CUSTOMS AUTHORITY FOR ADVANCE RULINGS
NEW CUSTOM HOUSE, BALLARD ESTATE, MUMBAI - 400 001
E-MAIL: cus-advrulings.mum@gov.in
The 04th of May, 2023
Ruling No. CAAR/Mum/ARC/33/2023
in
Application No. CAAR/CUS/APPL/90/2022/ O/o Commr-CAAR-MUMBAI

****

Name and address of the applicant:	M/s. Pagaria Infotech Ventures LLP
Commissioner concerned:	Commissioner of Customs, Mumbai III (Import), Air Cargo Complex, Sahar, Andheri [East], Mumbai
Present for the applicant:	Shri Ankush B. Pagaria, Shri Rajesh Gosalia
Present for the Department:	--

M/s. Pagaria Infotech Ventures LLP (hereinafter referred to as 'the applicant', in short) filed an application for advance ruling before the Customs Authority for Advance Rulings, Mumbai (CAAR, in short). The said application was received in the secretariat of the CAAR, Mumbai on 26.12.2022, along with its enclosures in terms of Section 28H (1) of the Customs Act, 1962 (hereinafter referred to as the 'Act'). The applicant is seeking advance ruling on the classification of 'Cryptogenic Device/Token' (ProxKey and ProxKey PRO) (hereinafter referred to as 'subject goods'), proposed to be imported and applicability of Sr. No. 2 of Notification No. 24/2005-Customs, dated 01.03.2005, as amended.

2.   The applicant is a registered LLP (Limited Liability Partnership) company involved in the business of trading. The applicant is intending to import 'Cryptogenic Device/Token' (ProxKey and ProxKey PRO) (herein after referred as 'subject goods'). In their submissions the applicant has stated the following:

2.1   Both ProxKey & ProxKey PRO represent the same product with same functions, technical specification with different brand name on hardware and its associated middleware/drivers & physical appearance in terms of color.

2.2   Products Overview, Features & Appearance-:
a.   Cryptographic Device/Token is very portable, easy-to-use and cost-effective solution for strong authentication, secure access and online transactions. It features a plug-and-play capability that brings convenience to end users and is designed to meet the demand for secure, fast and reliable external tokens with built-in secure mechanisms and designed to function with computer systems and automated data processing machined with varied configurations and operating systems.

b.   They are among the securest and lightest cryptographic USB tokens in the world, complying with the most stringent international standards, like ISO 7816 4, 8, 9, FIPS140-2 certified and possesses the most reliable encrypting capabilities like DES, 3DES and RSA. The chip embedded in the device is a highly secure data container as the private key stored on the chip and can never be exported. With this device, users can access web-based applications, corporate networks and carry out online transactions easily, conveniently for consumers; the convenience of a robust yet simple "plug and-play" solution is unbeatable

c.   The products also embodie an internal SPI Flash simulating CD-ROM for Auto Run Plug & Play feature, which provides the software package of mini-driver and allows the user to have a convenient experience.

2.3   Products Usage & Functioning

a.   The products closely resemble to USB Flash Drives/ Pen drive as covered under heading 8523 in physical appearance only but its functions, specifications & usage cannot even be remotely linked to USB Flash Drives/ Pen drive.

b.   The products used to generate the private key of digital signature which in turn is securely retained in the device and is used to authenticate an electronic record function, using the process of asymmetric cryptography and hash. The Information Technology Act, 2000 (ITA) defines a "digital signature" to mean authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of Section 3 of the ITA.

c.   Rule 3 of the Information Technology (Certifying Authorities) Rules, 2000 (extracted below for ready reference) specifies the manner in which information is to be authenticated by means of a digital signature viz., hash function. It would be observed there from that the digital signature shall be created and verified by the process of hash function using asymmetric cryptography. "Asymmetric crypto system" is defined in Section2(1) (f) of the ITA to mean a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature.

d.   The manner in which information be authenticated by means of Digital Signature. - A Digital Signature shall: -
(a)   Be created and verified by cryptography that concerns itself with transforming
Electronic record into seemingly unintelligible forms and back again;
(b)   Use what is known as "Public Key Cryptography", which employs an algorithm using two different but mathematical related "keys" – one for creating a Digital Signature or transforming data into a seemingly unintelligible form, and another key for verifying a Digital Signature or returning the electronic record to original form, the process termed as hash function shall be used in both creating and verifying a Digital Signature.

e.   Further the Information Technology Act 2000, mandates that the key pair of the user must be mandatorily generated on the FIPS -140-2 Level 2 validated cryptographic Module / Hardware. The Federal Information Processing Standard [FIPS] 140-2 is a U.S. government computer security standard used to approve cryptographic modules. The National Institute of Standards and Technology (NIST) issued the FIPS 140 Publication Series to coordinate the requirements and standards for cryptography modules that include both hardware and software components. Protection of a cryptographic module within a security system is necessary to maintain the confidentiality and integrity of the information protected by the module. This standard specifies the security requirements that will be satisfied by a cryptographic module.

f.   The products barely have only 1 critical component which determines the functioning of the product i.e. AS518 in the form of Crypto processor IC mounted on the PCB version no

K023314A having an USB Interface. AS518 series is a high-performance 32-bit micro-processor based on ARM Cortex-M. The IC has its own RAM, Memory, CPU and various interfaces like USB, SPI, and UART. The IC has built-in hardware algorithm coprocessor provides excellent performance DES/3DES, AES, SHA, RSA, ECC and other security algorithm module for signing, encryption and authentication. In common parlance these IC's together with all its embedded components, firmware and algorithms are also referred to as Crypto Modules, Crypto Processors, Co Processors, Crypto CPU. This Crypto IC along with its PCB version, Firmware and physical body are validated for FIPS 140-2 Cryptographic Module Validation Program. The various algorithms like DES, AES, RSA, ECDSA, HMAC, SHA, DRBG which the crypto processor support are approved by FIPS - Cryptographic Algorithm Validation Program [CAVP]. The, Crypto processor, PCB, USB Interface, Led Indicator, Plastic enclosure along with its firmware, driver and middleware together form the final product under discussion i.e. Cryptographic Device / Token

