Recommended Security Precautions /

Recomandări privind precauții de securitate

related to the use of the electronic identification means of certME /

legate de utilizarea mijloacelor de identificare electronică ale certME

certME RSP EN-RO

Document code: [Subject]

Document Version/Date: **v.1.0 - Jan.2021**

Document Security Level: **Public**

Important Notice

Address: 29 A Tudor Vladimirescu Avenue,

AFI Tech Park 1, Bucharest, Romania

Phone: 004-021-31.19.901

Fax: 004-021-31.19.905

Web: www.certsign.ro

Document History

Version	Date	Reason	The person who made the change
0.1	Jan 2021	First draft version publishing	Policies Manager
1.0	Feb 2021	First version	Policies Manager

This document was created and is the property of:

Owner	Author	Date created
certME	Policies Manager	Jan 2021

Distribution List

Destination	Date distributed
Intranet	Jan 2021
Public-Internet	Feb 2021

This document was approved by:

Version	Name	Date
0.1	certME Management	Jan 2021
1.0	PPMB	Feb 2021

Contents / Cuprins

1 Recommended Security Precautions

related to the use of the electronic identification means of certME

a) The certME mobile application only works on mobile devices equipped with secure elements or enclaves for storing keys and passwords.
b) For ease of use and increased security, the certME mobile application only works on mobile devices equipped with secure biometric authentication.
c) The certME mobile application only works on mobile devices that have active screen lock functions via PIN, pattern, password or biometric authentication. For the protection of users, deactivation of the screen lock leads to the deletion of all data associated with the certME means of identification and the impossibility of using it until a new identity verification is performed by one of the certME partners.
d) The certME mobile application does not work on rooted or jailbroken mobile devices. For the protection of users, the rooting or jailbreaking the device leads to the deletion of all data associated with the certME means of identification and the impossibility of using it.
e) Do not allow other people to record their biometric features on your device, not even family members. As long as you're the only person who can authenticate biometrically on your device, no one else can use your certME means of identification to identify you in the online environment or access your data.
f) Do not authorize identification or authentication requests if you have not initiated the transaction. If you see a random identification / authentication request on the screen, ignore it. If this happens again, contact our customer service and we will help you identify what needs to be done next.
g) Do not download unauthorized / illegal software and do not access links that promise free access to goods or functions that one would normally have to pay for. Google Play and the AppStore are recommended locations for software updates and installation of new applications.
h) Keep your software up to date. Regular updates to your operating system and applications ensure that you have the best protection against security risks. The most effective way to make sure your software is always up to date is to enable automatic updates.
i) Purchase mobile terminals only from authorized sellers or trusted persons who can prove that they are the rightful owners. Stolen devices are susceptible to hacking, are unsafe, and can cause problems with the performance of installed applications.
j) The only way to make sure that no one else adds applications or unwanted operations to your device is to not allow other people to access the device.

The certME mobile app is designed NOT to work on devices that:

- don’t support Secure Element/Enclave;
- are rooted/jailbroken;
- don’t support strong biometric authentication features;
- have lock screen security disabled;
- have biometric authentication disabled;

The certME mobile app is designed to delete all key material and all personal data associated with the user’s certME eID (rendering the electronic means of identification unusable) in the following cases:

- The device is rooted/jailbroken;

- The device's lock screen security is disabled;
- The device's biometric authentication is disabled.

