



# EUCC-Certified Product

## Supplementary Cybersecurity Information

# Document Change History



No.	Version	Status	Date	Description
1	A01	Void	2026.04.28	<i>Add cybersecurity information towards EUCC certified TOE, namely: 1. TMCICAO v1.0 on TMCOS 4.0 0.5 in ICAO BAC configuration v1.0 2. TMCICAO v1.0 on TMCOS 4.0 0.5 in ICAO EAC with PACE configuration v1.0</i>
2	A02	Void	2026.04.28	<i>Improve description.</i>
3	A03	Effective	2026.04.29	<i>Improve description.</i>

# TMC Certified Product

Under the European Cybersecurity Certification (EUCC) Scheme



No.	Product Name	Product Version	Certificate ID	Certificate Reference
1	<i>TMCICAO v1.0 on TMCOS 4.0 0.5 in ICAO BAC configuration</i>	<i>1.0</i>	<i>EUCC-3110-2026-2500080-01</i>	<i><a href="https://certification.enisa.europa.eu/certificates_en">https://certification.enisa.europa.eu/certificates_en</a></i>
2	<i>TMCICAO v1.0 on TMCOS 4.0 0.5 in ICAO EAC with PACE configuration</i>	<i>1.0</i>	<i>EUCC-3110-2026-2500081-01</i>	<i><a href="https://certification.enisa.europa.eu/certificates_en">https://certification.enisa.europa.eu/certificates_en</a></i>

## Cybersecurity support:

- The validity period for an EUCC product certificate is established in accordance with the EUCC regulation ([Implementing regulation - EU - 2024/482 - EN - EURLex](#)) and is set at five years.
- The product will be maintained during the validity of its certificate. Further arrangements regarding product support should be discussed and agreed upon with the TMC.

# TMC Certified Product

Under the European Cybersecurity Certification (EUCC) Scheme



**Guidance and recommendations to maintain the cybersecurity level for *TMCICAO v1.0 on TMCOS 4.0 0.5 in ICAO BAC configuration* and *TMCICAO v1.0 on TMCOS 4.0 0.5 in ICAO EAC with PACE configuration*:**

An MRTD chip programmed according to the requirements of the International Civil Aviation Organization. It is used by the holder for international travel. It addresses the advanced security methods for:

1. Basic Access Control and Active Authentication.
2. Password Authenticated Connection Establishment, Extended Access Control and Active Authentication.

The card issuer shall strictly manage the lifecycle of PKI keys and certificates in eMRTD, including secure generation, storage, and secure destruction. Given the sensitivity of the certified products, please contact our sales department at 010-82351818 to obtain detailed secure usage guidelines, requirements, and recommendations.

# TMC Certified Product

Under the European Cybersecurity Certification (EUCC) Scheme



- Contact for reporting vulnerability information, please refer to the TMC PSIRT (TMC Product Security Incident Response Team) website: <https://www.tsinghuaic.com/index/index/newsdetail/id/608?lang=en>
- The ICT Product Public Vulnerability Repository operated by TMC own could be access at the *ICT Product Public security advisories and bulletins* from <https://www.tsinghuaic.com/index/index/newsdetail/id/608?lang=en>

# THANKS

科技之光照亮幸福生活

THE LIGHT OF SCIENCE AND TECHNOLOGY BRIGHTENS HUMAN LIFE