en

Event | 26.03.2014

Greens/EFA 4th Document Freedom Day in the European Parliament: Open Standards in the field of Encryption

- **FOLLOW THE EVENT LIVE FROM 13H30**

Encryption, Free Software and Open Standards in the European Parliament

About the event

Edward Snowden stated in June 2013: "Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on". This is why the Greens/EFA 4th Document Freedom Day is hosting a seminar on Free Software and Open Standards to discuss how cryptography can break the grip of the surveillance state and a workshop on trustworthy encryption in the European Parliament. The event is solution-oriented, both in terms of current efforts in different technologist communities, and in terms of concrete action, here and now, in the European Parliament.

Programme

13h30 Part I - Workshop

Trustworthy encryption in the European Parliament

Opening by **Rebecca Harms, MEP**

Workshop lead by **Jonas Smedegaard**

After reaching out to the Free Software community in July 2013, the Greens/EFA initiated a pilot project to start using email encryption in the European Parliament: 10 parliamentary workers - politically elected and staffers - are equipped with a laptop running software selected from Debian and guided in using its security features to establish trusted communication. This is the first Greens/EFA DebianParl workshop after the EPFSUG launch of the project on 5 March.

See https://wiki.debian.org/DebianParl/GreensEFA

Coffee break

14h30 Part II - Seminar and debate

Cryptography - Breaking the grip of the surveillance state

Opening by **Carl Schlyter, MEP**

Speakers:

- Werner Koch - GNUPG
- Karen O'Donoghue - ISOC
- Joachim Strömbergson - SECWORKS
- Amaelle Guiton - SLATE

End - 16h00

Additional info

For further information see text below and the following pages:

- Campaign site http://documentfreedom.org/

- Planning pad https://icg.greens-efa.eu/p/DFD2014
- DebianParl wiki https://wiki.debian.org/DebianParl
- EPFSUG homepage: http://epfsug.eu/

The Document Freedom Day campaign is dedicated to highlighting the power of Open Standards. This effort is not limited to document formats. Free speech is a human right, and a cornerstone of any democratic society. To enable communication, it is important that documents can be opened and read by the people who are meant to receive them. In today's world, it is equally important that we have the ability to ensure that documents are read *only* by the people meant to receive them, to prevent a scenario where both censorship and self-censorship degrade the ability of citizens to speak freely to each other, develop new ideas, and drive the progress of our society.

Encryption can **only** work with open standards. If encryption tools are to be considered trustworthy, their workings must be fully transparent. The encryption programs themselves need to be Free Software, so that anyone can independently assess how they work, and verify that they do not contain any defects or back doors.

The encryption *methods* are perhaps even more crucial. Cryptography as a field is developing rapidly, and the topic has long been far too complex for any one individual to comprehend it fully. The best way of dealing with this complexity is to standardise cryptographic methods.

Such standards need to be created in a process that is open to public participation and assessment; collaborative; and fully transparent. In other fields of technology, closed, proprietary methods are merely an inefficient approach. In cryptography, such methods mean that the tools relying on them cannot be audited, and are therefore considered untrustworthy. In addition, the lack of independent review of the methods used frequently leads to poor-quality programs and systems.

Open Standards in the field of encryption, on the other hand, mean that encryption tools can rely on widely accepted methods which have been extensively reviewed, criticised, and validated by experts in the field. If those encryption tools are distributed as Free Software, the tools themselves can be efficiently audited. This is not only essential to ensuring that the tools do not contain any critical mistakes or back doors. It also opens those tools up to an ongoing process of improvement.

Recommended

Press release

markus-spiske-unsplash

Digital Omnibus: Greens/EFA call for digital enforceme…

18.11.2025

Press release

Foto von Sasun Bughdaryan auf Unsplash

GDPR: MEPs to vote on faster and fairer enforcement

21.10.2025

News

pexel

PLENARY FLASH: Greens/EFA Priorities 20 to 23 October

20.10.2025

Event

Webinar: Stop Chat Control

30.09.2025

Responsible MEPs

Rebecca Harms

Member

Please share

- E-Mail