Fortalecimiento del llavero de confianza en un proyecto geográficamente distribuido

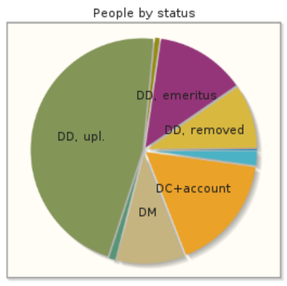
Gunnar Eyal Wolf Iszaevich
Desarrollador del Proyecto Debian
gwolf@debian.org

El proyecto Debian

- Proyecto de desarrollo de software libre, de ámbito mundial
- Más de 5400 personas han contribuido con el proyecto en sus 22 años: https://contributors.debian.org/contributors/flat
- Estratificación de la participación: *contribuidor* (participación no formal), *mantenedor (*responsable de uno o varios paquetes), *desarrollador* (miembro pleno del proyecto)
- Participación voluntaria (no corporativa, siempre a título individual)
- A octubre de 2015: 406 contribuidores, 233 mantenedores, 1005 desarrolladores

Participación en Debian

- Produce una de las distribuciones de Linux más empleadas del mundo
  - Incluyendo distribuciones derivadas (Ubuntu, Mint, Kali, etc.) cubre más del 50% de las instalaciones de Linux: http://w3techs.com/technologies/history_details/os-linux
- Alta responsabilidad del proyecto sobre las acciones de sus participantes («*¡Tengo root en millones de computadoras!*»)
- Contrato social ⇒ https://www.debian.org/social_contract
- Necesidad de vinculación fuerte persona ⇔ cuenta



https://nm.debian.org/public/stats/

Los llaveros que definen la participación en Debian

- La participacíón en (varias áreas de) Debian está limitada por el firmado de la misma por una llave OpenPGP que pertenezca a uno de los *llaveros de confianza* establecidos del proyecto
- Esquema de establecimiento de identidad: Anillo de confianza sujeto a un proceso de *curaduría*
  - *Curadores*: Equipo *keyring-maint*
  - Debería guardar relación 1:1 con la participación formal en el proyecto
  - Una de las misiones del equipo: Asegurar que los llaveros se mantengan al día ante retos y amenazas a los esquemas de cifrado asimétrico

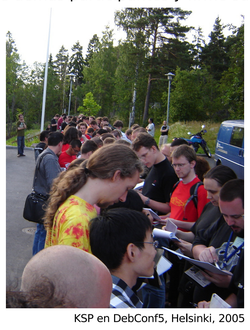
Prácticas culturales: Las fiestas de firmado de llaves (Key-Signing Parties, KSP)

Dado que el nivel de confianza en la identidad de un participante es dado por las firmas que cruza con otros, particularmente en un proyecto con amplia dispersión geográfica, se han popularizado las KSP.

En una KSP, se busca que cada participante verifique la identidad de todos los demás participantes y firme sus certificados.

Las KSP normalmente siguen el protocolo Sassaman-Zimmerman (Sassaman 2006). La verificación debe ser suficientemente confiable para satisfacer los requisitos de cada uno de los participantes — Por la misma naturaleza del modelo, no puede haber lineamientos globales; típicamente se solicita que los participantes verifiquen la identidad de cada interlocutor corroborando un documento oficial emitido por su gobierno local.

Si bien las KSPs (particularmente dentro del proyecto Debian) tienden a celebrarse en un marco de confianza, se ha demostrado que requieren también de una verificación minuciosa: Ante la prueba de un desarrollador bien conocido personalmente por el proyecto de emplear una identificación falsa (una tarjeta de identidad con gran similitud con las de la Unión Europea, emitida por la inexistente República Transnacional), una larga discusión, esta prueba llevó a replantear el manejo de las KSPs en grupos grandes (Srivastava 2006).



KSP en DebConf5, Helsinki, 2005

Distintos modelos de establecimiento de identidad

Infraestructura de llave pública (PKI)

