

SPEED POST

No. DGET – 2/2/2014 – MES/IS
Government of India
Ministry of Labour & Employment
Directorate General of Employment & Training
Shram Shakti Bhavan

New Delhi, dated 18th July, 2014

To

1. The Principal Secretaries of States/UTs dealing with Vocational Training and Implementation of Skill Development Initiative (SDI) Scheme.
2. The Directors/ Commissioners of all States/ UTs dealing with Vocational Training and Implementation of Skill Development Initiative (SDI) Scheme with a request to inform all VTPs under their control.

Subject: Installation of bio-metric attendance devices at registered VTPs under Skill Development Initiative (SDI) Scheme based on Modular Employable Skills (MES). - Specifications for Bio-metric devices- reg.

Ref: DGE&T order No. DGET-2/2/2014-MES/IS dated 26-03-2014

Sir/Madam,

As you are aware that it has been decided that a system of capturing bio-metric attendance of trainees shall be in place to capture the attendance of students twice a day and transfer to the central server by October, 2014. In compliance, all Vocational Training Providers (VTPs) under SDI scheme are required to purchase and get installed biometric devices for each training center as per the prescribed specifications. (Copy enclosed).

Therefore, it is requested to kindly direct all VTPs registered within your State/UT to purchase and get installed biometric devices as per the prescribe specifications before 01st October, 2014. The detail instructions regarding installation and operation of biometric machines shall be provided subsequently.

Encl: as above

Yours faithfully,



(Dinesh Nijhawan)
Director (SDI)
Ph: 011-23708071

Encl: as above.

Copy for necessary action to: All RDATs


Specifications of Biometric Attendance Device


It has been decided that a system of capturing bio-metric attendance of trainees shall be in place is capture the attendance of the students twice a day and transfer to the central server by October 2014. In order to comply with this decision all Vocational Training Providers (VTPs) under SDIS Scheme are required to purchase and get installed biometric devices for each training center complying with below mentioned specifications. The detail instructions regarding installation and operation of biometric machines shall be provided subsequently-

Hardware Specification		
S.No	Component	Specifications
1	Biometric Sensor and Extractor	All the parameters of Biometric Devices for Authentication should be as per latest STQC Scheme for Certification of UIDAI Biometric Devices (Authentication) http://stqc.gov.in/content/bio-metric-devices-testing-and-certification . STQC certified sensor and extractor only.
2	Processor	32-bit, ARM-9/x86 equivalent or higher, 400 MHz or higher frequency
3	Memory 	RAM 128 MB or higher, FLASH 256MB or higher Memory Capacity to store fingerprints >=3000 Memory Capacity to store transaction logs >= 1,00,000 Memory Capacity to store device operation logs >=1,00,000
4	Add on Memory	Micro SD Slot minimum 4 GB or more
5	Keypad	Minimum 16 key alpha numeric keypad with navigation keys, key size to be large enough for navigation, Or On screen key pad or QWERTY Keypad

6	OS/Software	Following OS with GUI Support, JVM or equivalent support & SDK for 3rd party application development: i. Linux 2.6 or higher ii. Windows iii. Android iv. Any other equivalent OS
7	Ports	USB 2.0 or higher – 1 or more nos.,RJ45(Ethernet)/ WiFi
8	Language Support	Unicode Support for all Indian Language including English
9	Status Indications	Multi Colour LED's/LCD (to indicate network connection, signal strength, to indicate battery charge remaining etc) or on screen display of all indicators like battery charge, network strength etc.
10	Other Indicators	Audio/ Visual capability: A/V indication either at device level or at application level for indicating various events like: a) Indication for placing finger b) Start of capturing c) End of capturing
11	Connectivity	Two channels of connectivity are mandatory for devices. First connectivity as GRPS is mandatory. Second connectivity can be through WiFi b/g/n / Fixed broadband. E.g.,GPRS + broadband, GPRS + WiFi, etc.
12	Non-volatile storage	Must be capable of storing audit trails of at least 1000 transactions
13	Display	Minimum 3.5" screen or higher, with atleast 262k colors TFT
15	Battery Backup	minimum 4 hours battery backup
16	Antenna	Internal, External / Extended External Antenna
17	Power Adaptor	AC/DC Adaptor with surge protection. Input 100-264V AC , 50Hz.
18	Environment	Storage not including battery: 0°C to 55°C.
		Operating temp: 0°C to 50°C.
19	Humidity	10-90% RH Non-condensing

20	Speaker	A facility should be provided for voice confirmation of the transaction, 1W or more.
22	Other Accessories	Durable Carry case, Multilingual user manual (English/Hindi), Screwdriver, damper, a white cloth (45cm x 45 cm).
23	Other features	External accessible slots for SIM and SD Cards
24	Support	Complete cover support with breakage replacement for a period of three years.
25	Security	2048-bit PKI, 256-bit AES, Base64, SHA-256 (<i>optional</i>)
26	GPS	Industry standard 16 channel NMEA compliant GPS support.
27	Environment, health and safety	RoHS certification (<i>optional</i>)
28	EMC compliance	FCC class A or equivalent (<i>optional</i>)
29	Ingress protection (IP) Compliance	Dust resistant , Water resistance (<i>optional</i>)

B	Client Application Specification	
S.No	Component	Specifications
1	NFIQ Quality  Software	Inbuilt NFIQ quality software either at device level or extractor Level to check the quality of fingerprint during enrolment
2	Enrolment client	Enrolment client application shall have the following functionalities <ul style="list-style-type: none"> • Enrolment of 10 fingerprints with identifier (Unique registration number) • Verification of NFIQ before accepting fingerprint for enrolment • De-duplication of fingerprint during enrolment for single candidate

3	 Authentication Client	<p>Authentication client application shall have following functionalities</p> <ul style="list-style-type: none"> • Authentication of fingerprints based on 1:n logic among the local storage of fingerprint templates • Attendance transaction logs to be stored internally • Voice enablement of Authentication output in English and Hindi
4	Integration	<p>Biometric fingerprint enrolment and Authentication client application should be integrated with DGET server application and should able to upload/download through SSL / https connections duly suiting the API/ Web services provided by DGET</p>
5	Remote update of software	<p>Device must support version control feature in order to remotely monitor and provision application and system software. Remote device management feature must be provisioned as a part of the device deployment.</p>
6	Reports	<p>The following reports should be generated at the device level</p> <ol style="list-style-type: none"> 1. Daily attendance report (batch wise and training centre wise) 2. Batch wise attendance report 3. Student wise attendance report 4. Trainers wise attendance report 5. Enrolment reports (displaying date of enrolment, number of fingerprints, etc.) 6. Consolidated training centre attendance report <p>More reports may be added in the future.</p>
7	Additional features	<ul style="list-style-type: none"> • Device operation logs should be captured and stored internally. Device operations like, switch on & off, enrolment of fingerprint & user, change of settings etc. shall be logged. • Date and time in the biometric device should be either of the GPRS connection or server timings. No option to change the data and time should be available in the biometric device. • Deletion of individual records (enrolment, attendance transaction

		logs, device operation logs should be disabled.
8	Output file format	Biometric data to be transferred to central server should be in XML format.