado de usuarios, Protector de pantalla, Encriptación de ficheros y directorios, Listado de eventos. Herramienta de desarrollo de software (SDK) disponible (vendido por separado).	Herramienta de desarrollo de software (SDK) vendidos por separado o descargas gratuitas (se recomienda comprarlos para evitar limitaciones).	Herramienta de desarrollo de software (SDK) vendidos por separado o descargas gratuitas (se recomienda comprarlos para evitar limitaciones).

2.5. Gestión de identidades

El incremento, tanto en número como en tipología, de los servicios y contenidos ofrecidos actualmente en Internet ha convertido a la identificación y a la autenticación de los usuarios en un aspecto clave para los profesionales del sector.

En este contexto, la identificación de acceso a la red ofrecida por los operadores de telecomunicaciones se limita solamente al uso de su infraestructura, por lo que los proveedores de servicios deben instalar mecanismos de identificación adicionales (principalmente usuario y contraseña) para permitir el acceso a sus servicios y contenidos. Por esta razón, cada vez que el usuario interacciona con un nuevo servicio en la red debe crear una nueva identidad exclusiva para ese servicio, lo que acaba generando una proliferación sín fín de identidades de usuario fragmentadas, e incluso repetidas, distribuidas entre los sistemas de diferentes proveedores.

Pero más allá de la propia ineficiencia de este sistema, esta situación está frustrando al usuario final que se ve obligado a gestionar un gran número de combinaciones de usuario y clave, que no tiene control sobre el uso que se hace de toda su información que se encuentra diseminada por Internet, y que, frecuentemente, no dispone de información suficiente sobre las políticas de seguridad con las que se almacenan sus datos personales. Para sobrellevar esta situación el usuario intenta reutilizar los mismos identificadores y claves o utilizar claves fáciles de recordar en el máximo número de proveedores de servicios, lo cual acaba impactando en la seguridad de sus datos. Todo esto le lleva a desconfiar del sistema y a ser reacio a proveer información más sensible, como sus medios de pago, necesaria a la hora de realizar transacciones comerciales en Internet [23].

2.5.1. Protección de identidades en Internet

Con respecto al uso de Internet, este ha crecido significativamente y la cuestión de la privacidad en línea se ha convertido en una gran preocupación para los usuarios. Estudios recientes [4] revelan que el uso de los Servicios de Internet y el Comercio Electrónico se ha reducido; además, muchos usuarios optan por proporcionar datos falsos cuando estos les son requeridos con el fin de proteger sus verdaderas identidades. Un estudio realizado en el año

2000 por el centro de investigación estadounidense Pew Internet & American Life Project, encontró que el 54 % de los usuarios de Internet creen que el sitio Web de seguimiento de usuarios es perjudicial e invasivo a la privacidad de estos; 24 % de los usuarios afirmó dar información falsa a un sitio Web y 20 % dió un correo electrónico alternativo o secundario a sitios web [12]. Además de esto, cada sitio maneja su propio modelo de autenticación, por lo cual existe la necesidad por parte del usuario de tener que autenticarse cada que este quiera gozar del servicio, razón por la cual la navegación entre sitio y sitio se hace pausada, además de tener que recordar tantas identificadores de acceso (como usuario y contraseña).

Con la finalidad de proteger verdaderas identidades y agilizar la navegación en internet cuando los usuarios acceden a servicios, surgen diversos proyectos que aportan conceptos para poder evitar este tipo de problemas.

2.5.2. Enfoques para la gestión de identidades

Existen dos enfoques básicos para la gestión de identidades en servicios de red [13]. El primero es el enfoque centralizado, donde una única entidad gestiona atributos y elementos de identificación de todos los usuarios de servicios de red y ofrece servicios de autenticación en nombre de los proveedores de servicio. Como ejemplo de este enfoque podemos citar la iniciativa .NET Passport de la empresa Microsoft. El enfoque alternativo es el descentralizado o federado, en el que los proveedores de servicios finales o de autenticación federan sus sistemas de gestión de identidades para permitir que los usuarios naveguen entre servicios sin re-autenticarse, aunque sin poner en riesgo la privacidad de los datos de usuario o la seguridad en el acceso a los servicios.

En Septiembre de 2001 se creó la Alianza Liberty con el propósito de elaborar un conjunto de estándares para Gestión de Identidades Federadas. Se trata de un consorcio de empresas, proveedores e instituciones interesadas en proporcionar estándares y directrices para gestión de identidades federadas con garantía de privacidad y seguridad para la información de Identidad de Red de los usuarios. La idea básica del proyecto es proporcionar un mecanismo abierto y estándar de Registro Único (Single Sign-On) que incluye autenticación descen-

tralizada y autorización desde múltiples proveedores. Este mecanismo de Registro Único permite a un usuario registrarse en un proveedor de servicios de gestión de identidades y que el registro se transfiera de forma transparente cuando navega hacia otros proveedores de servicio sin necesidad de autenticarse de nuevo. La infraestructura de gestión de identidades propuesta debe soportar todos los dispositivos de acceso desde los más convencionales a los más novedosos [13].

2.6. Federación de Identidades

La identidad federada, es hoy en día un movimiento dominante en el área de gestión de identidades. La federación de identidades se refiere a un modelo de gestión de identidades distribuido, en el que un sitio de internet, interesado en ofrecer facilidad de uso para los usuarios, eficiencia y economía, decide aceptar la información sobre la identidad y las operaciones de autenticación de otros sitios de internet. La federación se refiere al establecimiento de acuerdos comerciales, confianza criptográfica e identificadores de usuarios o atributos a través de políticas de seguridad de dominios, para permitir interacciones más fluidas entre dominios empresariales.

La arquitectura típica de una aplicación federada, es el Single Sign On (SSO), en la cual, un usuario después de acceder a un sitio de internet, es capaz de acceder a sus recursos en otros sitios basándose en la autenticación inicial.

Además de la mejora de la experiencia en línea de SSO, la gestión de identidades federadas puede ofrecer reducción en los gastos administrativos para los prestadores de servicios y un mejor modelo de negocios para los proveedores de servicios [17].

2.6.1. Proyecto Liberty Alliance

La mayor parte de las tecnologías de gestión de identidad que las organizaciones han implantado internamente se basan en modelos centralizados poco o nada apropiados en contextos multi-dominio. Por esta razón, Liberty Alliance define un nuevo modelo de gestión de identidad federada basado en arquitecturas abiertas y estándares, en contraposición a las

soluciones propietarias existentes en el mercado, que no permiten la interoperabilidad entre sistemas diferentes.

Los conceptos surgidos de la identidad de red federada basados en las especificaciones del Proyecto Liberty Alliance se proponen como una solución a todas las anteriores problemáticas y como nuevos habilitadores de negocio en este entorno [23].

Los dos conceptos claves de los sistemas de identidad federada son el Single Sign-On que hace uso de la identidad enlazada o federada y el intercambio de atributos del usuario.

El primero de ellos es el ya mencionado SSO que aporta al sistema la capacidad de que el usuario puede acceder a través de su propio proveedor de identidad y luego reutilizar la autenticación para acceder de forma sencilla a servicios en dominios externos. Es decir, el usuario se autentica una sola vez y puede retener el control sobre su información personal y preferencias, y saber como están siendo usadas por los proveedores de servicios a los que va accediendo con posterioridad. El segundo hace referencia a la posibilidad de enlazar juegos de atributos referentes a un mismo usuario, distribuidos en varias cuentas en diferentes proveedores de servicios para representar una única identidad en red.

Esto puede suceder gracias a que existe algo llamado Círculo de Confianza (CoT por sus siglas en inglés Circle of Trust) (Ver Figura 2.8), el cual está formado por un conjunto de proveedores de servicios web (SP, Service Providers) que han firmado un acuerdo de negocio para suministrar una serie de servicios a sus usuarios comunes, basado en una relación de confianza entre ellos, [1]. Además, de un Proveedor de Identidad (IDP, Identity Provider) y proveedores de atributos (AP, Attribute Providers) que disponen de los necesarios acuerdos de servicio, comerciales y de negocio para permitir al usuario realizar transacciones de forma transparente y sencilla entre todos ellos. Es decir, los SPs y los APs confían en la autenticación del usuario realizada por el IDP y no necesitan re-autenticarlo cuando este hace uso de sus servicios. El intercambio de atributos del usuario entre los APs y los SPs, siempre está bajo el control del propio usuario y mejora la facilidad de acceso y de uso de los servicios [23].

Permitir que los Proveedores de Servicios Web (SP) compartan las autenticaciones de los

usuarios es crítico tanto desde el punto de vista de los usuarios que se benefician de un acceso sencillo y rápido a los servicios de varias organizaciones, como desde el punto de vista de las diferentes organizaciones al permitirles desarrollar nuevas oportunidades de negocio adaptando sus servicios a las necesidades reales del usuario. Sin embargo, la compartición de esta información entre organizaciones presenta muchas problemáticas tanto a nivel técnico, como a nivel legal.

La federación de la identidad se convierte así en un nuevo componente clave de los sistemas de gestión de identidad permitiendo que la información personal y de autenticación pueda atravesar las fronteras de las organizaciones manteniendo su privacidad.
Para entender el funcionamiento del proyecto Liberty debemos detallar cómo se agrupan todas sus especificaciones en tres grandes módulos:

1. Liberty Identity Federation Framework (ID-FF): define la federación de la identidad y su gestión mediante funcionalidades como Single Sign-On simplificado, Global Sign-Out, y otras destinadas a la gestión de metadata (certificados y service end points) entre entidades Liberty.

2. Liberty Identity Web Services Framework (ID-WSF): define el marco para crear, descubrir y consumir servicios relacionados con la identidad. Algunas de sus funcionalidades básicas son: Compartición de atributos bajo permiso, descubrimiento de servicios de basados en la identidad, entorno de invocación SOAP, etc.

3. Liberty Identity Services Interfaces Specification (ID-SIS): es un conjunto de especificaciones que permiten desplegar servicios interoperables sobre ID-WSF. Estos servicios incluyen contactos, calendario, localización, presencia o alertas.

   En todos estos módulos las especificaciones se construyen adoptando y extendiendo los apropiados estándares existentes como SAML, SOAP, WS-Security, XML, entre otros, [23].

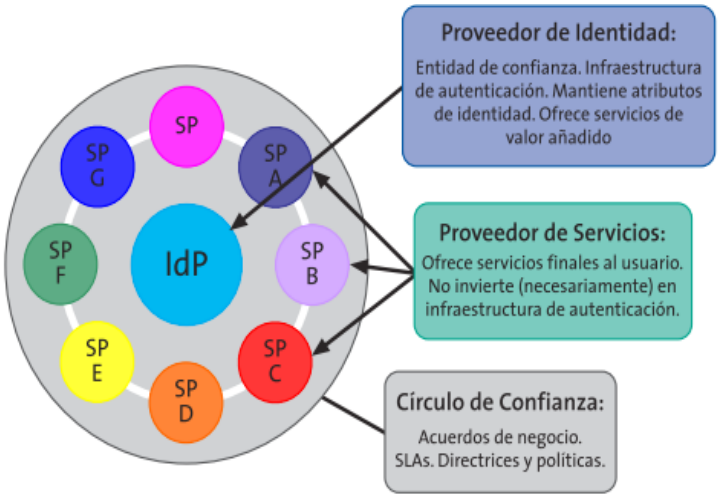

Figura 2.8: Diagrama de bloques del Círculo de Confianza [13]

2.7. OpenSSO

OpenSSO como su nombre lo indica **Open Single Sign-On** es un sistema empleado para un solo acceso a diversos sitios de Internet que requieren autenticación previa. Es de código fuente abierto y gratuito basado en el código de Sun Access Manager, originalmente creado por Sun Microsystems que posteriormente paso a ser parte Oracle y actualmente adquirido por la compañía **ForgeRock** en su nueva versión llamada **OpenAM**.

OpenSSO cuenta con un extensa documentación y guías para el desarrollo, instalación y soporte en páginas oficiales, además permite la administración del acceso de usuarios a sitios en Internet, la administración de la federación y la seguridad de servicios web, que se encuentran en versiones anteriores de **Sun Java System Access Manager** y **Sun Java System Federation Manager**. Tiene características que lo hacen seguro y fácil de integrar a otros sistemas, mismas que se mencionan a continuación:

1. Uso de SOAP para el intercambio de información, lo cual da seguridad en la transferencia de datos.
2. Uso SAML para el intercambio de información durante procesos de autenticación.
3. Uso del lenguaje Java como lenguaje base.

4. Uso de Web Services que permiten integrar los módulos de autenticación fácilmente.

5. Compatibilidad con contenedores web tales como GlassFish, Tomcat, Oracle Application Server, entre otros.

6. Es compatible con Sun Java System Directory Server y Open DS para el registro de información.

7. Compatible con diversas plataformas Widows y distribuciones de Linux.

8. Código fácil de desplegar dentro del contenedor web.

OpenSSO brinda diversos métodos de integración de servicios de Internet, de entre los cuáles se describen a continuación tres de ellos:

- **Integración mediante Fedlet**: Es una implementación de proveedores de servicios (SP) de peso ligero de protocolos SSO de **SAMLv2**. Permite que un proveedor de identidad (IDP) habilite un **SP** que no tenga implementada la federación. El **SP** sencillamente agrega el Fedlet a una aplicación web Java, el cual establece inicio de sesión único (SSO) entre una instancia de proveedor de identidad y la aplicación del proveedor de servicios sin necesidad de una completa configuración de un servidor con proveedor de identidades federadas con todas las funciones en el lado proveedor de servicios.

- **Integración mediante Policy Agent**: Es un Plug-in que puede ser instalado en el contenedor web. Las vesiones de OpenSSO ofrecen Policy Agents para la mayoría de los contenedores web. Con este tipo de integración no es necesario el uso de programación para la gestión de sesión y el control del acceso. El Policy Agent permite delegar al OpenSSO las funciones de autenticación y autorización del contenedor web.

- **Implantación e integración de servidores OpenSSO**: Es el método más completo para integración de servicios web, el cual se basa en la implantación y configuración de diversos servidores OpenSSO, que se comportan como proveedores (**SP**) de servicios o proveedores de identidad (**IP**). Cada SP se encarga de dar servicios al usuario delegando la responsabilidad de autenticación y gestión de identidades al **IP**.

2.8. Comparativa entre OpenSSO y OpenID

OpenSSO y OpenID son dos de los proveedores de identidad más empleados actualmente, aunque ambos presentan diferencias notables, se centran en llevar el control de acceso de los usuarios a diversos sitios Web, con la finalidad de dar facilidad y seguridad en cada acceso. El primero maneja el concepto de inicio de sesión única SSO, que trata de un servicio centralizado que coordina e integra la gestión de accesos (logins) y cuentas de usuarios en todos los sitios Web registrados para este, permitiendo al usuario acceder a distintos sitios de Internet autenticándose una sola vez. De esta manera se le permite navegar de sitio en sitio sin interrupción [25].

Por otro lado OpenID maneja el concepto de una Identidad Web única y funciona como un proveedor de identidades distribuido, gracias a que cuenta con múltiples servidores de confianza, en los cuales el usuario puede darse de alta para obtener las credenciales únicas como usuario y contraseña que permitan acceder a varios sitios. Es decir, el usuario se registra en cualquiera de estos servidores, tal es el caso de myOpenid, para posteriormente tener acceso con un solo usuario y contraseña a diversos servicios que soporten éste proveedor de identidades.

Se puede encontrar en [25] la tabla 2.2 que muestra una comparativa con notables diferencias entre ambos porveedores de identidad.

Criterio	OpenSSO	OpenID
Finalidad	SSO: Un solo login (más de una credencial)	ID: una sola credencial (más de un login)
Ámbito	Círculo de Confianza (Circle of Trust)	Aplicaciones web que soporten openID
Principal beneficiario	Empresas: federación	usuarios: simplicidad
Seguridad	Sistemas centralizado y robusto	Delegado en otro sistema
Protocolos soportados	IDFF 1.x, SAML 1.x y SAML 2.0	Diffie-Hellman

Tabla 2.2: Comparativa entre OpenSSO y OpenID

2.9. Proveedor de identidades por huella dactilar

El problema de robo de identidad, el cual es la acción de suplantar a otras identidades mediante la presentación de identidades robadas o pruebas de identidad ha venido recibiendo una creciente atención a causa de una búsqueda de un mejor método de protección de datos e identificación de individuos.

El uso reciente de sistemas federados de manejo de identidades digitales, sí por un lado han mejorado la gestión de la información y la identidad del usuario, por el otro lado no ofrecen soluciones específicas para resolver el robo de identidad. Un enfoque a tal problema es la adopción de sistemas biométricos de autentificación e identificación [3]. La integración entre un sistema biométrico y un proveedor de identidades es la parte central de esta investigación, su desarrollo será descrito en los siguientes capítulos.

Capítulo 3

Requerimientos y Metodología

Se describen los requerimientos y metodología a seguir, para cumplir el objetivo general del proyecto.

3.1. Requerimientos

Como se vió en los capítulos anteriores, el problema se centra en un sistema proveedor de identidades (empleando OpenSSO), cuya función es la gestión de las identidades de los usuarios, con la integración de un módulo biométrico (por huella dactilar) que valide el acceso de los mismos a los servicios. La figura 3.1 muestra el modelo que integra estos dos elementos, en donde intervienen los siguientes elementos para su elaboración:

1. **Proveedor de identidades**: Implantar y configurar el proveedor de identidades con el software libre OpenSSO.
2. **Módulo biométrico con las siguientes características**:
   - Implementado en lenguaje java para lograr integrarlo fácilmente al OpenSSO.
   - Empleo de un servidor de directorio como almacén, para su posterior integración al proveedor de identidades.
   - Desarrollo de una aplicación Web que funcione con los servicios de Internet.
   - Compatible con el sistema operativo Windows (XP/Vista/7).

3. **Integración el módulo biométrico al proveedor de identidades**: Se debe integrar el módulo biométrico al proveedor de identidades, realizando las configuraciones adecuadas para ambos.

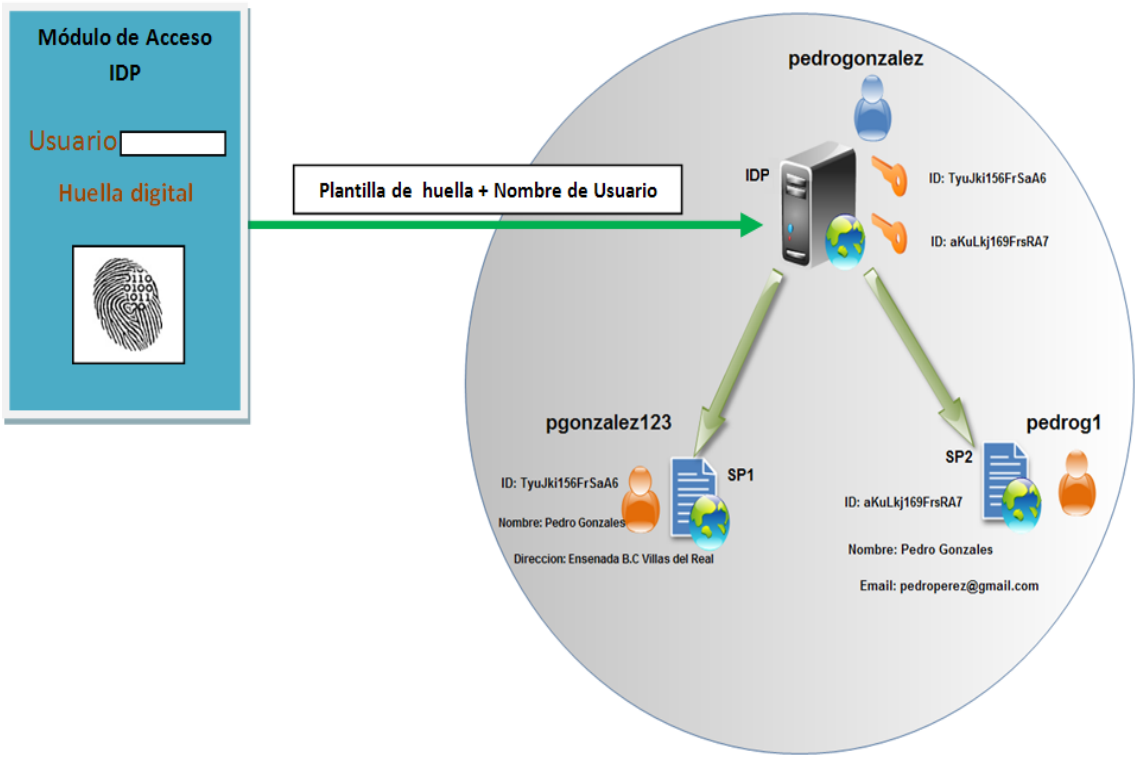

Figura 3.1: Proveedor de identidades con autenticación por huella dactilar

El proveedor de identidades con autenticación por huella dactilar como se muestra en la figura 3.1, está conformado por dos proveedores de servicios (SP1 y SP2) y un proveedor de identidades (IDP) que actúa como intermediario, facilitando el acceso a ambos SP con un solo acceso (Single-Sign-On) corroborando la identidad del usuario. Esto sucede gracias a que el IDP conoce la identidad del usuario y los servicios a los que este tiene acceso. El módulo de acceso es de reconocimiento biométrico por huella dactilar y está integrado al proveedor de identidades.