g.   Sec 3 of IT Act 2000 provides for "Authentication of Online record by affixing a Digital Signature". The Gazette Notification 735(E) dated 24th October 2004 which contains the Rules to be read in conjunction with section 16 of the IT Act 2000 defines the Secure Electronic Record to be one that has been authenticated by means of a Secure Digital Signature. To create a Secure Digital Signature a hardware token with cryptographic module has be used to create the key pair. The content to be signed /encrypted should go from the host system to the cryptographic device and the signed /encrypted content to be returned to the host system. The products are one such hardware token device with cryptographic processor to be used for the purpose and mentioned aforesaid. Further it is also submitted that user's private and public key pairs can be generated and retained only on the memory of the Crypto Processor / Module. The Crypto Processor / Module has very limited memory of 256 KB out of which only 64KB can be used to store the user's private and public key pairs. The user's key pairs reside in the memory of the Crypto Processor / Module and the private keys can never be exported.

h.   The products are used for digital signature authentication/identification purposes using a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature using the cryptographic modules / Crypto Processor / Crypto CPU and validated algorithms.

i.   The products cannot be operated on a standalone basis and it should be operated along with a computer system for its authentication and identification. The products when connected with the computer or ADP read the data embedded in the device and send the information to the network / server to get the authentication for the transaction. Thus it means that mere token/device alone is not sufficient and it has to get connected to the computer system to access the network / server to send the details for its authentication / identification. Cryptographic Device cannot work without an ADPS.

j.   Rule 2 of the Information Technology (Security Procedure) Rules, 2004 defines "hardware token" to mean a token which can be connected to any computer system using Universal Serial Bus (USB) port." Thus the IT law itself recognizes the Cryptographic Device as a device, which is connected to the computer system by using USB port

k.   The products have an auto run plug and play feature which when connected to the ADPS automatically install the drivers / middleware of the product which are preloaded in the memory of the product. The memory is 2MB in size and contains only the drivers / middleware of the product which is loaded from the factory during production. This memory is out of the scope of the crypto processor and in no manner impact, enhances, reduce the function and performance of the device core functionality. The driver and middleware preloaded in the product pertains to the

product only and cannot be used for any other purpose or as general purpose software. The user of the product in no manner can add, erase or modify any content in this memory.

2.4   The applicant wished to classify goods under heading 8471 80 00 - Other units of automatic data processing machines or 8473 30 99- Others - Parts and accessories of the machines heading 8471 (ADPS) and also eligible to avail benefit under Sr. 2 of Notification No 24/2005- Customs

1.   The applicant hereby submitted of following statements with respect to Interpretation of Law for classification of product 'Cryptographic Device/Token'-:

3.1   To determine the CTH of the goods reference is hereby made to the Rule 1 of 'general rules for the interpretation of the harmonized system' (GIR) which states as under:

"The titles of Sections, Chapters and sub-Chapters are provided for ease of reference only; for legal purposes, classification shall be determined according to the terms of the headings and any relative Section or Chapter Notes and, provided such headings or Notes do not otherwise require, according to the following provisions"

It is further submitted that the as per Rule 1 of 'General rules for the interpretation of the harmonized system' the headings, relative section or chapter notes should be applied first to determine the classification of goods. Also subsequent rules should be referred only when the classification cannot be done in accordance with Rule 1. Thus is clear that as principles laid down in GIR, for legal purposes, classification of goods shall be determined according to the terms of the headings and any relative Section or Chapter Notes. The goods under consideration are classified with reference to the headings and any relative Section or Chapter Notes.

3.2   For ease of reference, the relevant portions of CTH 8471 are reproduced as under:

8471	Automatic data processing machines and units, thereof; magnetic or optical readers, machines for transcribing data on to data media in coded form and machines for processing such data, not elsewhere specified or included	
8471 30	-	Portable automatic data processing machines, weighing not more than 10 kg, consisting of at least a central processing unit, a keyboard and a display:
8471 30 10	---	Personal computer
8471 30 90	---	Other
	-	Other automatic data processing machines :
8471 41	--	Comprising in the same housing at least a central processing unit and an input and output unit, whether or not combined :
8471 41 10	---	Micro computer
8471 41 20	---	Large or main frame computer
8471 41 90	---	Other
8471 49 00	--	Presented in the form of systems
8471 50 00	-	Processing units other than those of sub-headings 8471 41or 8471 49, whether or not containing in he same housing one or two of the following types of unit: storage units, input units, output units
8471 60	-	Input or output units, whether or not containing storage units in the same housing
8471 60 10	---	Combined input or output units
	---	Printer :
8471 60 24	---	Graphic printer

8471 60 25	----	Plotter
8471 60 29	----	Other
8471 60 40	---	Keyboard
8471 60 50	---	Scanners
8471 60 60	---	Mouse
8471 60 90	---	Other
8471 70	-	Storage units :
8471 70 10	---	Floppy disc drives
8471 70 20	---	Hard disc drives
8471 70 30	---	Removable or exchangeable disc drives
8471 70 40	---	Magnetic tape drives
8471 70 50	---	Cartridge tape drive
8471 70 60	---	CD-ROM drive
8471 70 70	---	Digital video disc drive
8471 70 90	---	Other
8471 80 00	-	Other units of automatic data processing machines
8471 90 00	-	Other

The products under consideration are proposed to classified under CTH 8471 80 00 in accordance as 'Other units of automatic data processing machines'.

3.3 Chapter Notes 5C lays down the principles for units to be regarded as being part of an automatic data processing system considered under 8471. Relevant extracts of the Notes

B. Automatic data processing machines may be in the form of systems consisting of a variable number of separate units.

C. Subject to paragraphs (D) and (E), a unit is to be regarded as being part of an automatic dataprocessing system if it meets all of the following conditions:
   (i) It is of a kind solely or principally used in an automatic data processing system;
   (ii) It is connectable to the central processing unit either directly or through one or more other units; and
   (iii) It is able to accept or deliver data in a form (codes or signals) which can be used by the system

Separately presented units of an automatic data processing machine are to be classified in heading 8471. However, keyboards, X-Y co-ordinate input devices and disk storage units which satisfy theconditions of (ii) and (iii) above, are in all cases to be classified as units of heading 8471.

