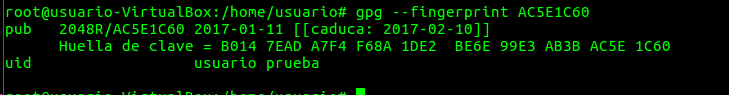


|  |  |
| --- | --- |
| **SEGURIDAD INFORMÁTICA** – 2º SMR | |
| UT5: Sistemas de identificación. Criptografía. | Práctica 4: PKI. |
| Nombre: | |
| Nota: | Observaciones: |

1. Por último vamos a utilizar la firma para garantizar que una clave pública pertenece realmente a quién dice pertenecer:
   1. Averigua cuál es el comando para obtener la huella dactilar/hash/fingerprint/resumen de la clave pública.

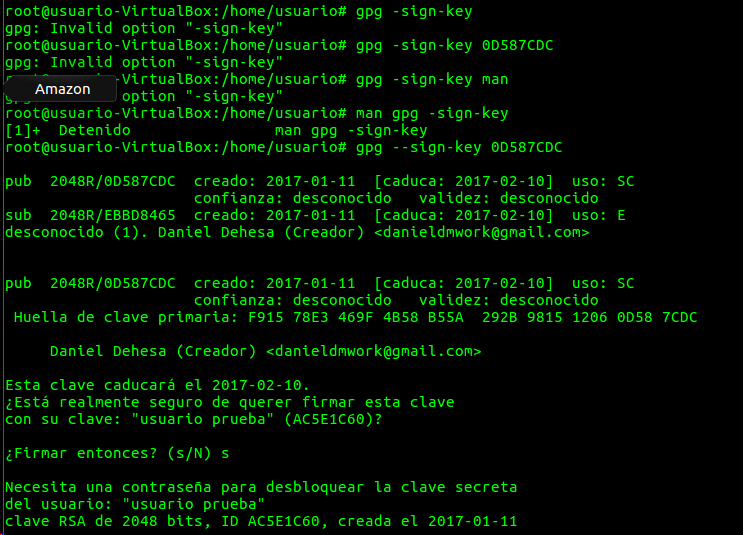


* 1. Obtén la huella de tu clave pública. Alguno de tus compañeros que use tu clave, deberá obtener la huella. Comprobad que ambos obtenéis el mismo valor. Esto garantizará la veracidad de la clave pública.



Dani tiene la misma clave que yo

* 1. Ahora tú podrás firmar la clave pública de tu compañero utilizando la opción –sign-key de gpg sobre su key. Haz dicha firma.



* 1. ¿Qué clave has tenido que utilizar para realizar la firma de la clave pública de tu compañero?

Su clave pública 

* 1. Explica el concepto Web Of Trust.

Herramienta de navegación segura en internet. Su sistema consiste en un semáforo que muestra las reputaciones de las páginas web. La información se basa principalmente en las valoraciones de la comunidad y en los fuentes de confianza, como las listas de sitios de suplantación de identidad

Date cuenta que tú has verificado que la clave pública pertenece realmente a tu compañero, con lo cual has verificado su validez. Por esa razón tienes autoridad para firmar su clave pública y podrás distribuir su clave a otros que la puedan necesitar. Lee este pequeño artículo y explica que tiene que ver con esto que acabamos de hacer <http://eventos.barrapunto.com/eventos/11/10/01/148217.shtml>