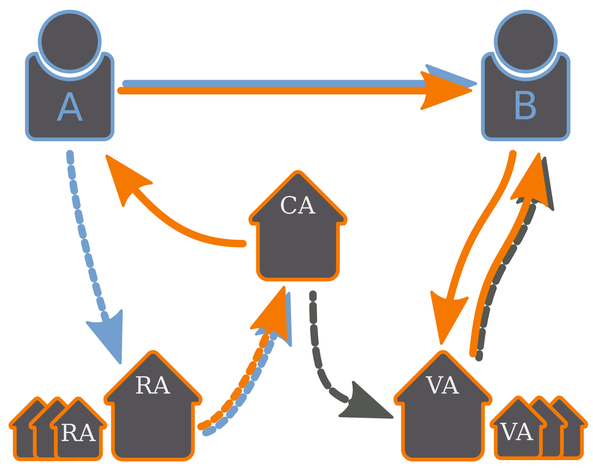
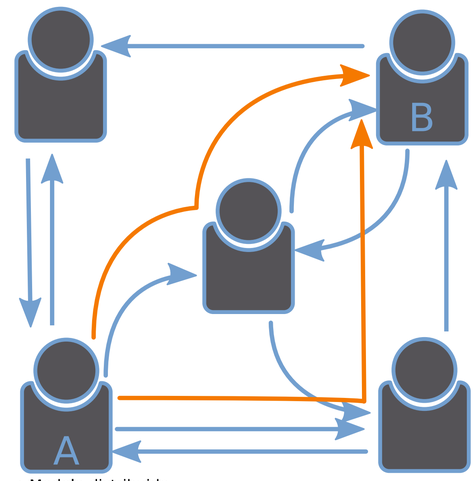


Imagen: Wikipedia
Public Key Infrastructure

- Modelo centralizado
- Dependiente de un conjunto de autoridades certificadoras
  - Establece *confianza última* en las CAs para un sistema dado
- Cada certificado es firmado por una *única* CA
- Estándar de la industria, particularmente relevante por TLS/SSL (RFC 5246)
  - Presente en todos los navegadores Web, adecuable a cualquier comunicación TCP/IP
- Estándar de certificados X.509 (RFC 5280)

Anillo de Confianza (WoT)



- Modelo distribuido
- Cada entidad participante puede *validar* la entidad de otros participantes
  - No indica confianza en la entidad misma, sino en su *identidad*
- Un conjunto de participantes se constituye en una red denominada *llavero*
- Todo certificado puede ser firmado por cualquier cantidad de otras entidades
  - La confianza se establece de forma *transitiva*
  - Varias métricas para establecer la confianza (McBrunett 1997, Cederlöf 2004, Penning 2004, Penning 2015)
- Estándar de certificados y comunicación OpenPGP (RFC 4880)

Diferencias entre Wot y PKI al plantear una migración forzosa de certificados

- Una AC en PKI puede mandatar la migración a certificados con determinada fuerza criptográfica dada en un plazo dado:

(3) Subscriber Certificates

	Validity period ending on or before 31 Dec 2013	Validity period ending after 31 Dec 2013
Digest algorithm	SHA1*, SHA-256, SHA-384 or SHA-512	SHA1*, SHA-256, SHA-384 or SHA-512
Minimum RSA modulus	1024	2048

CA / Browser Forum Baseline Requirements, v. 1.1.8 (as of 5 June 2014)

- La motivación para que un cliente de PKI renueve su certificado es *directa y económica*
  - No contar con un certificado le impedirá realizar transacciones
- Los participantes de Debian *benefician* al proyecto con su trabajo
  - *El proyecto* es el principal interesado en contar con certificados al día de todos los desarrolladores
  - Un desarrollador sin un certificado válido y acorde con los estándares del proyecto ve limitado o entorpecido su trabajo
  - Si bien hay cientos de desarrolladores en determinados países o regiones centrales, hay decenas en regiones con baja densidad
  - No todo desarrollador participa del *entorno social* del proyecto
  - Aspecto social: Los desarrolladores *tienen derecho* a participar en el proyecto

⇒ Plantear un proceso que *bloquee efectivamente* la participación de un amplio número de desarrolladores se arriesga a un fuerte rechazo

¿Por qué ya no es suficiente 1024R?

Table 7.2: Key-size Equivalence.

Security (bits)	RSA	DLOG		EC
		field size	subfield	
48	480	480	96	96
56	640	640	112	112
64	816	816	128	128
80	1248	1248	160	160
112	2432	2432	224	224
128	3248	3248	256	256
160	5312	5312	320	320
192	7936	7936	384	384
256	15424	15424	512	512

Table 7.3: Effective Key-size of Commonly used RSA/DLOG Keys.