2 Recomandări privind precauții de securitate

a) Aplicația mobilă certME funcționează numai pe dispozitive mobile dotate cu elemente sau enclave securizate pentru stocarea cheilor și a parolelor.
b) Pentru ușurință în utilizare și securitate sporită, aplicația mobilă certME funcționează numai pe dispozitive mobile dotate cu mijloace de autentificare biometrică sigure.
c) Aplicația mobilă certME funcționează numai pe dispozitive mobile care au activă funcția de blocare a ecranului prin PIN, tipar, parolă sau autentificare biometrică. Pentru protecția utilizatorilor, dezactivarea funcției de blocare a ecranului conduce la ștergerea tuturor datelor asociate mijlocului de identificare certME și imposibilitatea utilizării acestuia până la reefectuarea verificării identității la unul dintre partenerii certME.
d) Aplicația mobilă certME nu funcționează pe dispozitive mobile "rooted" sau "jailbroken". Pentru protecția utilizatorilor, aplicarea unui proces de "rooting" sau "jailbreak" asupra dispozitivului conduce la ștergerea tuturor datelor asociate mijlocului de identificare certME și imposibilitatea utilizării acestuia.
e) Nu permiteți altor persoane să înregistreze elemente biometrice în dispozitivul dumneavoastră, nici măcar membrilor familiei. Atât timp cât sunteți singura persoană care se poate autentifica biometric în dispozitivul dumneavoastră, nimeni altcineva nu vă poate folosi mijlocul de identificare certME pentru a vă identifica în mediul online sau a accesa datele dumneavoastră.
f) Nu autorizați cererile de identificare sau autentificare dacă nu ați inițiat dumneavoastră tranzacția. Dacă vedeți o cerere de identificare/autentificarea aleatorie pe ecran, ignorați-o. Dacă se întâmplă din nou, contactați serviciul nostru pentru clienți și vă vom ajuta să identificați ce trebuie făcut în continuare.
g) Nu descărcați aplicații software neautorizate / ilegale și nu accesați link-uri care va promit acces gratuit la bunuri sau funcții care în mod normal costă. Google Play și AppStore sunt locațiile recomandate pentru a face actualizări software și instalarea de aplicații noi.
h) Mențineți aplicațiile software actualizate la zi. Actualizările periodice ale sistemului de operare și ale aplicațiilor vă asigură că aveți cea mai bună protecție împotriva riscurilor de securitate. Cel mai eficient mod de a vă asigura că software-ul este actualizat mereu este să activați actualizările automate.
i) Achiziționați terminale mobile doar de la vânzătorii autorizați sau persoane de încredere care pot demonstra că sunt proprietarii de drept al acestora. Dispozitivele furate sunt susceptibile la hacking, sunt nesigure și pot cauza probleme în performanța aplicațiilor instalate.
j) Singura modalitate de a vă asigura că nimeni altcineva nu adaugă aplicații sau nu face operații nedorite pe dispozitivul dumneavoastră este să nu permiteți accesul altor persoane la dispozitiv.

Aplicația mobilă certME este proiectată să nu funcționeze pe dispozitive care:
• nu acceptă Secure Element / Enclave;
• sunt înrădăcinate / jailbroken;
• nu acceptă caracteristici puternice de autentificare biometrică;
• ați dezactivat securitatea ecranului de blocare;
• au dezactivat autentificarea biometrică;

Aplicația mobilă certME este concepută pentru a șterge toate materialele cheie și toate datele personale asociate cu ID-ul certME al utilizatorului (care face inutilizabile mijloacele electronice de identificare) în următoarele cazuri:
• Dispozitivul este înrădăcinat / jailbroken;
• Securitatea ecranului de blocare a dispozitivului este dezactivată;

VAT Code: RO18288250, Trade Register: J40/484/2006, Registered Capital: 1,971,000;
Registered Office: 107A Oltenitei Avenue, C1 Building, Ground Floor, S4, 041303, Bucharest
Telephone: +40 31 101 18 70; Fax: +40 21 311 99 05; E-mail: office@certsign.ro;
ISO 9001-26325/06/R, ISO 14001-EMS-3928/R, OHSAS 18001-OHS-957, ISO 27001-111/10 : RINA SIMTEX-RENAR;
ISO 9001-IT-85030, ISO 14001-IT-84805, OHSAS 18001-IT-84806, ISO 27001-IT-850322: IQNET
ISO 20000-1 - ITSMS-31/13: ACCREDIA; Personal Data Operator, registered under No. 3160

- Autentificarea biometrică a dispozitivului este dezactivată.