3.2. Plan de trabajo

Para cumplir con los requerimientos, se propuso la metodología que se muestra en la tabla 3.1.

Face	**Descripción**
Implantación de un Servidor de directorio	Instalar y configurar un servidor de directorio LDAP, empleando openDS, mismo que servirá como almacén de información para OpenSSO y el módulo biométrico
Implantación del proveedor de identidades	Instalación y configuración de Glassfish, sobre el cual será implantado openSSO
	Instalación del software libre OpenSSO
	Configuración de openSSO para autenticación con LDAP
Diseño e implementación del un módulo de autenticación por huella dactilar	Configuración e instalación de las herramientas necesarias para el desarrollo del módulo biométrico
	Diseñar e implementar el módulo con apoyo de herramientas
Integración del módulo biométrico al proveedor de identidades	Realizar los ajustes y configuraciones necesarias en el proveedor de identidades y módulo biométrico, para exista una integración funcional entre ambos
Pruebas.	Realizar pruebas de acceso a servicios con el módulo biométrico del proveedor de identidades con diversos usuarios

Tabla 3.1: Plan de trabajo

Capítulo 4

Implantación del servidor de directorios

Se describe la etapa de instalación y configuración del servidor de directorios, que será empleado como almacén del proveedor de identidades y el módulo biométrico.

4.1. Servidores de directorios

Los servidores de directorio son empleados como almacenes centralizados de identidades dentro de una organización. Como tal, constituyen una ubicación ideal para almacenar certificados de usuarios en empresas que usan la codificación por certificado. Los directorios facilitan la localización de certificados en servidores de red, incluidos los servidores LDAP (Lightweight Directory Access Protocol, Protocolo ligero de acceso a directorios). Después de localizar un certificado, puede agregarlo a la lista de identidades de confianza para no tener que buscarlo otra vez. Estos directorios permiten realizar búsquedas de información que se traducen en identidades de usuarios de manera rápida.
El servicio de directorio LDAP está basado en el modelo cliente-servidor. Uno o más servidores LDAP contienen los datos que conforman el árbol de directorio LDAP o base de datos troncal, un cliente LDAP se conecta con un servidor LDAP para hacer una consulta. El servidor contesta con la respuesta correspondiente, o bien con una indicación de donde puede el cliente hallar más información.

4.2. Recursos para el Servidor de directorios

Para contener las identidades de los usuarios inscritos en el proveedor de identidades, es necesario configurar e instalar un servidor de directorios soportado por el proveedor de identidades. En el caso de este proyecto se ha empleado OpenDS, por ser gratuito e integrarse fácilmente a las necesidades del proveedor de identidades OpenSSO; de tal manera que para instalar y configurar este recurso son necesarias las siguientes herramientas:

1. JDK 6 Update 20 versión para Windows, se puede descargar de la página:
   - http://www.oracle.com/technetwork/java/javase/downloads/index.html
2. OpenDS 2.0.0, se puede descargar de la página:
   - https://www.opends.org/
3. Computadora con Windows XP.
4. Dominio en red, que permite el acceso a LDAP como un recurso público en internet.

Como se muestra en la figura 4.1 se cuenta con un dominio en red **sp.tuburrita.com** con la dirección IP **149.231.215.169**, lo cual facilita el acceso en red a este recurso.

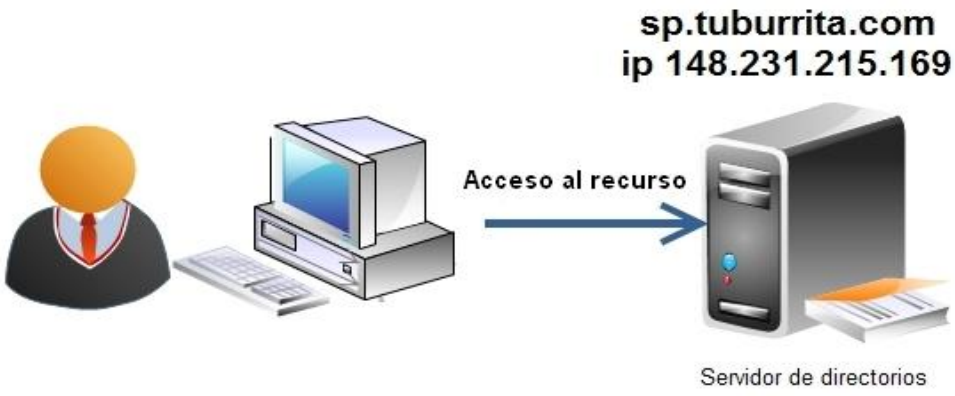

Figura 4.1: Módulo LDAP

Cabe señalar que el recurso LDAP puede ser instalado en sistema operativo Windows o Linux, esto es irrelevante y en nuestro caso se instaló en Windows XP (más adelante se

mencionará el por qué de esto).

El recurso LDAP fue instalado de acuerdo a las especificaciones mencionadas en las páginas oficiales del openSSO (ver anexo). Una vez hecho esto el recurso está listo para ser empleado por el proveedor de identidades y el módulo de autenticación biométrica.

Capítulo 5

Implantación del proveedor de identidades

Se describen las herramientas necesarias para la implantación del proveedor de identidades, así como también la arquitectura y el funcionamiento del mismo.

5.1. Servidor de aplicaciones

El servidor de aplicaciones dentro de este proyecto, es el elemento que realiza la función de contenedor del sistema y por ende, es necesario que este sea compatible con el proveedor de identidades. Para el proyecto se eligió GlassFish, que es un servidor de aplicaciones desarrollado por Sun Microsystems que implementa la tecnología de plataforma Java EE y permite ejecutar aplicaciones que siguen esta especificación. Es gratuito y de código libre, se distribuye bajo las licencias CDDL y GNU GPL.
GlassFish está basado en el código fuente donado por Sun y Oracle Corporation. Tiene como base al servidor Sun Java System Application Server de Sun Microsystems, un derivado de Apache Tomcat. Soporta las últimas versiones de tecnologías como: JSP, JSF, Servlets, Java API para Servicios Web (JAX-WS), Arquitectura Java para Enlaces XML (JAXB) y muchas otras tecnologías. Glasfish será empleado para implantar el openSSO como proveedor de identidades.

Para instalar y configurar el servidor de aplicaciones es necesario revisar las notas de la versión de OpenSSO correspondiente que se encuentran en páginas oficiales.

Antes de implantar el proveedor de identidades fue necesario instalar y configurar las siguientes herramientas y recursos conforme a las notas oficiales de la versión de OpenSSO:

1. JDK 6 Update 20 versión para Linux, que se puede descargar de la página:
   - http://www.oracle.com/technetwork/java/javase/downloads/index.html
2. Glassfish V2 UR2 versión para Linux, que se puede descargar de la página:
   - http://glassfish.java.net/downloads/v2ur2-b04.html
3. Computadora con 1 GB Ram y sistema operativo Linux Ubuntu 8.0.4 instalado con versión de lenguaje en inglés.
4. Dominio en red que permite al acceso a los servicios contenidos en el servidor de aplicaciones como se muestra en la figura 5.1. En este caso **idp.jserna.com** con ip **149.231.215.170.**

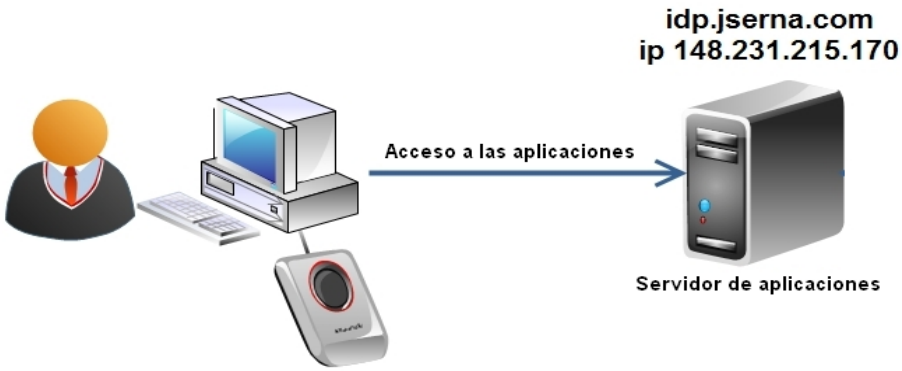

Figura 5.1: Módulo servidor de aplicaciones

5.2. Proveedor del identidades

La base de nuestro proyecto se centra en el proveedor de identidades, el cual es implantado dentro del servidor de aplicaciones Glassfish anteriormente mencionado. Pare este proyecto el proveedor de identidades se implanto utilizando la version OpenSSO Express 8, además de ser configurada de acuerdo a la hoja "notas oficialesz de acuerdo a nuestras necesidades. Dicho proveedor de identidades tiene la siguiente arquitectura:

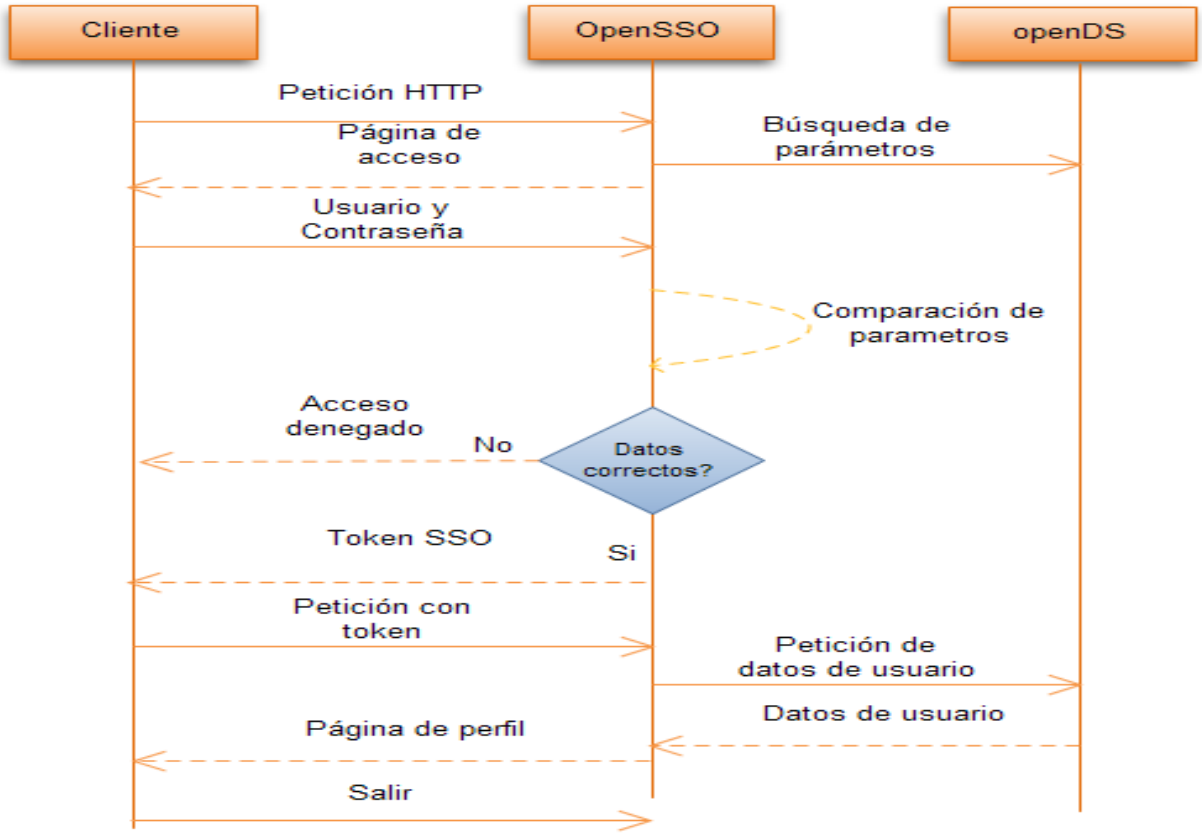

Figura 5.2: Arquitectura de comunicación entre el proveedor de identidades y el servidor de directorios OpenDS

Como se muestra en el diagrama 5.2, el proveedor de identidades hace una petición de usuario y contraseña del lado del clienta, para después comparar estos datos con los almacenados en el OpenDS. Sí los datos no concuerdan, OpenSSO deniega al acceso al usuario, en caso contrario, envía un token de sesión al usuario, con el cual posteriormente los datos del perfil de usuario son mostrados en una página.

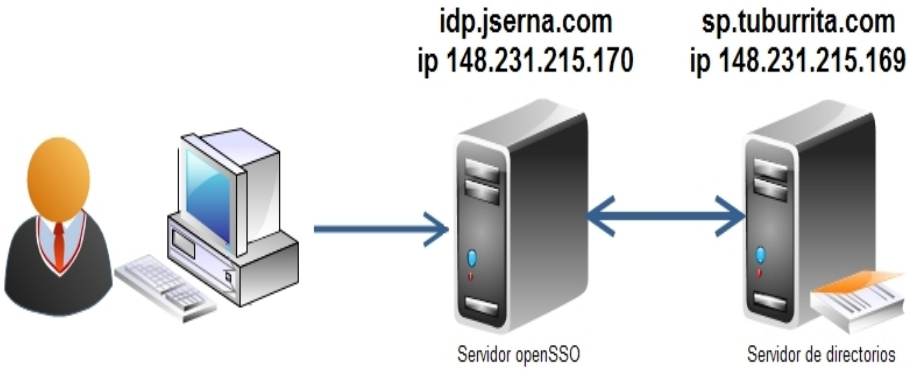

Figura 5.3: Diagrama de bloques del proveedor de identidades y el servidor de directorios

Como se muestra en la figura 5.3, el modulo LDAP y el proveedor de identidades están montados sobre dos servidores distintos, los cuales cuentan con un dominio, para ser fácilmente localizados por cualquier cliente.

Capítulo 6

Módulo de autenticación biométrico

En este capítulo se describen los requerimientos y herramientas necesarias para el desarrollo del módulo biométrico; así como también el funcionamiento y flujo de información dentro del módulo.

6.1. Herramientas y requerimientos

El módulo por huella dactilar, cumple la función de validación de accesos a diversos servicios en Internet. Para implementarlo fue necesario utilizar herramientas que se especializan en este tipo de desarrollo, tomando en cuenta la compatibilidad y correcto funcionamiento con el sistema openSSO y los servicios en Internet.
Se debe considerar que openSSO trabaja y está desarrollado con Java, por lo cual es conveniente el empleo de herramientas de desarrollo que trabajen bajo este lenguaje. Además de ello, debe funcionar para servicios de Internet, lo cual nos indica que debe ser soportado por los navegadores Web.
Es necesario pensar también en el usuario final, quien hará uso de estos servicios y por ende del módulo de acceso biométrico; quien comúnmente emplea el sistema operativo Windows como intermediario entre la computadora y el navegador.
Dicho módulo de autenticación debe trabajar en modo de verificación (ver capítulo 2), para así emplear un nombre de usuario y huella con la intención de restringir o dar acceso dentro de algún servicio.

En base a lo anterior, los requerimientos para el módulo serán:

1. Interfaz física para captura de la huella (lector de huellas).

2. Interfaz Web gráfica en Java, que permita al usuario introducir su huella y nombre de usuario.

3. Web Service en Java, que compare la huella y el nombre de usuario almacenados con las recibidos.

No es posible probar un módulo de autenticación biométrica sin previamente tener almacenadas las plantillas de las huellas, por lo cual fue necesario desarrollar también un módulo auxiliar para inscripción de los usuarios, con las siguientes características:

1. Interfaz física para captura de la huella (lector de huellas).

2. Interfaz Web gráfica en Java, que permite al usuario introducir su huella, nombre de usuario y otros datos extras que sirven como perfil de usuario (nombre, correo, etc.).

3. Web Service en Java, que almacena la huella, el nombre de usuario y los datos extra.

Cabe mencionar que el almacén de datos para ambos casos es un módulo con OpenDS, que consiste en un servidor de directorios compatible tanto para el OpenSSO como para el módulo biométrico.

6.1.1. Lectores de huellas dactilares

La primera fase de todo sistema biométrico, es la adquisición de la característica biométrica y para ello, es necesario el uso de sensores. En el caso particular del proyecto se requiere un lector de huellas dactilares, con el cual se logre capturar la imagen de la huella para después ser procesada.

Los dos tipos de lectores de huella más empleados son los ópticos y por capacitancia. Los **lectores ópticos**, tienen un arreglo de diodos sensible a la luz que genera una señal eléctrica en respuesta a fotones de luz. Cada diodo graba un pixel, un pequeño punto que representa

la luz que le es reflejada.

Colectivamente, la luz y perfiles oscuros forman una imagen de la huella leída. El proceso de lectura comienza cuando se coloca su dedo sobre la ventana del lector, el cual tiene su propia fuente de iluminación, típicamente un arreglo de LEDs, para iluminar las crestas de la huella digital. Con esto se genera una imagen invertida del dedo, con áreas más oscuras que representan más luz reflejada (las crestas del dedo) y áreas más claras que representan menos luz reflejada (los valles entre las crestas) (Ver Figura 6.1) [11].

Figura 6.1: Imagen de la huella dactilar, en donde las áreas oscuras representan las crestas y las áreas blancas los valles [11]

Lectores de Capacitancia, al igual que los anteriores, generan una imagen de las crestas y valles que conforman una huella digital, pero utilizan corriente eléctrica.

La figura 6.2 muestra un ejemplo de sensor capacitivo. El sensor está hecho de uno o más chips que contienen un arreglo de pequeñas celdas. Cada celda incluye dos placas conductoras, cubiertas con una capa aislante [11].

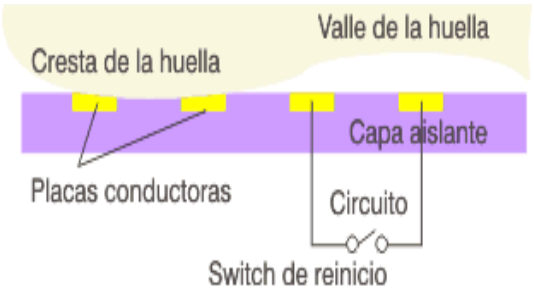

Figura 6.2: Diagrama del sensor de huellas capacitivo [11]

La principal ventaja de un lector capacitivo es que requiere una verdadera forma de huella digital y no sólo un patrón de luz y oscuridad que haga la impresión visual de una huella digital. Esto hace que el sistema sea más difícil de engañar [11]. Sin embargo los métodos ópticos son la técnica de adquisición de huella más común, además de ser económicos [22].