D. Heading 8471 does not cover the following when presented separately, even if they meet allof the conditions set forth in paragraph (C):

(i) printers, copying machines, facsimile machines, whether or not combined;
(ii) apparatus for the transmission or reception of voice, images or other data, including apparatusfor communication in a wired or wireless network (such as a local or wide area network);
(iii) loudspeakers and microphones;
(iv) television cameras, digital cameras and video camera recorders;
(v) Monitors and projectors, not incorporating television reception apparatus.

E.   Machines incorporating or working in conjunction with an automatic data processing machineand performing a specific function other than data processing are to be classified in the headings appropriate to their respective functions or, failing that, in residual headings

3.4   Explanatory notes of WCO for CTH 8471

a.   Subject to the provisions of Notes 5 (D) and (E) to this Chapter, this heading also covers separately presented constituent units of automatic data processing systems. These may be in the form of units having a separate housing or in the form of units not having a separate housing and designed to be inserted into a machine. Constituent units are those defined in Part (A) above and in the following paragraphs, as being parts of a complete system.

b.   An apparatus can only be classified in this heading as a unit of an automatic data processing system if it:
    (a) Performs a data processing function;
    (b) Meets the following criteria set out in Note 5 (C) to this Chapter:
    (i) It is of a kind solely or principally used in an automatic data processing system;
    (ii) It is connectable to the central processing unit either directly or through one or more other units; and
    (iii) It is able to accept or deliver data in a form (codes or signals) which can be used by the system.
    (c) Is not excluded by the provisions of Notes 5 (D) and (E) to this Chapter.

c.   In accordance with the last paragraph of Note 5 (C) to this Chapter, keyboards, X-Y co-ordinate input devices and disc storage units which satisfy the conditions of items (b) (ii) and (iii) above, are in all cases to be classified as constituent units of data processing systems.

d.   If the unit performs a specific function other than data processing, it is to be classified in the heading appropriate to that function or, failing that, in a residual heading (see Note 5 (E) to this Chapter). If an apparatus does not meet the criteria set out in Note 5 (C) to this Chapter, or is not performing a data processing function, it is to be classified according to its characteristics by application of General Interpretative Rule 1, if necessary in combination with General Interpretative Rule 3 (a).

Compliance of Chapter note 5C by the product

Principles	Comments
It is of a kind solely or principally used in an automatic data processing system	The ADP system send the data to the product for signing / Encryption / Authentication. The content on the ADP system which is to be signed /Encrypted should go from the ADP system to the product and the signed /Encrypted/ Authentication content is returned to the host system. Thus it means that mere token/device alone is not sufficient and it has to get connected to the computer system to receive the data from ADP System signing / Encryption / Authentication. Product cannot work without a computer system. Even the product does not have its own power source. To perform its data processing functions it need to draw power from its host ADPS.

It is connectable to the central processing unit either directly or through one or more other units	Rule 2 of the Information Technology (Security Procedure) Rules, 2004 defines "hardware token" to mean a token which can be connected to any computer system using Universal Serial Bus (USB) port." Thus the IT law itself recognizes the Cryptographic Device as a device, which is connected to the computer system by using USB port.
It is able to accept or deliver data in a form (codes or signals) which can be used by the system	The content to be signed flows thought the USB port to product and after the electronic record received by the product is converted into an unintelligible form by the private key, another key i.e. the public key returns the electronic record to the original form along with the signature (in this case digital) and transmits the data back to the ADPM to enable it to be printed or electronically transmitted to another device through mail or any other form of transfer. The documents would have the inscription "Digitally Signed by _ _ _ _"
Not excluded by the provisions of Notes 5 (D) and (E) to this Chapter	The product is specifically not covered under list of goods as mentioned in note 5(D). Also product is also excluded from Clause 5(E) since the device has only one core component which is a crypto processor which performs data processing function.

3.5   Classification opinion of WCO for Sub heading 8471 80 is reproduced as under
Cryptographic processor containing a Data Encryption Standard (DES) encryption algorithm, which is connected as a peripheral device to one or more automatic data processing machines from which it receives commands to perform pre-programmed operations. Its function is to provide the necessary data security functions (e.g., authentication and encryption) which would otherwise have to be performed by software loaded onto the host automatic data processing machine; this eliminates the need for storage of certain security data bases in the automatic data processing machine(s). The functions of the apparatus are controlled by firmware (a chip containing a programme) installed in the product at the manufacturing process. The apparatus has an RS 232C physical interface to an automatic data processing machine. With suitable modification of the firmware, it can be used in various financial institutions for purposes such as generating the cryptographic values used in credit or debit cards or for providing data security in financial transactions. Adoption: 1998

3.6   The products under consideration confirm the same functions, usage and specifications of a crypto processor which is connected as peripheral device to an ADP machines through USB. Thus even in the classification opinion of the WCO the product is rightly classifiable under 8471 80 which is evidence by a specific reference to the product. The product contains a crypto processor in the form of IC mounted on the PCB with USB interface to perform the security functions of signing, encryption and authentication.

8473	Parts and accessories (other than covers, carrying cases and the like) suitable for use solely or principally with machines headings 8470 to 8472	
	-	Parts and accessories of the machines
		heading 8470:

8473 21 00	--	Of the electronic calculating machines of sub-heading 8470 10, 8470 21 or 8471 29
8473 29 00	--	Other
8473 30	-	Parts and accessories of the machines heading 8471:
8473 30 10	---	Microprocessors
8473 30 20	---	Motherboards
8473 30 30	---	Other mounted printed circuit boards
8473 30 40	---	Head stack
	---	Other :
8473 30 91	----	Network access controllers
8473 30 92	----	Graphic and intelligence based script technology (GIST) cards for multilingual computers
8473 30 99	----	Other

The products also merit classification under 8473 30 99 Parts and Accessories (Other than covers, carrying cases and the like) suitable for use solely or principally with machines of heading 8470 to 8472, 847330-Parts and Accessories of machines of heading 8471 are capable of directly connecting to and designed for use with an Automatic Data Processing System (Hereafter known as ADPS) of Heading 8471. Relevant headings reproduced as under

The accessories covered by this heading are interchangeable parts or devices designed to adapt a machine for a particular operation, or to perform a particular service relative to the main function of the machine, or to increase its range of operations. Further accessory is in the nature of having a secondary, supplementary or subordinate function by accompanying as a subordinate; aiding in a secondary way; being additional; contributing or being contributory

The products are also in the nature of an accessory which has to be used only with ADP machine for a very distinct function of generating digital certificates and signing, encryption & authentication of data. The said function is relative or supplementary to the main function of ADP System.

