



# Cifrado punto a punto en HTML5 con KHTML



Bilbao, Mayo 2010

Eduardo Robles Elvira

[edulix@gmail.com](mailto:edulix@gmail.com)

<http://blog.edulix.es>

KDE España



**Introducción**



## **Seguridad vs. Privacidad**



Introducción



**Seguridad:**  
Es un estado mental  
**me siento seguro**



Introducción



**Privacidad:**  
Parábola de la cerveza, y el servicio



**Seguridad en el Escritorio**



## **Seguridad en el Escritorio: Ejemplos**



## Kmail cliente de correo con cifrado PGP

N  
o  
H  
T  
M  
L  
M  
e  
s  
s  
a  
g  
e

**Encryption in KMail**

**From:** Oliver White <[redacted]>  
**To:** [redacted]  
**Date:** Today 14:36:38

**Encrypted message**

**Message was signed by Oliver White <[redacted]> (Key ID: 0xE1AF37A1).  
The signature is valid and the key is ultimately trusted.**

This message is encrypted and signed, but KMail will automatically decrypt it and check the signature once it's asked for the password. Encrypting the email is as simple as clicking on the padlock button before sending the mail, and signing the email is done in a similar way.

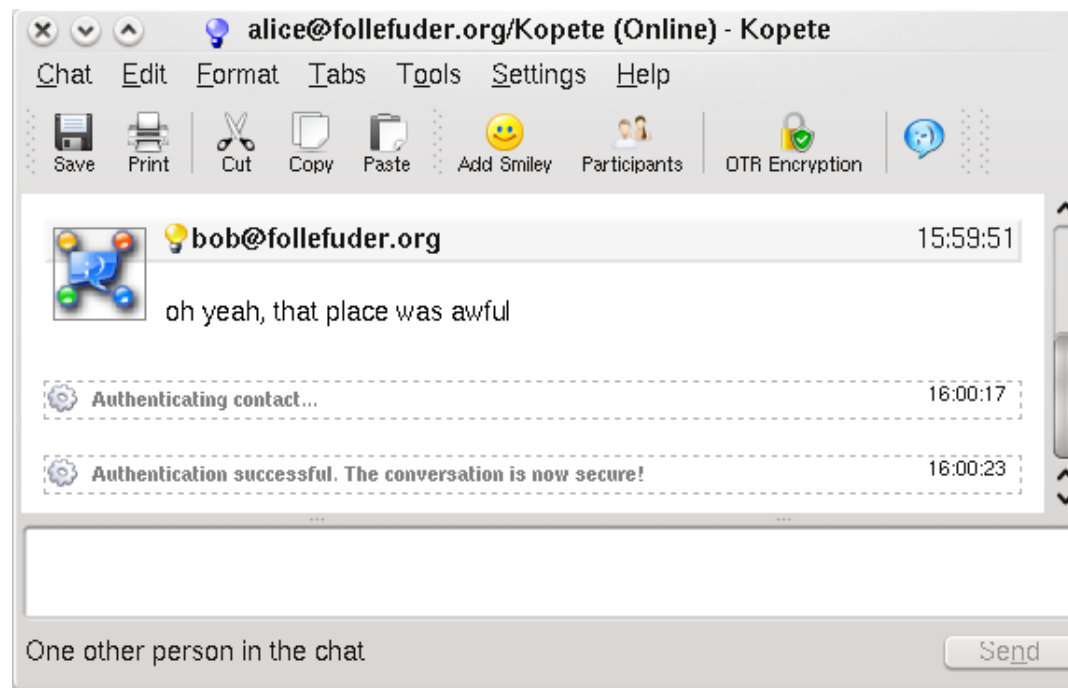
KMail can use GnuPG as its encryption program, and GnuPG itself is capable of importing keyrings from PGP. KMail comes with simple tools to select keys from your keyring, for choosing who to encrypt to, or for selecting your own private key.

