Cifrado punto a punto en HTML5 con KHTML

Bilbao, Mayo 2010

Eduardo Robles Elvira

edulix@gmail.com

http://blog.edulix.es

KDE España

Seguridad vs. Privacidad

Eduardo Robles Elvira <edulix@gmail.com>,2010

Seguridad:

Es un estado mental

me siento seguro

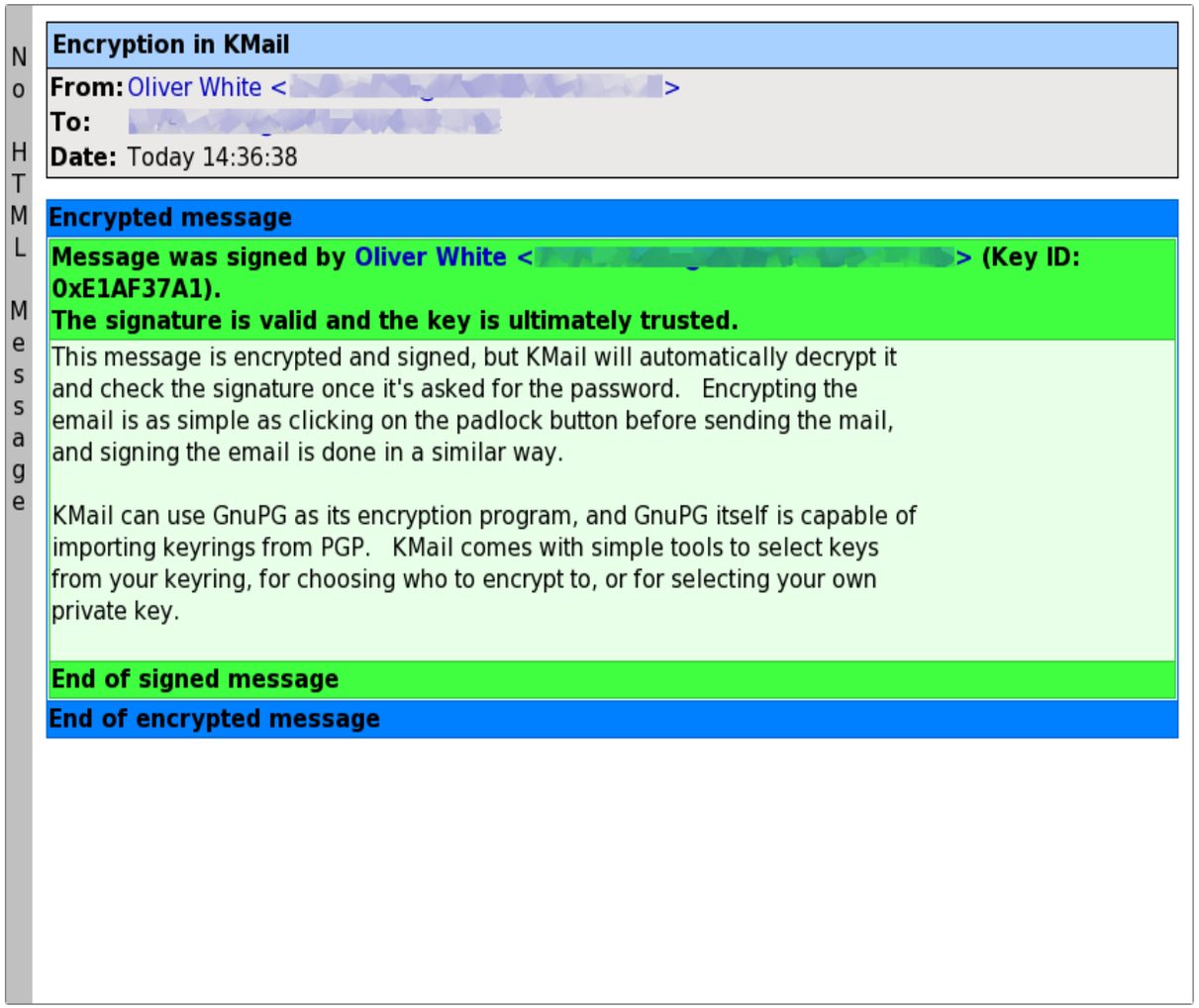
Privacidad:
Parábola de la cerveza, y el servicio

