Technical Specifications for iData™ IrisAccess® EAC (Entry Access Control)

iData™ EAC

The world's leading iris recognition entry access control software is iData™ IrisAccess® EAC.

A highly versatile offering, IrisAccess® seamlessly interfaces with virtually any PACS (Physical Access Control System) via configurable Wiegand, relays, GPI/O and RS232/422 connections.

Comprehensive integration is also available through development kits and import tools that link user credentials, workforce management and reporting.

iData IrisAccess® EAC provides best of breed biometric authentication and security in an integrated or stand-alone environment that has been proven across many enterprises.

- iData™ IrisAccess® EAC software has a fully automatic image and template quality process that ensures that only good iris templates are enrolled and encrypted in the system.
- iDentityCheck™ makes it virtually impossible to have a duplicate iris record entry in the system providing unparalleled accuracy. **iDentity**☑™
- Security measures and features include encryption of user data, credentials, countermeasures and tamper alarms that meet the highest requirements.
- Support for virtually any type of Card – PROX, iClass, MiFare, DESFire, PIV, CIV, etc.

IrisAccess® EAC Application Suite includes the following primary software components

IrisServer

Controls the IrisAccess database and communications to and from the iCAM iris readers and IrisAccess® system applications. IrisServer is responsible for managing the distribution of enrollment data, transaction logs, and all other ancillary data communications. Only one IrisServer application per network is required.

IrisManager

Manages the system configuration, permissions, and user data. Up to 10 IrisManager applications can be placed on one network. Only one instance can be logged in and active at any given time to ensure database integrity. IrisManager is used to securely add iris readers to the system. IrisManager also controls the creation of operators and administrator accounts on the system and restricts enrollments by connected PCs.

IrisEnroll

Provides iris enrollment for all current and legacy iCAM models including the newest iCAM7000S, iCAM7000 and iCAM4000 series readers. The application is used to enroll iris data, capture a face image and enroll and encode card data as specified. Up to 32 concurrent enrollment units maybe deployed per network. IrisEnroll TD100 (USB iCAM) can also be used to enroll iris data and face images. IrisEnroll iCAM TD100 does not have card reader enrollment or encoding capability.

IrisMonitor

Allows for real-time monitoring of system status and user activities with optional audio alerts. Up to 10 IrisMonitor applications can be placed on one network. IrisMonitor can report many activities, including iCAM tamper detection, network communication loss, and many other system attributes.

Included Utility Applications

IrisDBAdmin

Provides backup, upgrade and merge utilities. For use with the IrisServer.

iCAM7000Update / iCAM7000SUpdate

Enables update of firmware in the iCAM7000 Series and iCAM7000S series respectively.

ICUAdmin7000-2

Enables update of firmware in the ICU 7000-2 identity controller. Review specifications and requirements as needed.

Client Certificate Manager

Creates and manages digital certificates for network communication security between Iris Server and iCAM7 Iris Readers.

Import User

A utility to import user data from a CSV text (MS Excel file). Useful for preloading user information before enrollments begin.

Iris Enroll TD100

Additional enrollment application for using the iCAM TD100 for iris enrollment.

## Device Administration & Operation Mode Management

IrisAccess iCAM7 series iris readers can be configured in multiple operational modes which are selectable within the device's web "WebConfig" application.

Available Operational Modes:

- Operational Mode 1 (Option 1): Networked iCAM Control (iris data processed on PC workstation or on an ICU7000-2 series controller)ally impossible to have a duplicate iris record entry in the system providing unparalleled accuracy.
- Operational Mode 3 (Option 3): On-Device iCAM Authentication (1:N / 1:1 and 3 factor authentication.)

Networked iCAM Control / Iris Image Capture Mode

The iCAM7 Iris Reader will operate as part of an IrisAccess system for enrollment or recognition when communicating with a computer using Iris Access EAC software, iData EAC Toolkit and or in conjunction with an Identification Control Unit (ICU7000-2).

**Typical System Configuration**
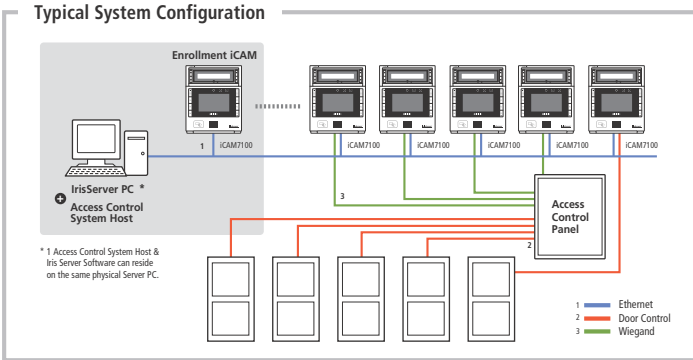
On Iris Reader or Off Iris Reader Matching is possible

The iCAM7 series iris readers provide iris identification (biometric matching) inside the device. All iris data and PII (Personally Identifiable Information) is encrypted inside the iCAM.

