



# Hirsch Verification Station™

## RUU-201™

*The Hirsch Verification Station™ confirms the identity of a cardholder to a Personal Identity Verification (PIV) smart card. The Verification Station supports a variety of identity verification modes, including HSPD-12 FIPS 201 and Cogent BioGate. The unit includes a Hirsch ScramblePad®, a contact smart card reader, a contactless smart card*

*reader, a Cogent Systems minutiae-based fingerprint biometric reader, an LCD display and a processor capable of PKI certificate validation. The Verification Station is suitable for use at issuance, for remote standalone verification, for network connected verification, for enrollment to a Hirsch Velocity Physical Access Control System (PACS), and for use as a conventional door/gate access reader.*

### Features

- Four Applications in One Unit
  - Issuance
  - Remote Verification
  - Enrollment to PACS
  - Door/Gate Access Reader
- Standalone or Networked
- PKI Option
- Dual Ports
  - Wiegand or RS-232
  - Ethernet or RS-485
- Protected PIN
  - Scrambling Digits Display
  - Viewing Restrictors
  - Privacy
- Contact Card Reader
  - Reads FASC-N & CUID
  - Reads Expiration Date
  - Reads Biometric Templates
  - Reads CHUID
  - Reads Print & Face (Photo) Buffers
- Contactless Card Reader
  - Reads FASC-N & CUID
  - Reads Expiration Date

- Biometric Fingerprint Reader
  - Uses Minutiae Algorithms
  - Unaffected by Water
  - Match in Reader
  - PIN-protected Template
- LCD Display
  - 4 Lines X 16 Character
- Rugged, All-Weather Housing

### Description

The Hirsch Verification Station is designed to FIPS 201 standards to perform a variety of verification and authentication functions. It can also be configured for general purpose applications.

A typical "Standalone" sequence of operation might be as follows:

- Insert Contact Smart Card
- Enter PIN (unlocks buffers)
  - Print
  - Photo
  - Fingerprint
- Place Finger on Platen
- Identity Confirmation Annunciated

If the Verification Station is network connected, the unit can also validate the PKI (Public Key Infrastructure) certificate on the card by contacting a Certificate Authority prior to verifying identity.

When the Verification Station is used to confirm identity prior to enrollment in a Hirsch Velocity Physical Access Control System (PACS), data can be transferred from the card to the PACS to facilitate enrollment into the local PACS. This will increase accuracy and save time normally expended in the process of typing in the person's name, affiliation, expiration date, and other data printed on the card.

When the Verification Station is used for door access, either the contactless or contact reader can be used for normal access. Both readers are configured to read the Federal Agency Smart Credential – Number

(FASC-N) from the CardHolder Unique IDentity (CHUID) container in the smart card's processor. The FASC-N numbering scheme is intended to ensure interoperability and uniqueness of cards issued by federal agencies to federal employees and contractors. It is a 14-digit number derived from the Agency Code (4 digits), System/Site Code (4 digits), and the Credential Number (6 digits). The RUU-201 reads the FASC-N and the expiration date in the CHUID and, if configured to do so, forwards this information as a 75 bit Wiegand (with parity) string to the external Hirsch MATCH™ Universal Reader Interface for “authorization” by the PACS.

If the Ethernet port is connected, the Verification Station can also validate the PKI certificate on the card prior to forwarding the bit string to the PACS. Of course the PACS can also utilize an OCSP (Online Credential Status Provider) or CRL (Credential Revocation List) to validate certificates for enrolled PIV credentials.

FIPS 201 requires the biometric template to be accessed only from the contact reader interface and only after entry of a PIN, so when higher assurance of identity is required, the Verification Station can perform a biometric check prior to forwarding the FASC-N and expiration date to the PACS. This is effectively three-factor authentication (PIN + Card + Biometric).

Although FIPS 201 establishes PKI as the highest means of unmanned assurance for physical access, the Verification Station recognizes the use of biometrics as higher assurance since a lost or stolen card that only verifies PKI (PKI = Card-only) could result in unauthorized entry.

For general purpose applications (non-FIPS 201), the RUU-201 can be used to



**RUU-201-DT  
Desktop Unit**

Contactless reader located behind Hirsch logo.

enroll biometric templates, encode smart cards, and read biometric templates from the contactless reader without a prerequisite PIN entry.

### **ScramblePad**

The ScramblePad provides a very high security approach to access because the digits are randomly scrambled each time the START button is pressed. A bystander cannot acquire the code by seeing which buttons were pressed (pattern recognition). No wear pattern develops on the buttons. Horizontal and vertical light guides narrow the viewing field so only one person directly in front of the keypad can see the display.

Also, since the PIN code is so secure and traceable to its owner, it is not likely to be loaned out – a constant risk with card technologies. Thus each user is held accountable for his/her individual PIN code use.

Note: For compliance with FIPS 201, the Verification Station uses a ScramblePad designed specifically for use with the Verification Station. It does not communicate directly with a Hirsch controller nor will it send a PIN

to the controller as a second factor of authentication.