6.1.2. Selección del lector de huellas

En el mercado existe una gran variedad de marcas y modelos de lectores de huellas, los precios varían de acuerdo al tipo y fabricante. De entre los más económicos y conocidos, se probaron tres, los cuales se mencionan en la tabla 6.1.

Lectores	APC Biopod	Microsoft DG2-00004	U.are.U 4000B
Imagen			
Fabricante	APC	Microsoft	Digital Persona
Tipo	Capacitivo	Óptico	Óptico
S.O. Compatibles	Windows 98, ME, 2000 y XP.	Windows XP, Windows vista.	Windows XP, Windows vista.
Software de prueba	Microsoft Passport, Softex Omni Pass.	Digital Persona Password Manager 2.0.	Digital Persona One Touch for Windows.
SDKs Compatibles	Se necesita contactar al distribuidor en la página http://www.apc.com/	Griaule Fingeprint SDK 2009	Digital Persona One Touch for Windows Software Development Kit, Griaule Fingeprint SDK 2009, VeriFinger SDK.
Interfaz	USB	USB	USB

Tabla 6.1: Comparativa entre lectores de huella dactilar

Como se observa en la tabla 6.1, el lector óptico **U.are.U 4000B** de Digital Persona, muestra compatibilidad con los tres SDK mencionados y con la mayoría de los sistemas operativos. Estas son características que facilitan el desarrollo del módulo biométrico, razón por la cual es el lector de huellas que se utilizó.

6.1.3. Software de desarrollo para huellas dactilares

Las herramientas de desarrollo para huellas dactilares, permiten crear programas con cierta lógicas para gestión de huellas. Esto lo logran facilitando funciones para controlar

el lector de huellas, adquisicion de plantillas que contienen la información biométrica de la huella, comparación de plantillas, mostrar la huella, etc. Dichas funciones son básicas para lograr una gestión de huella dentro de la lógica de un programa.
Existen diversas marcas de herramientas de este tipo y cada una se puede manejar en uno o más lenguajes de programación. Esto se logra gracias a que estas se presentan como librerías que fácilmente se pueden agregar a los entornos de desarrollo de los lenguajes de programación.
Es importante recordar que para este proyecto se implantará un módulo biométrico en el sistema OpenSSO de código abierto en lenguaje Java, razón por la cual es conveniente utilizar para el módulo biométrico una herramienta de desarrollo en este lenguaje.

La tabla 6.2 muestra tres herramientas de desarrollo para huellas, en donde se presentan los lenguajes de programación, sensores y precios para las mismas.

Como se observa en la tabla 6.2, la herramienta Fingerprint SDK, maneja la mayoría de los lenguajes de programación. En [7] se pueden encontrar una gran cantidad de ejemplos, manuales y soporte técnico, además, Griaule Biometrics presenta certificaciones del FBI y consiguió el mérito FCV2006.

Herramientas	Fingerprint SDK 2009	VeriFinger SDK	DigitalPersona One Touch
Compañia	Griaule Biometrics	Neurotechnology	DigitalPersona
Lenguajes	C++, C++ .NET 2005, C#, C# .NET 2005 Visual Basic 6, VB .NET 2005, ASP.Net, Java, Delphi 6-7.	C++, C#, Visual Basic .NET, Visual Basic 6, Java, Delphi 7.	ANSI C, C++, C#, Java, VB.NET
Sistemas Operativos	Windows 2000, Windows XP, Windows 2003, Windows Vista, Linux x86	Microsoft Windows 2000/XP/Vista/7 (32/64 bit), Linux 32/64 bit, Mac OS X	Microsoft Windows 2000/XP/Vista/7 (32/64 bit), Linux (32/64 bit), Mac OS X, Windows Server 2003/2008 (32/64-bit), Linux (kernel 2.4 y 2.6)
Software de prueba	Microsoft Passport, Softex Omni Pass.	Digital Persona Password Manager 2.0.	Digital Persona One Touch for Windows.
SDKs Compatibles	Se necesita contactar al distribuidor en la página http://www.apc.com/	Griaule Fingeprint SDK 2009	Digital Persona One Touch for Windows Software Development Kit, Griaule Fingeprint SDK 2009, VeriFinger SDK.
Interfaz	USB	USB	USB

Tabla 6.2: Comparativa entre lectores de huella dactilar

6.2. Diseño del módulo biométrico

El diseño de todo sistema es fundamental, por más pequeño que este sea. Con un buen diseño, aseguramos el correcto funcionamiento y comunicación entre los diversos módulos. Tal es el caso del módulo de autenticación biométrica, el cual a su vez está dividido en submódulos que deben ser fácilmente adaptables a un sistema en donde se requiere de un método de autenticación.

En nuestro caso el módulo biométrico está conformado por un submódulo de captura y un submódulo para la comparación de las huellas e información del usuario (nombre de usuario). Otro diseño empleado es el de un módulo auxiliar de inscripción de huella dactilar, mismo que cumple la función de obtener la plantilla de la huella del usuario, además de otros datos

que puedan servir como perfil del mismo, para ser almacenados en un módulo LDAP.

Una previa captura de la información como se muestra en el diagrama de la figura 6.3 servirá para mantener un registro del usuario, con el que posteriormente se podrá comparar su información (huella, nombre de usuario), además de servir para almacenar el perfil del usuario (nombre, apellido, correo, etc.). Como se observa en el diagrama, la huella y los datos del usuario son capturados del lado del cliente, que envía los datos a través de un Web Service para ser almacenados en un modulo OpenDS (LDAP).

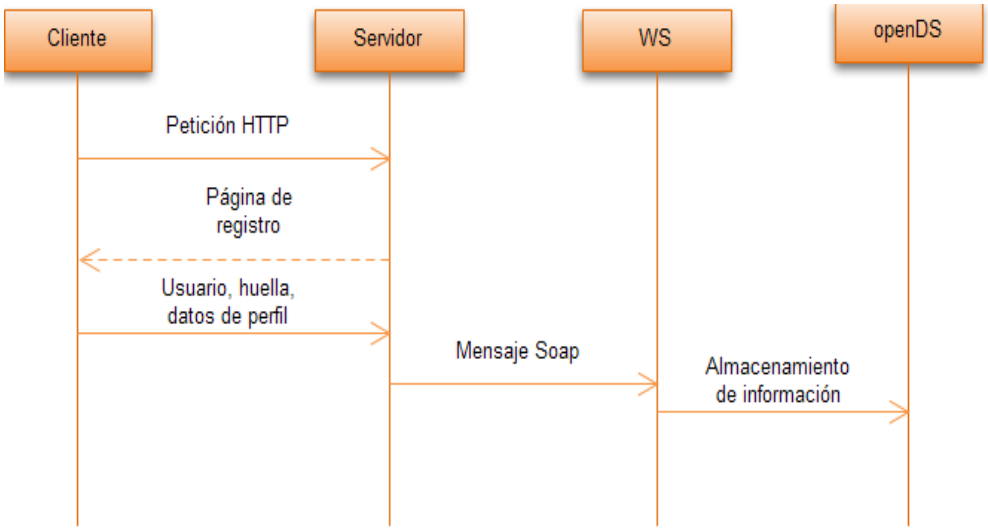

Figura 6.3: Arquitectura del módulo de captura de huella

En la figura 6.4, se observa una arquitectura de comunicación entre los diferentes submódulos para verificación de huella. Primero la huella y el nombre del usuario son capturados del lado del cliente para después ser enviada a un Web Service que procesa la huella y el nombre de usuario los compara con la información almacenada con el módulo OpenDS. Una vez comparada la información, un mensaje de éxito o rechazo es enviado al cliente.

Las arquitecturas mencionadas anteriormente, se implementarón de la siguiente forma:

1. Módulo de registro desarrollado con un Applet, que incluye:

   (a) Cuadro de texto para introducir nombre de usuario.

   (b) Panel que muestra la huella capturada.

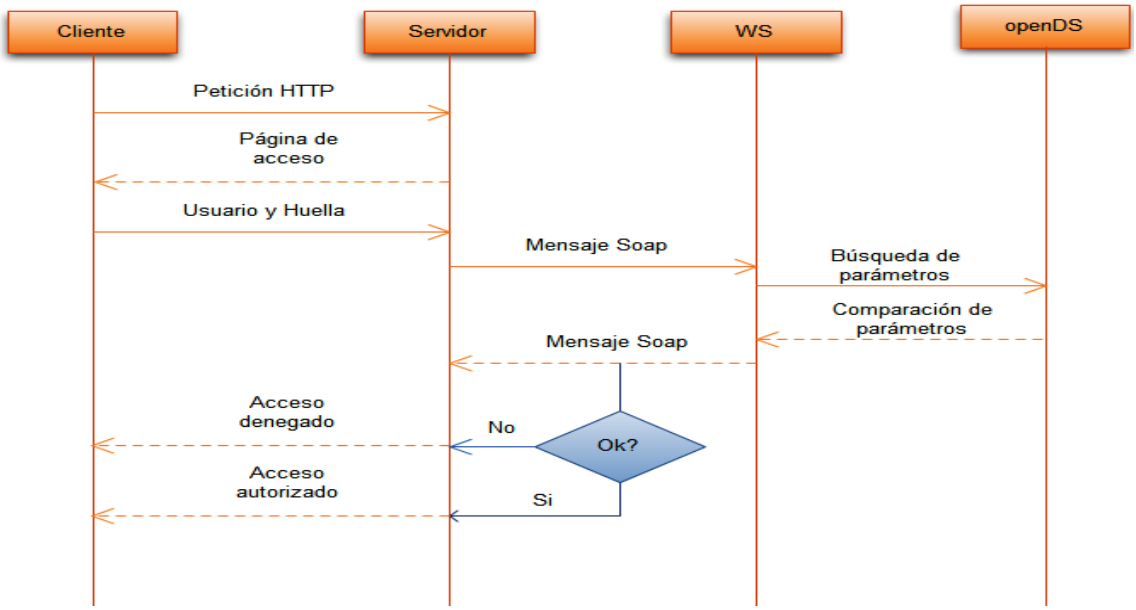

Figura 6.4: Arquitectura de comunicación del módulo de autenticación biométrico

(c) Cuadros de texto para captura del nombre, correo y otros datos personales que sirvan como perfil.

2. Modulo de autenticación desarrollado con Applet que incluye:

(a) Cuadro de texto para introducir nombre de usuario.

(b) Panel que muestre la huella capturada.

Dichos módulos envían los datos a un Web Service ya sea para comparar o almacenar la información según sea el caso y emplean un servidor de directorios OpenDS como almacén de información.

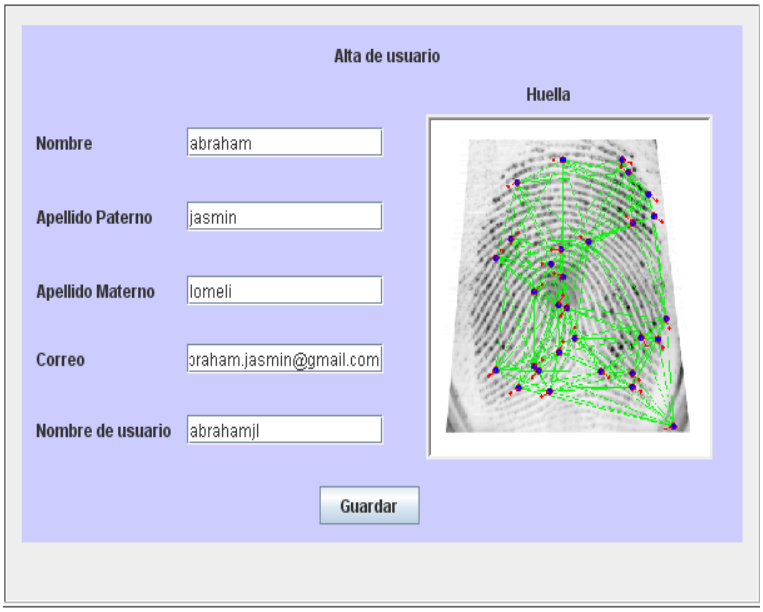

Figura 6.5: Interfaz gráfica del módulo de registro con huella dactilar

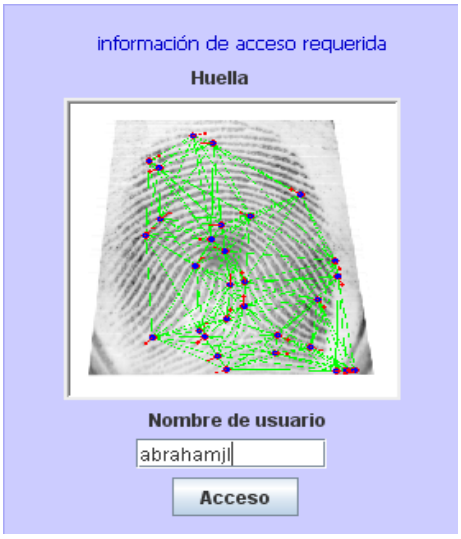

Figura 6.6: Interfaz gráfica del módulo de acceso por huella dactilar

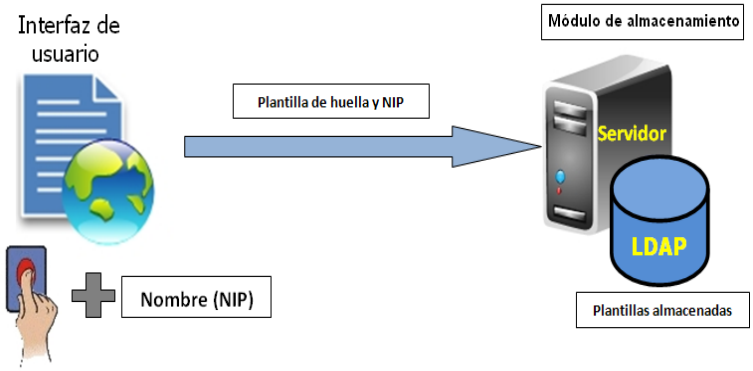

Figura 6.7: Diagrama de bloques del módulo de registro

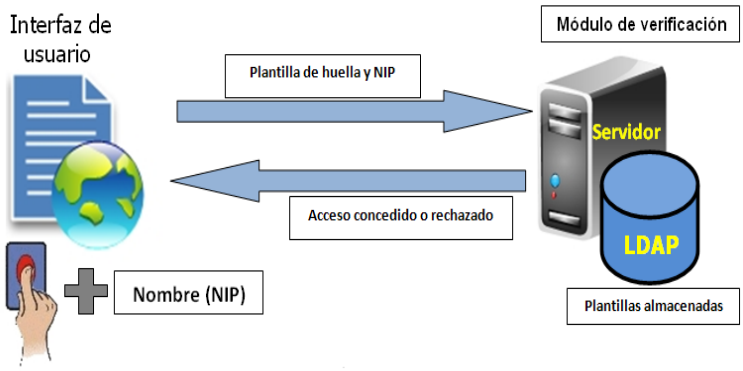

Figura 6.8: Diagrama de bloques del módulo de autenticación

6.3. Desarrollo del módulo biométrico

Para el desarrollo, fué importante instalar y configurar de manera correcta las herramientas para implementación de módulos biométricos, este proceso se llevo a cabo con las siguientes herramientas y recursos:

1. JDK 6 Update 20 versión para Windows previamente instalado.
2. Glassfish V2 UR2 versión para Windows, que se puede descargar de la página:
   - http://glassfish.java.net/downloads/v2ur2-b04.html

   Esta herramienta se usó, para publicar los módulos de huella dactilar como recurso en Internet.
3. NetBeans 6.8 previamente instalado, que se puede descargar de la página:
   - http://netbeans.org/

   Que se empleó para realizar la implementación de cada módulo y Web Service de autenticación y registro de huella.
4. Fingerprint SDK 2009 Java, que se puede descargar de:
   - http://www.griaulebiometrics.com/

   Para las librerías de desarrollo de módulos de huella dactilar.
5. Lector de huellas U.are.U Digital Persona 4000B, como dispositivo de interfaz para las huellas dactilares.
6. Dominio en red sp.tuburrita.com con ip 149.231.215.169.
7. Servidor de directorios previamente instalado con el mismo dominio, como almacén de datos para los módulos.
8. Computadora con sistema operativo Windows XP, para ser empleada como servidor.

Cabe mencionar que el módulo biométrico, se integró dentro del sistema servidor con Windows XP con domino **sp.tuburrita.com**, sitio en el cual se encuentra el servidor de directorios, por convención, para reducir el gasto de servidores en éste proyecto, la arquitectura empleada se muestra en la figura 6.9.

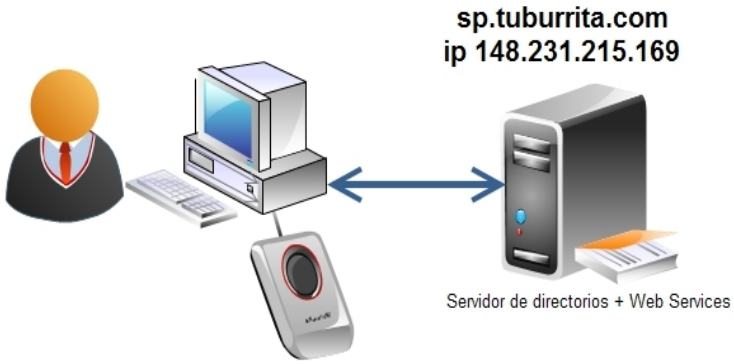

Figura 6.9: Diagrama de bloques del módulo biométrico

Capítulo 7

Proveedor de identidades federadas con autenticación por huella dactilar

En este capítulo se describen el funcionamiento de la integracion del proveedor de identidades federadas y el módulo biométrico.

7.1. Integración del módulo proveedor de identidades al módulo biométrico

La integración del módulo biométrico al proveedor de identidades es la parte fundamental este proyecto. La interacción entre ambos elementos nos brinda una herramienta de acceso y gestión de identidades, ofreciendo a cada usuario la ventaja de poder acceder a cualquier sitio en donde este registrado sin necesidad de recordar alguna clave.

7.1.1. Arquitectura de comunicación

En la figura 7.1 y 7.2 se muestra la comunicación entre el proveedor de identidades y el módulo de huella dactilar, formando una federación de dos servicios a los cuales es posible acceder medienta huella dactilar y nombre de usuario y un único proveedor de identidades federadas centralizado para estos servicios (A y B).

El proveedor de identidades y el módulo de huella se comunican mediante un intercambio de datos mediante el protocolo SOAP, llevando acabo los siguientes pasos en el proceso de autenticación y gestión de identidades:

1. El usuario realiza la petición de acceso al servicio A:

2. El servidor OpenSSO atiende esta petición enviándole al usuario la página de autenticación por huella dactilar.

3. El usuario ingresa su huella, nombre de usuario y la envia para validar el acceso.

4. El proveedor de identidades federadas evalua y envia la información al Servicio Web de verificación de huella dactilar.

5. Sí los datos son correctos, el Web Service devuelve al proveedor de identidades un mensaje de "OK". Sí son erroneos regresa a pedir los datos del usuario.

6. El proveedor de identidades interpreta el mensaje "OK" enviando un Token de sesión al cliente que servirá para el control del usuario.

7. El proveedor de identdades, hace la peticion de los datos del usuario, aceptando así la identidad del usuario como valida para el servicio A.

Sí el usuario nuevamente realiza una petición de acceso a un servicio B, que se encuentra dentro del círculo de confianza del proveedor de identidades, este hace la petición del token de sesión y proporciona al cleinte el acceso sin necesidad de tener que se autenticado nuevamente.

