

Eru forrit öruggari á SIM kortinu en á handtækinu?

ÓLAFUR PÁLL EINARSSON OG STEFÁN ÞORVARÐARSON

Hvaðan kemur SIM kortið

- SIM (Subscriber Identity Module)
 - Auðkennir farsímanotanda á móti farsímanetinu
 - Velur dulritunarlykla fyrir áframhaldandi samskipti
 - Geymir gögn fyrir símtækið þegar slökkt er á því



Umhverfi SIM kortsins

- SIM kortið er mun lokaðara umhverfi símtækið
 - Þarft að vera í samstarfi við fjarskiptafélagið sem á kortið
 - Takmarkað pláss (16-256Kb)
 - Takmarkaðra viðmót (SIM toolkit / NFC)
 - Dreifing á hugbúnaði á kortum er lokaðari
 - Forritað í JavaCard
 - Meira öryggi?



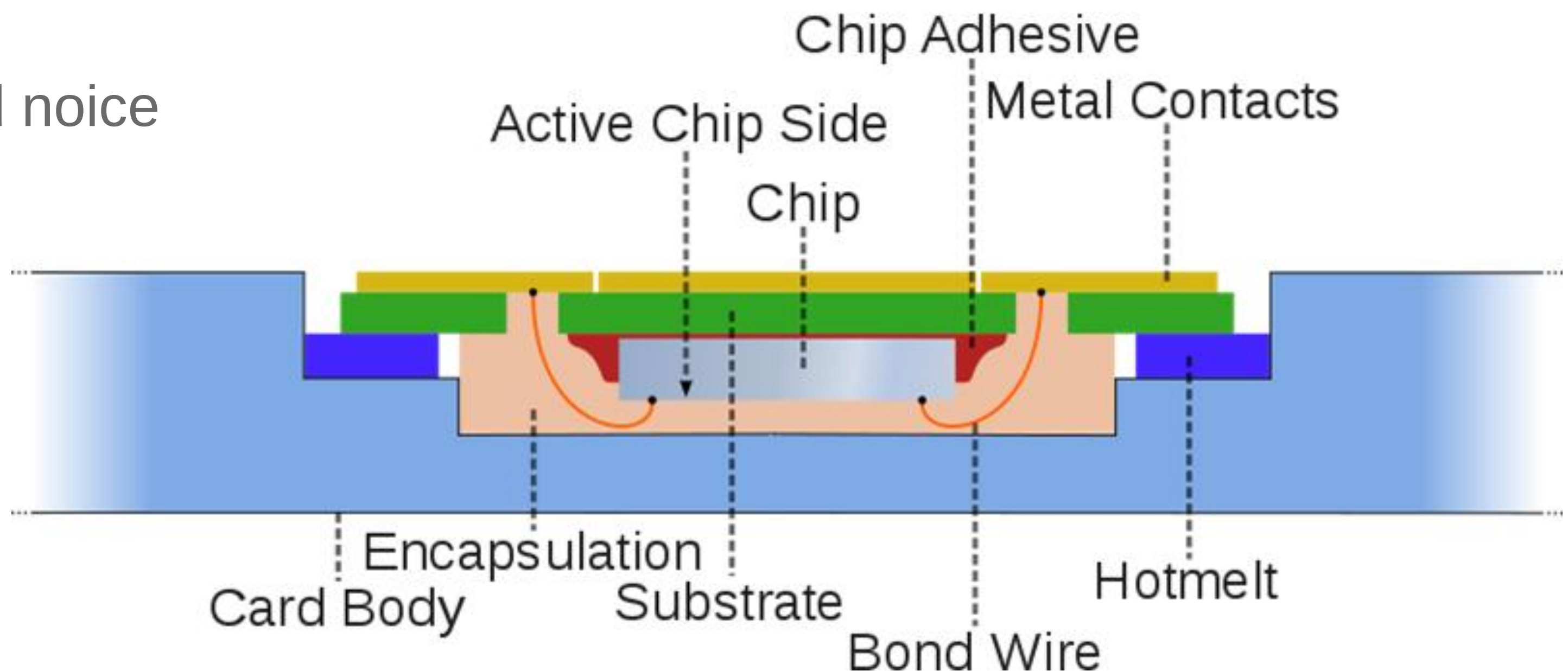
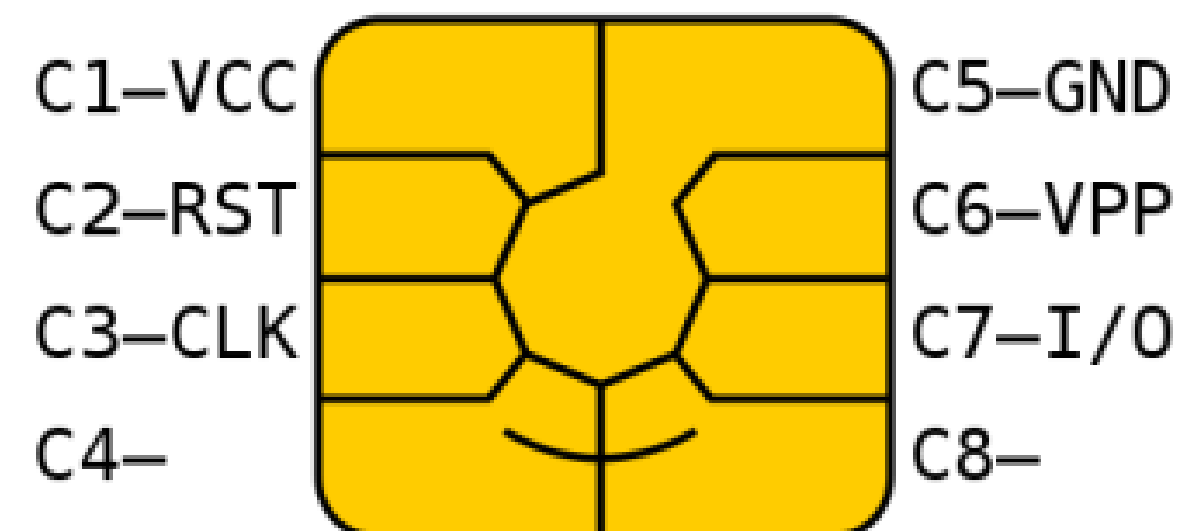
Hvernig forrit eiga heima á SIM?

