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

CLARIFICATION NOTE

Subject: Clarification Note ref. to Confirmation Nr. A-SIT-1.115 (AliasLab CryptoAccelerator, release 3.4.3), dated 2015-07-27[1]

To AliasLab SpA

To whom it may concern

Dear Sir or Madam,

Regarding the above mentioned Confirmation Certificate pursuant to § 18 para. 5 SigG and following your clarification request, we are pleased to specify the following:

(1) Our Confirmation Certificate has only in scope the SSCD (AliasLab CryptoAccelerator, release 3.4.3) and not the SSCD system environment as clearly stated in Chapter 4, point (1) of the same Confirmation Certificate and required by the Austrian Signature Law as well as the European Signature Directive (1999/93/EC)[2].

(2) Credentials management and Strong Authentication methods described in paragraph *"1. Product Description"* of the same Confirmation Certificate are, therefore, out of scope from the SSCD confirmation itself and have to be considered as general recommendations for appropriate deployment scenarios according to Austrian regulations (SigG and SigV).

(3) The Strong Authentication methods described within the referred Confirmation Certificate have not to be considered the only accepted methodologies; in fact, alternative Strong Authentication methods, that are equivalent in terms of security (i.e. the signature-creation-data used for signature generation can be protected by the legitimate signatory against the use of others with the same level of reliability) and respect of general recommendations from SigG and SigV, are also acceptable.

(4) The elements necessary for the implementation of the Strong Authentication methods (OTP devices, OTP validation servers, SMS Gateways, SecureCall Servers, signature pads, PIN entry devices, etc.) as well as the more general system environment elements are out of scope from the SSCD certification. We leave the evaluation of these aspects to the relevant Supervisory Authority of any European country that implements Directive 1999/93/EC (e.g. AGID - Agenzia per l'Italia Digitale for Italy). This also corresponds to the statement made in paragraph *"4. Operating Conditions"* of the same Confirmation Certificate: *"The validity of this confirmation is subject to the conditions stated below. The measures taken shall be ascertained by the CSP's security and certification policy in accordance with § 12 SigV, integrated into the guidance of the signatory and their effect shall be ensured by means of supervision."*

[1] published at: https://www.a-sit.at/pdfs/bescheinigungen_sig/1115_confirmation_cryptoaccelarator343_signed.pdf

We remain at disposal of AliasLab or eventually interested National Supervisory Authorities for any additional clarification might be needed.

Sincerely,

SIGNATURE INFORMATION	**Signatory**	Reinhard Posch
	Date/Time-UTC	2015-08-21T10:31:09+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 § 4 art. 1 of the Signature Act.	

Prof. Dr. Reinhard Posch
Director

A-SIT, Secure Information Technology Center – Austria

[2] see recital (15) of Directive 1999/93/EC*: 'Annex III covers requirements for secure signature-creation devices to ensure the functionality of advanced electronic signatures; it does not cover the entire system environment in which such devices operate;'*