FaaS Terms of Service

Each FaaS customer gets dedicated, not shared FaaS instance which is, based on customer preferences, localized for their use. In order to do that, each customer must provide us certain minimal resources (such as FQDN for web server, TLS certificate, mail smarthost) which are in detail explained in page on becoming FaaS user.

However, although FaaS customer instance is dedicated, this couldn't be achieved for all of the FaaS infrastructure. Namely, all FaaS instances access key material that's stored in a single "partition" of an HSM. That means all FaaS-using Federations have the same signing key/certificate. That's not a problem per se, as such we enforce strict controls over system access to the machines which is limited only to FaaS operations in order to prevent e.g. one federation from impersonating SAML metadata of another federation. However, if a federation decides to stop using FaaS service, they cannot take the signing key with and as consequence the federation would in this transition need to perform signing key rollover.

FaaS customer is the owner of the data in its FaaS registry application. The data is stored in relational database on the system. In the case that FaaS customer wants to step out from using the FaaS service, he has the right to take its data from the system: the data from the database and aggregated XML metadata.

FaaS service is managed by development and operations team.

FaaS development team is responsible for:

- Providing L3 customer support which includes:
    - Processing request to use FaaS service;
    - Processing and resolving enquiries about FaaS;
- Development of the service.

FaaS customer instances are managed on the daily basis by the FaaS operations team, which is responsible for:

- Deployment of new customer instances;
- Timely system and security updates for the whole software stack. Urgent security updates are performed immediately. All other updates are implemented during maintenance window which is on first Tuesday in a month, 17:00-19:00 CEST. In a case of public holiday, maintenance window is moved to next suitable day.
- Daily backup of software configuration and data, kept for two weeks;
- Backup snapshot of VM, guaranteed at least monthly (currently 7 last days and 3 previous Sundays snapshots are kept);
- Support for timely recovery of the service;
- Changes to FaaS-related configuration;
- Maintain system according to security best practices;
- Maintain system and application logs for audit trails;
- Monitoring system, network and specific services.