The basic elements of the security mechanisms for the Smart Space Smart-M3 platform

Kirill Yudenok, ETU OSLL

Smart-M3 over HIP

- working of the Smart Space Smart-M3 platform over the Host Identity Protocol (HIP);
- supporting of some base security mechanisms that are inherited from the protocol.

Host Identity Protocol

- hosts mobility and multihoming;

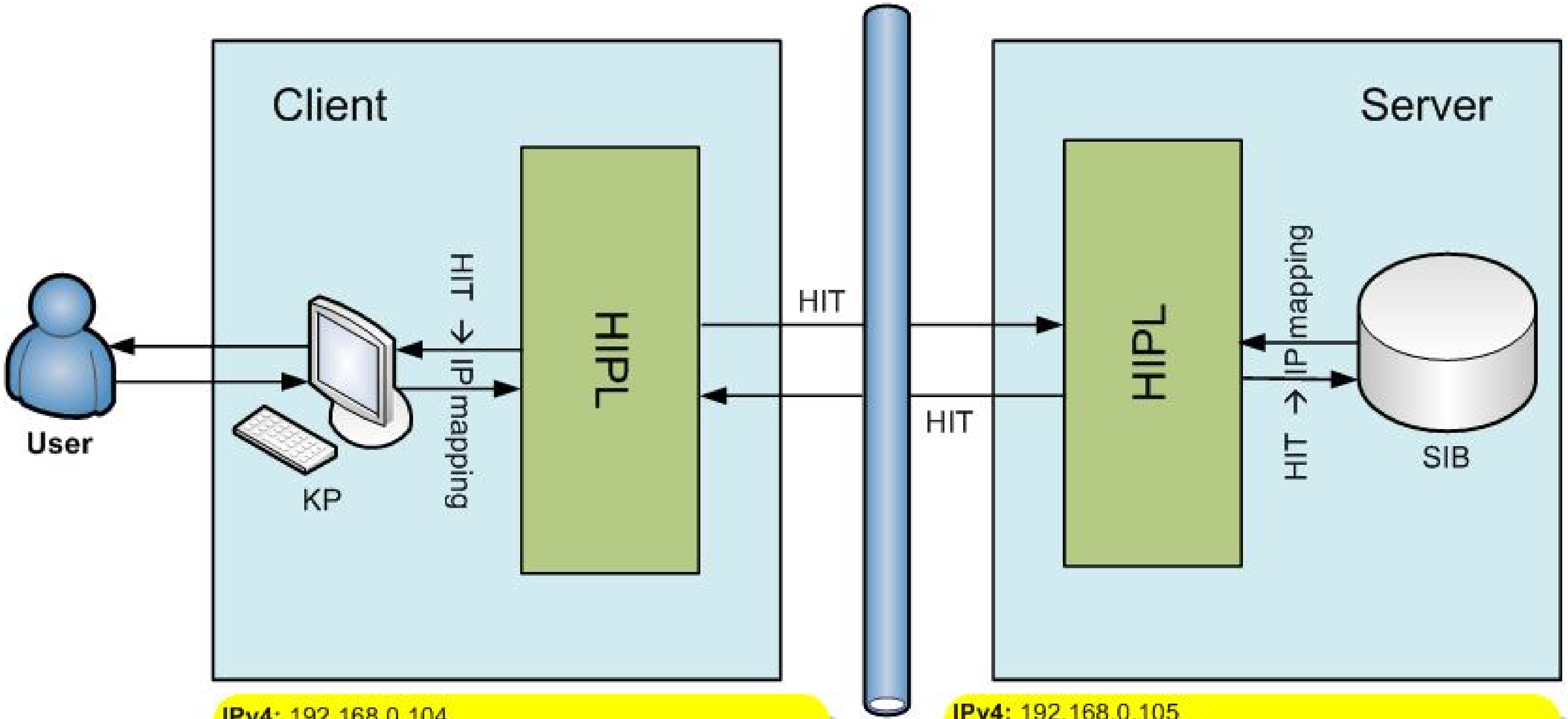
- security and privacy over IPv4 and IPv6 networks;

- NAT traversal and Name Lookup.

Smart-M3 over HIP

- HIP allows working with IPv4/IPv6 applications;
- using HIPL realization of HIP;
- mapping IP → HIT [LSI – IPv4 addresses of HIP], change SIB IP to HIP LSI and connect as usual.