### **Biometric Fingerprint Reader**

The Hirsch Verification Station will capture the fingerprint image, perform a quality check, extract the minutiae and perform a biometric verification against templates retrieved from the PIV card. If the biometric verification is successful, the FASC-N and expiration date are transmitted to the PACS, where authorization decisions are made to determine whether access is granted.

### **Card Readers**

Both contact and contactless card readers are included in the Verification Station. This allows verification of both interfaces at issuance as well as use of the Verification Station as a physical access door reader. For customers whose verification requirements are as yet undefined or expected to change, this allows great flexibility in a single unit.

Typically, for FIPS 201, the contact reader will be used with biometric or PKI requirements, and either reader can be used for FASC-N or CHUID requirements.



## Specifications

### General

- Keypad User Codes: Operation of the START button lights and scrambles the digits. After entering the PIN and pressing the # key (not labeled), the numeric string is sent directly to the card via the Verification Station's contact card reader.
- Biometric Fingerprint Reader:
  - INCITS 378-2004 Interoperable Minutiae Algorithm
  - Fingerprint Sensor: Silicon (500dpi), 320 X 480
  - Fingerprint capture unaffected by water
  - Allowable Fingerprint Rotation: +/- 180°
  - Enrollment: Single Finger, Multiple Enrollments
  - Extraction & ID Time: 1.5 seconds
  - FRR: 0.01% - 0.001%
  - FAR: 0.01% - 0.0001%
  - Template Size: 784 bytes
  - Compatible with Cogent Systems BioGate family of biometric readers in non-FIPS 201 mode
- Reads NIST SP 800-73-1 End Point Cards

- Contact Smart Card Reader: ISO 7816
- Contactless Smart Card Reader: ISO 14443-A, B
  - Card Read Range: to 1.0 in. (2.5 cm)
- Includes CD with configuration software
- Downloadable Firmware

### Communications

- LAN Port: Ethernet TCP/IP
  - 10/100
- Serial Ports: RS-232, RS-485
  - Baud Rate: 9600 – 115 Kbps programmable
- Wiegand Port: 75 bit with parity standard
  - User programmable up to 128 bits

### Electrical

- Wiring types:
  - 2 pair, stranded, twisted, overall shield for RS-485, RS-232 and Wiegand
  - CAT5/CAT6 for Ethernet
- Wiring Distance: Refer to controller specifications
- LCD Display: 16 character X 4 lines
- Contact Card Indicator: Dynamic 3 color LED for status
- Biometric Indicator: Dynamic 3 color LED bank for status
- Keypad Display: 7 segment

- RUU-201: Red LED
- RUU-201-HI: White incandescent
- Keypad Annunciation:
  - Audible: 7-tone prompt on pressing START, and 1 tone feedback for each button
- Operating Power: 15-60VDC, 300mA @ 24VDC (425mA for HI) operational
  - Terminal block, jack or RJ45 PoE
  - Jumper option for 12-15VDC terminal and jack
  - Jumper option for 48VDC 802.3af PoE

### Physical

- Housing: Durable ABS
- One-Piece Molded Keyface on Keypad
- Recommended Mounting
  - ADA 48"
  - Follow local codes
- Dimensions:
  - 8.46"H x 9.45"W x 4.63"D (214.88mm x 239.97mm x 117.6mm)
- Shipping Weight: 2 lb. (.9kg)
- Operating Temperature Range:
  - 32° to 131°F (0° to 55°C)
- Relative Humidity: 0 to 90%, non-condensing
- Keypad Viewing Restriction (Display Angle):
  - RUU-201 ± 4° horizontal; ± 26° vertical
  - RUU-201-HI ± 20° horizontal 26° vertical

# Systems With Integrity

## Ordering Information

Model #	Description	Comments
RUU-201	Hirsch Verification Station	Personal Identity Verification (PIV) Station for FIPS 201 and general purpose applications. Includes ScramblePad, INCITS 378 fingerprint reader, ISO 7816 contact smart card reader, ISO 14443-A, B contactless smart card reader, and LCD display. Operates standalone or networked (for PKI function). For verification, PACS enrollment, or door access. Ethernet, RS-485, RS-232 and Wiegand ports. Requires 15-60 VDC, 300mA @ 24VDC or PoE. Reads NIST SP 800-73 compliant End-Point cards. Includes CD with configuration software.
RUU-201-HI	Hirsch Verification Station – High Intensity	Personal Identity Verification (PIV) Station for FIPS 201 and general purpose applications. Includes ScramblePad (with high intensity display for high ambient light environments), INCITS 378 fingerprint reader, ISO 7816 contact smart card reader, ISO 14443-A, B contactless smart card reader, and LCD display. Operates standalone or networked (for PKI function). For verification, PACS enrollment, or door access. Ethernet, RS-485, RS-232 and Wiegand ports. Wall mounted. Requires 15-60 VDC, 425mA @ 24VDC or PoE. Reads NIST SP 800-73 compliant End-Point cards. Includes CD with configuration software.
RUU-201-DT	Hirsch Verification Station – Desktop	Desktop version of RUU-201 Verification Station, with desk stand and plug-in power supply that accepts 100VAC-240VAC input line voltages.