For the ease of reference relevant portions of chapter 8523 are also reproduced as under:

8523		Discs, tapes, solid-state non-volatile , storage devices, "smart cards" and other media for the recording of sound or of other phenomena, whether or not recorded , including matrices and masters for the production of discs, but excluding products of chapter 37
	-	Semi-conductor media
8523 51 00	--	Solid-state non-volatile storage devices
8523 52	--	Smart cards
8523 52 10	---	SIM cards
8523 52 20	---	Memory Cards

8523 52 90	---	Other
8523 59	--	Other
8523 59 10	---	Proximity cards and tags
8523 59 90	---	Other

3.8   Chapter Notes to 85
Note 6: for the purposes of heading 85.23:
"Solid-state non-volatile storage devices" (for example, "flash memory cards" or "flash electronic storage cards") are storage devices with a connecting socket, comprising in the same housing one or more flash memories (for example, "FLASH E2PROM") in the form of integrated circuits mounted on a printed circuit board. They may include a controller in the form of an integrated circuit and discrete passive components, such as capacitors and resistors;

3.9 WCO Explanatory notes for Chapter 85
This Chapter covers all electrical machinery and equipment, other than:
(a)   Machinery and apparatus of a kind covered by Chapter 84, which remains classified there even if electric (see the General Explanatory Note to that Chapter). and
(b)   Certain goods excluded from the Section as a whole (see the General Explanatory   Note to Section XVI).

3.10 WCO Explanatory notes for heading 8523

a.   This heading covers different types of media, whether or not recorded, for the recording of sound or of other phenomena (e.g., numerical data; text; images, video or other graphical data; software). Such media are generally inserted into or removed from recording or reading apparatus and may be transferred from one recording or reading apparatus to another.

b.   The media of this heading may be presented recorded, unrecorded, or with some pre-recorded information, but capable of having more information recorded on them.

c.   Solid-state, non-volatile data storage devices for recording data from an external source (See Note 6 (a) to this chapter). These devices (also known as "flash memory cards" or "flash electronic storage cards") are used for recording data from an external source, or providing data to, devices such as navigation and global positioning systems, data collection terminals, portable scanners, medical monitoring appliances, audio recording apparatus, personal communicators, mobile phones, digital cameras and automatic data processing machines. Generally, the data are stored onto, and read from, the device once it has been connected to that particular appliance, but can also be uploaded onto or downloaded from an automatic data processing machine.

d.   The media use only power supplied from the appliances to which they are connected, and require no battery.

e.   These non-volatile data storage devices are comprised of, in the same housing, one or more flash memories ("FLASH E2PROM/EEPROM") in the form of integrated circuits mounted on a printed circuit board, and incorporate a connecting socket to a host appliance. They may include capacitors, resistors and a microcontroller in the form of an integrated circuit. Example of solid state non-volatile storage devices are USB flash drives.
        The product under consideration in no manner merits classification under heading 8523. The product is very specific to its data processing functions which has a very specific and apt entry under the heading 8471 80. The WCO Explanatory notes for Chapter 85 itself excludes products which are specifically covered under 84.

3.11   Explanatory notes of WCO for heading 8523 which inter alia expressly denotes that the data must be transferrable from the ADP system to the product and also capable of transferring to other ADPS. Further the product should also have capability to record more information onto the media. For the product under the consideration even the private keys of the digital signature are generated inside the product and retained in its secured container in encrypted form and not transferred from the ADP. Further even the private key in the secured container, whether generated or imported in the product, cannot be exported or read by the ADP system to which it is connected. It can only be used by the product to perform its cryptographic functions like signing, encryption and authentication on the data received from the ADPS within the boundary of its crypto processor and return back the processed data to the ADPS.

3.12   Even though the product contains small flash storage of 2 MB for auto run plug and play feature loaded with its middleware from factory, it does not merit classification under heading 8523 as functions and characteristics should be borne in mind while determining the classification. The product does not have any function which can even remotely be related to that of a flash drive as used in general parlance. The classification of goods should be based on its primary function. When a user buys the product under consideration, he buys it for its function of Digital Signature, Signing, Encryption and Authentication and not to use as a flash drive or pen drive. Further the presence of the auto run facility for loading the middleware of the product is only a matter of convenient and its presence or absence does not impact the functioning of the product for its intended use. Even in the absence of the flash memory in which the middleware is loaded, the same could also be downloaded freely from the internet or external sources for the intended use of the product. The fact that the user of the product in no manner can add, erase or modify any content in this memory itself justifies that it cannot be categorized under heading 8523 or any other its sub headings. The product cannot be compared with a device of nature mentioned under chapter heading 8523

3.13   In view of the above submission, the product under consideration merits classification under 8471 80 00 as other units of automatic data processing machines or under 8473 30 99- Others - Parts and accessories of the machines heading 8471 (ADPS). However, the product has specific character which are in consonance with principles laid to Chapter note 5C of 84, WCO Explanatory notes to 8471 80 and specific product entry of WCO classification opinion under 8471 80, the product with classifiable under the product with classifiable under CTH 8471 80 00 as other units of automatic data processing machines and eligible to avail benefit under benefit under Sr. 2 of Notification No 24/2005- Customs

2.   The applicant in their CAAR-I form declared that they intend to import the impugned devices, under the jurisdiction of Commissioner of Customs, Mumbai III (Import), Air Cargo Complex, Sahar, Andheri [East], Mumbai- 400099. His application, therefore was forwarded to the jurisdictional commissioner of customs for comments. However, no reply has been received, though reminders have also been sent.