7.1.2. Ventajas

- Requiere de un acceso de usuario único para uno o más servicios de Internet.
- Empleo de huella dactilar como método de identificación biométrico.
- Gestión de identidades empleando el sistema openSSO de Sun Java Microsystems.
- Servidor de directorio openDS, para minimizar tiempos de respuesta en búsquedas de datos.
- Uso de Web Services para intercambio de datos en diversas plataformas.

7.1.3. Desventajas

- Requiere de un dispositivo lector de huellas dactilares.
- Requiere de la instalación de un controlador para dispositivo lector de huellas.
- Requiere de liberias para gestión de huellas dactilares, las cuales pueden variar por el costo de licencia.
- La petición debe ser desde el sistema opetativo Windows.

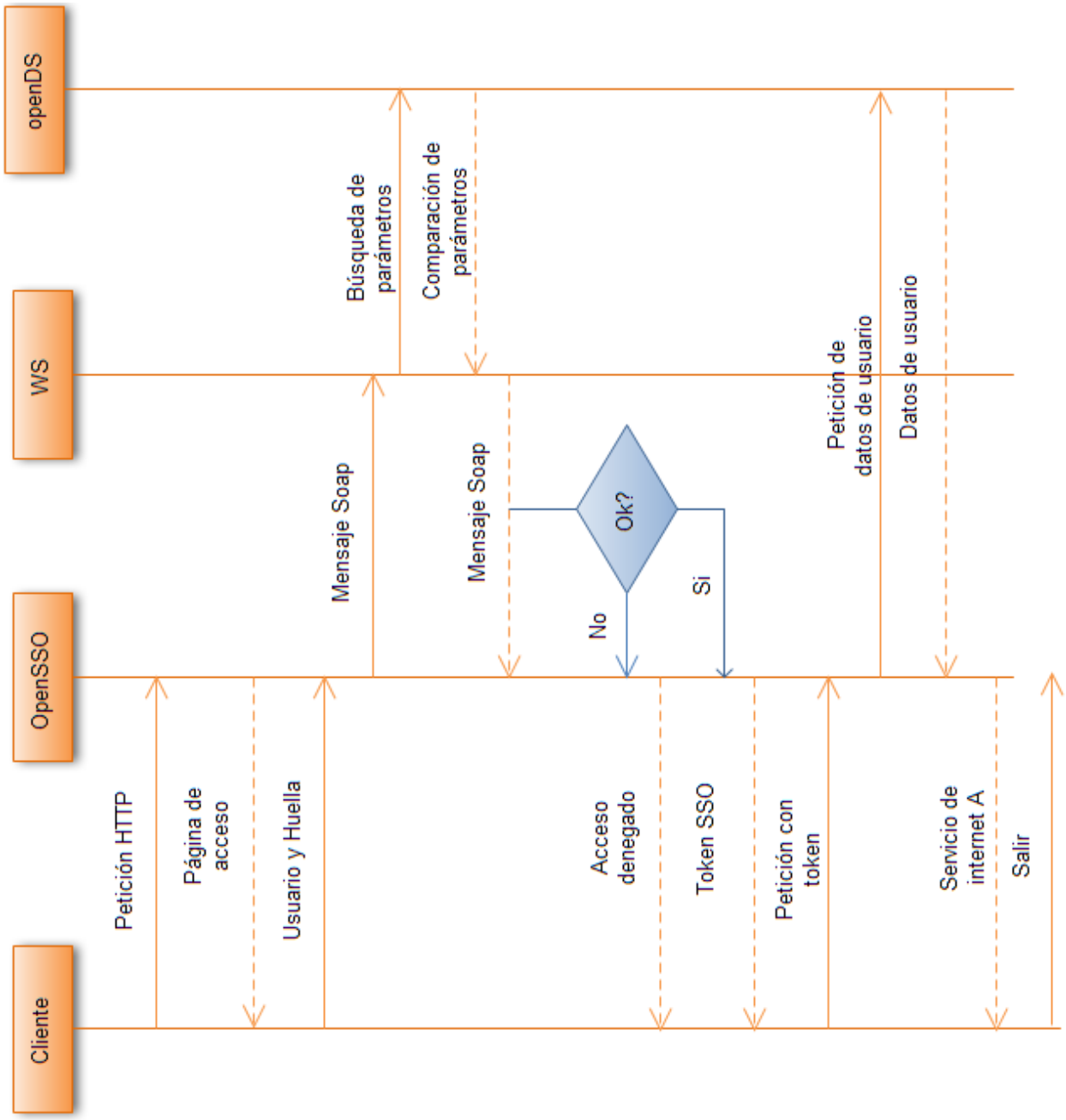

Figura 7.1: Arquitectura de comunicación entre el proveedor de identidades y el módulo biométrico en el acceso aun servicio A

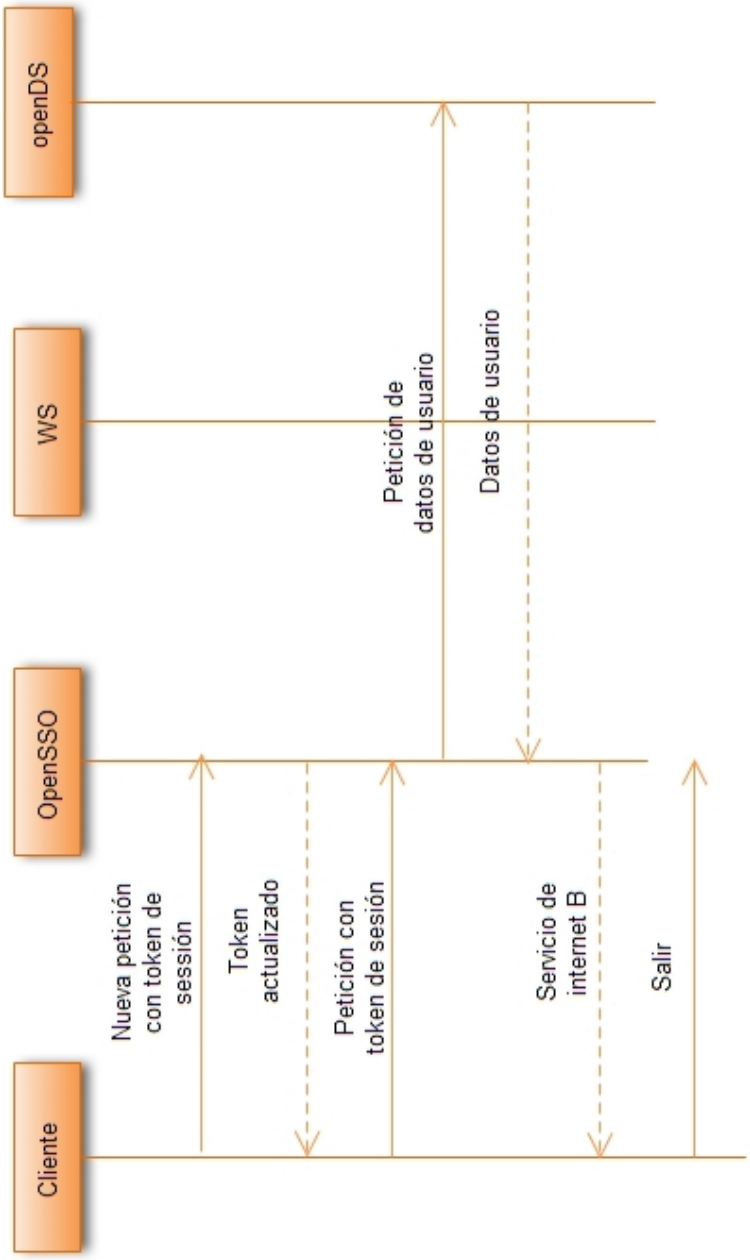

Figura 7.2: Arquitectura de comunicación entre el proveedor de identidades y el módulo biométrico en el acceso aun servicio B

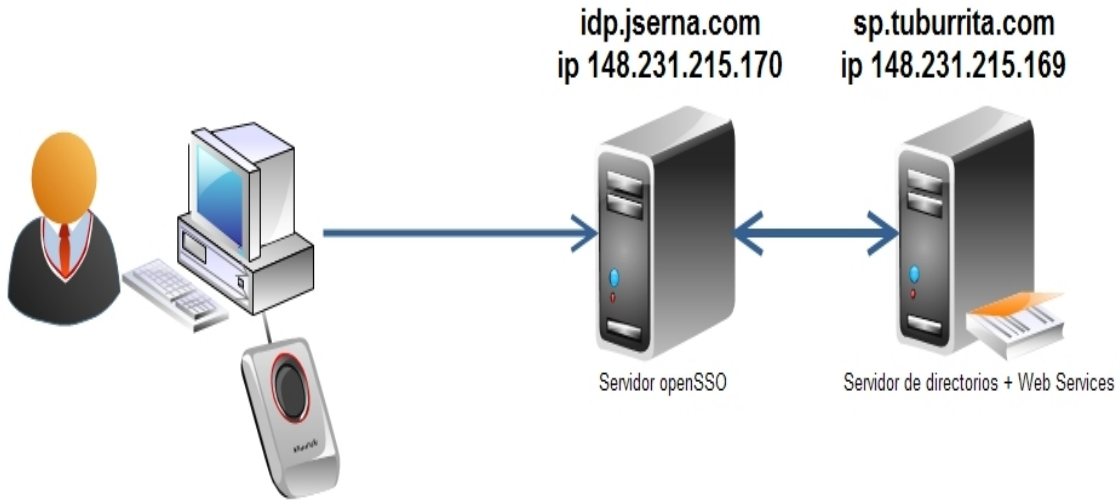

Figura 7.3: Diagrama de bloques del proveedor de identidades con autenticación por huella dactilar

Capítulo 8

Pruebas y Resultados

En este capítulo se describen las pruebas de autenticación de acceso realizadas al proveedor de identidades federadas con autenticación por huella dactilar a dos servicios de Internet que se encuentran dentro de un círculo de confianza.
Dichas pruebas demuestran el funcionamiento del módulo de autenticacón por huella dactilar y los conceptos de proveedor de identidades, círculo de confianza, Single Sign On, federación de identidades, entre otros previemente mencionados en esta investigación, así como el uso de le huella dactilar como metódo de acceso.

Cabe mencionar que para realizar las pruebas, se configuró en la Universidad Politécnica de Cataluña en España, un proveedor de identidades federadas con autentcación por huella con dos servicios de prueba, mismo que sirvió para forjar nuestra investgación en cuestión de federación de identidades con autenticación por huella, para acceder a servicios remotos.

8.1. Registro de huella y perfil en el IDP

Caso de prueba : Registro de usuario por huella dactilar	
Propósito	Demostrar el funcionamiento del módulo registro de usuario por huella dactilar dentro del proveedor de identidades.
Prerequisitos	▪ Plugin de entorno de ejecución de java(JRE, Java Runtime Environment). ▪ Lector de huella dactilar. ▪ Sistema operativo Windows XP.
Datos de prueba	▪ Nombre y apellido. ▪ Nombre de usuario y correo electrónico ▪ Huella dactilar.
Flujo	1. Acceder al sitio: ▪ http:\\idp.sahuaroapps.com:8080\openam\UI\Login 2. Dar click en la liga de acceso al registro 3. Llenar los datos personales correspondientes. 4. Introducir la huella dactilar. 5. Guardar los datos capturados.
Resultado	La huella y el perfil del usuario quedan almacenados para ser reconocidos por el proveedor de identidades.

Tabla 8.1: Caso de prueba: Registro de usuario por huella dactilar

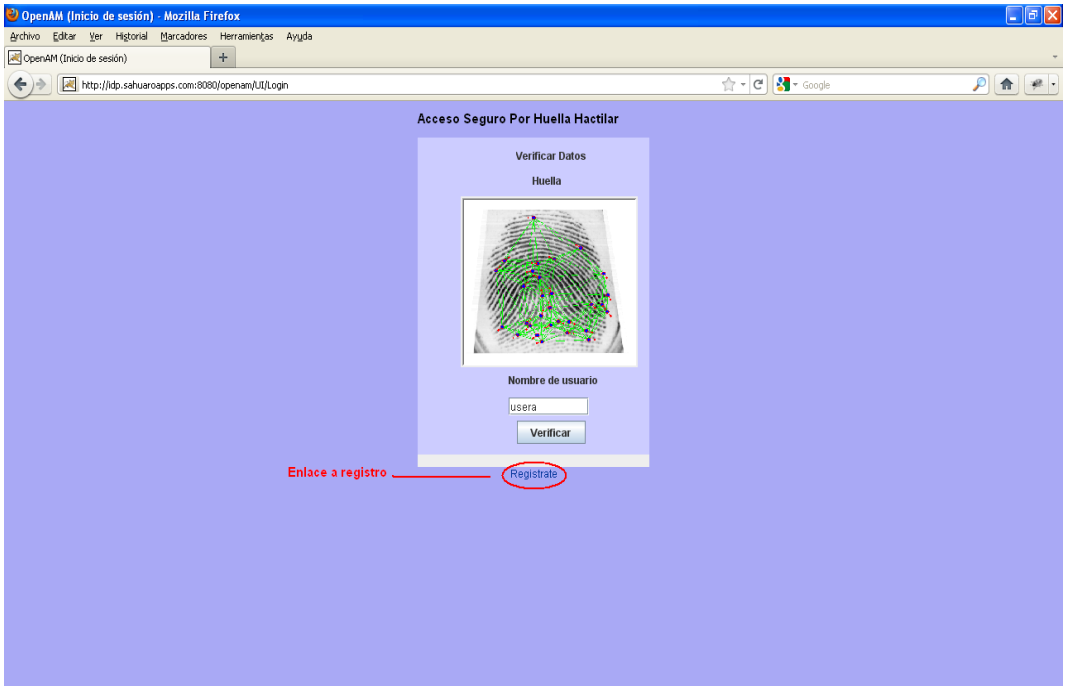

Figura 8.1: Enlace de acceso a registro de proveedor de identidades con huella dactilar

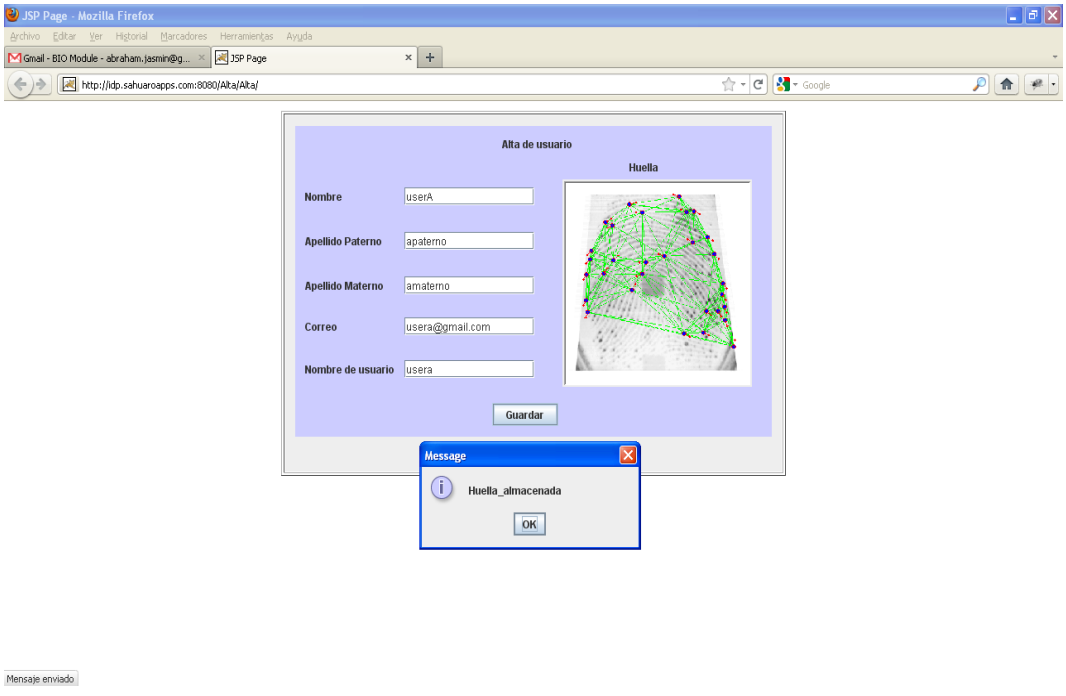

Figura 8.2: Página de ingreso de información de registro al proveedor de identidades por huella dactilar

8.2. Acceso a un servicio de Web

Caso de prueba : Acceso a un servicio dentro del círculo de confianza	
Propósito	Demostrar el funcionamiento de un acceso local a un servicio Web que se encuentra dentro de un círculo de confianza.
Prerequisitos	▪ Sistema operativo indistinto. ▪ Perfil de usuario previamente registrado dentro del Servicio Web (nombre y contraseña).
Datos de prueba	▪ Nombre de usuario y correo electrónico ▪ Contraseña.
Flujo	1. Acceder al sitio Web de reservación de autos: ▪ http://canet.upc/openam/samples /saml2/useCaseDemo/home.jsp 2. Dar click en la liga de acceso local (Local login). 3. Enseguida aparecerá la pantalla de acceso, en la cual se debe introducir usuario y contraseña. 4. Con los datos de acceso correctos, obtenemos acceso a la página principal del servicio, caso contrario, nos deniega el acceso. 5. Una vez aprobada la validación, podemos ser participes del servicio.
Resultado	Obtenemos el acceso local aun servicio Web que se encuentra dentro del círculo de confianza.

