REPUBLIC OF ESTONIA
INFORMATION SYSTEM AUTHORITY

TÜV NORD CERT

Our Ref: 09.01.2026 No 9-7/25-0361/2645

Confirmation Letter

Dear Sir/Madam

Information System Authority (RIA) confirms, that as of today and to our best knowledge there have been no cases related to Smart-ID, in which, as a result of device compromise (e.g. through phone rooting), user private key components copied from a user´s device could be reused on another device.

However, we must emphasise that recently the number of incidents connected to Smart-ID, as well as the associated financial losses, has increased. The attacks are being performed in a way where a Smart-ID user is persuaded to visit a website where a new Smart-ID account can be created. On that website, the victim is instructed to enter verification code that is displayed on the attacker's mobile device. By doing so, the attacker's device becomes linked to the newly created Smart-ID account. Subsequently, the attacker convinces the victim to use their Smart-ID PIN-codes or their Estonian ID-card and its PIN-codes on the website. As a result of these actions, a Smart-ID account is successfully activated on the attacker's device, while the identity associated with the Smart-ID account is that of the victim. As this new Smart-ID account on the attacker's device is fully legitimate, it can be used for various further fraudulent activities - for example, to access the victim's bank accounts and/or to obtain multiple instant loans.

These incidents are the result of social engineering and do not involve any technical compromise of the Smart-ID solution, nor the extraction or reuse of cryptographic key material from a user's device.

Yours faithfully

Joonas Heiter
Director General

Tais Vakrõõm
+372 58058709
tais.vakroom@ria.ee