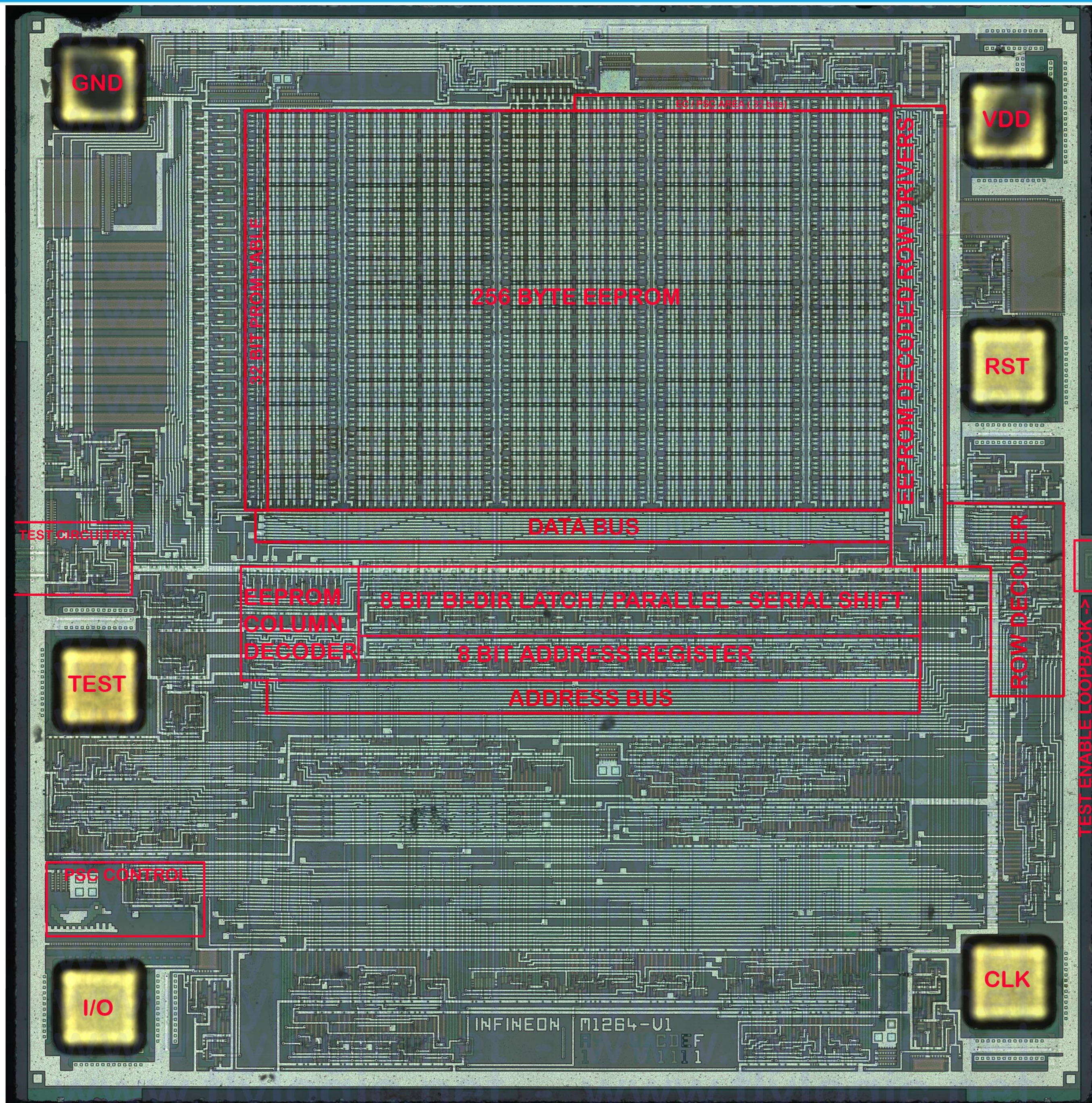
- Stuðningsforrit fyrir farsímaþjónustu
 - Stýring inn á farsímanet erlendis (Roaming)
 - Fylgjast með að réttar stillingar séu á handtækjum
- Hugbúnaður með hátt öryggisstig
 - Rafræn skilríki
 - Auðkenningar
 - Rafrænar undirskriftir
 - Dulritun
 - OTP (One-Time-Password)
 - Greiðslumiðlun og bankaþjónustur
 - NFC mobile payment



