Biometría.

¿Identificación o credencial?

V Jornadas Reconocimiento Biométrico de Personas.

Huesca, 2-3 de septiembre de 2010

somos
tecnología
y explotación

BBVA
Tecnología
y Operaciones

Objetivo

BBVA Tecnología y Operaciones

Compartir las expectativas y experiencias del sector financiero.

BBVA
Tecnología y Operaciones

Identificar a clientes y empleados de forma natural, sin necesidad de que haya un intercambio explícito de credenciales de acceso

BBVA
Tecnología y Operaciones

Escasas y poco prometedoras …

Analicemos la situación actual …

BBVA Tecnología y Operaciones

La utilidad fundamental de la identificación de los usuarios, cuando acceden a los sistemas, es evitar el fraude o, más genéricamente, los comportamientos desleales.

BBVA Tecnología y Operaciones

Vamos a revisar distintas situaciones…

BBVA Tecnología y Operaciones

Caso 1: Cliente que va a hacer una operación de ventanilla.

- Debe decirle al empleado de ventanilla quién es. Proceso de identificación del cliente.
- Si la operación lleva algún tipo de riesgo debe demostrarle, mediante el DNI, que realmente es quien dice ser. Proceso de validación de la credencial del cliente.

BBVA Tecnología y Operaciones

Caso 2: Cliente que va a hacer una operación en el ATM.

- Debe decirle al ATM quién es. Para ello introduce la tarjeta en el ATM. Proceso de identificación del cliente.

- Si la operación lleva algún tipo de riesgo debe demostrarle, mediante el PIN, que realmente es quien dice ser. Proceso de validación de la credencial del cliente.

BBVA Tecnología y Operaciones

Caso 3: Cliente que va a hacer una operación en la Banca por Internet.

- Debe decirle a la aplicación web quién es. Para ello teclea el código de usuario en la aplicación web. Proceso de identificación del cliente.
- Si la operación lleva poco riesgo debe demostrarle, mediante la clave de acceso, que realmente es quien dice ser. Proceso de validación de la credencial del cliente.
- Si la operación lleva más riesgo debe haber una demostración más compleja de suplantar.

BBVA Tecnología y Operaciones

Caso 4: Empleado que va a hacer una operación en los sistemas el banco.

- Debe decirle a la aplicación quién es. Para ello teclea su usuario en la aplicación. Proceso de identificación del empleado.
- Debe demostrar, mediante la contraseña, que realmente es quien dice ser. Proceso de validación de la credencial de empleado.

BBVA
Tecnología y Operaciones

Caso 5: Empleado que ha olvidado su contraseña.

- Debe decirle a la aplicación quién es. Para ello teclea su usuario en la aplicación. Proceso de identificación del empleado.
- Debe demostrar, ahora sin contraseña, que realmente es quien dice ser. Proceso complejo de validación del empleado sin credencial.

Biometría. ¿Identificación o credencial?
Análisis de los casos de uso

BBVA Tecnología y Operaciones

Caso 1	Utilidad principal	Identificación	Credencial	Riesgo evitado	Volumen de población aplicable Poca Mucha
Operación de cliente en ventanilla	Mejora de procesos				

Análisis

- El interés fundamental en este caso estaría en conseguir que cuando se acerca el cliente a la ventanilla, el empleado que tiene que atenderle ya tuviera sus datos en pantalla.
- En este sentido su aplicación fundamental sería la identidad.
- Podría aplicarse como credencial a operaciones de muy poco riesgo.
- No puede aplicarse a operaciones de riesgo. Debería existir una credencial independiente.
- Se utilizarían técnicas de biometría facial no colaborativa.
- Su utilidad fundamental es la mejora del proceso de atención del cliente en oficina.
- Hay que preseleccionar la población, por ejemplo, clientes habituales de cada oficina.

Biometría. ¿Identificación o credencial?
Análisis de los casos de uso

BBVA Tecnología y Operaciones

Variante Caso 1	Utilidad principal	Identificación	Credencial	Riesgo evitado	Volumen de población aplicable Poca Mucha
Operación de cliente en ventanilla	Seguridad				

Análisis

- El interés fundamental en este caso estaría en conseguir que cuando se acerca el cliente va a cerrar una operación que tenga riesgo pueda demostrarle biométricamente al empleado del banco que es quién dice ser.
- En este sentido su aplicación fundamental sería la mejora de la seguridad del proceso.
- Exige un proceso previo de alta en el servicio de identidad biométrica.
- Podría utilizarse reconocimiento facial o lectura de huella digital.
- Puede aplicarse a todo cliente al que previamente se le haya dado de alta en el sistema biométrico.
- Al ser un proceso asistido por el empleado no requiere un nivel de exigencia alto en cuanto a falsos positivos o falsos negativos.

