



## **SISTEMAS BIOMETRICOS DE AUTENTIFICACION BASADOS EN LA TECNOLOGIA DE HUELLA DACTILAR DE DIGITALPERSONA.**

El presente documento detalla las capacidades que un sistema de autenticación de usuarios con mecanismos biométricos debe tener, y que digitalPersona ha desarrollado en su totalidad. Estas características se pueden resumir en tres grandes apartados: Seguridad, Conveniencia y Clase Empresarial.

### **I. SEGURIDAD.**

Filosofía integral. Se debe medir la seguridad de un sistema como una cadena en la que se tendrá la seguridad del eslabón más débil. Un Sistema Empresarial de Autenticación debe asegurar que cada parte del proceso de principio a fin es segura a través de todo el sistema para ser considerado un sistema seguro.

#### **La comunicación debe ser segura y confiable.**

*A través de todas las comunicaciones internas y en red, el sistema debe garantizar que el dato no sea interceptado o modificado.*

1. Comunicación encriptada por llave pública y privada (PKI). Con los sensores U.are.U 4000 de digitalPersona se asegura que la huella viaje cifrada (encriptada) a 128 bits con llaves pública y privada desde el sensor hacia la computadora. Esto garantiza que no se pueda sustraer la huella –y por tanto utilizarla para fines fraudulentos- al momento de su lectura.
2. Challenge / Response Link. El sistema “estampa” electrónicamente la información de la huella desde el sensor para eliminar la posibilidad de ataques continuos.
3. Red interna de certificados X.509. El sistema emite certificados X.509 dentro de la red de PRO para asegurar que el dato es válido y seguro.

#### **Procesamiento biométrico operado solamente por sistemas confiables.**

*Para máxima protección de la empresa, el sistema biométrico no debe permitir el procesamiento de datos en una computadora que no sea segura o sea susceptible a ataques.*

1. Extracción de características basada en el Servidor. Las redes U.are.U PRO procesarán huellas solamente en el Servidor para evitar estaciones inseguras de Windows como 98/Me.
2. Comparación de plantillas basada en el Servidor. Los certificados son emitidos solamente a computadoras confiables (Win 2000 / XP) para permitir la comparación de huellas, pero todas las demás se comparan en el Servidor.

#### **Las credenciales deben ser almacenadas en forma segura y deben ser confiables.**

*Una vez que un usuario ha sido registrado en el sistema, debe evitarse que sus registros sean modificados o robados.*

1. Registros encriptados por PKI. Toda la información interna es encriptada a 128 bits y firmada por la llave privada de las computadoras que los crearon.
2. Acceso con Credenciales Protegidas. La modificación de los registros puede ser lograda solamente al autenticar completamente el sistema.

#### **Asegurar que el dedo utilizado es real.**

*El sistema biométrico debe proveer una seguridad razonable de que lo que le es presentado al sistema es una credencial válida (un dedo real).*

1. Rechazo de dedo falso. Lectura tridimensional que permite la lectura de huella viva. Con su tecnología óptica y capacitiva mide profundidad de surcos de la huella. Esto garantiza que se trata



de una huella de una persona viva al momento de la lectura y no de una falsificación (en papel, látex, etc.) que se pudiese fabricar.

2. Substracción de imagen latente. Se remueve (borra) electrónicamente la imagen de la huella del dedo dejada en la ventana del sensor de forma que no pueda ser utilizada contra el sistema mismo.

## II. CONVENIENCIA O FACILIDAD DE USO.

El usuario final es guiado por la conveniencia o la facilidad de uso. Por ello los sistemas tradicionales de password han fallado: si el usuario tiene la opción siempre va a escoger passwords sencillos y fácilmente memorizables, o tendrán un solo password para todos sus sistemas. Cuando los administradores de sistemas exigen políticas más restrictivas, el usuario disminuye su nivel de seguridad escribiendo su password en hojas de papel. Y cuando el administrador exige cambios cada 30/60/ 90 días se tiene que contar con un servicio de help desk. El usuario no debería tener que aprenderse un password muy robusto.

### **El sistema biométrico debe ser más fácil de usar que los sistemas de password.**

*El proceso de autenticación debe ser más rápido, simple y fácil.*

1. Autenticación con un solo toque del dedo. Los usuarios pueden ingresar al sistema solamente colocando su dedo en el sensor, sin clicks de Mouse o selecciones de menú.
2. Reemplazo de password con un solo toque del dedo. Los usuarios pueden abrir aplicaciones protegidas y sitios de web con un solo toque del sensor, sin teclear adicionalmente o seleccionar opción con el ratón.
3. Capacidad de roaming. Los usuarios pueden cambiarse de estación en estación (computadora a computadora) sin necesitar de registrarse en cada una.