iCAM7 Option 3 + Option 1
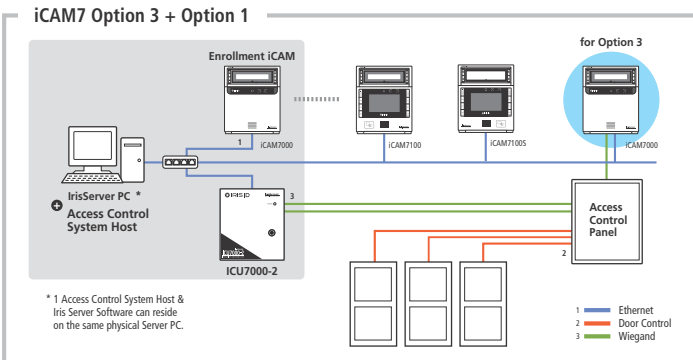
Sample Legacy Configuration

The diagram below includes the following: Enrollment iCAM in Option 1. Two iCAM4000's communicating to the ICU7000-2 for matching, and Two iCAM7 Iris Readers in option 3 Mode (on device matching). Many other configurations are possible.

iCAM7 + Legacy iCAM4000
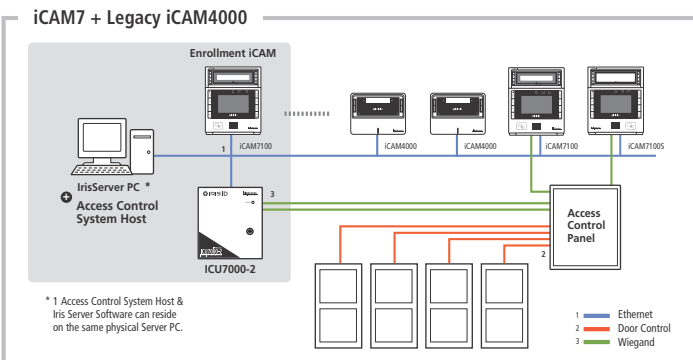
DES and 3 DES encryption options are available. The 3 DES encryption can be set by the end user. Note: The ICU7000-2 is offered as an optional solution for off device matching.

In all cases the IrisServer does not have to be online continuously. (*Legacy iCAM4000 series units cannot perform iris matching on the device.)

iCAM7 also has an integrated relay (dry contact) and can control a 3rd party door lock controller directly.

Using Smart Card with encoded templates and On-Device Verification Mode

The iCAM7 series iris readers can operate as complete stand-alone authentication readers. For verification (1:1 matching) of iris templates which have been encoded on contactless smart cards. The iris template data is securely stored on the contactless smart card during the enrollment process. When the card is presented to the iris reader, the encrypted templates are read from the card and are compared to the live iris presented.

iCAM7 Smart Card Mode
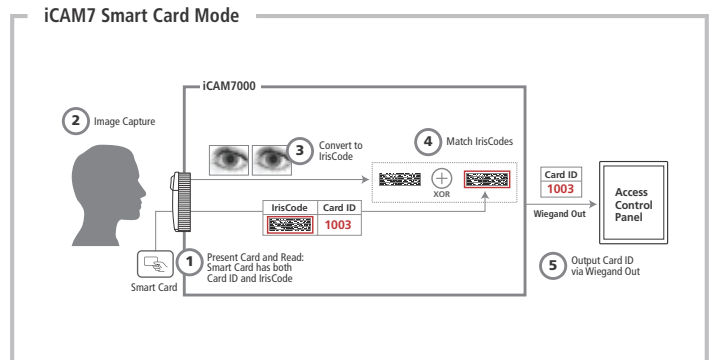
The verified card ID is output to the 3rd party access control system. This operation does not require a network connection.

The iCAM7 series will support virtually any 3rd party wiegand based access control panel.

System Requirements for iData™ IrisAccess® EAC

The IrisAccess EAC software – Iris Server, Remote Enrollment stations, remote Iris Monitor stations require a static IP address for the PC on the network.

IrisAccess EAC supports MS SQL, Oracle, and MS Access database types.

Supported Computer Hardware Recommendations: IrisAccess EAC Software Application and iCAM Entry Application
Operating systems – Windows 2000/XP, Windows Vista, Windows 7 , Windows 8.1, Windows 10, Windows 2008 & 2012 server Pentium Compatible 1.8 (or higher) GHz Processor
1 GB or higher Memory (OS dependent) – 10 GB Hard Disk space (or greater)
CD/DVD Drive (For Software Installation) – Ethernet Port (100 Mbps recommended)
If older generation ICU4000-W (4 Channel) are being used it may be preferable to have 1 Serial Port for ICU configuration OR 1 USB 2.0 (or higher) port using a USB to Serial adapter
Legacy Support – An ICU7000-2 (Dual channel ICU) is supported with legacy iCAM4000's 1 ICU7000-2 per 2 iCAM4000's. IrisAccess EAC 3.10 or higher is required to use the ICU7000-2

Aditech Ltd.

Unit 7 Midshires Business Park, Smeaton Close, Aylesbury, Bucks, HP19 8HL. UK

www.aditech.co.uk
Tel: +44 (0)1296 398085 - Fax: +44 (0)1296 337755