Eurosmart welcomes ARM’s certification of the M33 and M35P cores using a subset of the requirements of Protection Profile [PP] PP-0084. This helps solidify the status of Common Criteria and especially the SOG-IS members as the go-to-centre for high assurance certification in the world. With ARM referencing PP-0084, it shows the critical importance of this Eurosmart initiative as a key standard for security requirements for high-security ICs.

PP-0084 refers to a complete Secure IC concept and includes the assumptions on its environment and threats. However, it should be noted that (1) the scope of certification of M33 and M35P cores only covers a subset of the PP-0084, and (2) only considers some of the applicable attacks.

Eurosmart promotes high-level certifications by SOG-IS, as SOG-IS mandates security evaluations based on concrete penetration testing on real devices, conducted by skilled security experts. This concrete testing on real devices by skilled experts must be the key approach for any companies using the M33 and M35P in their high-security ICs all associated threats and testing must be performed including the tests not included in the M33 and M35P certifications, this is important to ensure that PP-0084 Common Criteria certifications remain as the state of the art for High Security ICs.

M33 and M35P Certification on Hardware Description Language

The M33 and M35P were certified as a soft macro, that is the certification was performed on Verilog Hardware Description Language (HDL). This approach allows companies that wish to use the cores in a certification of their product to re-use some of the evaluation results from the existing certification. This would in theory allow companies using the cores to have a quicker certification. However, it should be noted that the guidance and limitations of the certification would have to be stringently followed. This approach has been welcomed by Eurosmart and its members. The idea of using certified IP blocks has also been discussed in the Eurosmart group ISCI.

However, a direct re-use of certified IP is based on defining and using a common threat landscape. The AVA_VAN.5 level on PP-0084 includes physical attacks as threats. In ARM certification, physical attacks are not considered. “Due to the form of the certification scope (Verilog), only a limited amount of
**attacks is directly applicable and countered by the TOE. For example, physical attacks are not countered by this TOE.**

So, the assurance claim of this ST does not include all assurance components of PP-0084. Penetrations tests must cover the whole attack classes in the JHAS attack method in order to reach the AVA_VAN.5 level.

Eurosmart members suggest considering the writing of a dedicated Protection Profile based on a VHDL Core description (or any other IP) with related threat definition along with guidance documents for integrators that can be used then verified during the final Product certification.

**Possible misinterpretation of the certification results**

Eurosmart has though one major area of concern. The pre-certification of the soft macro might create the impression that including such a core automatically fulfils the certification requirements of governmental and trade bodies. However, in most cases, such requirements include both conformance to an EAL and conformance to a specific Protection Profile. None of these requirements are provided with an IP only certification.

Therefore, special care must be taken in the way that this certification is marketed. End-users must not be under the illusion that if they use the certified core that they automatically have an EAL6+ AVA_VAN.5 certified product. To simply take a soft macro and design it into the secure IC product, and believe that all testing associated with AVA_VAN.5 and the requirements of the JIL/JHAS document “Application of Attack Potential to Smartcards” are covered, is dangerous and will leave end-users exposed to attacks that they falsely perceive to be protected against. This is very critical for both invasive attacks, including glitching and side-channel, and non-invasive attacks. These attacks and the functionality of the final product cannot be gauged by HDL based simulation alone. This would leave the IC developer open to liability issues if the product was compromised, especially if they have made security claims for their product. This could also lead to brand damage for ARM.

**In summary**

Eurosmart welcomes all contributions to the ideas and innovation of security certification. The Eurosmart members believe that third-party verification of security claims is fundamental to build a secure connected society, and welcome ARM’s contribution to this goal. This certification must though be used correctly, and end-users must be fully aware of its limitations and their requirements to implement security in their final secure IC products. It is a necessary condition if they want their final ICs to be PP-0084 Common Criteria certified.
About us

Eurosmart, the Voice of the Digital Security Industry, is an international non-profit association located in Brussels, representing the Digital Security Industry for multisector applications. Founded in 1995, the association is committed to expanding the world’s Digital secure devices market, developing smart security standards and continuously improving the quality of security applications.

Our members

Members are manufacturers of secure elements, semiconductors, smart cards, secure software, High Security Hardware and terminals; biometric technology providers; system integrators; application developers and issuers.

EUROSMART members are companies (BCA, Fingerprint Cards, G+D Mobile Security, GS TAG, IDEMIA, IN Groupe, Infineon Technologies, Inside Secure, Internet of Trust, Linxens, Nedcard, NXP Semiconductors, +ID, Prove & Run, Qualcomm, Real Casa de la Moneda, Samsung, Sanoïa, Sarapis, , STMicroelectronics, Thales, Tiempo Secure, Trusted Objects, WISekey, Winbond, Xilinx), Testing and Inspection and certification companies (Bureau Veritas, SGS,) laboratories and certification body companies (JTSEC, Keolabs, Serma, Brightsight, Red Alert Labs, Cabinet Louis Reynaud, Trust CB), research organisations (Fraunhofer AISEC, Institut Mines-Telecom - IMT, ISEN - Institut Supérieur de l’Électronique et du Numérique Toulon), associations (SCS Innovation cluster, Smart Payment Association, SPAC).

EUROSMART and its members are also active in many other security initiatives and umbrella organisations at EU-level, like CEN, ECIL, ETSI, ECSO, ESIA, ETSI, GP, ISO, SIA, TCG and others.