3.   A personal hearing was held on 30.01.2023 at 15:30 hrs. Shri Ankush B. Pagaria and Shri Rajesh Gosalia represented the applicant. No one appeared on behalf of the commissioner of customs. The representatives reiterated the contents of CAAR-1 application. They invited attention to CTHs 8471 80 00 and 8473 30 99. Further they referred to WCO advisory on the classification of cryptographic device recommending classification under CTH 8471 80. They requested to issue a classification ruling based on WCO advisory as well as description of CTH 8471 8000. Applicant has made exhaustive submissions primarily focusing on technical features of the products, their usages, legal framework governing classification of cryptographic device including provisions of information technology act 2000, relevant extracts of first schedule to the Customs Tariff Act, 1975, HSN Explanatory Notes and provisions of General Rules of Interpretation. At serial no. 11 of the CAAR 1 form applicant has declared that question(s) raised in instant application is not

pending in the applicant's case in any of the forums mentioned in section 28(I) of the Customs Act, 1962.

5.1   At the outset and at the cost of repetition I agree with the following submissions of the applicant.

5.1.1   The applicant is a registered LLP (Limited Liability Partnership) company involved in the business of trading. The applicant is intending to import 'Cryptogenic Device/Token' (ProxKey and ProxKey PRO) (herein after referred as 'subject goods').

5.1.2   The applicant is seeking advance ruling on the classification of 'Cryptogenic Device/Token' (ProxKey and ProxKey PRO) (hereinafter referred to as 'subject goods'), proposed to be imported and applicability of Sr. No. 2 of Notification No. 24/2005-Customs, dated 01.03.2005, as amended.

5.1.3   Both ProxKey & ProxKey PRO represent the same product with same functions; technical specification with different brand name on hardware and its associated middleware/drivers & physical appearance in terms of color.

5.1.4   Cryptographic Device/Token is very portable, easy-to-use and cost-effective solution for strong authentication, secure access and online transactions. It features a plug-and-play capability that brings convenience to end users and is designed to meet the demand for secure, fast and reliable external tokens with built-in secure mechanisms and designed to function with computer systems and automated data processing machined with varied configurations and operating systems. They are among the securest and lightest cryptographic USB tokens in the world, complying with the most stringent international standards, like ISO 7816 4, 8, 9, FIPS140-2 certified and possesses the most reliable encrypting capabilities like DES, 3DES and RSA. The chip embedded in the device is a highly secure data container as the private key stored on the chip and can never be exported. With this device, users can access web-based applications, corporate networks and carry out online transactions easily, conveniently for consumers; the convenience of a robust yet simple "plug and-play" solution is unbeatable. The product also embodies an internal SPI Flash simulating CD-ROM for Auto Run Plug & Play feature, which provides the software package of mini-driver and allows the user to have a convenient experience.

5.1.5
a.   The products closely resemble to USB Flash Drives/ Pen drive as covered under heading 8523 in physical appearance only but its functions, specifications & usage cannot even be remotely linked to USB Flash Drives/ Pen drive. The product used to generate the private key of digital signature which in turn is securely retained in the device and is used to authenticate an electronic record function, using the process of asymmetric cryptography and hash. The Information Technology Act, 2000 (ITA) defines a "digital signature" to mean authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of Section 3 of the ITA.

b.   Rule 3 of the Information Technology (Certifying Authorities) Rules, 2000 (extracted below for ready reference) specifies the manner in which information is to be authenticated by means of a digital signature viz., hash function. It would be observed there from that the digital signature shall be created and verified by the process of hash function using asymmetric cryptography. "Asymmetric crypto system" is defined in Section2(1) (f) of the ITA to mean a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature.

c.   The manner in which information be authenticated by means of Digital Signature. - A Digital Signature shall-:

I. Be created and verified by cryptography that concerns itself with transforming Electronic record into seemingly unintelligible forms and back again;

II. Use what is known as "Public Key Cryptography", which employs an algorithm using two different but mathematical related "keys" – one for creating a Digital Signature or transforming data into a seemingly unintelligible form, and another key for verifying a Digital Signature or returning the electronic record to original form, the process termed as hash function shall be used in both creating and verifying a Digital Signature.

d. Further the Information Technology Act 2000, mandates that the key pair of the user must be mandatorily generated on the FIPS -140-2 Level 2 validated cryptographic Module / Hardware. The Federal Information Processing Standard [FIPS] 140-2 is a U.S. government computer security standard used to approve cryptographic modules. The National Institute of Standards and Technology (NIST) issued the FIPS 140 Publication Series to coordinate the requirements and standards for cryptography modules that include both hardware and software components. Protection of a cryptographic module within a security system is necessary to maintain the confidentiality and integrity of the information protected by the module. This standard specifies the security requirements that will be satisfied by a cryptographic module.

e. The products barely have only 1 critical component which determines the functioning of the product i.e. AS518 in the form of Crypto processor IC mounted on the PCB version no K023314A having an USB Interface. AS518 series is a high-performance 32-bit micro-processor based on ARM Cortex-M. The IC has its own RAM, Memory, CPU and various interfaces like USB, SPI, and UART. The IC has built-in hardware algorithm coprocessor provides excellent performance DES/3DES, AES, SHA, RSA, ECC and other security algorithm module for signing, encryption and authentication. In common parlance these IC's together with all its embedded components, firmware and algorithms are also referred to as Crypto Modules, Crypto Processors, Co Processors, Crypto CPU. This Crypto IC along with its PCB version, Firmware and physical body are validated for FIPS 140-2 Cryptographic Module Validation Program. The various algorithms like DES, AES, RSA, ECDSA, HMAC, SHA, DRBG which the crypto processor support are approved by FIPS - Cryptographic Algorithm Validation Program [CAVP]. The, Crypto processor, PCB, USB Interface, Led Indicator, Plastic enclosure along with its firmware, driver and middleware together form the final product under discussion i.e. Cryptographic Device / Token.

5.2 I find that possible tariff headings required to be examined for the classification of impugned goods i.e. cryptographic device/token under the first schedule of Customs Tariff Act, 1975 are 8523, 8471 and 8473. Recourse is required to be taken to HSN Explanatory Notes and GRI. In view of exclusion made in HSN Explanatory Notes for chapter 85 the machinery and apparatus of a kind covered by chapter 84 stands excluded from the scope of any of the headings of chapter 85. In view of this and also due to technicalities discussed in para 5.1.5 earlier I observed that 8523 is not the appropriate classification heading for the impugned products.

