Certificate Analysis

DANIEL RYCHLÝ & IMRICH NAGY

NXP JCOP 5.2 ON SN100.C58 SECURE ELEMENT

ToE

Laboratory

Attacker models

Physical resistance

SFR

SAR

Maintenance report

New site

Evaluation

RED HAT ENTERPRISE LINUX VERSION 7.1

ToE

Scope

Attacker models

SAR

SFR

Testing

Conclusion

ST33TPHF2E MODE TPM 2.0, TPM FIRMWARE 0X49.0X40 & 0X49.0X41

ToE

Attacker models

SFR

SAR

Physical resistance

Evaluation

Thank You