Tabla 8.2: Acceso a un servicio Web

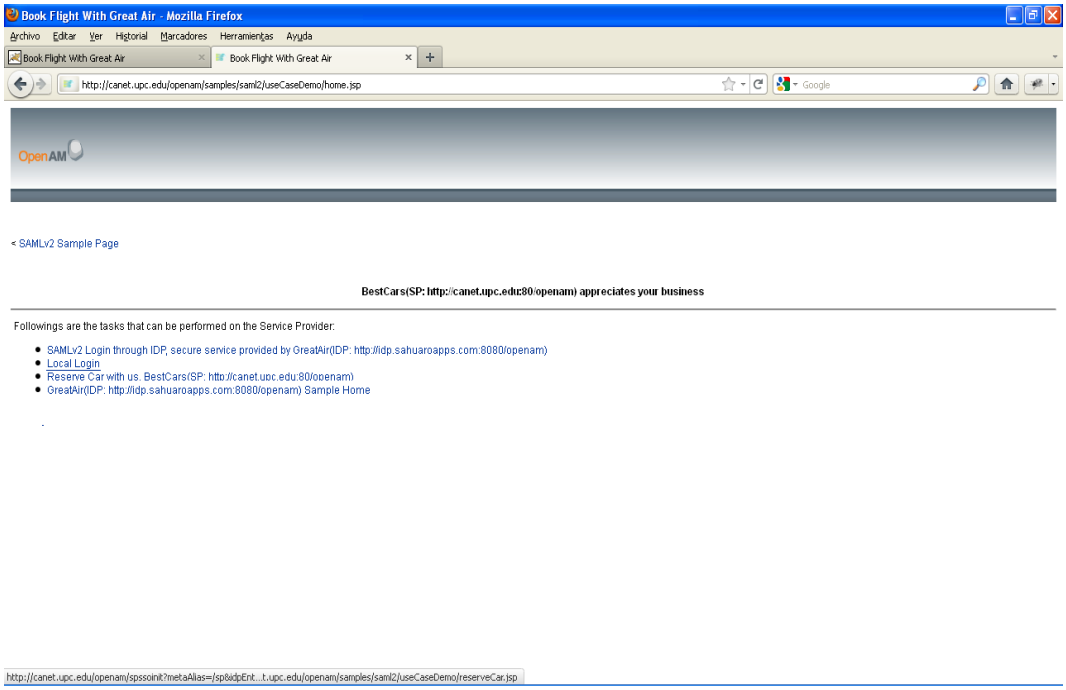

Figura 8.3: Página de acceso al servicio Web de reservación de autos

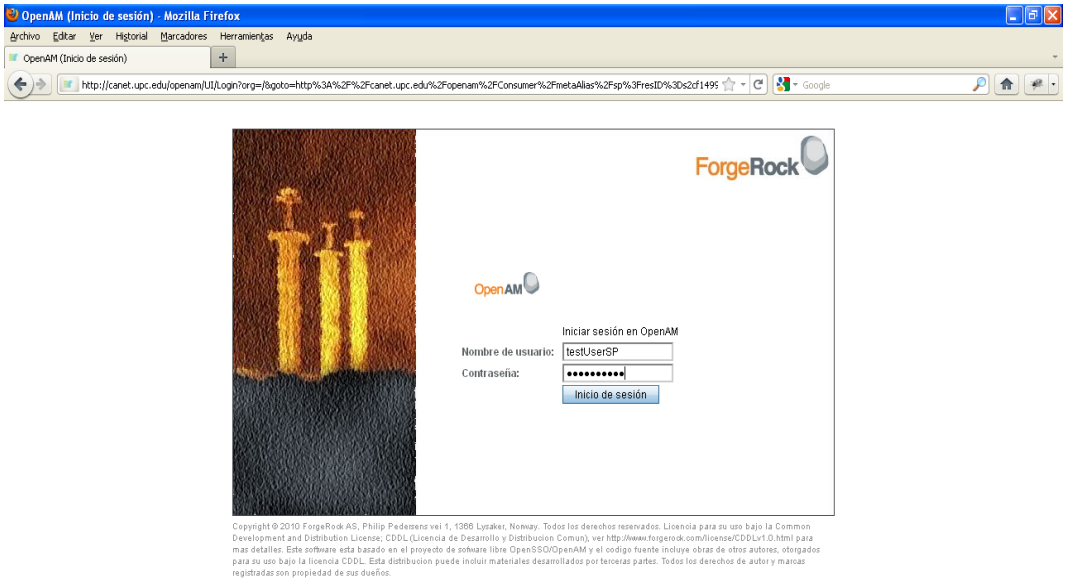

Figura 8.4: Autenticación del usuario

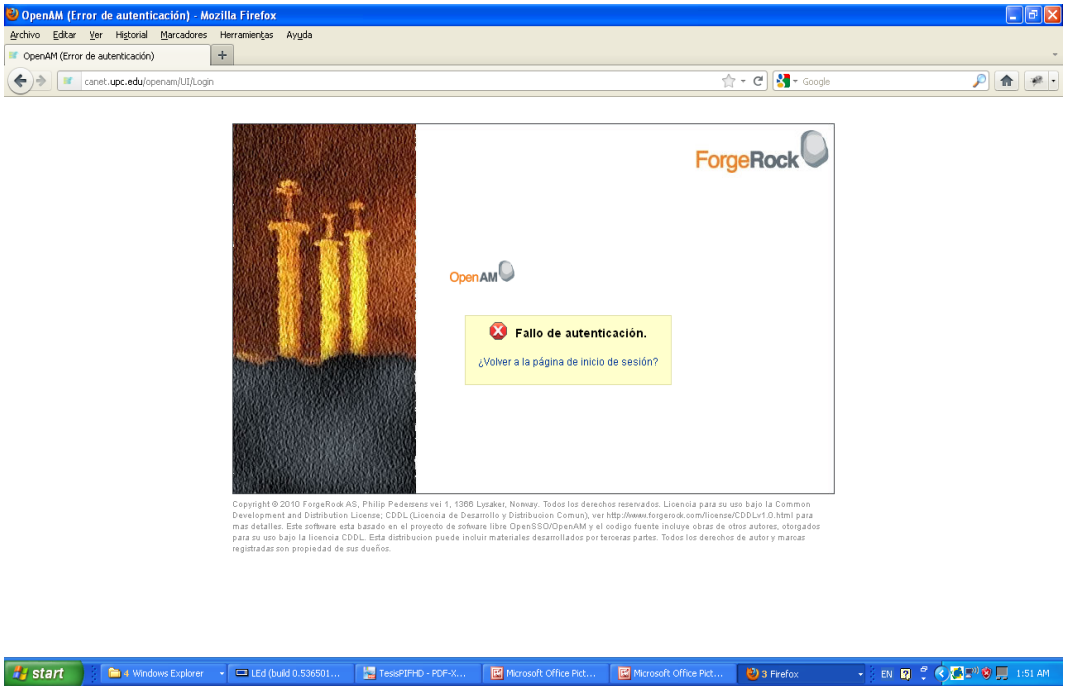

Figura 8.5: Negación de acceso

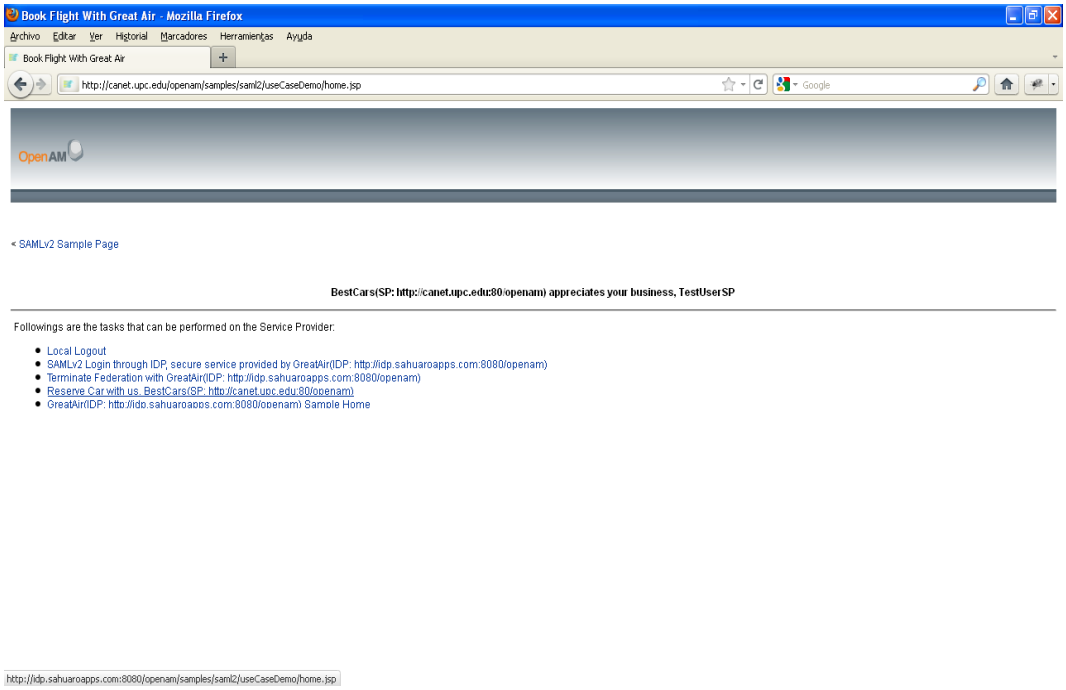

Figura 8.6: Autorización de acceso

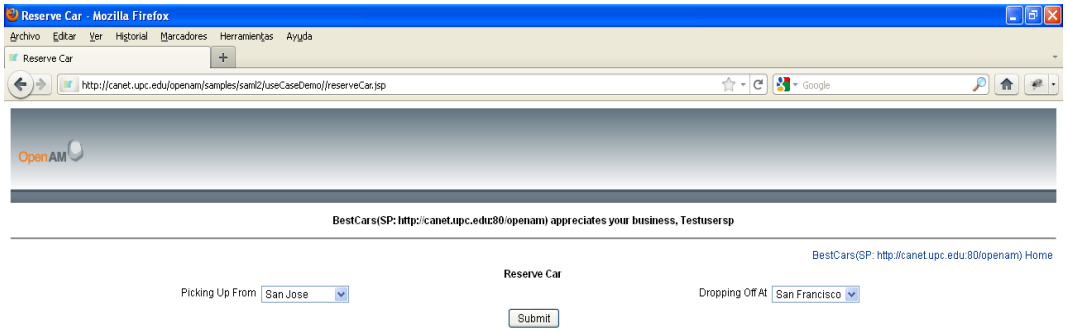

Figura 8.7: Servicio Web de prueba

8.3. Acceso a un servicio por huella dactilar

Caso de prueba: Acceso a un servicio Web por huella dactilar	
Propósito	Mostrar el funcionamiento de un acceso local por huella dactilar a un servicio Web que se encuentra dentro de un círculo de confianza .
Prerequisitos	▪ Sistema operativo Windows XP. ▪ Perfil de usuario (datos personales) y credenciales de acceso (nombre y huella dactilar) previamente registrados dentro del Servicio Web
Datos de prueba	▪ Nombre de usuario. ▪ Huella dactilar.
Flujo	1. Acceder al sitio Web de reservación de vuelos: ▪ http://idp.sahuaroapps.com:8080/openam/samples/saml2/useCaseDemo/home.jsp 2. Dar click en la liga de acceso local(Local login). 3. Enseguida aparecerá la pantalla de acceso, en la cual se debe introducir usuario y huella dactilar. 4. Con los datos de acceso correctos, obtenemos acceso a la página principal del servicio, caso contrario, nos deniega el acceso. 5. Una vez aprobada la validación, podemos ser participes del servicio.
Resultado	Obtenemos el acceso local por medio de huella dactilar aun servicio Web que se encuentra dentro del círculo de confianza.

Tabla 8.3: Caso de prueba: Acceso por huella

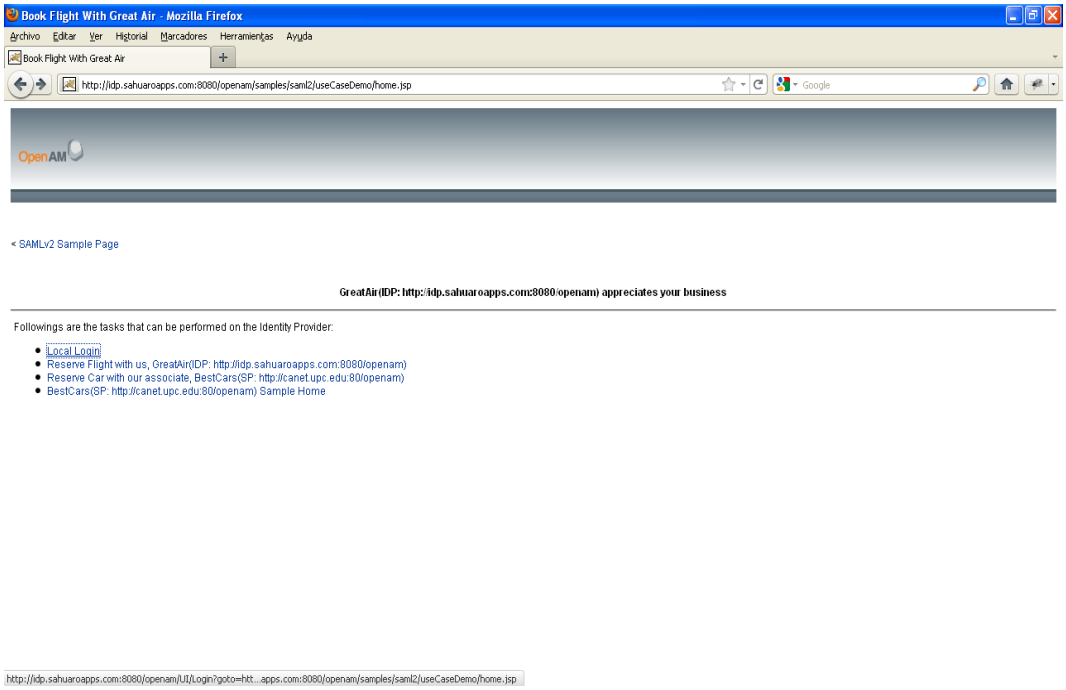

Figura 8.8: Página de acceso al Servicio Web de reservación de vuelos

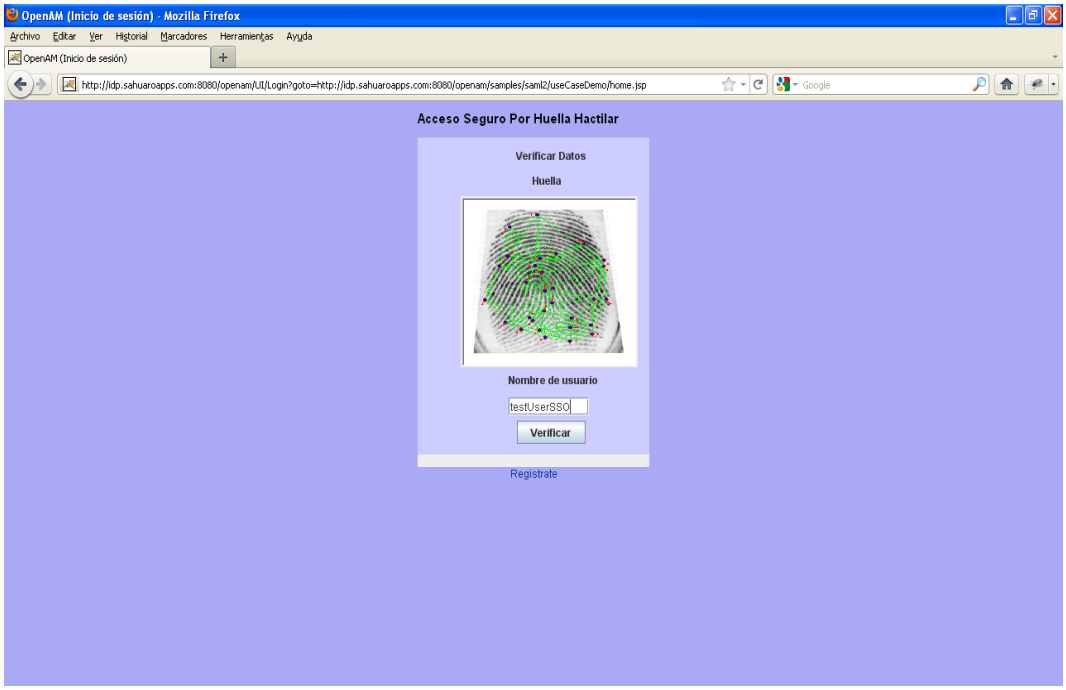

Figura 8.9: Autenticación del usuario por huella

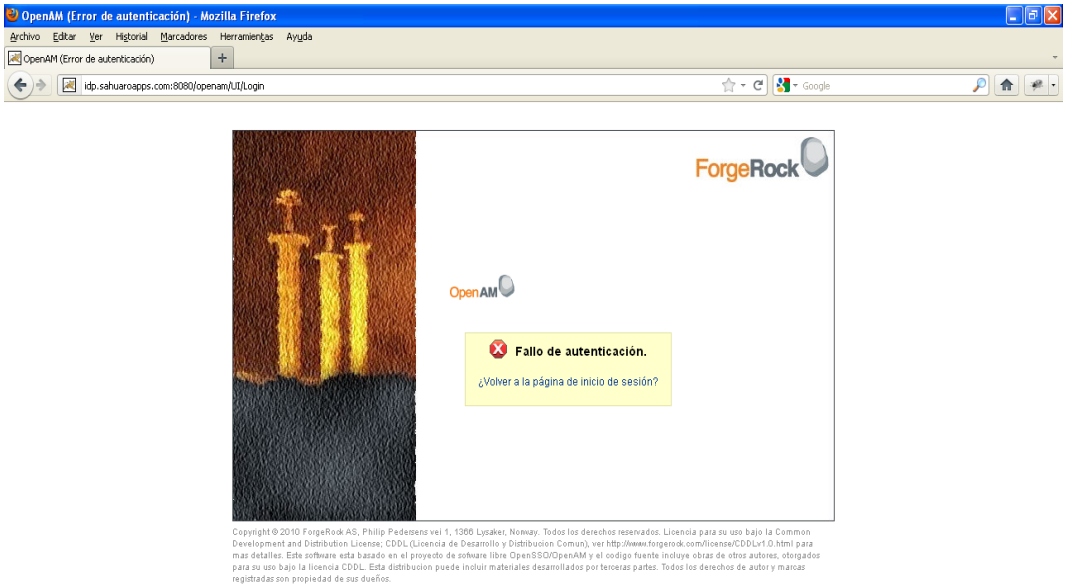

Figura 8.10: Negación de acceso por huella

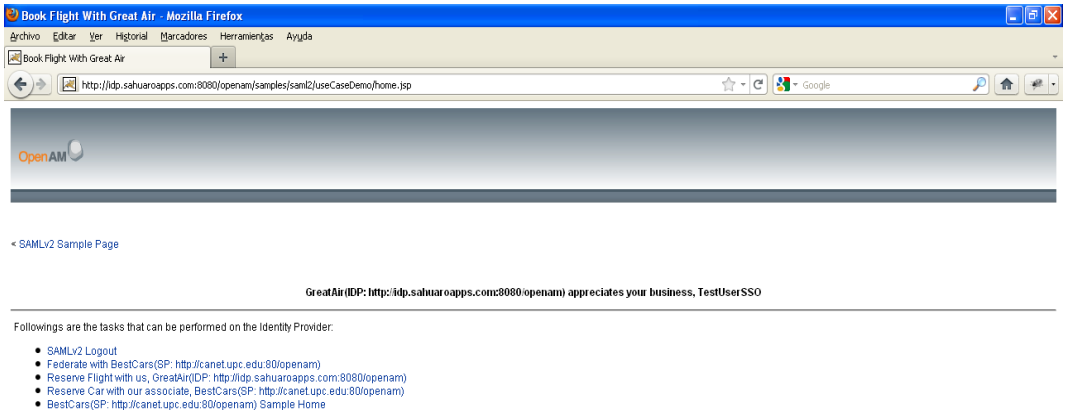

Figura 8.11: Autorización de acceso por huella

8.4. Interacción entre servicios Web sin federación de identidades

Caso de prueba: Acceso a un servicio Web por huella dactilar	
Propósito	Demostrar el comportamiento de cambio de servicio Web con cuentas que no han sido federadas.
Prerequisitos	▪ Sistema operativo Windows XP. ▪ Perfil de usuario (datos personales) y credenciales de acceso (nombre y huella dactilar) previemente registrados dentro del Servicio Web
Datos de prueba	▪ Nombre de usuario. ▪ Huella dactilar.
Flujo	1. Acceder al sitio Web de reserva de vuelos: ▪ http://idp.sahuaroapps.com:8080/openam/samples/saml2/useCaseDemo/home.jsp 2. Dar click en la liga del servicio de reserva de vuelos. 3. Enseguida aparecerá la pantalla de acceso, en la cual se debe introducir usuario y huella dactilar. 4. Con los datos de acceso correctos, obtenemos acceso al la pagina principal del servicio, caso contrario, nos deniega el acceso. 5. Una vez aprobada la validación, logramos el acceso y somos reconocidos por el servicio. 6. Seleccionamos la opción del ir al servicio de reserva de autos, en el cual no somos reconocidos por falta de inicio de sesión.
Resultado	Obtenemos el acceso local por medio de huellea dactilar aun primer servicio Web que se encuentra dentro del circulo de confianza, pero al cambiar de servicio, el usuario no es reconocido por falta de inicio de sesión.