Innviðir SIM korts - vélbúnaður

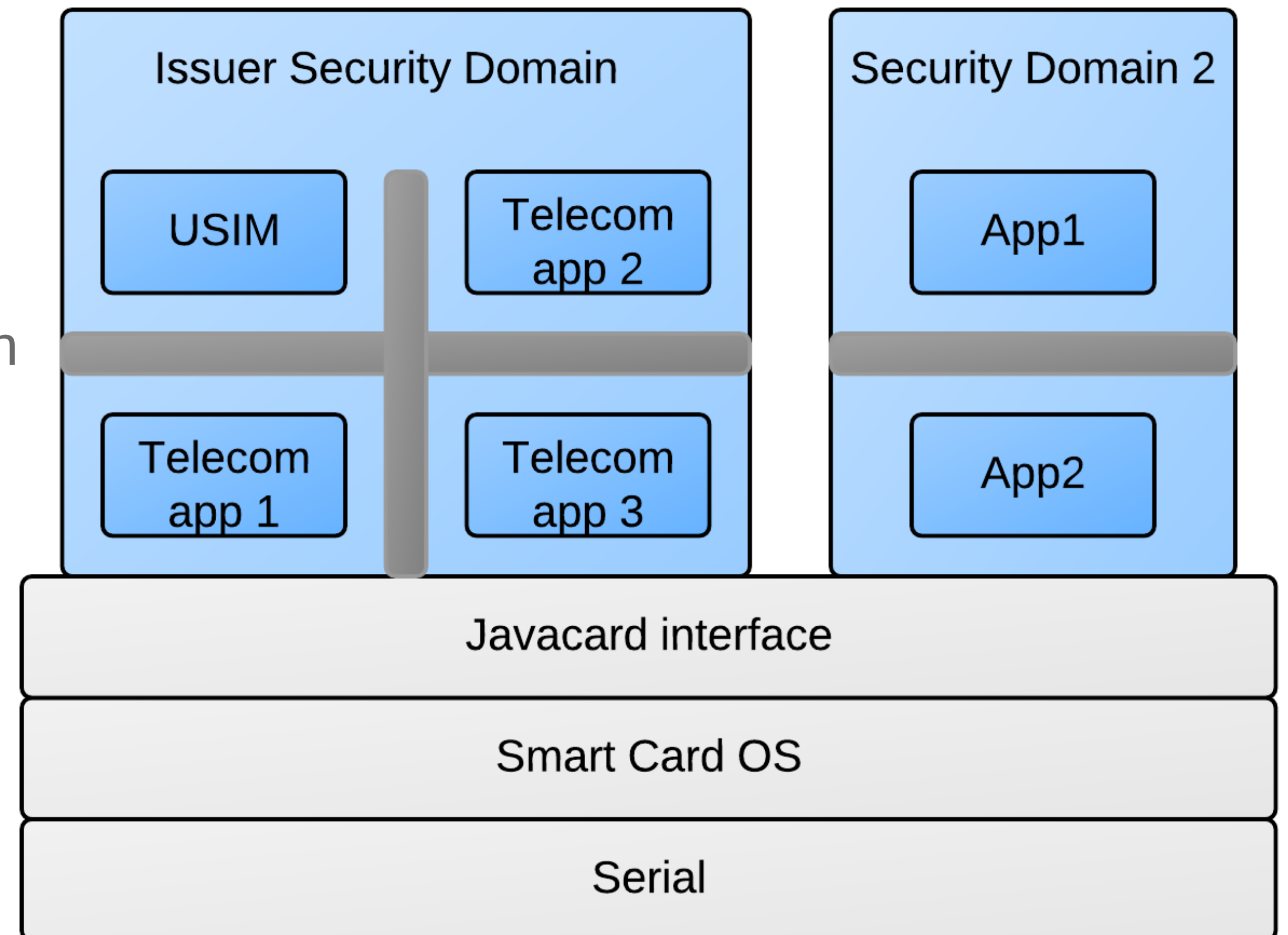
- Vélbúnaður
 - Smart kort
 - Sér örgjörvi og minni
 - Serial samskipti
- Varnir
 - Top-layer Sensor Meshes
 - Reduce power signal and add noise
 - Low-frequency Sensor



