
Vérification formelle d'une carte à puce pour une certification Critères Communs

Adel Djoudi¹, Martin Hána¹, and Nikolai Kosmatov*²

¹THALES [France] – THALES – France

²Thales Research and Technology – THALES – France

Résumé

Ce résumé étendu présente la vérification formelle récente d'une implémentation de machine virtuelle de carte à puce réalisée par Thales à l'aide de la plateforme de vérification Frama-C. Elle a été réalisée en vue d'une certification Critères Communs de niveau EAL6 (pour laquelle le certificat a été délivré en 2021). Les propriétés visées incluent les propriétés de sécurité habituelles, telles que l'intégrité et la confidentialité, qui doivent être assurées par le mécanisme de contrôle d'accès de la machine virtuelle. Ce travail a été initialement publié à FM 2021.

*Intervenant