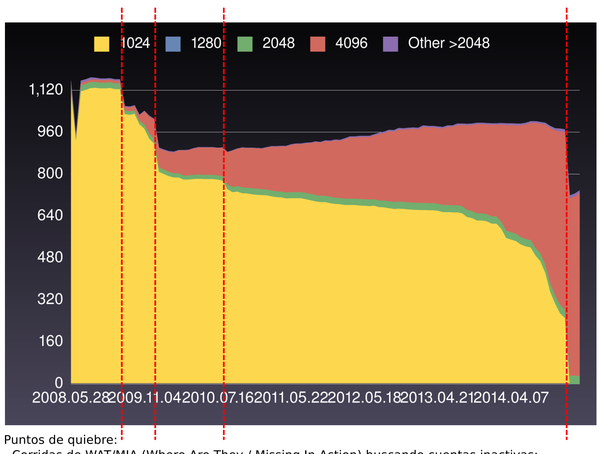
RSA/DLOG Key	Security (bits)
512	50
768	62
1024	73
1536	89
2048	103

Table 7.4: Security levels (symmetric equivalent).

Security Level	Security Protection (bits)	Comment	
1.	32	Attacks in "real-time" by individuals	Only acceptable for auth. tag size
2.	64	Very short-term protection against small organizations	Should not be used for confidentiality in new systems
3.	72	Short-term protection against medium organizations, medium-term protection against small organizations	
4.	80	Very short-term protection against agencies, long-term prot. against small organizations	Smallest general-purpose level, ≤ 4 years protection (E.g. use of 2-key 3DES, $< 2^{60}$ plaintext/ciphertexts)
5.	96	Legacy standard level	2-key 3DES restricted to $\sim 10^6$ plaintext/ciphertexts, ≈ 10 years protection
6.	112	Medium-term protection	≈ 20 years protection (E.g. 3-key 3DES)
7.	128	Long-term protection	Good, generic application-indep. recommendation, ≈ 30 years
8.	256	"Foreseeable future"	Good protection against quantum computers unless Shor's algorithm applies.

(Smart 2012)

Evolución histórica del llavero de Desarrolladores de Debian



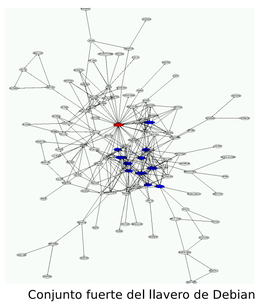
Puntos de quiebre:
- Corridas de WAT/MIA (Where Are They / Missing In Action) buscando cuentas inactivas: 23-08-2009 (38 llaves), 27-05-2008 (95 llaves)
- Remoción de las llaves PGPv3 (31-08-2010) (15 llaves)
- Remoción definitiva de llaves <2048 (01-01-2015) (287 llaves, casi 25% de los desarrolladores)

Métricas de llaves y llaveros

A lo largo del tiempo, los llaveros y las llaves que los conforman van cambiando; parte de la tarea de *keyring-maint* es asegurar que su operación se mantiene en parámetros seguros. Algunas métricas:

- **Conjunto fuerte** (strong set): El subconjunto más grande de llaves entre todas cuales hay un camino bidireccional de confianza.
- **Distancia Mínima** (Shortest Distance): Tomando dos llaves cualquiera del llavero, la longitud de la ruta más corta entre ellas. Pueden ser llaves del conjunto fuerte o de otro subconjunto — indica la cercanía entre dichas dos llaves arbitrarias.
- **Distancia Promedio Mínima** (Mean Shortest Distance, MSD): Medida frecuentemente utilizada para averiguar qué tan confiable es la identidad de un participante. Para una llave en el conjunto fuerte, el promedio de su distancia a todas las demás llaves del mismo.
  - Naturalmente, se considera la *dirección del firmado*: Una llave con bajo MSD ha recibido muchos certificados, o ha sido firmada por otras llaves con bajo MSD. Esto es independiente de cuántos certificados hayan sido hechos *por* esta llave
  - Una llave puede haber certificado a todas los demás del conjunto fuerte, sin aumentar su MSD.