Smart-M3 – HIP scheme



IPv4: 192.168.0.104
HIT: 2001:0015:53f8:b832:6936:a111:dc01:2c93
LSI: 1.0.0.1

IPv4: 192.168.0.105
HIT: 2001:001d:509f:db61:87f3:6e0e:ee7d:7aab
LSI: 1.0.0.2

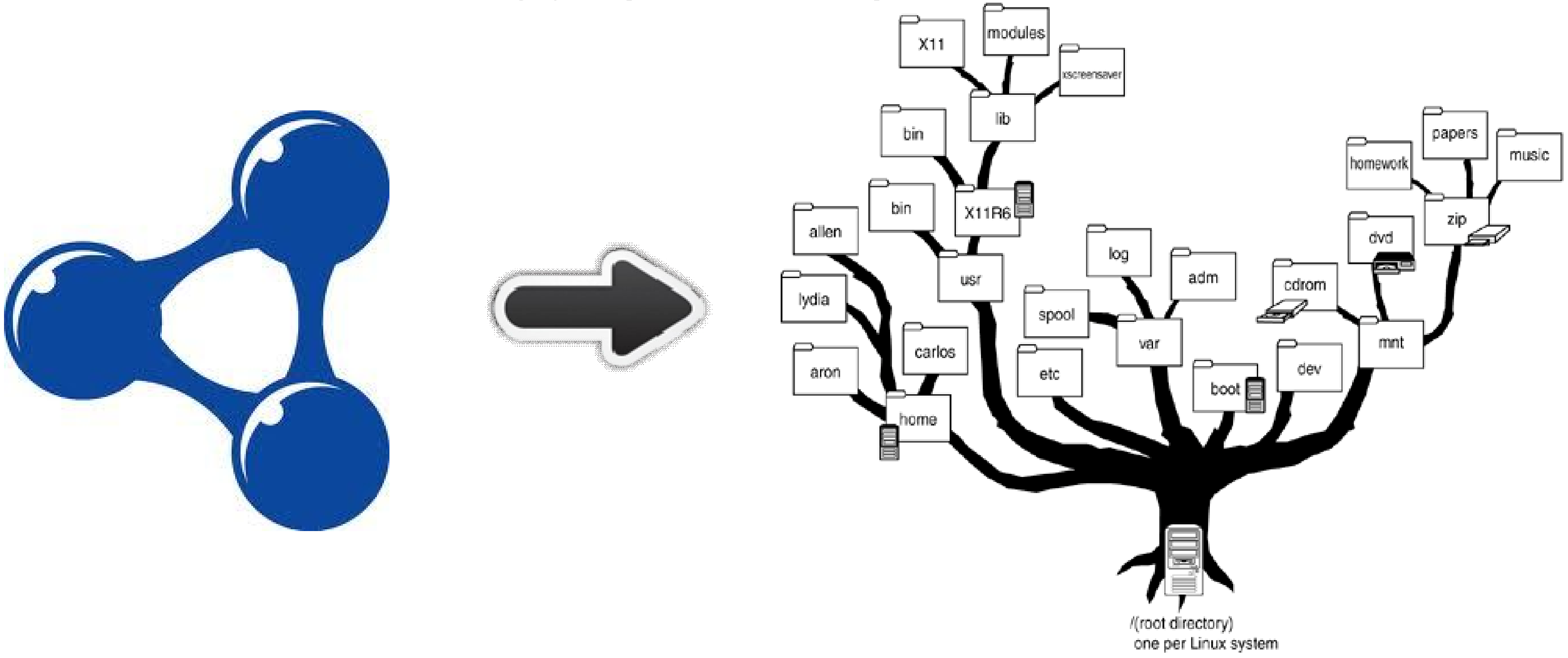
RDF-graph mapping to the VFS

- mapping of Smart Space (SS) RDF-graph triples to the virtual file system (VSF), which will use basic FS security mechanisms, as ACL, roles;

- mapping model is similar to the discretionary security model and can be easily extended to the role.

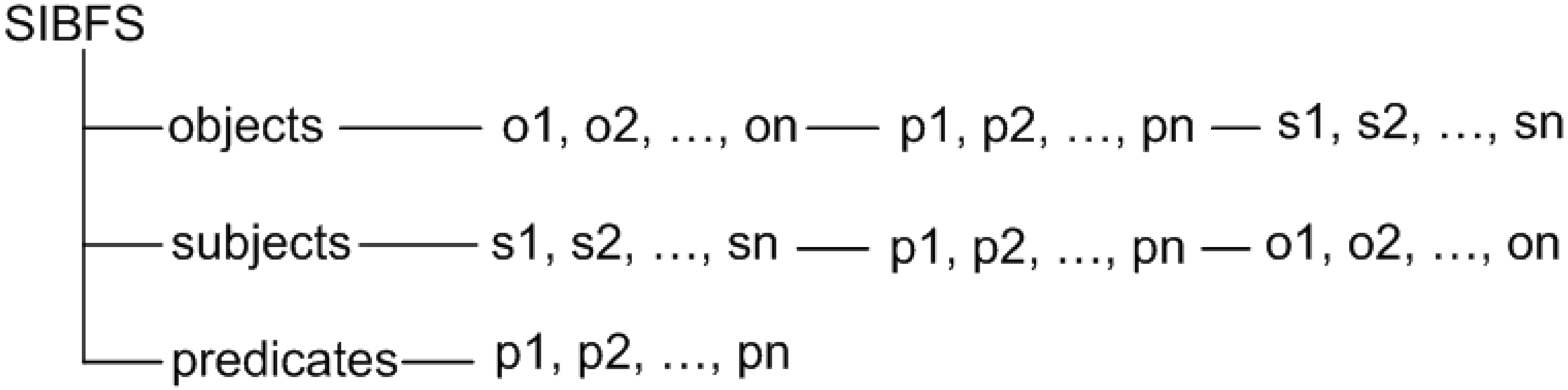
RDF-graph mapping to the VFS

- RDF-graph mapping to the VFS allows us to set permissions rights in a Linux-usual way;
- this implementation can be realized with the FUSE technology (fusekit);



