Contribution ID: **11**

Type: **not specified**

django-ca, HSM and open source contribution

Tuesday, 4 June 2024 14:15 (30 minutes)

django-ca is a feature rich certificate authority written in Python and maintained for around 10 years. As I write this talk submission, I am working with the maintainer to add HSM support to the application, so that it can be used inside of Sunet and various other security sensitive installations.

A related blog post: https://kushaldas.in/posts/django-ca-hsm-and-poc.html

Talk outline:

- Kushal's introduction
- Introduction to django-ca/ certificate authority in general
- Introduction to HSM (Hardware security module)
- Python cryptography (https://cryptography.io)
- Explanation of PrivateKey sign implementation in python cryptography
- Our privatekey implementations using HSM
- Initial proof of concept development
- Design from the upstream
- Lessons learned for the big change
- Current status (hoping to get things ready for the conference in main branch)
- Importance of PoC and talking to upstreams in Open Source projects

Length

30 minutes

Optional: Speaker / convener biography

Kushal Das is a public interest technologist working at Sunet (https://sunet.se) where he helps to build secure and privacy focused tools and services. He is Cpython core developer & a director at the Python Software Foundation. He is also part of the core team of the Tor Project, and a long time contributor to Fedora Project. In 2004 he founded Linux Users' Group of Durgapur. He also helps out journalists/activists with digital security trainings. He regularly blogs at https://kushaldas.in.

Primary author: DAS, Kushal (Sunet)

Presenter: DAS, Kushal (Sunet)

Session Classification: Talks and presentations

Track Classification: Talks and presentations