Zentrum für sichere Informationstechnologie – Austria
Secure Information Technology Center – Austria

A-1030 Wien, Seidlgasse 22 / 9
Tel.: (+43 1) 503 19 63–0
Fax: (+43 1) 503 19 63–66

A-8010 Graz, Inffeldgasse 16a
Tel.: (+43 316) 873-5514
Fax: (+43 316) 873-5520

http://www.a-sit.at
E-Mail: office@a-sit.at

DVR: 1035461 ZVR: 948166612 UID: ATU60778947

Subject: Confirmation Certificate A-SIT-VI-16-057 (Secure Signature Creation Device: CardOS V5.3 QES, V1.0), dated 2016-06-24[1]

To Atos IT Solutions and Services GmbH
To whom it may concern

Dear Sir or Madam,

The German Federal Office for Information Security ("Bundesamt für Sicherheit in der Informationstechnik" – BSI) has issued an Assurance Continuity Maintenance Report (BSI-DSZ-CC-0921-2014-MA-01) for the Common Criteria certificate BSI-DSZ-CC-0921-2014 that is underlying the confirmation certificate A-SIT-VI-16-057 (Secure Signature-Creation Device: CardOS V5.3 QES, V1.0) issued by A-SIT.

The certified product CardOS V5.3 QES, V1.0 itself did not change. The changes are related to the scope and method on how to use the product, specifically as a qualified electronic signature creation device according to Regulation (EU) 910/2014 ("eIDAS")[2].

Thus **the confirmation certificate A-SIT-VI-16-057 stays valid** and the Assurance Continuity Maintenance Report has to be applied to the confirmation certificate. When using the product as a qualified electronic signature creation device the guidance documentation as listed in the confirmation certificate has to be used, whereby – as a consequence of the application of the Assurance Continuity Maintenance Report – the following constraints have to be taken into account:

- When using the product with on chip generated **RSA keys only the key length values 3072 bit and 3584 bit provide a required level of security** of at least 100 bit. If other key length values for RSA keys generated by the product are being used, a specific assessment on the appropriateness supported by Atos and Infineon has to be made within the context of the specific application. The **trust service provider using the product has**

[1] published at: https://www.a-sit.at/pdfs/bescheinigungen_sig/VI-16-057_bescheinigung_cardos-v53qes_signed.pdf
[2] REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

to take appropriate measures to ensure that key length values providing the right level of security are used.

- Constraints on cryptographic algorithms and parameters have to be considered. These constraints may cover in particular RSA, DSA, Elliptic Curve cryptography, hash algorithms, or random number generation.

Sincerely,

A-SIT Secure Information Technology Center – Austria

SIGNATURE INFORMATION	**Signatory**	Reinhard Posch
	Date/Time-UTC	2017-07-17T23:33:02+02:00
	Verification	Information about the verification of the electronic signature can be found at: https://www.signaturpruefung.gv.at
Note	This document is signed with a qualified electronic signature. According to Art. 25 para. 2 of the Regulation (EU) No 910/2014 of 23. July 2014 ("eIDAS-Regulation") it shall have the equivalent legal effect of a handwritten signature.	

Prof. DI Dr. Reinhard Posch, Director