PV204 Project Phase 1

- Nomit Sharma, Matěj Grabovský, Milan Šorf

• Certified Products

- The Common Criteria Recognition Arrangement covers certificates with claims of compliance against Common Criteria assurance components.
- Chosen certificates by our team:
    a. NXP JCOP 4 P71 (Nomit Sharma).
    b. genuscreen 7.0 (Matěj Grabovský).
    c. vinCERTcore v4.0.5.5733 (Milan Šorf).

• Certificate: NXP JCOP 4 P71

- Developed in Germany and Evaluated in Netherlands.
- Valid till 25-07-2024.
- EAL6+ Compliant.
- **Target of Evaluation:** Smart Card Controller, Test and Boot Software and use of Cryptographic Primitives.
- **Assumed Attacker Model:** Applets without Native Methods, Bytecode Verification, Protected Storage of Keys and Protection during Packaging, Finishing and Personalisation.
- **Device Scrutinization:** Data leakage protection, Integrity of application data and sensitive results, TOE security counters manipulation.
- **Security Assurance Requirement (SAR):** Security of TOE and provision of Security policy model.
- **Security Functional Components (SFR):** Java Card Virtual Machine, Configuration Management, Cryptographic Functionality, Random Number Generator, Data Storage and Protection, Memory and PIN Management, Error Detection Code, Hardware Exception Handling and Module Invocation.
- **Out of Scope of Certification:** Java Card Applets, Secure Box Native Library and Crypto Library.
- **Critical Evaluation and Conclusions:** Detailed TOE evaluation, Conformance to the Protection Profile.

- # Certificate: genuscreen 7.0

- Distributed Packet Filtering Firewall System with VPN and IPsec capabilities.
- Developed and Evaluated in Germany.
- EAL4+ compliant.
- **Target of Evaluation:** Software only with distributed (genuscreen) and central management (genucenter) part.
- **Assumed Attacker Model:** Initialization and physical security of components, Reliable timestamps, GUI over trusted network connected directly to the device, breakage, sniffing and modification of data.
- **Device Scrutinization:** Software as network filters, SSH connection between genucenter and genuscreen, firewall components management, scrutinization performed by vendor and independent evaluator.
- **Security Assurance Requirement (SAR):** From specification till analysis, includes development architecture, user guidance, life cycle coverage, security, testing and analysis.
- **Security Functional Components (SFR):** Firewall and Network Separation, IPsec and SSH, Administration, Identification, Authentication, Audit, General Management Facilities and Random Number Generation.
- **Out of Scope of Certification:** Hardware components, Cryptocard usage, central management software, remote maintenance and dynamic routing.
- **Critical Evaluation and Conclusions:** Reliance on OpenBSD and LibreSSL, wide range of functionality considered, testing might have been more extensive.

- # Certificate: vinCERTcore v4.0.5.5733
- Developed and Evaluated in Spain.
- EAL4+ compliant.
- **Target of Evaluation:** Software server and use of external user repository and IT products with HSM.
- **Assumed Attacker Model:** Trusted external IT products, OS, HSM, no physical access to TOE and no malware attack on TOE from same OS.
- **Device Scrutinization:** Similar to assumed attacker model and set of assumptions.
- **Security Assurance Requirement (SAR):** From basic design till vulnerability analysis and included basic modular design, preparative procedures, development tools, security objectives and analysis of coverage.
- **Security Functional Components (SFR):** Security alarms, audit data generation and review, user identity association, potential violation analysis, cryptographic operation, access control, data integrity, identification and authentication.
- **Out of Scope of Certification:** Hardware Security Model and External Web Interface.
- **Critical Evaluation and Conclusions:** Independent testing covered 100 percent SFR and TSFI, TOE does not present any exploitable vulnerabilities and since description of the testing process is missing, the evaluation results are not convincing.