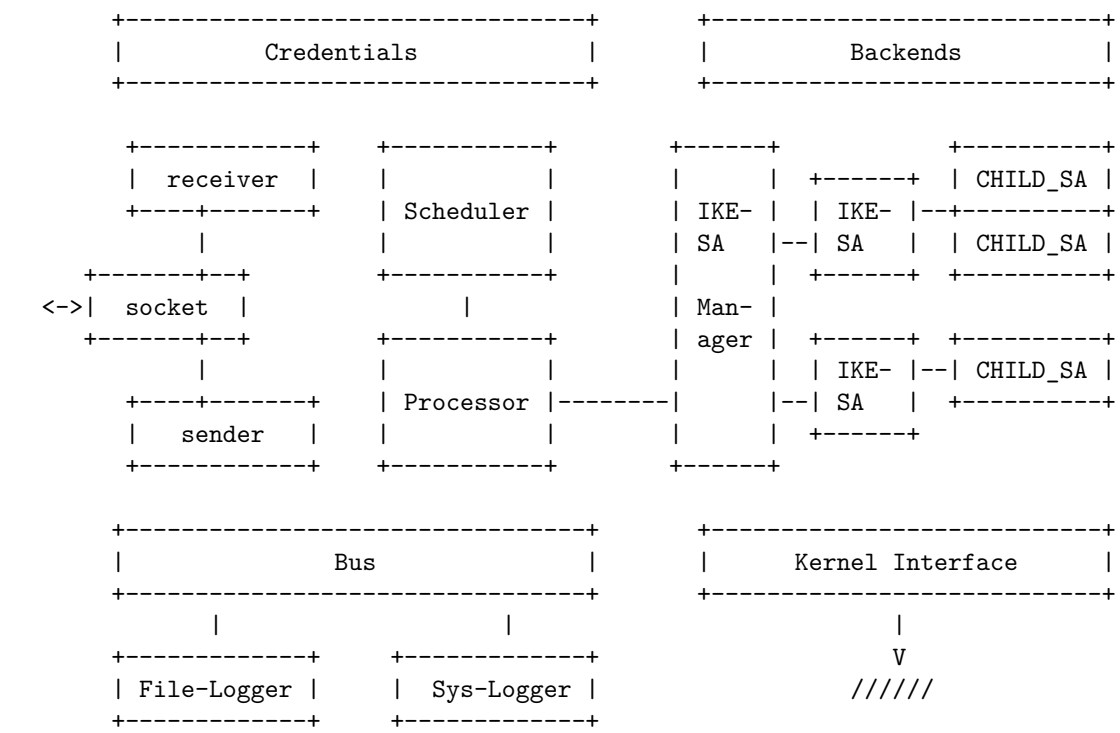
Notes

Strongswan

Charon è il daemon ed ha la seguente architettura



RFC 92

Di base IKEv2 utilizza ECDH per stabilire il segreto condiviso tra initiator and responder. La complessità del problema di DH è equivalente al problema del logaritmo discreto (rispettivamente nel gruppo moltiplicativo, per quello glassico e nel gruppo elliptic curve).

Il problema alla base è che per i computer classici questo problema risulta di complessità esponenziale, mentre per i computer quantistici questo potrebbe diventare un problema di complessità esponenziale.

La sicuretta di IKEv2 in questo modo viene compromessa.

Si cerca di fare in modo che questo sia resistente ad attacchi quantum-computer, questa famiglia di crittosistemi è conosciuta come post-quantum cryptography.

E' essenziale realizzare un o più scambi di chiave post-quantum in congiunzione con lo scabmio di chiae tramite ECDH per fare in modo che la risultante chiave condivisa sia resistente ad attacchi quantum.

Allo stato attuale non esistono scambi di chiave post-quantum che sono studiati bene tanto quanto ECDH, realizzare multipli scambi di chiave

Extension

Si vuole mantenere la retrocompatibilità realizzando molteplici