Tabla 8.4: Caso de prueba: Interacción entre servicios Web sin federación de identidades

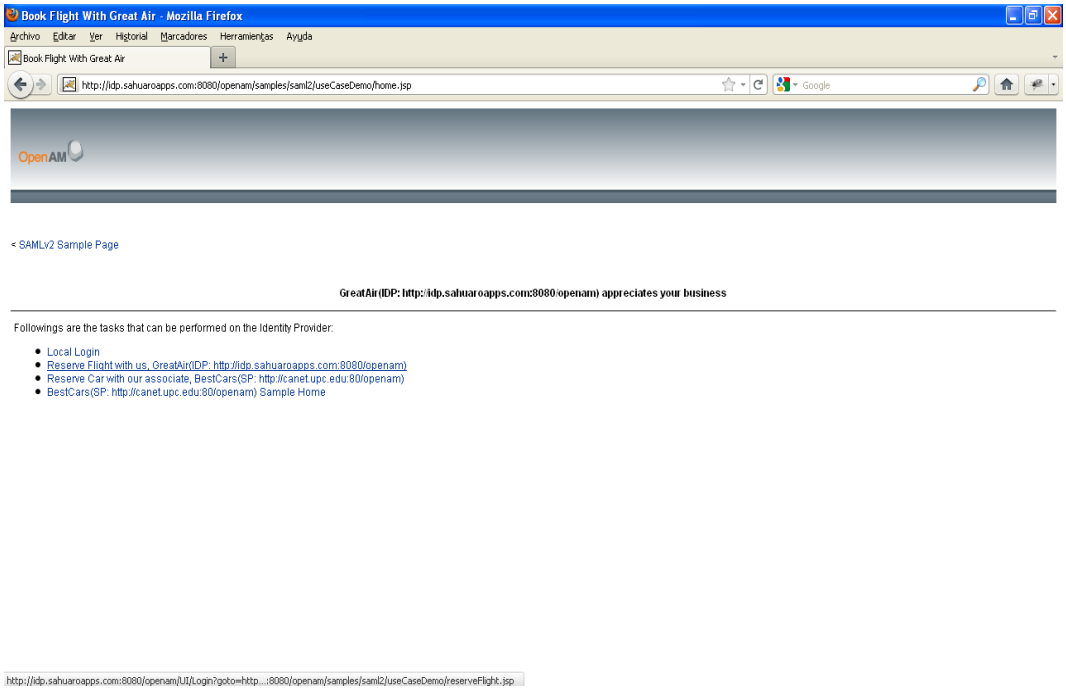

Figura 8.12: Página de acceso al servicio Web de reservación de vuelos

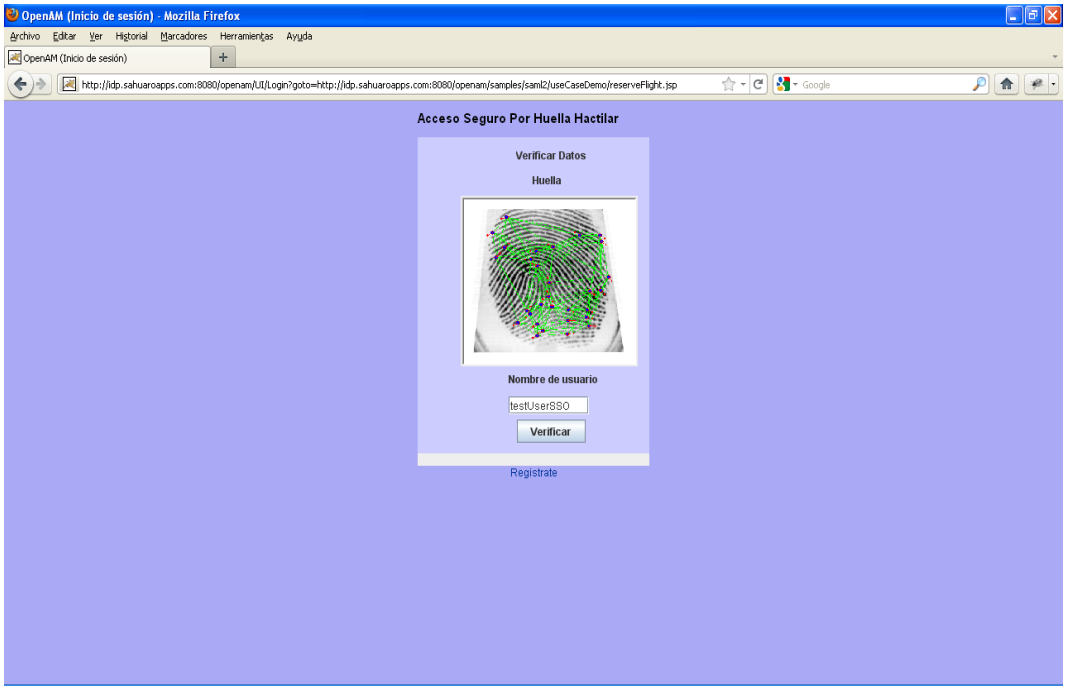

Figura 8.13: Autenticación de usuario por huella

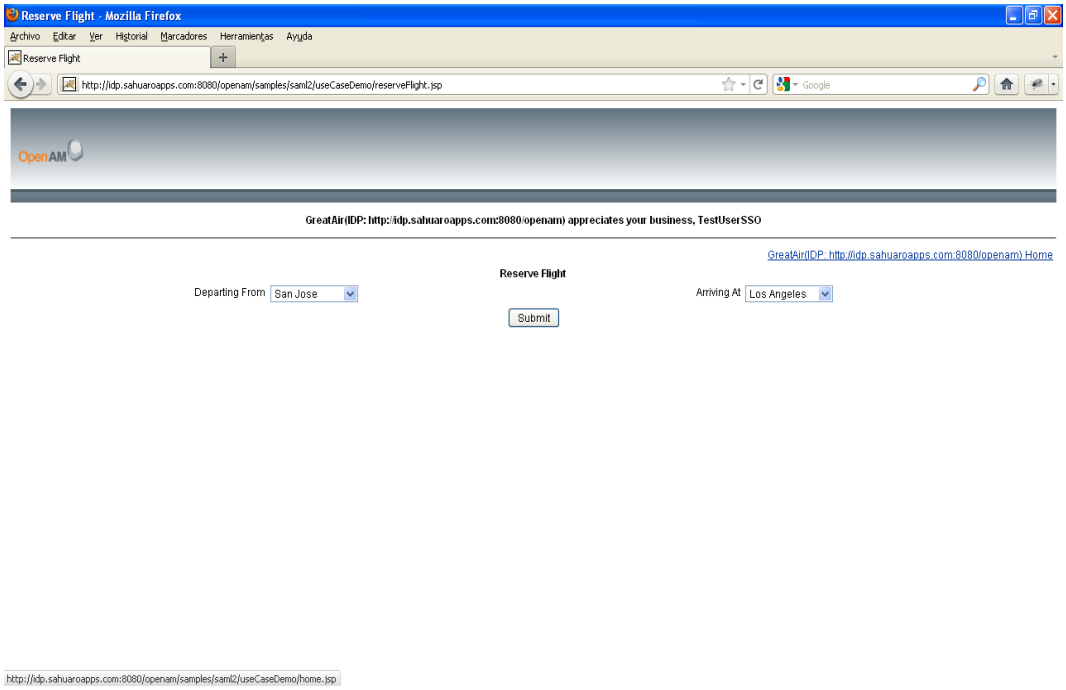

Figura 8.14: Servicio autorizado

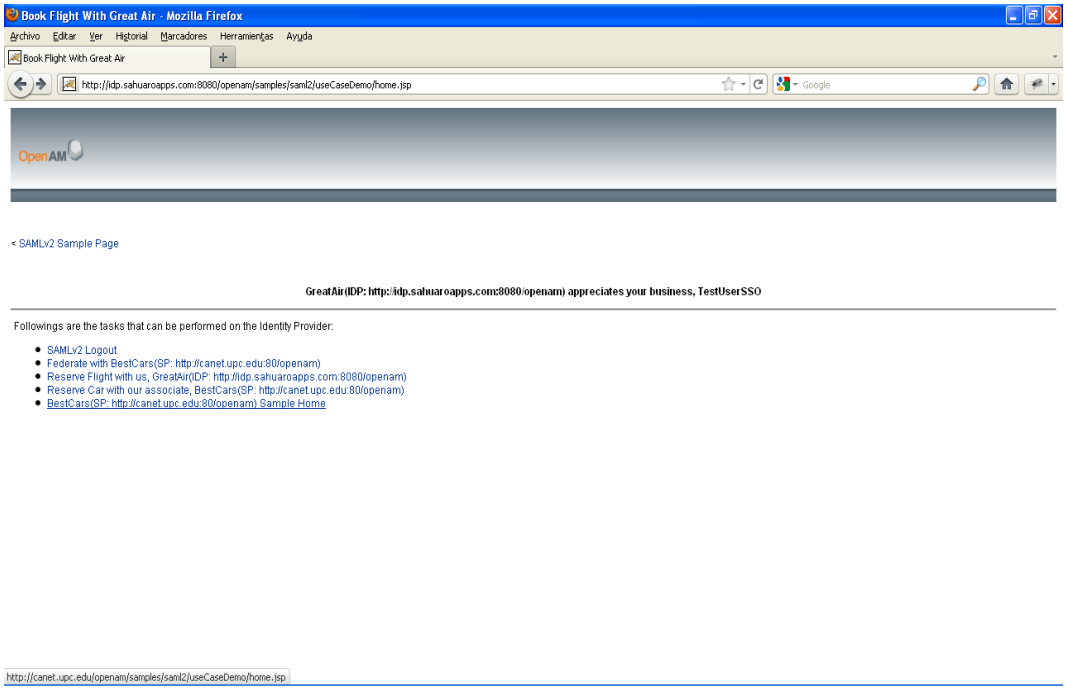

Figura 8.15: Accediendo al servicio Web de reservación de autos

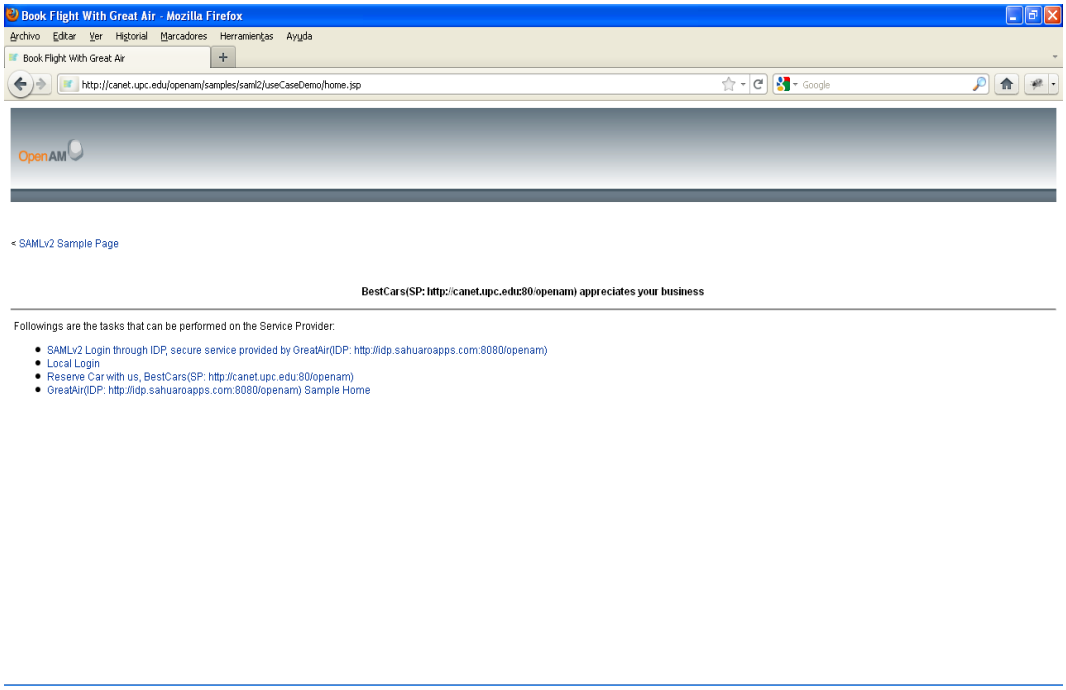

Figura 8.16: Servicio sin autorización de acceso

8.5. Federación de identidades

Caso de prueba: Federación de identidades	
Propósito	Demostrar el funcionamiento de interacción entre servicios Web dentro de un círculo de confianza con identidades federadas.
Prerequisitos	▪ Sistema operativo Windows XP. ▪ Perfil de usuario (datos personales) y credenciales de acceso (nombre, contraseña y huella dactilar) previamente registrados dentro de los Servicios Web.
Datos de prueba	▪ Nombres de usuario de ambos servicios. ▪ Huella dactilar y contraseña del primero y segundo servicio respectivamente.
Flujo	1. Acceder al sitio de reserva de autos: ▪ http://canet.upc.edu/openam/samples/saml2/useCaseDemo/home.jsp 2. Seleccionar la liga de acceso seguro a través del IDP. 3. Enseguida aparecerá la pantalla de acceso del IDP, en la cual se debe introducir usuario y huella dactilar. 4. Nuevamente aparecerá la pantalla de autenticación por usuario y contraseña del servicio del servicio reservación de autos. 5. Una vez validados los datos en esta doble autenticación, logramos el acceso y somos reconocidos para los servicios de reserva de autos y de reserva de vuelos.
Resultado	Con una doble autenticación logramos la federación de dos cuentas de usuario diferentes en 2 diferentes servicios. Con esto lograremos acceder a dos servicios Web diferentes con una sola autenticación la próxima vez que se requiera.