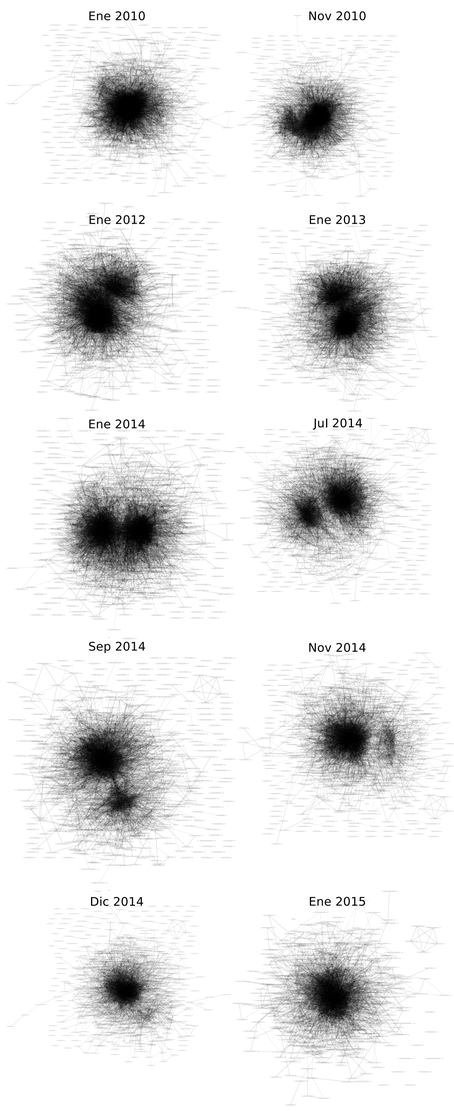
Desde que se tienen registros confiables de actividad del equipo (mayo 2008), keyring-maint ha logrado mantener el conjunto fuerte por encima del 82% del llavero total.



Conjunto fuerte del llavero de Debian en el 2000, de un universo de 119 llaves (Darxus 2002)

Relaciones de identidad: *Envejecimiento* y reestablecimiento

Si un proyecto que refleja sus relaciones de identidad en llaveros de confianza pervive en el tiempo como lo hace Debian (22 años), muchas de sus llaves pueden ir cayendo en el olvido y reflejando relaciones incorrectamente. El grafo del llavero comienza a mostrar una disociación hacia fines de 2010 (coincide con cuando inicia el esfuerzo coordinado para abandonar 1024R); esta disociación crece de forma congruente con la evolución histórica mostrada en el panel izquierdo, y para diciembre de 2014 es ya un conjunto muy tenue, lo cual indica que buena parte de las llaves eliminadas no formaban ya parte del conjunto fuerte al momento de corte.



Referencias

Brennen, V. Alex (2008). *The Keysigning Party HOWTO*. URL: http://www.cryptnet.net/fdp/crypto/keysigning_party/en/keysigning_party.html.

Callas, Jon y col. (2007). *OpenPGP Message Format*. Inf. téc. RFC 4880. Internet Engineering Task Force. URL: https://tools.ietf.org/html/rfc4880.

Cederlöf, Jörgen (2004). *Dissecting the leaf of trust*. URL: http://www.lysator.liu.se/~jc/wotsap/leafoftrust.html.

Cooper, David y col. (2008). *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. Inf. téc. RFC 5280. Internet Engineering Task Force. URL: https://tools.ietf.org/html/rfc5280.

Darxus (2002). *Graphing the Debian Keyring Web of Trust*. URL: http://www.chaosreigns.com/code/sig2dot/debian.html.

Dierks, Tim y Eric Rescorla (2008). *The Transport Layer Security (TLS) Protocol Version 1.2*. Inf. téc. RFC 5246. Internet Engineering Task Force. URL: https://tools.ietf.org/html/rfc5246.

Kahn Gillmor, Daniel, Jonathan McDowell y Gunnar Wolf (2014). *Status of the Debian OpenPGP keyring*. Debian Project. URL: https://summit.debconf.org/debconf14/meeting/11/status-of-the-debian-openpgp-keyring/.

McBurnett, Neal (1997). *PGP Web of Trust Statistics*. URL: http://bcn.boulder.co.us/~neal/pgpstat/.

Penning, Henk P. (2004). *Computing shortest paths in WOTs*. URL: http://pgp.cs.uu.nl/doc/shortest-paths-in-wots.php.

— (2015). *analysis of the strong set in the PGP web of trust*. URL: http://pgp.cs.uu.nl/plot/.

Sassaman, Len y Phil Zimmerman (2006). *Efficient Group Key Signing Method*. URL: https://web.archive.org/web/20061205200342/http://sion.quickie.net/keysigning.txt.

Smart, Nigel (2012). *ECRYPT II Yearly Report on Algorithms and Keysizes (2011-2012)*. Inf. téc. 7th Framework Programme, European Commission. URL: http://www.ecrypt.eu.org/documents/D.SPA.20.pdf.

Srivastava, Manoj (2006). *Please revoke your signatures from Martin Krafft's keys*. URL: http://lists.debconf.org/lurker/message/20060525.073637.78ce0660.en.html.