Eduardo Robles Elvira <edulix@gmail.com>,2010

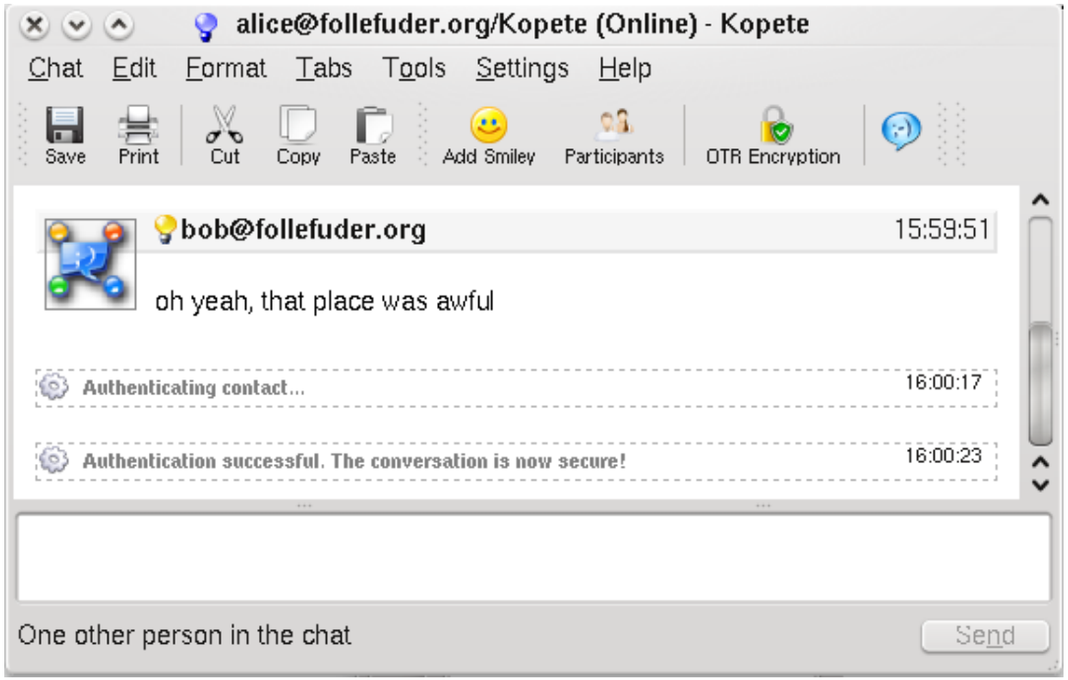
Seguridad en el Escritorio: Ejemplos

Eduardo Robles Elvira <edulix@gmail.com>,2010

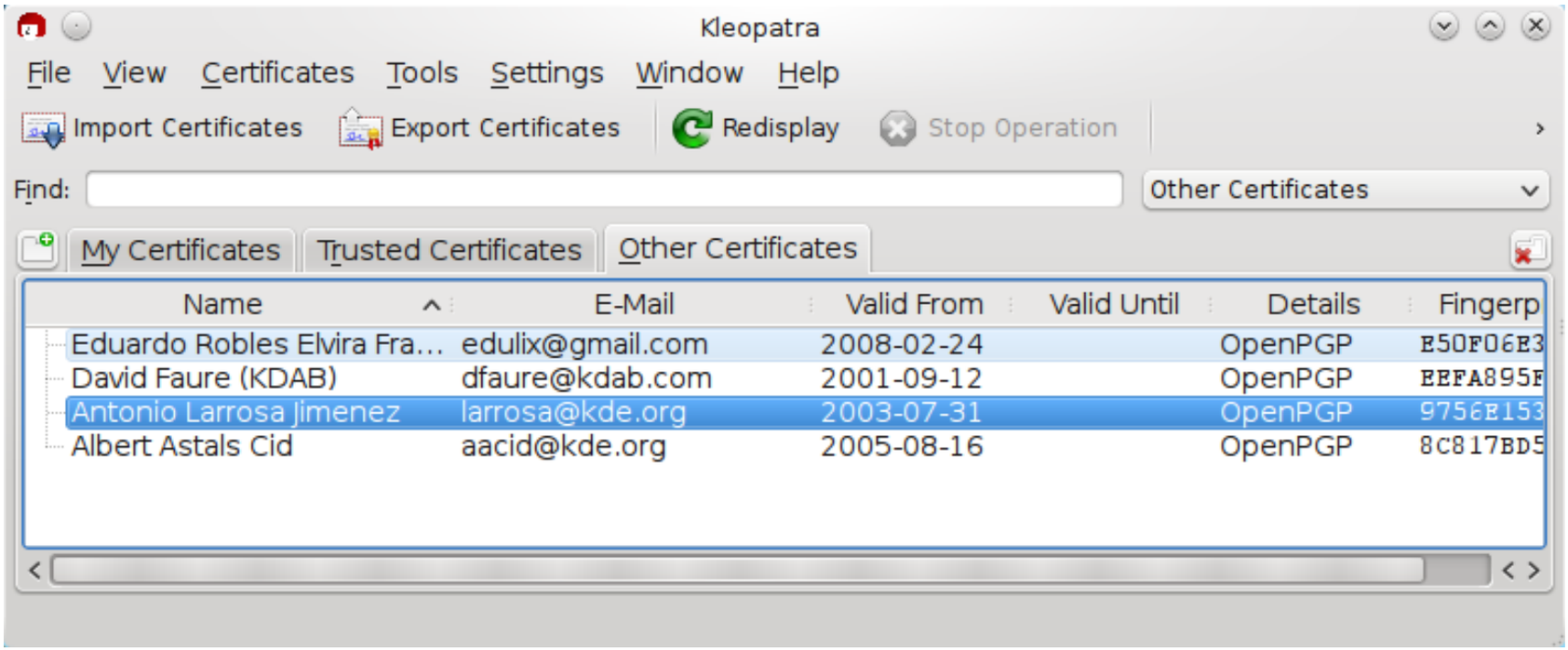
Kmail cliente de correo con cifrado PGP



Kopete OTR


alice@follefuder.org/Kopete (Online) - Kopete
Chat Edit Format Tabs Tools Settings Help
Save Print Cut Copy Paste Add Smiley Participants OTR Encryption
bob@follefuder.org 15:59:51
oh yeah, that place was awful
Authenticating contact... 16:00:17
Authentication successful. The conversation is now secure! 16:00:23
One other person in the chat
Send

Administrador de certificados



Seguridad en la web:

https, SSL
Banca electrónica
Compras
Firmas digitales

Eduardo Robles Elvira <edulix@gmail.com>,2010

¿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

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**

Aplicaciones web

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

- **Pequeña extensión de HTML**
  - **<input type="text" name="field" encryption="gpg" encryption-key="6C1F5316"/>**
  - ** ciphertext **

Implementación

- **Demo!!**
  1. **HTML**
  2. **Konqueror**
  3. **Explicar características de seguridad**

Implementación

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

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

Preguntas

- **Preguntas**

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

Licencia

Eduardo Robles Elvira <edulix@gmail.com>,2010