5.3 In terms of rule 1 and rule 3 of GRI I find following functional features of the impugned goods are critical in deciding matter of their classification.
The Information Technology Act 2000, mandates that the key pair of the user must be mandatorily generated on the FIPS -140-2 Level 2 validated cryptographic Module / Hardware. The Federal Information Processing Standard [FIPS] 140-2 is a U.S. government computer security standard used to approve cryptographic modules. The National Institute of Standards and Technology (NIST) issued the FIPS 140 Publication Series to coordinate the requirements and standards for cryptography modules that include both hardware and software components. Protection of a cryptographic module within a security system is necessary to maintain the confidentiality and integrity of the information protected by the module. This standard specifies the security requirements that will be satisfied by a cryptographic module.

Sec 3 of IT Act 2000 provides for "Authentication of Online record by affixing a Digital Signature". The Gazette Notification 735(E) dated 24th October 2004 which contains the Rules to be read in conjunction with section 16 of the IT Act 2000 defines the Secure Electronic Record to be one that has been authenticated by means of a Secure Digital Signature. To create a Secure Digital Signature a hardware token with cryptographic module has be used to create the key pair. The content to be signed /encrypted should go from the host system to the cryptographic device and the signed /encrypted content to be returned to the host system. The product is one such hardware token device with cryptographic processor to be used for the purpose and mentioned aforesaid. Further it is also submitted that user's private and public key pairs can be generated and retained only on the memory of the Crypto Processor / Module. The Crypto Processor / Module has very limited memory of 256 KB out of which only 64KB can be used to store the user's private and public key pairs. The user's key pairs reside in the memory of the Crypto Processor / Module and the private keys can never be exported.

The products are used for digital signature authentication/identification purposes using a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature using the cryptographic modules / Crypto Processor / Crypto CPU and validated algorithms.

The products cannot be operated on a standalone basis and they should be operated along with a computer system for its authentication and identification. The product when connected with the computer or ADP reads the data embedded in the device and sends the information to the network / server to get the authentication for the transaction. Thus it means that mere token/device alone is not sufficient and it has to get connected to the computer system to access the network / server to send the details for its authentication / identification. Cryptographic Device cannot work without an ADPS.

Rule 2 of the Information Technology (Security Procedure) Rules, 2004 defines "hardware token" to mean a token which can be connected to any computer system using Universal Serial Bus (USB) port." Thus the IT law itself recognizes the Cryptographic Device as a device, which is connected to the computer system by using USB port.

The products have an auto run plug and play feature which when connected to the ADPS automatically install the drivers / middleware of the product which are preloaded in the memory of the product. The memory is 2MB in size and contains only the drivers / middleware of the product which is loaded from the factory during production. This memory is out of the scope of the crypto processor and in no manner impact, enhances, reduce the function and performance of the device core functionality. The driver and middleware preloaded in the product pertains to the product only and cannot be used for any other purpose or as general purpose software. The user of the product in no manner can add, erase or modify any content in this memory.

Applicant by their own admission has stated that the products under consideration merits classification under 8471 80 00 as other units of automatic data processing machines or under 8473 30 99- Others - Parts and accessories of the machines heading 8471 (ADPS). However, notwithstanding applicant's admission and in view of GRI, I find it essential to examine each of these headings in sequential manner separately.

5.4   For the ease of reference, the relevant portions of CTH 8471 are reproduced as under:

8471		Automatic data processing machines and units, thereof; magnetic or optical readers, machines for transcribing data on to data media in coded form and machines for processing such data, not elsewhere specified or included
8471 30	-	Portable automatic data processing machines, weighing not more than 10 kg, consisting of at least a central processing unit, a keyboard and a display:
8471 30 10	---	Personal computer
8471 30 90	---	Other

	-	Other automatic data processing machines :
8471 41	--	Comprising in the same housing at least a central processing unit and an input and output unit, whether or not combined :
8471 41 10	---	Micro computer
8471 41 20	---	Large or main frame computer
8471 41 90	---	Other
8471 49 00	--	Presented in the form of systems
8471 50 00	-	Processing units other than those of sub-headings 8471 41or 8471 49, whether or not containing in the same housing one or two of the following types of unit: storage units, input units, output units
8471 60	-	Input or output units, whether or not containing storage units in the same housing
8471 60 10	---	Combined input or output units
	---	Printer :
8471 60 24	---	Graphic printer
8471 60 25	----	Plotter
8471 60 29	----	Other
8471 60 40	---	Keyboard
8471 60 50	---	Scanners
8471 60 60	---	Mouse
8471 60 90	---	Other
8471 70	-	Storage units :
8471 70 10	---	Floppy disc drives
8471 70 20	---	Hard disc drives
8471 70 30	---	Removable or exchangeable disc drives
8471 70 40	---	Magnetic tape drives
8471 70 50	---	Cartridge tape drive
8471 70 60	---	CD-ROM drive
8471 70 70	---	Digital video disc drive
8471 70 90	---	Other
8471 80 00	-	Other units of automatic data processing machines
8471 90 00	-	Other

5.5   I also find Chapter Notes 5C lays down the principles for units to be regarded as being part of an   automatic data processing system considered under 8471. Relevant extracts of the Notes

B.   Automatic data processing machines may be in the form of systems consisting of a variable number of separate units.

C.   Subject to paragraphs (D) and (E), a unit is to be regarded as being part of an automatic dataprocessing system if it meets all of the following conditions:

  I.   It is of a kind solely or principally used in an automatic data processing system;

  II.   It is connectable to the central processing unit either directly or through one or more other units; and

  III.   It is able to accept or deliver data in a form (codes or signals) which can be used by the system

    Separately presented units of an automatic data processing machine are to be classified in heading 8471. However, keyboards, X-Y co-ordinate input devices and disk storage units which satisfy theconditions of (ii) and (iii) above, are in all cases to be classified as units of heading 8471.

