BLUE LINE
TECHNOLOGY

WHITE PAPER

TWO FACTOR (2FA) AUTHENTICATION

With Facial Recognition

Deter, Detect, Delay, Defend.

Creating the most effective video camera systems which provide the highest level of protection for building occupants and property across sectors and industries

Facial recognition is quickly becoming the most advanced biometrics authentication technology. Blue Line developed First Line Software from the ground up, providing the highest accuracy and ease of integration in the field today.

FL
SOFTWARE

Table of Contents

1. Purpose and Scope

Two Factor Authentication (2FA) is becoming a powerful prevention protocol for thwarting unauthorized access, fraud, and cyberattacks as we move towards a cyber driven world. There are more and more high risk transactions being performed online and this is propagated by cloud based computing. The physical security world is driving to protect their sensitive information, control staff and the public from accessing restricted areas. There now is an increasing need to verify and authenticate the user's identity, which means this market is becoming very competitive.

As security becomes more technically driven, so does the analytics behind it to address security needs. More two factor methods will come to fruition and will not only have to address the security concerns of the end user, they will also have to be flexible to the client's network and current infrastructure. This white paper will explain the details of how our two-factor method works and the practical use case scenarios that would benefit the clients.

2. What Is Two Factor Authentication? (2FA)

The current access control aids in controlling doors/locations for unintended usages or access. To prevent misuse, access control provides a way to monitor, control, and manage a door's "status". The access control software can allow/deny a user of the token based on door locations, timeframe and by authorization.

The issue resides in the fact that the token, if used alone, could be lost, taken, misplaced, or given to another user to gain access. Thus, the pure means of controlled security is now at risk and vulnerable. Biometric two factor authentications provide the ability to present a token which will be authenticated with facial recognition to make sure it is the valid token holder therefore securing access to restricted areas.

Two factor authenticators are classified by the following:

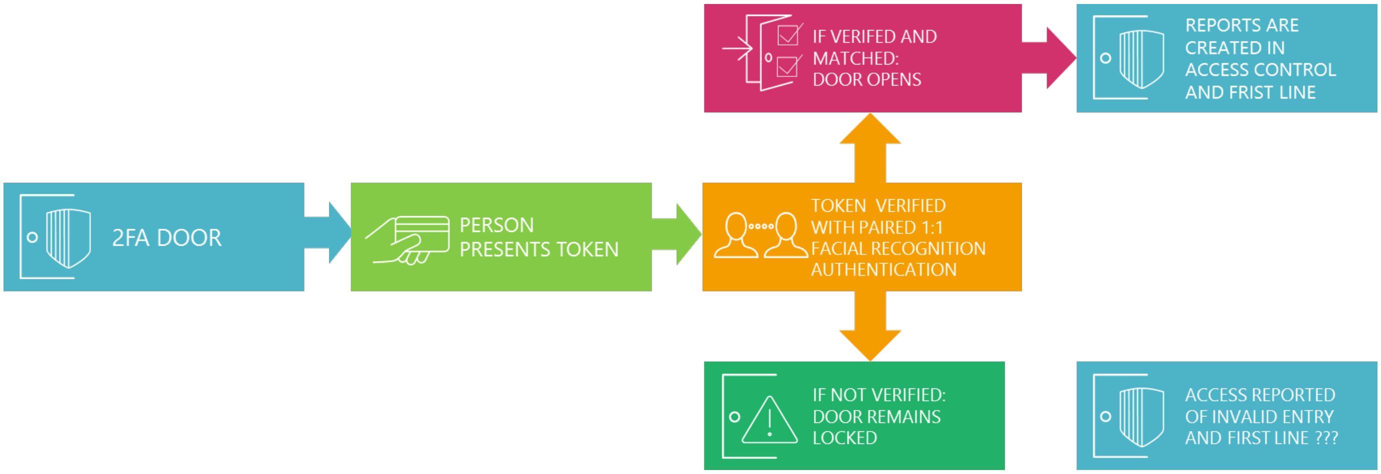
- something you know (password)
- something you have (HID, fob, cryptographic key)
- and something you are (fingerprint, face, iris).

Two factor authentication makes the user prove that he or she is a valid subscriber, the user authenticates to a system or application over a network by proving that he or she has possession and control of one or more of the authenticators. For example, a pin number and ID badge with no security guard present or at a controlled door are not secret enough to enable a true two factor authentication unless it is tied to a biometric authenticator or an authenticating hardware which produces the secrete key unknown to the subscriber.