Tabla 8.5: Caso de prueba: Federación de identidades

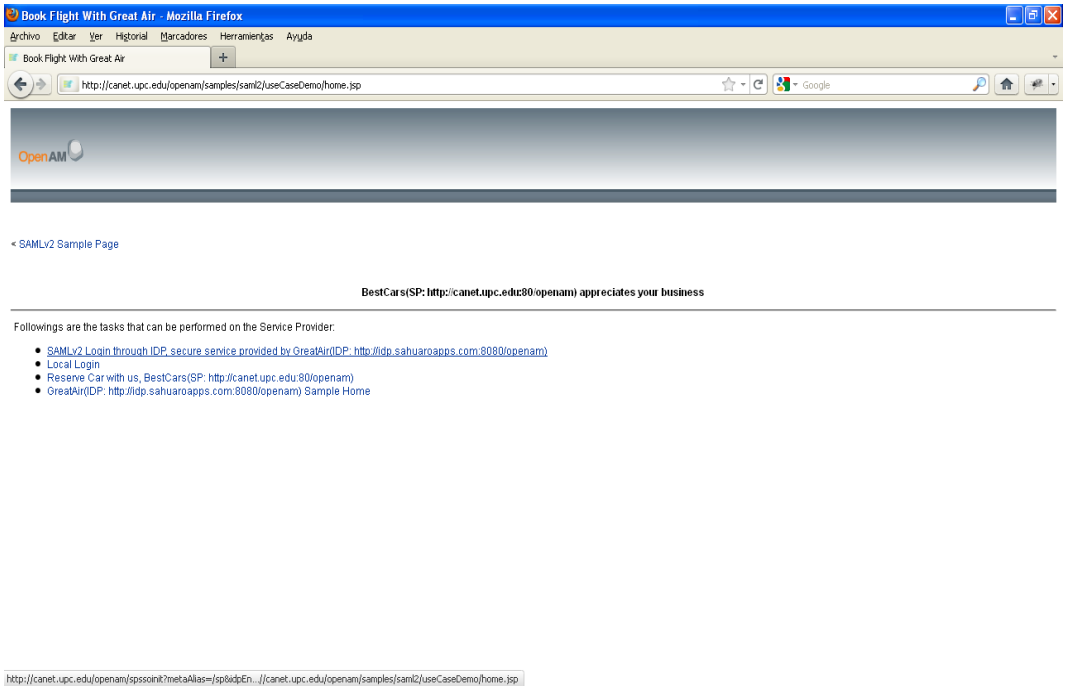

Figura 8.17: Selección de acceso seguro por medio del IDP

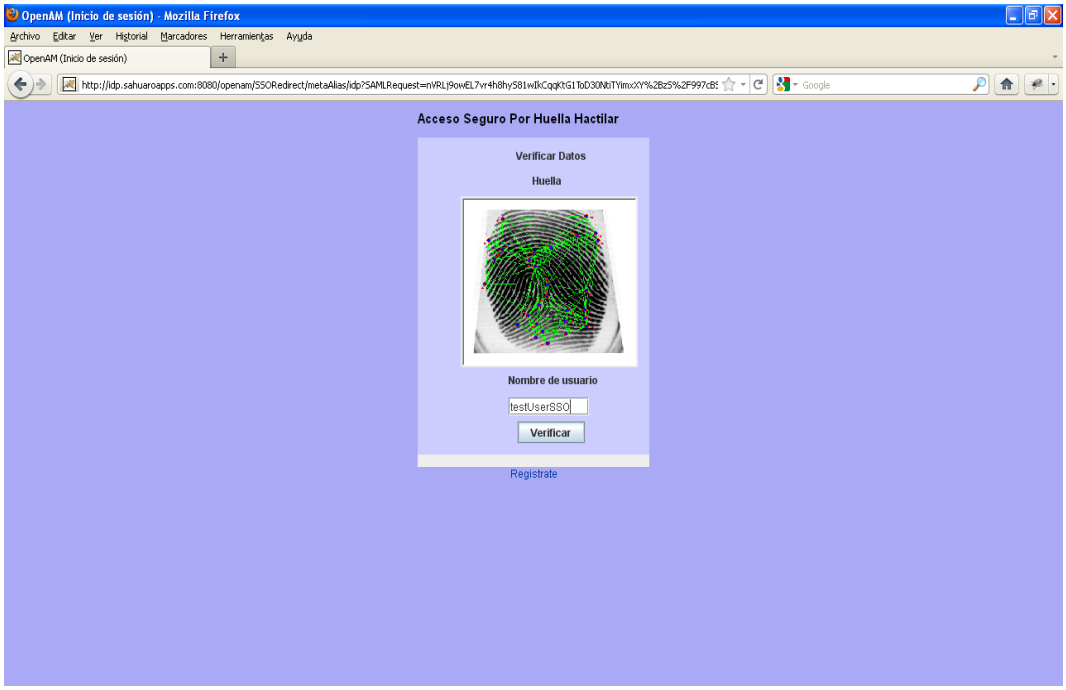

Figura 8.18: Autenticación en el IDP

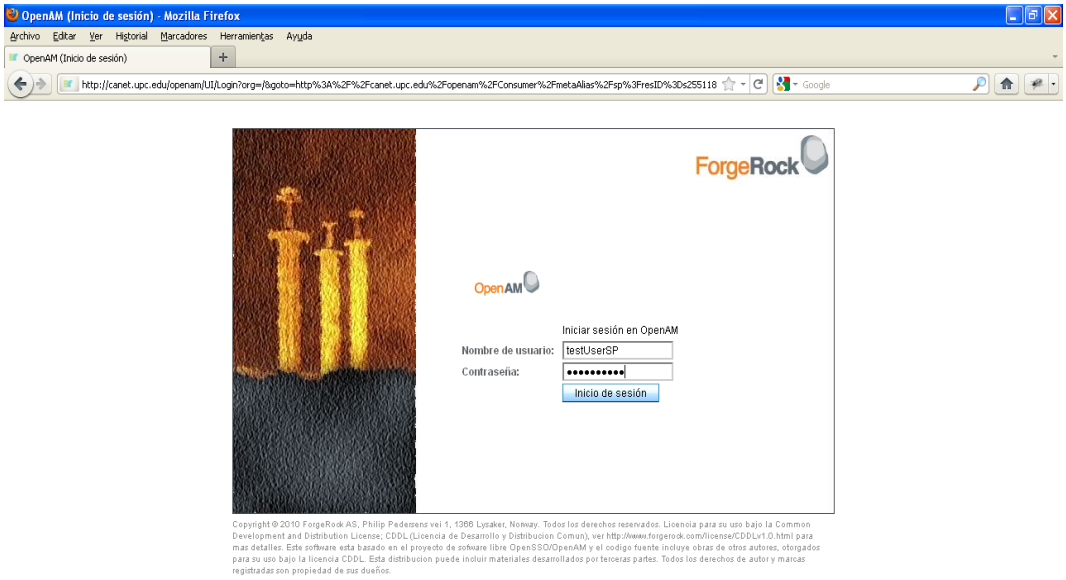

Figura 8.19: Autenticación en servicio Web

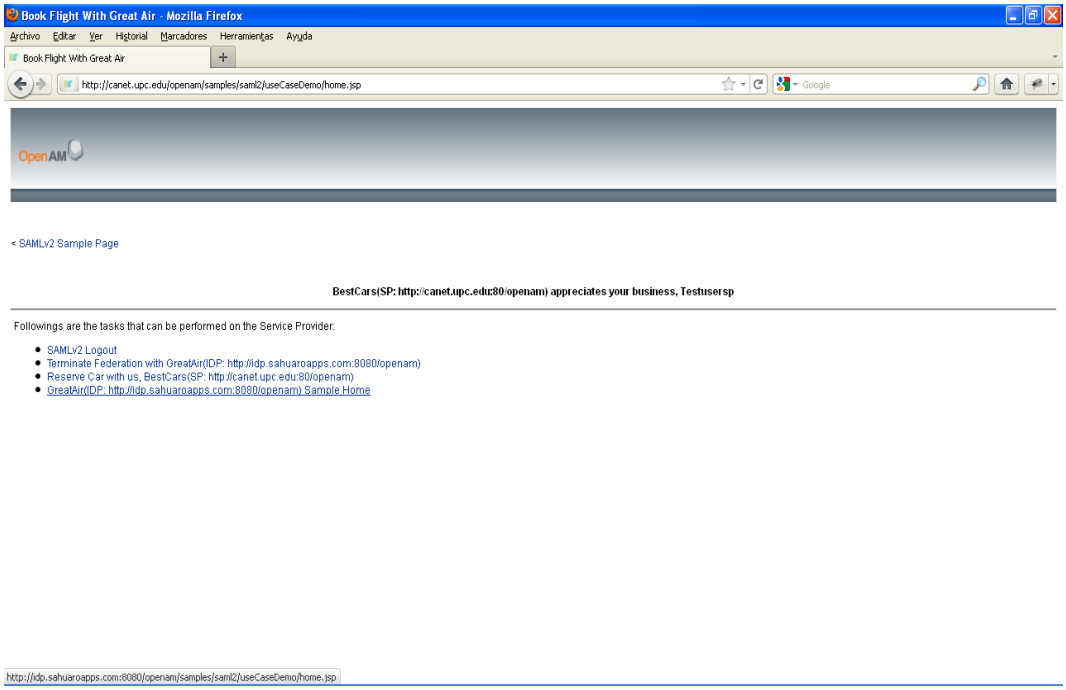

Figura 8.20: Servicio Web de reservación de autos

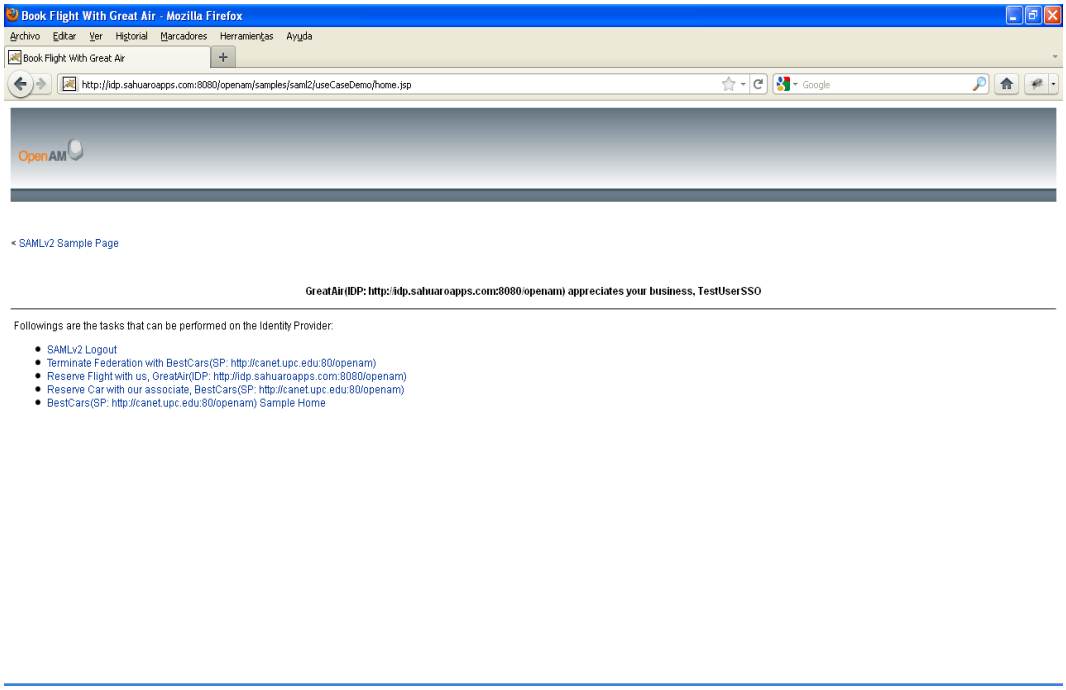

Figura 8.21: Servicio Web de reservación de vuelos

8.6. Inicio de sesión único (SSO, Single Sign On)

Caso de prueba: Federación de identidades	
Propósito	Demostrar el acceso a dos servicios Web dentro de un círculo de confianza con una sola autenticación de cuentas federadas.
Prerequisitos	▪ Sistema operativo Windows XP. ▪ Perfil de usuario almacenado en el proveedor de identidades. ▪ Nombre de usuario y huella dactilar almacenados el proveedor de identidades. ▪ 2 cuentas de usuario con cuenta previamente federada en dos servicios Web.
Datos de prueba	▪ Nombre de usuario previamente registrados en el IDP. ▪ Huella dactilar.
Flujo	1. Acceder al sitio de reserva de vuelos: ▪ http://idp.sahuaroapps.com:8080/openam/samples/saml2/useCaseDemo/home.jsp 2. Seleccionar la liga de reserva de vuela con acceso seguro a través del IDP. 3. Enseguida aparecerá la pantalla de acceso del IDP, en la cual se debe introducir usuario y huella correspondiente a las cuentas federadas anteriormente. 4. Enseguida nos muestra la página de reserva de vuelos, en donde el usuario es reconocido y se le provee una identidad. 5. Ir al menú principal y seleccionamos ir al servicio Web asociado de reserva de autos. 6. El acceso es concedido al usuario y de igual manera se le provee de una identidad.
Resultado	Se logra el acceso a dos servicios Web diferentes dentro del círculo de confianza con un solo Login.

Tabla 8.6: Caso de prueba: Inicio de sesión único

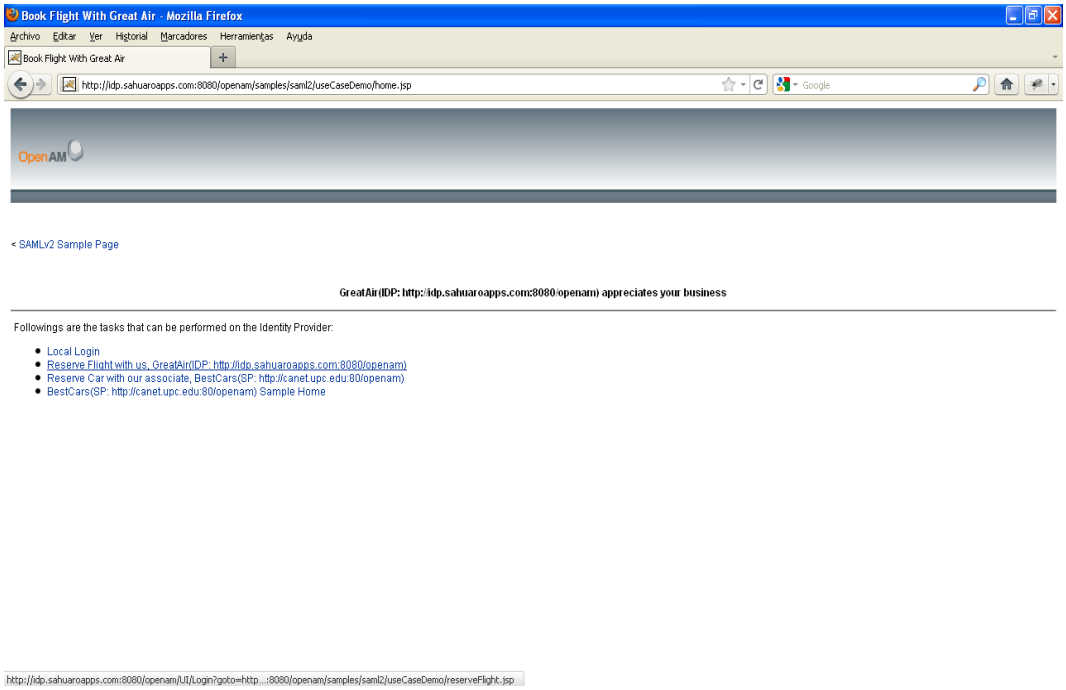

Figura 8.22: Selección de acceso seguro por medio del IDP dentro del servicio reserva de vuelos

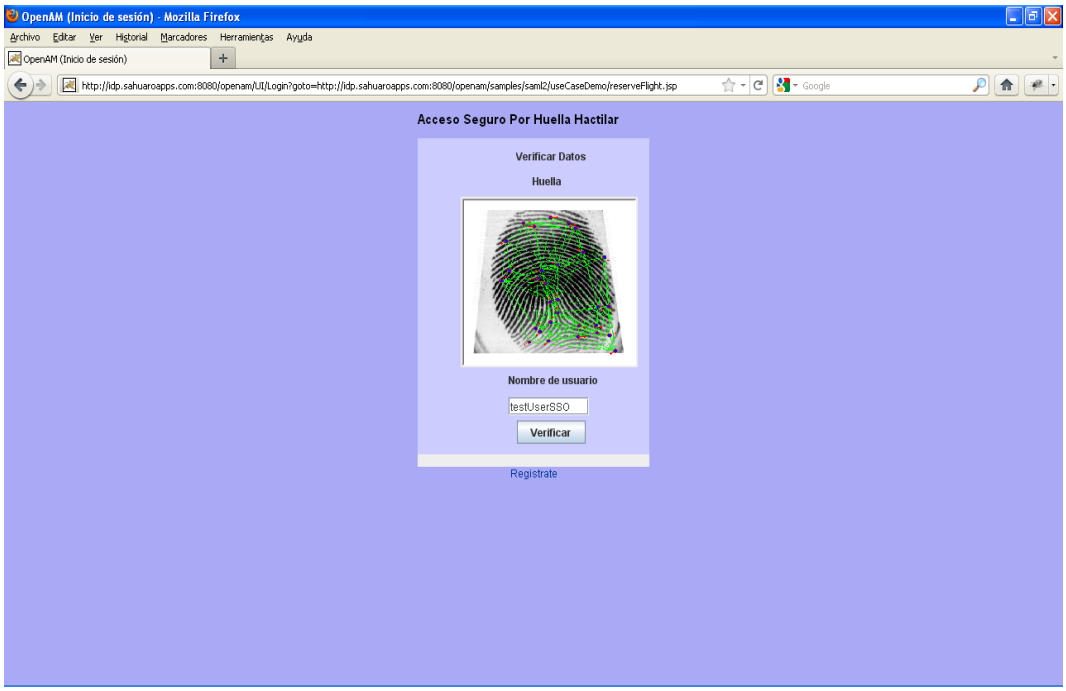

Figura 8.23: Autenticación por huella

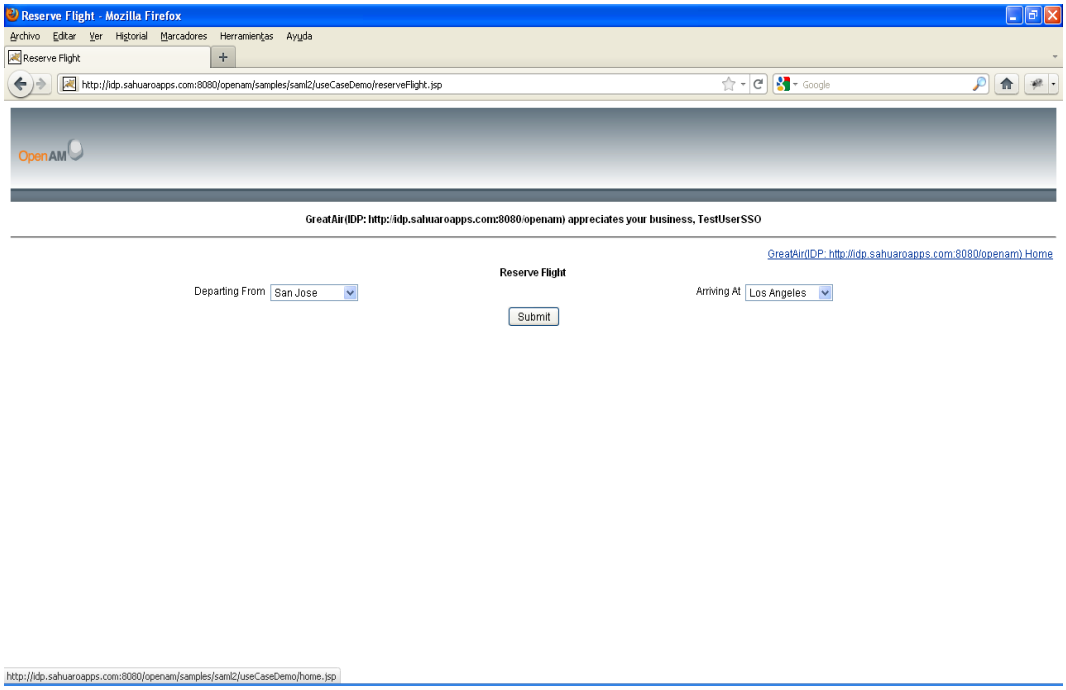

Figura 8.24: Servicio reserva de vuelos

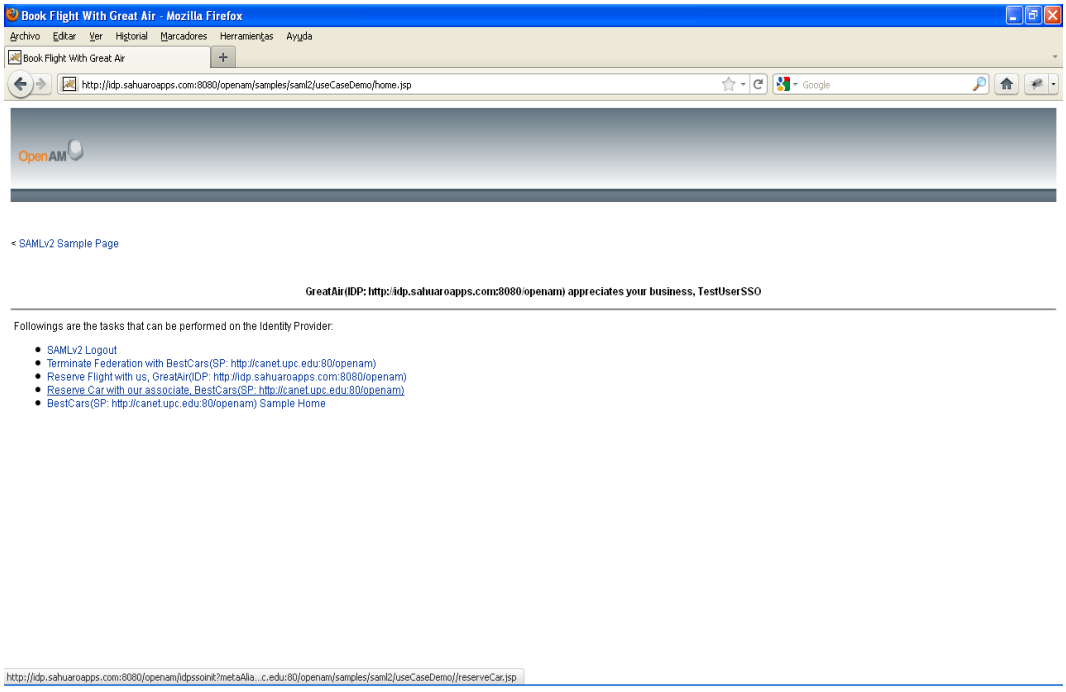

Figura 8.25: Acceso al servicio reserva de autos

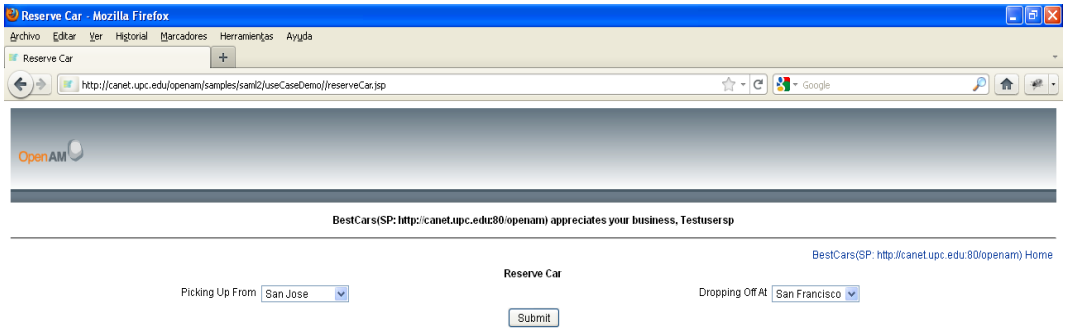

Figura 8.26: Servicio reserva de autos

8.7. Cierre de sesión único (SLO, Single Log Out)

Caso de prueba: Federación de identidades	
Propósito	Demostrar el cierre de sesión único de cuentas de usuarios federadas en dos servicios Web dentro de un círculo de confianza.
Prerequisitos	▪ Sistema operativo Windows XP. ▪ Perfil de usuario almacenado en el proveedor de identidades. ▪ Nombre de usuario y huella dactilar almacenado en el proveedor de identidades. ▪ 2 cuentas de usuario previamente federadas en dos servicios Web. ▪ Previo acceso a través del IDP a cualquiera de los servicios Web.
Datos de prueba	▪ Nombre de usuario previamente registrados en el IDP, para previo registro. ▪ Huella dactilar para previo registro.
Flujo	1. Tener previo acceso a través del IDP con la cuenta federada a cualquiera de los dos servicios (reserva de vuelos y reserva de autos): ▪ http://idp.sahuaroapps.com:8080/openam/samples/saml2/useCaseDemo/home.jsp ▪ http://canet.upc/openam/samples/saml2/useCaseDemo/home.jsp 2. Posteriormente el usuario es reconocido y tiene acceso en ambos servicios. 3. Seleccionar la opción de SAMLv2 LogOut. 4. Enseguida será cerrada la sesión para ambos servicios.
Resultado	Se logra el cierre de sesión único a dos servicios Web diferentes dentro del círculo de confianza con un solo LogOut.