D.   Heading 8471 does not cover the following when presented separately, even if they meet allof the conditions set forth in paragraph (C):

  I.   printers, copying machines, facsimile machines, whether or not combined;

II.   apparatus for the transmission or reception of voice, images or other data, including apparatusfor communication in a wired or wireless network (such as a local or wide area network);

III.   loudspeakers and microphones;

IV.   television cameras, digital cameras and video camera recorders;

V.   Monitors and projectors, not incorporating television reception apparatus.

E.   Machines incorporating or working in conjunction with an automatic data processing machine and performing a specific function other than data processing are to be classified in the headings appropriate to their respective functions or, failing that, in residual headings

5.6   Applicant has produced following table in support of their claim to compliance of Chapter note 5C by the product

Principles	Comments
It is of a kind solely or principally used in an automatic data processing system	The ADP system send the data to the product for signing / Encryption / Authentication. The content on the ADP system which is to be signed /Encrypted should go from the ADP system to the product and the signed /Encrypted/ Authentication content is returned to the host system. Thus it means that mere token/device alone is not sufficient and it has to get connected to the computer system to receive the data from ADP System signing / Encryption / Authentication. Product cannot work without a computer system. Even the product does not have its own power source. To perform its data processing functions it need to draw power from its host ADPS.
It is connectable to the central processing unit either directly or through one or more other units	Rule 2 of the Information Technology (Security Procedure) Rules, 2004 defines "hardware token" to mean a token which can be connected to any computer system using Universal Serial Bus (USB) port." Thus the IT law itself recognizes the Cryptographic Device as a device, which is connected to the computer system by using USB port.
It is able to accept or deliver data in a form (codes or signals) which can be used by the system	The content to be signed flows thought the USB port to product and after the electronic record received by the product is converted into an unintelligible form by the private key, another key i.e. the public key returns the electronic record to the original form along with the signature (in this case digital) and transmits the data back to the ADPM to enable it to be printed or electronically transmitted to another device through mail or any other form of transfer. The documents would have the inscription "Digitally Signed by _ _ _ "
Not excluded by the provisions of Notes 5 (D) and (E) to this Chapter	The product is specifically not covered under list of goods as mentioned in note 5(D). Also product is also excluded from Clause 5(E) since the device has only one core component which is a crypto processor which performs data processing function.

5.7   In order to examine further details HSN Explanatory Notes are required to be visited. In numerous apex court judgements, the honourable court has admitted importance of HSN Explanatory Notes in deciding the matter of classification under Custom Tariff Act, 1975.

HSN Explanatory note for CTH 8471 reads as follows:

a.   Subject to the provisions of Notes 5 (D) and (E) to this Chapter, this heading also covers separately presented constituent units of automatic data processing systems. These may be in the form of units having a separate housing or in the form of units not having a separate housing and designed to be inserted into a machine. Constituent units are those defined in Part (A) above and in the following paragraphs, as being parts of a complete system.

b.   An apparatus can only be classified in this heading as a unit of an automatic data processing system if it:

(a) Performs a data processing function;

(b) Meets the following criteria set out in Note 5 (C) to this Chapter:

(i) It is of a kind solely or principally used in an automatic data processing system;

(ii) It is connectable to the central processing unit either directly or through one or more other units; and

(iii) It is able to accept or deliver data in a form (codes or signals) which can be used by the system.

(iv) Is not excluded by the provisions of Notes 5 (D) and (E) to this Chapter.

c.   In accordance with the last paragraph of Note 5 (C) to this Chapter, keyboards, X-Y co-ordinate input devices and disc storage units which satisfy the conditions of items (b) (ii) and (iii) above, are in all cases to be classified as constituent units of data processing systems.

d.   If the unit performs a specific function other than data processing, it is to be classified in the heading appropriate to that function or, failing that, in a residual heading (see Note 5 (E) to this Chapter). If an apparatus does not meet the criteria set out in Note 5 (C) to this Chapter, or is not performing a data processing function, it is to be classified according to its characteristics by application of General Interpretative Rule 1, if necessary in combination with General Interpretative Rule 3 (a).

5.8   Classification opinion of WCO for Sub heading 8471 80 is reproduced as under -

Cryptographic processor containing a Data Encryption Standard (DES) encryption algorithm, which is connected as a peripheral device to one or more automatic data processing machines from which it receives commands to perform pre-programmed operations. Its function is to provide the necessary data security functions (e.g., authentication and encryption) which would otherwise have to be performed by software loaded onto the host automatic data processing machine; this eliminates the need for storage of certain security data bases in the automatic data processing machine(s). The functions of the apparatus are controlled by firmware (a chip containing a programme) installed in the product at the manufacturing process. The apparatus has an RS 232C physical interface to an automatic data processing machine. With suitable modification of the firmware, it can be used in various financial institutions for purposes such as generating the cryptographic values used in credit or debit cards or for providing data security in financial transactions. Adoption: 1998.

5.9   Now let us examine the scope of CTH 8473 Parts and accessories (other than covers, carrying cases and the like) suitable for use solely or principally with machines headings 8470 to 8472. The relevant extracts are reproduced below.

Here I find that the CTH 8473 30 covers Parts and accessories of the machines heading 8471. Applicant has submitted that the products also merit classification under 8473 30

8473		Parts and accessories (other than covers, carrying cases and the like) suitable for use solely or principally with machines headings 8470 to 8472
	-	Parts and accessories of the machines heading 8470:
8473 21 00	--	Of the electronic calculating machines of sub-heading 8470 10, 8470 21 or 8471 29
8473 29 00	--	Other
8473 30	-	Parts and accessories of the machines heading 8471:
8473 30 10	---	Microprocessors
8473 30 20	---	Motherboards
8473 30 30	---	Other mounted printed circuit boards
8473 30 40	---	Head stack
	---	Other :
8473 30 91	----	Network access controllers
8473 30 92	----	Graphic and intelligence based script technology (GIST) cards for multilingual computers
8473 30 99	----	Other

99 Parts and Accessories (Other than covers, carrying cases and the like) suitable for use solely or principally with machines of heading 8470 to 8472, 8473 30-Parts and Accessories of machines of heading 8471 are capable of directly connecting to and designed for use with an Automatic Data Processing System (Hereafter known as ADPS) of Heading 8471. The accessories covered by this heading are interchangeable parts or devices designed to adapt a machine for a particular operation, or to perform a particular service relative to the main function of the machine, or to increase its range of operations. Further accessory is in the nature of having a secondary, supplementary or subordinate function by accompanying as a subordinate; aiding in a secondary way; being additional; contributing or being contributory.