Biometría. ¿Identificación o credencial?
Análisis de los casos de uso

BBVA Tecnología y Operaciones

Caso 2	Utilidad principal	Identificación	Credencial	Riesgo evitado	Volumen de población aplicable Poca Mucha
Operación de cliente en ATM	Mejora de procesos	✓	✗	↓	

Análisis

- El interés fundamental en este caso estaría en conseguir que cuando se acerca el cliente al ATM, este le pueda identificar sin necesidad de tarjeta.
- En este sentido su aplicación fundamental sería la identidad.
- Podría aplicarse como credencial a operaciones de muy poco riesgo. Disposición de efectivo limitado.
- El nivel de exigencia en falsos positivos debería estar en el 100% y falsos negativos debería ser altísimo.
- Se utilizarían técnicas de biometría facial colaborativa o huella digital.
- Su utilidad fundamental es la mejora del proceso de atención del cliente en el ATM y permitirle operar sin tarjeta.

Biometría. ¿Identificación o credencial?
Análisis de los casos de uso

BBVA Tecnología y Operaciones

Variante Caso 2	Utilidad principal	Identificación	Credencial	Riesgo evitado	Volumen de población aplicable Poca Mucha
Operación de cliente en ATM	Seguridad				

Análisis

- El interés fundamental en este caso estaría en conseguir que cuando un cliente se ha identificado en el ATM, con su tarjeta, pueda cerrar una operación sin teclear el PIN.
- En este sentido su aplicación fundamental sería la seguridad.
- Podría aplicarse a todas las operaciones que ahora exigen PIN.
- El nivel de exigencia en falsos positivos y falsos negativos debería ser muy alto.
- Se utilizarían técnicas de biometría facial colaborativa o huella digital.

Biometría. ¿Identificación o credencial?
Análisis de los casos de uso

BBVA Tecnología y Operaciones

Caso 3	Utilidad principal	Identificación	Credencial	Riesgo evitado	Volumen de población aplicable Poca Mucha
Acceso de cliente en Banca por Internet	Mejora de Procesos y Seguridad	✓	✓	↑	

Análisis

- El interés fundamental en este caso estaría en conseguir que el cliente pudiera acceder a sus cuentas por Internet sin necesidad de teclear ni su usuario ni su contraseña.
- En este sentido su aplicación combina la identidad con la sustitución de la primera clave de acceso.
- Podría aplicarse como credencial a operaciones de poco riesgo. Por ejemplo, operaciones predefinidas contra cuentas preexistentes.
- El nivel de exigencia en falsos positivos debería estar en el 100% y falsos negativos debería ser altísimo.
- Se utilizarían técnicas de biometría facial colaborativa preferiblemente, aunque podría utilizarse huella digital.
- Debe analizarse el nivel de seguridad ante problemas de predictibilidad y reinyección. Deben diseñarse contramedidas específicas.

No recomendable:

- **Aplicable a poblaciones pequeñas**
- **Impacto altísimo de un error en la identificación**

Biometría. ¿Identificación o credencial?
Análisis de los casos de uso

BBVA Tecnología y Operaciones

Variante Caso 3	Utilidad principal	Identificación	Credencial	Riesgo evitado	Volumen de población aplicable Poca Mucha
Acceso de cliente en Banca por Internet	Seguridad	✗	✓	↑	

Análisis

- El interés fundamental en este caso estaría en conseguir que el cliente pudiera acceder a sus cuentas por Internet tecleando su usuario sin necesidad de teclear su contraseña.
- Podría aplicarse como credencial a operaciones de poco riesgo. Por ejemplo, operaciones predefinidas contra cuentas preexistentes.
- El nivel de exigencia en falsos positivos y falsos negativos debería ser muy alto.
- Se utilizarían técnicas de biometría facial colaborativa preferiblemente, aunque podría utilizarse huella digital.
- Debe analizarse el nivel de seguridad ante problemas de predictibilidad y reinyección. Deben diseñarse contramedidas específicas.

Biometría. ¿Identificación o credencial?
Análisis de los casos de uso

BBVA Tecnología y Operaciones

Caso 4	Utilidad principal	Identificación	Credencial	Riesgo evitado	Volumen de población aplicable Poca Mucha
Acceso de empleados	Seguridad	✓	✓	↑	

Análisis

- El interés fundamental en este caso estaría en conseguir que el empleado pudiera acceder a los sistemas sin necesidad de teclear su usuario ni su contraseña.
- En este sentido su aplicación combina la identidad con la sustitución de la primera clave de acceso.
- El nivel de exigencia en falsos positivos debería estar en el 100% y falsos negativos debería ser altísimo.
- No se puede aplicar a grandes colectivos.
- Se utilizarían técnicas de biometría facial colaborativa preferiblemente, aunque podría utilizarse huella digital.
- Debe analizarse el nivel de seguridad ante problemas de predictibilidad y reinyección. Deben diseñarse contramedidas específicas. En este caso el riesgo específico es mucho menor que en caso del acceso a Internet.