Tabla 8.7: Cierre de sesión único

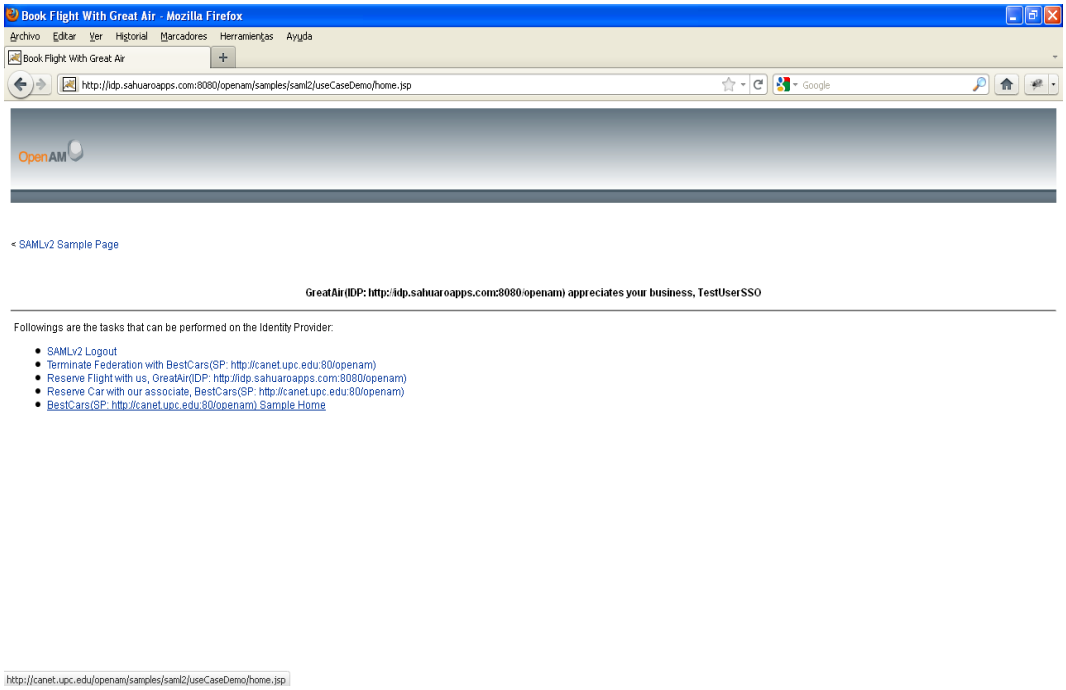

Figura 8.27: Servicio Web reserva de vuelos

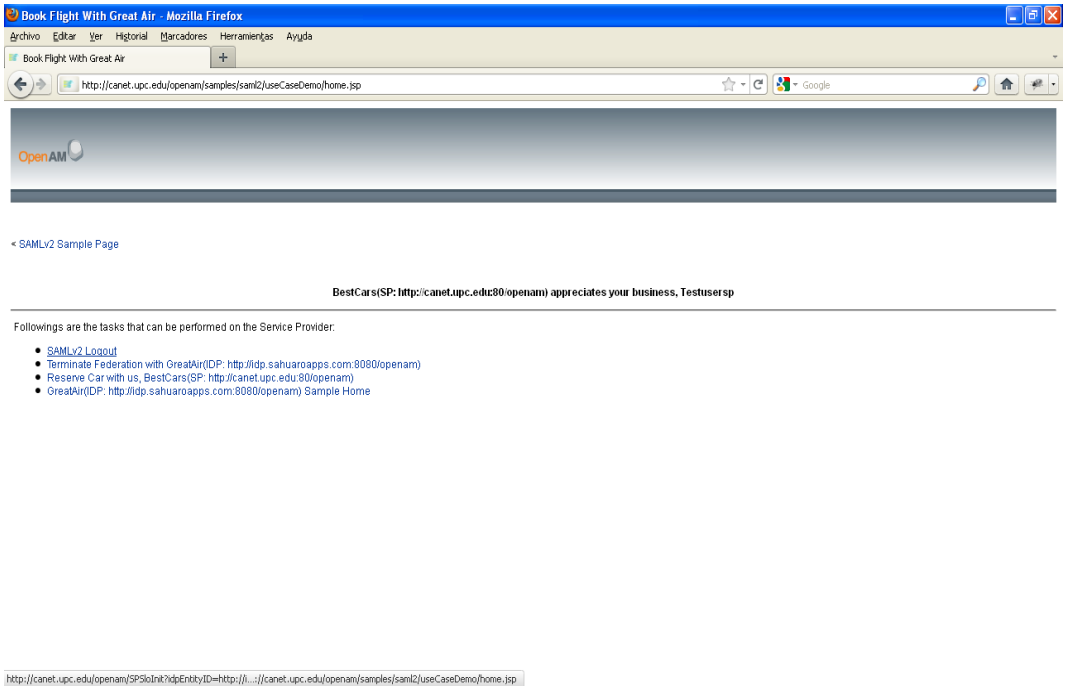

Figura 8.28: Servicio Web reserva de autos

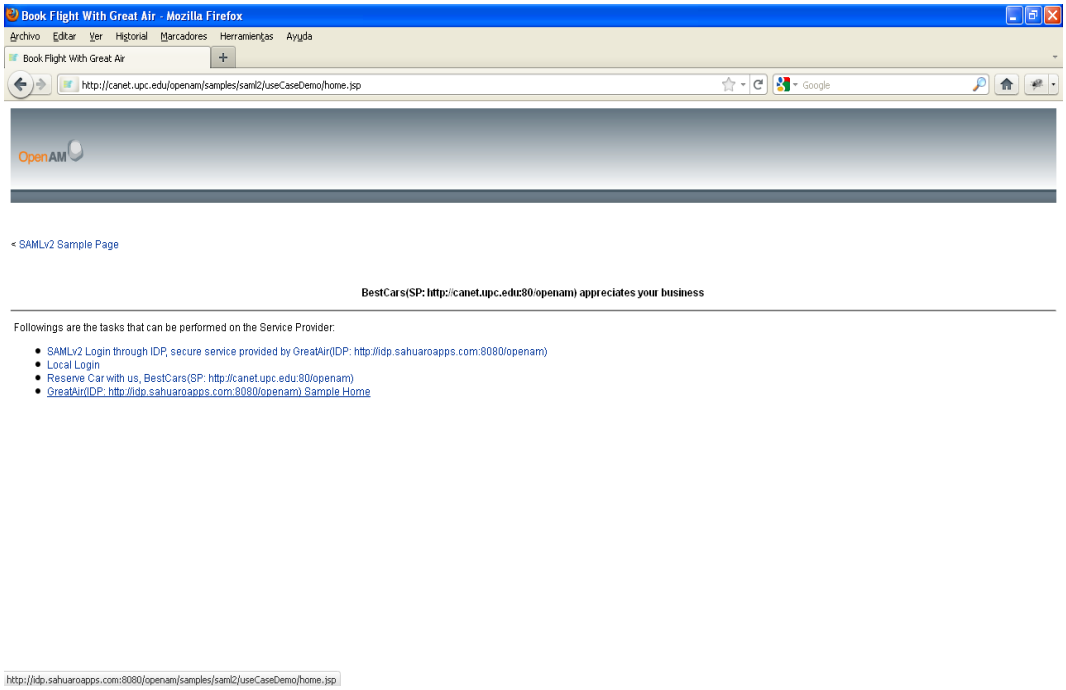

Figura 8.29: Cierre de sesión en reserva de autos

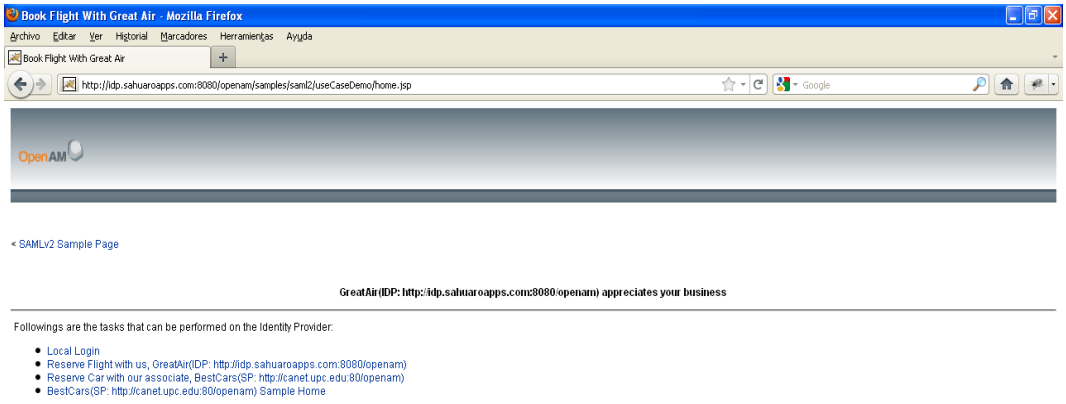

Figura 8.30: Cierre de sesión en reserva de vuelos

8.8. Terminando federación de cuentas

Caso de prueba: Federación de identidades	
Propósito	Demostrar el termino de la federación de cuentas de usuarios.
Prerequisitos	▪ Sistema operativo Windows XP. ▪ Perfil de usuario almacenado en el proveedor de identidades. ▪ Nombre de usuario y huella dactilar almacenado en el proveedor de identidades. ▪ 2 cuentas de usuario previamente federadas en dos servicios Web. ▪ Previo acceso a través del IDP a cualquiera de los servicios Web.
Datos de prueba	▪ Nombre de usuario previamente registrados en el IDP, para previo registro. ▪ Huella dactilar para registro previo.
Flujo	1. Tener acceso previo a través del IDP con la cuenta federada a cualquiera de los dos servicios (reserva de vuelos y reserva de autos): ▪ http://idp.sahuaroapps.com:8080/openam/samples/saml2/useCaseDemo/home.jsp ▪ http://canet.upc/openam/samples/saml2/useCaseDemo/home.jsp 2. Seleccionar la opción Terminar Federación. 3. Enseguida las cuentas dejarán de estar federadas.
Resultado	Se logra terminar la federación cuando un usuario lo requiere.

Tabla 8.8: Caso de prueba: Termino de federación

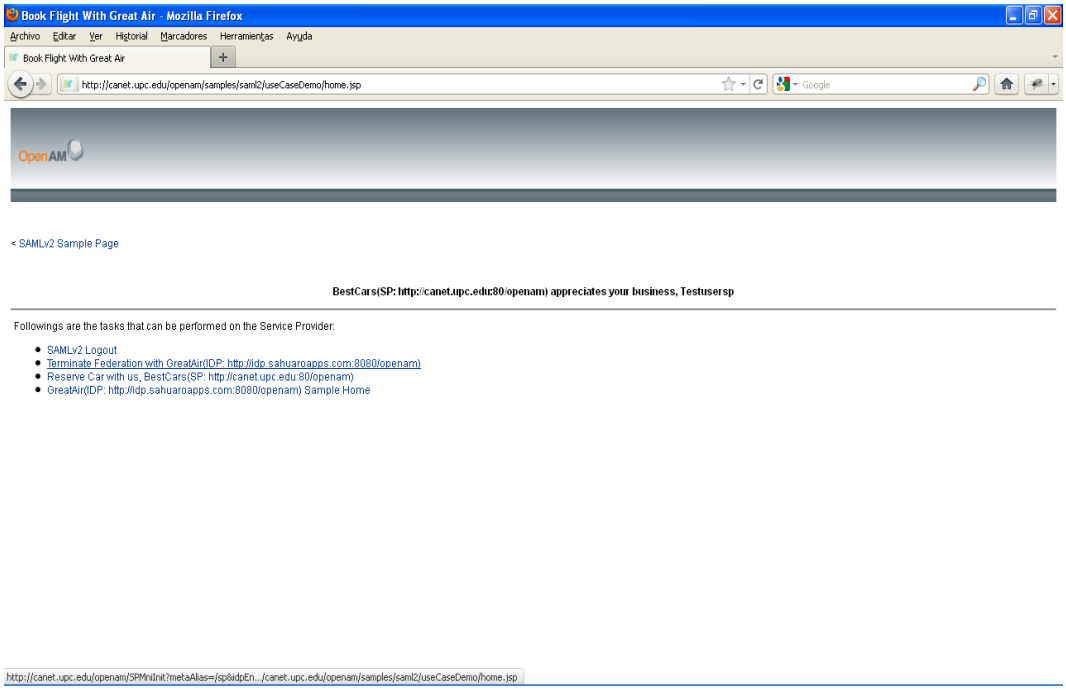

Figura 8.31: Terminando federación de cuentas

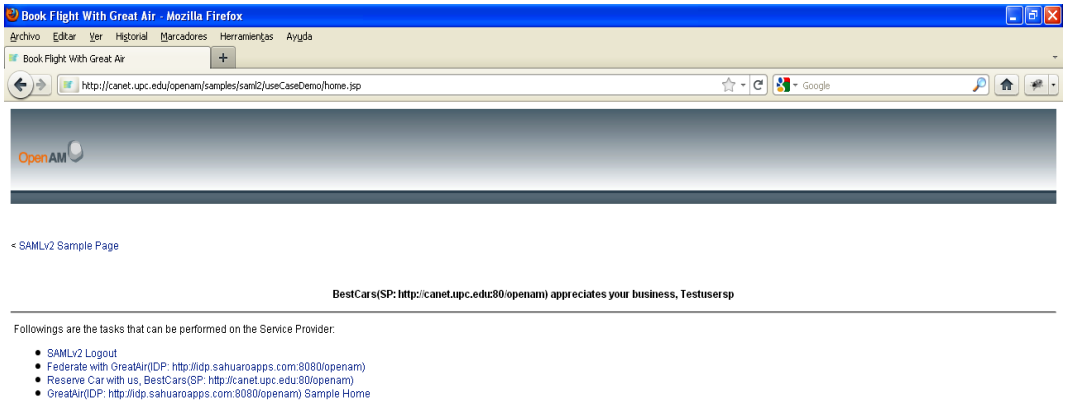

Figura 8.32: Federación de cuentas terminada

8.9. Conclusiones

De las pruebas realizadas al sistema presentado, destacan las siguientes conclusiones:

- Un método de acceso más seguro y aceptable tanto para los usuarios como para los prestadores de servicios, es el modulo de acceso por huella dactilar.
- La huella dactilar como método de autenticación, difícilmente puede ser robada, además de ser algo que no puede ser olvidado.
- El sistema proveedor de identidades empleado, maneja protocolos de acceso estandarizados y seguros, deslindando al desarrollador de servicios de la parte dentro del desarrollo.
- El proveedor de identidades, se encarga de reconocer al usuario como un usuario legítimo dando acceso a otros servicios dentro del círculo de confianza.
- Una única autenticación dará acceso al usuario a otros servicios dentro de un círculo de confianza, al autenticarse con el módulo de acceso aportado por proveedor de identidades.
- El módulo de acceso por huella dactilar dentro de proveedor de identidades, demuestra facilidad de uso y seguridad de acceso, tomando en cuenta que el usuario tendrá acceso a más de un servicio al autenticarse una vez por medio de huella dactilar.

Bibliografía

[1] Identidad federada. http://blogs.sun.com/identidad/category/Identidad+federada. Accesada:Octubre 16, 2008.

[2] A. K. Jain A. Ross. Information fusion in biometrics. pattern recognition letters 24 (2003) 2115-2125. Disponible en: http://www.computerscienceweb.com/.

[3] Elisa Bertino Abhilasha, Anna Squicciarini. Privacy preserving multi-factor authentication with biometrics. *DIM'06*, Noviembre 2006.

[4] Mansour Alsaleh and Carlisle Adams. Enhancing Consumer Privacy in the Liberty Alliance Identity Federation and Web Services Frameworks. *Work*, pages 59 – 77, 2006.

[5] Juan Carlos Hoyos Arbeláez Andrés Madrigal Gonzáles, Jaime León Ramírez Madrigal. Diseño de un sistema biométrico de identificación usando sensores capacitivos para huellas dactilares. *Revista de la Facultad de Ingeniería Universidad de Antioquia*, 39:21–32, Marzo 2007.

[6] Salil Prabhakar Anil K. Jain, Arun Ross. An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Tenchnology*, 14, Enero 2004.

[7] Griaule Biometrics. http://www.griaulebiometrics.com/. Accessada: Agosto, 2009.

[8] R. Cappelli D. Maio, D. Maltoni. Fvc2002: Fingerprint verification competition. proc. int. conf. pattern recognition (icpr). pages 744–747, Agosto 2002.

[9] Edgar Danielyan. The lures of biometrics. *The Internet Protocol Journal*, 7:15–34, Marzo 2004.

[10] Kresimir Delac and Mislav Grgic. A survey of biometric recognition methods. *Electronics*, (June):16–18, 2004.

[11] TEC ELECTRÓNICA. Sistemas biométricos. http://www.tec-mex.com.mx/. Accesada: Noviembre 5, 2008.

[12] S. Fox. Trust and privacy online: Why americans want to rewrite the rules. http://www.pewinternet.org/Reports/2000/Trust-and-Privacy-Online.aspx?r=1. Accesada:Agosto, 2010.

[13] Juan Carlos Yelmo García. Aplicación de la tecnología liberty en el contexto de los servicios de internet móvil. *Universidad Politécnica de Madrid*, Octubre 2005.

[14] Karina Toscano Gualberto Aguilar, Gabriel Sánchez. Reconocimiento de huellas dactilares usando características locales. *Revista de la Facultad de Ingeniería Universidad de Antioquia*, 46:101–109, Diciembre 2008.

[15] García Ortega Victor Hugo. Sistema de reconocimiento de huellas dactilares para el control de acceso a recintos. *Evaluation*, pages 119–124, 2001.

[16] Barrios Alejandro R. Luque José A. Sistema de identificación mediante huella digital. *TECNICA*, 8:11–17, 1999.

[17] Paul Madsen, Yuzo Koga, and Kenji Takahashi. Federated identity management for protecting users from ID theft. *Proceedings of the 2005 workshop on Digital identity management - DIM '05*, page 77, 2005.

[18] Luciano Martín Baenz Moyano. Extracción de características de galton de huellas dactilares por procesamiento digital de la imagen. universidad tecnológica nacional, facultad regional córdoba. Disponible en: http://www.cneisi.frc.utn.edu.ar/papers/736ea8ecf9f30f83571ddd6d4412.pdf. Accesada: Junio 2010.

[19] Paola Neri, Celia Perez, and Araceli Tlamanca. Sistema evolutivo reconocedor de huellas digitales. *Universidad Anahuac de Xalapa.* Disponible en

: http://www.fgalindosoria.com/informatica/informaticos/investigadores/Paola_Neri_Ortiz/Sistema_evolutivo_reconocedor_de_huellas_digitales/Sistema_evolutivo_reconocedor_de_huellas_digitales.htm. Accesada: Junio 2010.

[20] Articulos Network World. Técnicas de seguridad biométricas. http://www.idg.es/Comunicaciones/articulo.asp?id=161095. Accessada: Octubre 21, 2008.

[21] Antonio Requejo Novella. Introducción a la gestion de identidades. *Red Seguridad*, 19:120–121, 2005.

[22] Reza Adhami Peter Meenen. Fingerprinting for security. *Potentials, IEEE*, Agosto/Septiembre 2001.

[23] Sandra García Polo, Antoine De Poorter, and Manel Medina. Fidelity : Sistema de Gestión Federada de la Identidad Digital basado en Liberty Alliance.

[24] A. K. Jain S. Prabhakar, S. Pankanti. Biometric recognition: Security and privacy concerns. *IEEE Security & Privacy*, pages 33–42, Marzo/Abril 2003.

[25] J.L. de la Rosa Triviño S.Gálvez Rojas, J. Lago Cabrera. Opensso y openid. comparativa y capacidad de integración. Disponible en: http://www.mundointernet.es/IMG/pdf/ponencia151_2.pdf. Accesada: Junio 2010.

[26] J. L. Wayman. Fundamentals of biometric authentication technologies. *Int. J. Image Graphics*, 1:93–113, 2001.

[27] David D. Zhang. Automated biometrics: Technologies and systems. *IEEE Security & Privacy*, page 2, 2000.