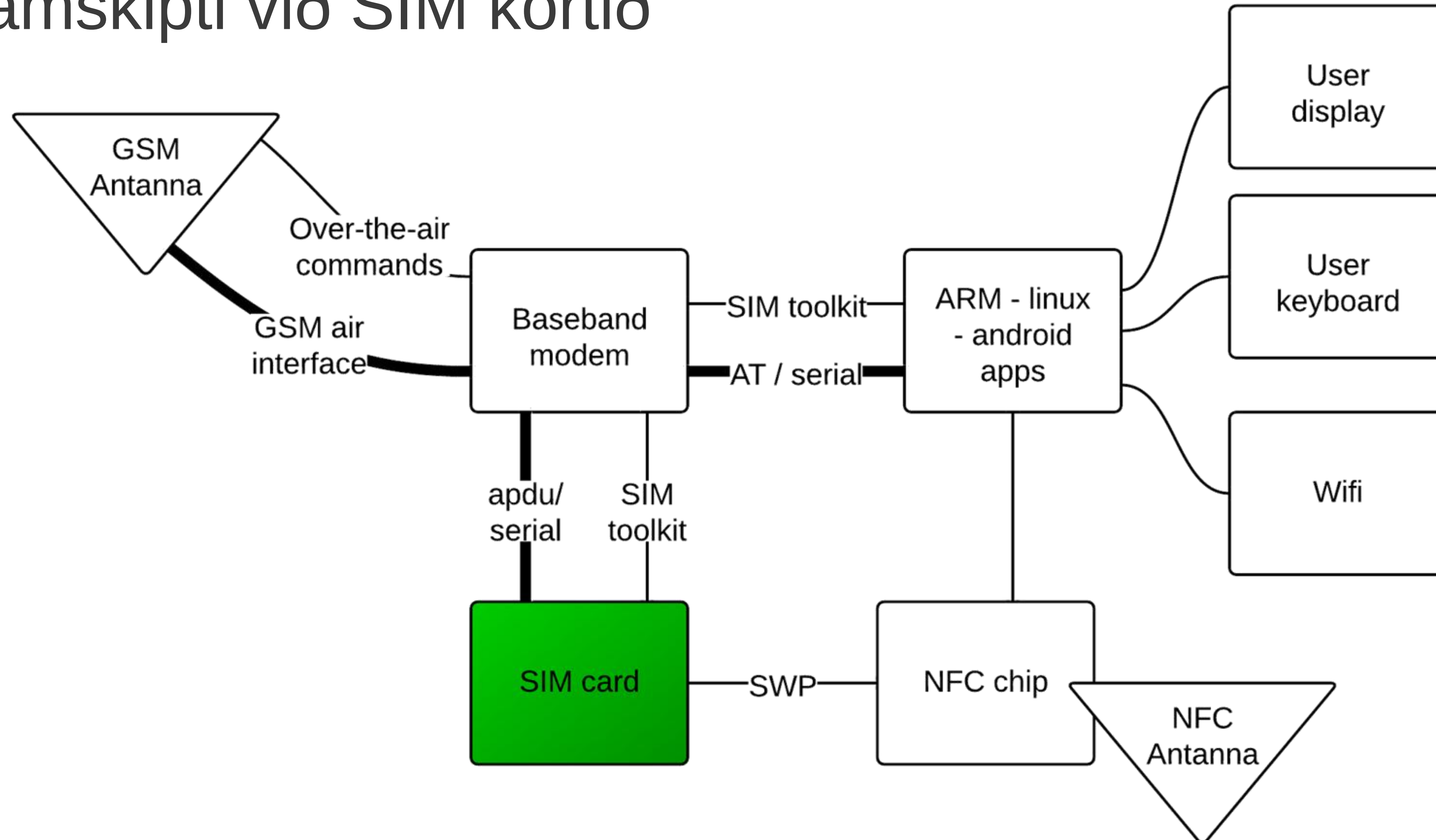


Innviðir SIM korts - hugbúnaður

- Stýrikerfi
- Javacard
 - Forritunarmál
- Security domain
 - Krefst auðkenningar fyrir alla meðhöndlun
- Applet firewall
 - Stoppar samskipti tveggja óháðra forrita
 - Shareable interfaces



Samskipti við SIM kortið



Samantekt

- SIM kort henta ekki öllum tegundum af þjónustu
 - Einfalt viðmót
 - Lítið geymslupláss
- Aðgangur að SIM korti í höndum fjarskiptafélags
- Margar öryggisráðstafanir
 - Ekki hægt að lesa leynilykla út úr korti

Takk fyrir