**End of signed message**

**End of encrypted message**

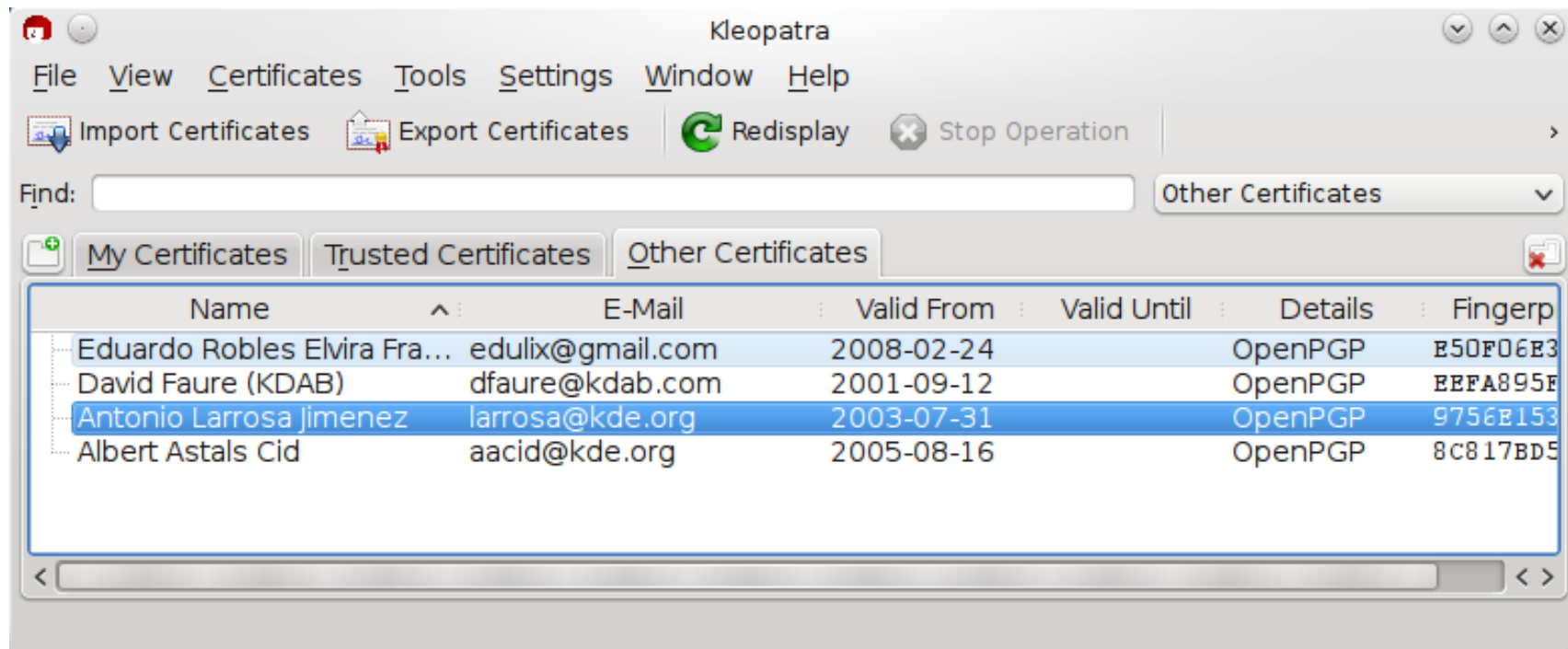


## Kopete OTR





## Administrador de certificados







**Seguridad en la web**



## **Seguridad en la web:**

**https, SSL  
Banca electrónica  
Compras  
Firmas digitales**



Seguridad en la web



**¿cual es la diferencia?**

**Cifrado punto a punto**

**VS**

**Cifrado cliente servidor**



## Hushmail

- Ejemplo de cifrado punto a punto
- state of the art
- Almacena los datos cifrados
- demo



## Problemas con Hushmail

- **Confiar en el servidor**
- **Cifrado en cliente mediante java/javascript**
- **Recomiendan clientes no-web**
- **NSA**



**Solución**



**La solución es clara:**  
Implementar cifrado punto a punto...  
**directamente en el navegador**



Solución



- **Evolución de https:**
  - misma estrategia, integración con el navegador
- **Independencia del servidor:**
  - el usuario recupera el poder sobre sus datos



- **Google vs. privacy**
- **Aplicaciones web 2.0 beta**
  - **Gmail**
  - **Gtalk**
  - **...**



- **Pequeña extensión de HTML**

- `<input type="text" name="field" encryption="gpg" encryption-key="6C1F5316"/>`
- `<div encryption="gpg">ciphertext</div>`





Implementación



- **Demo!!**

- 1.**HTML

- 2.**Konqueror

- 3.**Explicar características de seguridad



- **Proof of concept**

- **No presentado al W3C**
- **Sólo GPG en modo texto**
- **Habría que usar xhtml serialization y XML Signature**



**Implementación**



- **Futuro**

- **Webkit**
- **Webapps html5**
- **Public-html5 mailling list**
- **PGP 1999**



Preguntas



- Preguntas





**Bonus**



- **KHTML**

- **Parser**
- **Dom vs. impls**
- **Widgets pintados fuera de pantalla**
- **DIV: problemática**



Licencia



**Transparencias bajo Licencia CC-by-sa 3.0**  
**<http://creativecommons.org/licenses/by-sa/3.0/>**