No recomendable:

•Impacto altísimo de un error en la identificación

Biometría. ¿Identificación o credencial?
Análisis de los casos de uso

BBVA Tecnología y Operaciones

Variante Caso 4	Utilidad principal	Identificación	Credencial	Riesgo evitado	Volumen de población aplicable Poca Mucha
Acceso de empleados	Seguridad				

Análisis

- El interés fundamental en este caso estaría en conseguir que el empleado pudiera acceder a los sistemas tecleando su usuario y sin teclear su contraseña.
- El nivel de exigencia en falsos positivos es alta. La exigencia en falsos negativos sí es muy alta.
- Se utilizarían técnicas de biometría facial colaborativa preferiblemente, aunque podría utilizarse huella digital.
- Debe analizarse el nivel de seguridad ante problemas de predictibilidad y reinyección. Deben diseñarse contramedidas específicas. En este caso el riesgo específico es mucho menor que en caso del acceso a Internet.
- Podría utilizarse como sistema para desactivar el salvapantallas y para evitar que se active.

Biometría. ¿Identificación o credencial?
Análisis de los casos de uso

BBVA Tecnología y Operaciones

Caso 5	Utilidad principal	Identificación	Credencial	Riesgo evitado	Volumen de población aplicable Poca Mucha
Reactivación de la contraseña	Mejora del Proceso y Seguridad	✗	✓	↑	

Análisis

- El interés fundamental en este caso estaría en conseguir que el empleado pudiera cambiar su contraseña sin necesidad de recordarla.
- Es una alternativa a los nunca bien afinados procesos de reactivación de contraseñas.
- El nivel de exigencia en falsos positivos es alta. La exigencia en falsos negativos sí es muy alta.
- Se utilizarían técnicas de reconocimiento de voz preferiblemente, aunque también podrían utilizarse biometría facial colaborativa y huella digital.

Biometría. ¿Identificación o credencial?

Resumen del análisis de los casos de uso

BBVA Tecnología y Operaciones

	Mejora del proceso	Seguridad	Identificación	Credencial de poco riesgo	Credencial de riesgo	Riesgo evitado	Población objetivo	Población preseleccionada	Proceso asistido	Reconocimiento facial no colaborativo	Reconocimiento facial colaborativo	Reconocimiento de huella digital	Reconocimiento de voz	Alta previa	Falsos positivos	Falsos Negativos	Control predictibilidad y reinyección
C1.- Operación de cliente en ventanilla	✓	✗	✓	✓	✗	↓	↓	✓	✓	✓	✗	✗	✗	✗	4/5	3/5	✗
Variante Caso 1	✗	✓	✗	✓	✓	↑	↑	✗	✓	✗	✓	✓	✗	✓	4/5	3/5	✗
C2.- Operación de cliente en ATM	✓	✗	✓	✓	✗	↓	↓	✓	✗	✗	✓	✓	✗	✓	100 %	5/5	✗
Variante Caso 2	✗	✓	✗	✓	✓	↑	↑	✗	✗	✗	✓	✓	✗	✓	4/5	4/5	✗
C3.- Acceso de cliente por Internet	✓	✓	✓	✓	?	↑	↓	✓	✗	✗	☑	✓	✗	✓	100 %	5/5	✓
Variante Caso 3	✗	✓	✗	✓	✗	↑	↑	✗	✗	✗	☑	✓	✗	✓	4/5	4/5	✓
C4.- Acceso de empleados	✓	✓	✓	✓	✓	↑	↑	?	✗	✗	☑	✓	✗	✓	100 %	5/5	✓
Variante Caso 4	✗	✓	✗	✓	✓	↑	↑	✗	✗	✓	☑	✓	✗	✓	4/5	5/5	✓
C5.- Reactivación de la contraseña de empleados	✓	✓	✗	✓	✓	↑	↑	?	✗	✓	✓	✓	☑	✓	4/5	5/5	✗

Conclusiones

BBVA Tecnología y Operaciones

1.- Cuando se utiliza la biometría como elemento de identificación del cliente:

- **Se hace por razones de mejoras de los procesos**
- **No puede aplicarse a colectivos grandes**
- **No mejora la seguridad sustancialmente**

2.- No puede utilizarse el mismo elemento biométrico como identificador y como credencial, ya que la población objetivo es reducida y el impacto ante un error potencial de identificación es altísimo.

Posibles vías de investigación y mejoras (I de II)

BBVA Tecnología y Operaciones

1.- Para los casos **3 y 4 no recomendados (que son el acceso a Internet sin usuario ni contraseña y el acceso de empleados a los sistemas sin utilizar el usuario y la contraseña)** puede trabajarse en la posibilidad de obtener de forma combinada la probabilidad de ser el sujeto "A" y la probabilidad del segundo candidato "B".

Si las diferencias no son importantes debería denegarse la identidad.

2.- Hay que mejorar el proceso de alta de los datos biométricos del usuario.

Posibles vías de investigación y mejoras (II de II)

BBVA Tecnología y Operaciones

3.- Hay que explorar la identidad electrónica del usuario, ligando la biometría con los hábitos y comportamiento del usuario.

- **El objetivo es mejorar la capacidad de los sistemas de identificar los usuarios.**
- **Como implantadores de soluciones, necesitamos sistemas de identificación de usuarios que incorporen la biometría como un elemento más. No compramos sistemas biométricos, compramos sistemas de identificación de usuarios.**

Muchas gracias

V Jornadas Reconocimiento Biométrico de Personas.

Huesca, 2-3 de septiembre de 2010

somos
tecnología
y explotación

BBVA
Tecnología
y Operaciones