VFS directory structure

- mapping RDF-graph to the special VFS directory structure for a more accurate setting of access rights to the SS triples (information);



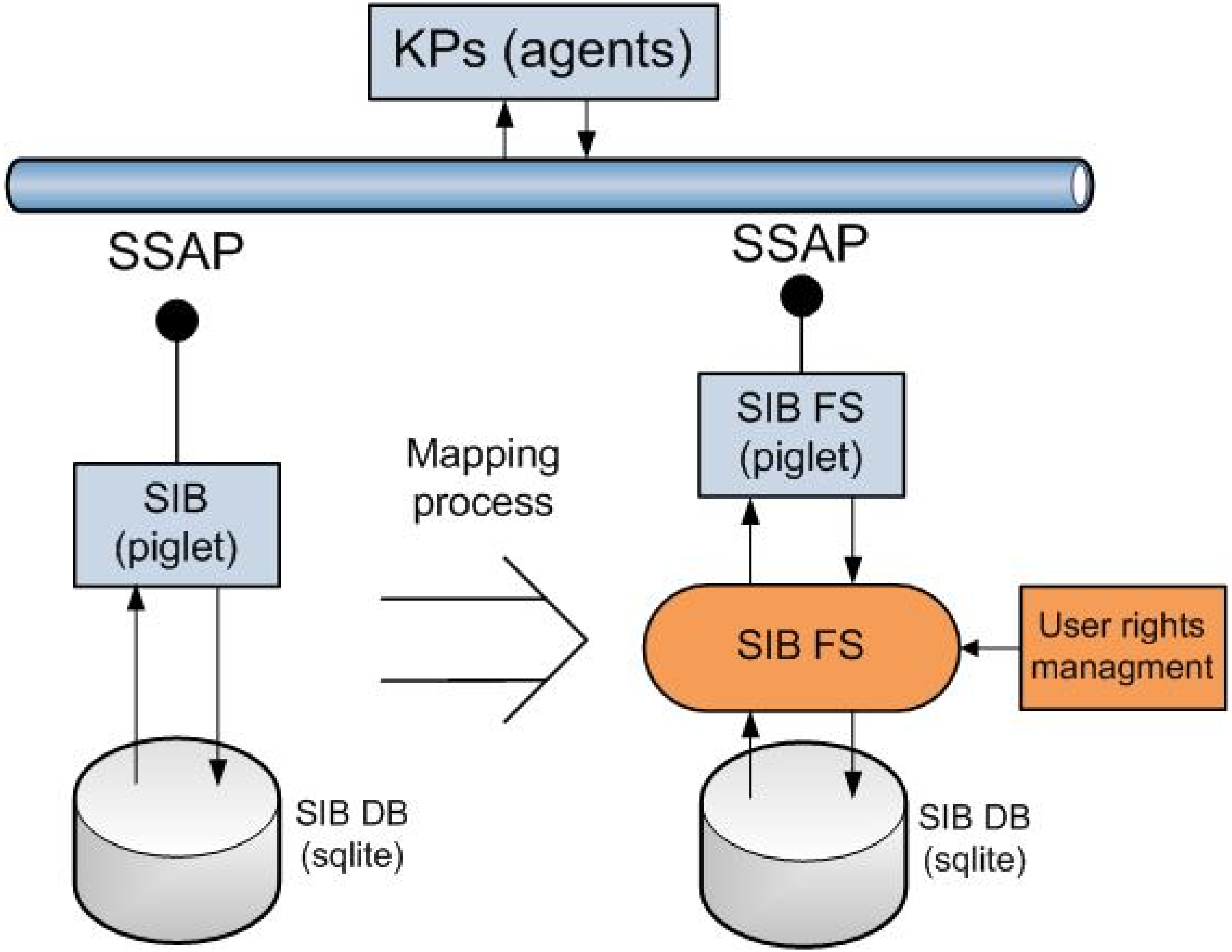
SIBFS

objects — o1, o2, …, on — p1, p2, …, pn — s1, s2, …, sn

subjects — s1, s2, …, sn — p1, p2, …, pn — o1, o2, …, on

predicates — p1, p2, …, pn

The place of RDF-graph mapping



Future steps

- HIP-agent development;
- implementation of mapping model to the Smart-M3 platform;
- set permissions tool development for mapping FS;