5.10   It is observed that the applicant has not ruled out possibility of classification of goods under consideration under 8473 30 and specifically 8473 30 99 as the product is also in the nature of an accessory which has to be used only with ADP machine for a very distinct function of generating digital certificates and signing, encryption & authentication of data. The said function is relative or supplementary to the main function of ADP System. Notwithstanding this I find that classification opinion of WCO for sub heading 8471 80 incudes under its scope a cryptographic processor containing a Data Encryption Standard (DES) encryption algorithm, which is connected as a peripheral device to one or more automatic data processing machines from which it receives commands to perform pre-programmed operations. Its function is to provide the necessary data security functions (e.g., authentication and encryption) which would otherwise have to be performed by software loaded onto the host automatic data processing machine; this eliminates the need for storage of certain security data bases in the automatic data processing machine(s). The functions of the apparatus are controlled by firmware (a chip containing a programme) installed in the product at the manufacturing process. The product contains small flash storage of 2 MB for auto run plug and play feature loaded with its middleware from factory. The product does not have any function which can even remotely be related to that of a flash drive as used in general parlance. Applicant has stated that when a user buys the product under consideration, he buys it for its function of Digital Signature, Signing, Encryption and Authentication and not to use as a flash drive or pen drive. Further, as put forth by the applicant, the presence of the auto run facility for

loading the middleware of the product is only a matter of convenience and its presence or absence does not impact the functioning of the product for its intended use. Even in the absence of the flash memory in which the middleware is loaded, the same could also be downloaded freely from the internet or external sources for the intended use of the product.

On the bases of foregoing I agree with the applicant's contention that the classification of goods should be based on its primary function. On the ground of provisions of GRI the specific heading will prevail over the general heading. Moreover, the product has specific character which are in consonance with principles laid to Chapter note 5C of 84, WCO Explanatory notes to 8471 80 and specific product entry of WCO classification opinion under 8471 80. There is nothing contrary to this opinion in the chapter 84 to the first schedule to the Customs Tariff Act, 1975. HSN/WCO classification opinion has a significant guidance value in deciding the matters of classification under the Customs law. Honorable Supreme Court has in their judgment in the case of Collector of Central Excise, Shillong v. Wood Craft Products Ltd. (1995) 3 SCC 454. observed as under: -

"Accordingly, for resolving any dispute relating to tariff classification, a safe guide is the internationally accepted nomenclature emerging from the HSN. This being the expressly acknowledged basis of the structure of the Central Excise Tariff in the Act and the tariff classification made therein, in case of any doubt the HSN is a safe guide for ascertaining the true meaning of any expression used in the Act."

In the case of Collector of Customs, Bombay Vs Business Forms Ltd, 2002-TIOL-277-SC-CUS-LB, the Hon'ble Supreme court held that Explanatory Notes to HSN need to be given due consideration for classifying goods. There are few more apex court judgments echoing similar views. Hence, based on foregoing discussion, I find that the product will be classifiable under CTH 8471 80 00 as other units of automatic data processing machines.

5.11   On perusal of provisions of notification 24/2005-Cus I find that the entry 8471 is mentioned at serial no. 8 that extends the benefit of exemption from whole of the duty of Customs leviable on all goods covered under heading 8471 of first schedule of Customs Traffic Act, 1975. Applicant has incorrectly quoted and claimed eligibility to avail benefit under benefit under Sr. 2 of Notification No 24/2005- Customs.

6.   On the basis of foregoing I rule that the 'Cryptogenic Device/Token' (ProxKey and ProxKey PRO) fall under Tariff entry 8471 80 00: Other units of automatic data processing machines of chapter 84 of the first schedule of the Customs Tariff Act, 1975. Said goods are eligible for duty exemption under serial number 8 of the notification. No. 24/2005- Customs amended from time to time.

4\5\2023

(Narendra V. Kulkarni)
Customs Authority for Advance Rulings,
Mumbai

This copy is certified to be a true copy of the ruling and is sent to: -

1. M/s. Pagaria Infotech Ventures LLP 901, Mayuresh square, Plot 17 Sec-15, CBD Belapur, Navi Mumbai, 400614
   Email: ankush@pagariagroup.com

2. The Commissioner of Customs, Mumbai III Import, Air Cargo Complex, Sahar, Andheri East, Mumbai – 400099.
   Email: import.acc@gov.in

3. The Customs Authority for Advance Rulings, O/o the Chief Commissioner of Customs, Delhi Zone, New Customs House, Near IGI Airport & Cargo Complex, New Delhi-110037
   Email: cus-advrulings.del@gov.in

4. The Principal Chief Commissioner of Customs, Mumbai Customs Zone-I, Ballard Estate, Mumbai - 400001.
   Email: ccu-cusmum1@nic.in

5. The Chief Commissioner (AR), Customs Excise & Service Tax Appellate Tribunal (CESTAT), West Block-2, Wing-2, R.K. Puram, New Delhi - 110066.
   Email: cdrcestat123@gmail.com, ccar.cestat-delhi@gov.in

6. The Member (Customs), Central Boards of Indirect Taxes & Customs, North Block, New Delhi-110001.
   Email: mem.cus-cbec@nic.in

7. The Commissioner (Legal), CBIC Offices, Legal/CX.8A, Cell, 5th floor, Hudco Vishala Building, C-Wing, Bhikaji Cama Place, R. K. Puram, New Delhi – 110066.
   Email: anishgupta.irs@gov.in, commr.legal-cbec@nic.in

8. The Webmaster, Central Boards of Indirect Taxes & Customs.
   Email: webmaster.cbec@icegate.gov.in

9. Guard file.

(P. Vinitha Sekhar)
Secretary, Additional Commissioner
Customs Authority for Advance Rulings,
Mumbai.