### **La interacción del usuario con el sistema debe ser natural y simple.**

1. Lectura de 360 grados. El usuario puede colocar su huella en cualquier ángulo con respecto a la ventana de lectura del sensor. Esta característica es esencial cuando se planea utilizar los sensores de huella en un ambiente múltiple y masivo, ya que no exige que se coloque el dedo en una postura fija, difícil de replicar en un ambiente de mucha transaccionalidad con el sensor.
2. Captura rápida de imagen. El sensor es inteligente para saber en qué momento tomar una imagen y está optimizado para hacerlo en milisegundos.

### **Completa Automatización de Passwords.**

1. One Touch Logon. U.are.U 4000 PRO asegura/impide el acceso a las computadoras Windows con un toque del dedo en el sensor al momento de iniciar la operación de Windows. Asegura también que el sistema Windows sea protegido contra accesos indebidos al desbloquear la estación con la huella.
2. One Touch Sign On. Acceso a cualquier aplicación WIN32 cliente-servidor y aplicaciones Java con un toque del dedo en el sensor, enviando el usuario y password de la aplicación al aplicar la huella.
3. One Touch Crypto. Cifrar/descifrar archivos a 128 bits con la huella dactilar.
4. One Touch Internet. Acceso a aplicaciones tipo Web (Intranet/Internet) transmitiendo el usuario y password de la aplicación al aplicar la huella en el sensor.



### III. CLASE EMPRESARIAL.

El sistema biométrico debe tener un fuerte nivel de madurez empresarial, con herramientas útiles para usuarios y administradores. Debe trabajar en diversos ambientes y ser intuitivo en su uso.

#### Fácil para administradores.

*Los administradores necesitan herramientas que provean una buena solución con poca configuración requerida, que puedan utilizarse en su ambiente.*

1. Utilizar la base de datos de Windows existente. No se necesitan crear o mantener nuevas bases de datos. La base de datos de PRO utiliza la actual de Windows. Todos los permisos y configuraciones son soportados por PRO.
2. Administración central. El Servidor PRO permite a los usuarios controlar todas las funciones de la red desde una consola central, incluyendo cómo se enrolan los usuarios, cómo la utilizan y cómo se autentifican en el sistema.
3. Políticas adecuables. PRO incluye una herramienta que puede crear de forma sencilla políticas de autenticación de credenciales para todo dominio, Workstation o usuario individual.
4. Herramientas de implementación remota. Las estaciones de trabajo de PRO pueden ser instaladas remotamente desde la consola de administración.

#### Fácil para los usuarios finales.

*Los usuarios deben encontrar el sistema fácil de usar. Esto ayuda en una aceptación rápida y menores solicitudes de asistencia, haciendo una implementación muy manejable.*

1. Wizards gráficos. El usuario interactúa con el sistema con interfaces gráficas simples.
2. Herramientas de drag and drop. Los passwords pueden ser reemplazados por herramientas de drag and drop.
3. Soporte a aplicaciones de Windows y de Internet. Cualquier aplicación que requiera de usuario y password puede ser soportada.

#### Integración con Active Directory de Microsoft.

1. Aprovecha la infraestructura actual de autenticación de Active Directory del cliente. Una sola administración de seguridad al utilizar las facilidades de AD, evita la duplicidad de funciones de seguridad.
2. Balanceo de cargas basado en AD.
3. Base de datos de AD. El sistema biométrico debe integrarse a la estructura de base de datos de Active Directory.
4. Organización y políticas. Debe aprovechar la organización y políticas de Active Directory. Integrado a las Políticas de Grupo de AD, sin consolas adicionales ni doble administración de base de datos.
5. Herramientas de administración. Basadas en AD de Microsoft como Microsoft Management Console y en políticas estándar de Windows.
6. Facilidad de utilizar password random. Cada vez que el usuario inicie sesión con su huella, el servidor le genera un password aleatorio robusto (mayúsculas, min, especiales, números, etc) de 256 caracteres.
7. Seguridad de los objetos de la huella. El agregar y borrar dedos es administrado centralmente por un administrador de seguridad.
8. Identity Lockbox. PRO automáticamente almacena y mantiene las credenciales de logon de un usuario (p.e. nombre de usuario y password) para cada aplicación que acceda, creando así un "Identity Lockbox" dentro de Active Directory que es protegido por su huella dactilar.
9. Single Action Shut Off. Habilidad que tiene el administrador para borrar el acceso de un usuario a todas las aplicaciones utilizando el DP PRO Identity Lockbox dentro de Active Directory.