This form of 2FA makes us much harder for imposters to replicate or steal the variables as they must steal the authenticating hardware and replicate the biometrics that are specifically unique to that person and get the two authenticators to match.

3. Using 2FA with Facial Recognition

First Line utilizes the existing access control hardware to intercept the data transmission via Wigand to match the token authentication (via HID, card access



2FA DOOR

PERSON PRESENTS TOKEN

TOKEN VERIFIED WITH PAIRED 1:1 FACIAL RECOGNITION AUTHENTICATION

IF VERIFED AND MATCHED: DOOR OPENS

REPORTS ARE CREATED IN ACCESS CONTROL AND FRIST LINE

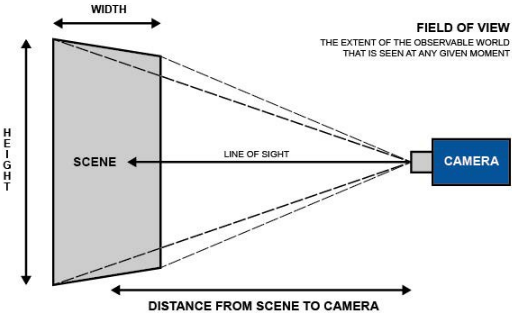
IF NOT VERIFIED: DOOR REMAINS LOCKED

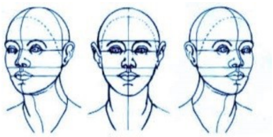
ACCESS REPORTED OF INVALID ENTRY AND FIRST LINE ???

4. Flexible Advantages

Facial Capture

Something to understand about facial recognition is that the cameras are operating like eyes and not a security system. The challenge was to offer a system that does not interrupt or alter someone’s actions excessively or be unwieldy. With the lighting and position challenge, there are occlusions (i.e. ball caps, facial expressions which tilt head too far or down, objects between camera and face, or another person) which can cause concerns. By creating a filter transformation based method to overcome some of these problems, we established an innovative pose compensation which significantly helps overcome pose variations and other negative factors in face recognition.


WIDTH
FIELD OF VIEW
THE EXTENT OF THE OBSERVABLE WORLD THAT IS SEEN AT ANY GIVEN MOMENT
HEIGHT
SCENE
LINE OF SIGHT
CAMERA
DISTANCE FROM SCENE TO CAMERA



Understanding traffic flow of the location and its lighting is essential for facial recognition. Cameras can be placed for "facial capture on the fly" without too much deviation from the original traffic flow. However, cameras intended for specific access control need to be mounted to identify people while walking or in a position which requires the person to look directly at the camera for access entry.

Consistent lighting is key when it comes to facial recognition. Poor lighting or fluctuating lighting conditions can lead to images being degraded to the point where any type of identification can become extremely difficult. Areas that cast shadows or facilitate direct sunlight into the cameras must be avoided. Some areas can have light added to improve quality. Additionally, the camera's iris and shutter speed can be adjusted to provide a consistent image regardless of the environmental conditions. The camera is capturing 30 frames per second to accommodate people moving.

Creating Security

Our customers also can choose to detect "unknown" persons of interest. This unique feature allows a controlled area to be monitored. For example, a convenience store may use the "unknown" feature for night time entry. They will not be entering the faces of each of their patrons, but a criminal will think twice as they will not be able to conceal their face on entry. The "unknown" can also be used for controlled areas or environments.

Identifying clients or specific individuals of interest, gives the user the situational awareness needed to address the circumstances presented. Facial Recognition combines with the user's current security system, networking, access control and monitors. Facial recognition software can tell the user who is present. The security cameras follow their actions while the access control reportsentry.

CONVENIENCE STORE
CONVENIENCE STORE
CONVENIENCE STORE
CONVENIENCE STORE

5. Summary

Facial recognition provides a unique perspective on the value of security and what it means to the customer. Blue Line Technology provides several layers of service for customers simultaneously. Blue Line Technology's First Line Facial Recognition system was designed for the private sector with the goals of creating a safer and more secure environment, while allowing multiple client locations to work seamless.

First Line Facial Recognition Software provides one of the highest accuracy rates in the market at a fraction of the cost, making it affordable without compromising quality.

For more information, contact Blue Line Technology
636-496-7100 • www.bluelinetechnology.com