How to implement GOST cryptography. Sberbank case.

Session Topic or Project
Key points, problems and opportunities in the context of HLF GOST implementation and a little demo of using GOST key in HLF network.

Session Leader
Vladimir Popov

Time Slots and Spaces
Day 1, Aurum , 14:30 - 15:30

Experience Level of Participants
Intermediate

Session Language
Russian

Programming Language(s)

- C / C++
- Go
- Java
- Javascript
- Python
- Rust
- Other

The Plan
1. The problem: why do we need GOST (as well as other local standards) implementation?
2. Architecture overview.
3. Different approaches to implementation
4. Sberbank implementation details and problems.
5. Demo

The Goals
Attendees will get understanding of

- difficulties and possible shortcuts when implementing custom cryptographic algorithms, such as GOST
- what are the different ways to implement GOST
- HLF specific problems