Web Authentication Client

User manual

Version 1.0

www.umpi.it

Versioning

Version 1.0.0 (15th May 2023)	First release

Index

IMPORTANT NOTICE

UMPI reserves the right to make changes to its products or to discontinue any biometric product or service without notice, and advises its customers to obtain the latest version of relevant information to verify, before placing orders, that the information being relied on is up to date.

UMPI warrants performance of its products to the specifications applicable at the time of sale in accordance with UMPI's standard warranty. Testing and other quality control methods are used to the extent UMPI deems necessary to support this warranty.

Certain applications using fingerprint-based verification/recognition systems may involve potential risks of personal injury or severe property or environmental damage (critical applications).

UMPI products are not designed, intended, authorized or warranted to be suitable for use in life-support devices, applications or systems or other critical applications.

UMPI assumes no liability for applications assistance, customer product design, software performance, or infringement of patents or services described herein. Nor does UMPI warrant or represent that any license, either express or implied, is granted under any patent right, copyright, mask work right, or other intellectual property right of UMPI covering or relating to any combination, machine, or process in which such products or services might be or are used.

1. Introduction

The goal of this document is to illustrate the service application installed on the client side that can be used for biometric authentication in web applications.

With WebAuthentication application installed on client computer it is possible to perform Multi Factor Authentication (**MFA**) to server services with a ***passwordless authentication***.

1.1. Biometric Web Authentication

User authentication is implemented with two factors using UMPI fingerprint scanners:

- User fingerprint (something the user is)
- Fingerprint scanner from UMPI (something the user has)

So, the authentication factors handled by the biometric service are the fingerprint models, acquired with a scanner manufactured by UMPI.

Fingerprint model should be considered a private data in clear format, and as such is stored encrypted on the user computer, and never exposed.

What is exchanged between server and client is not the fingerprint, but the user attestation, a proof that the computer has stored credentials and the user is present.

1.1.1. User enrolment

At user enrolment a fingerprint is acquired and safely stored on the client side.

Under the user data folder "C:\Users\[USERNAME]\AppData\Roaming\UMPI\" there are all files (encrypted with AES256) related to user fingerprints and accounts.

This folder is accessible only by the user and the computer administrator, and can be put under backup system for further safety.

1.1.2. Account Recovery

Hardware could be lost or broken; fingers could suffer injuries. A recovery system should be put in place to recovery the account.

Best practice, is to think ahead and

- register multiple recovery channels (email, phone number),
- register the same user using more than one computer, that will be used as backup if an hardware fails,
- have a backup UMPI scanner if the device is lost or broken,
- also useful is registering a recovery account with a different fingerprint of a different hand, in the case of injury.

1.2. Fingerprint best practice

Best practice for fingerprint acquisition includes:

1. Prefer **forefinger** (index) or **middle-finger** rather than thumbs. Never acquire little-fingers.
2. Acquire the **centre of the fingerprint** and not finger tips: these are small and there are less unique characteristics (**Figure 1**).
3. Stay still during acquisition: tilting or moving the finger distort the fingerprint image.

4. Apply as much pression as to have a flat acquisition, but do not push too much, or the fingerprint will be distorted.
5. Do not use under direct sunlight.

What to do if the fingerprint is rejected?

1. If a second acquisition is required, raise up the finger and place it again.
2. If the finger is wet, dry it on a cloth.
3. If the finger is dry, **warm up the finger** rubbing it against other fingers, or by breathing on it, before the acquisition.
4. The fingerprint can be placed on the sensor surface before the acquisition starts, to let the natural skin perspiration moisturize the fingerprint.

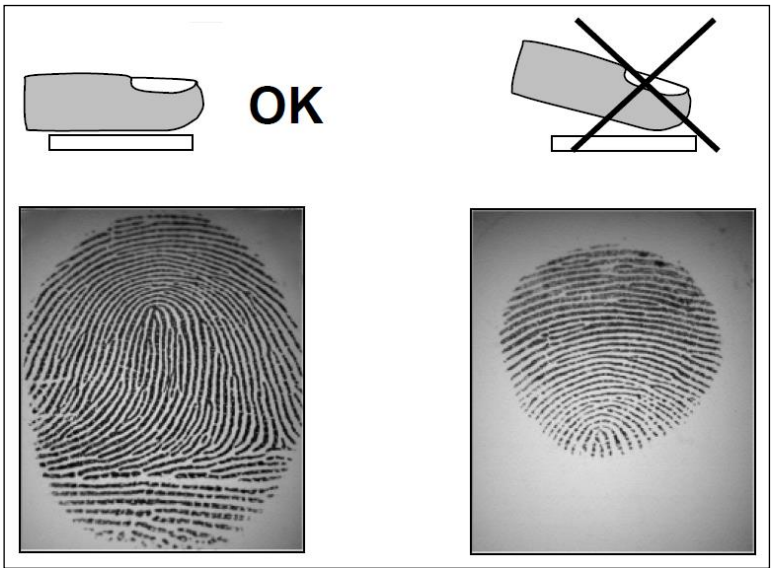

Figure 1: good and bad fingerprint acquisition, lateral view,

For a good performance of the scanner, simple maintenance is required:

- Clean with a soft cloth the acquisition surface from dust and grease, if present.
- Do not use solvents, do not spray detergents or other liquids on the acquisition surface.

2. Web Authentication client

This chapter is the description of the application installed on user computer to perform authentication on a web application.

A **web application** is an application set up by a department/service provider, and is hosted on a server (outside of user computer), used through an internet connection.

While trying to access a compatible web application, the WebAuthentication client is automatically called by the web application to perform the task of user creation or user verification.

2.1. App installation

To set the scanner in an operational mode, the scanner should be installed with its drivers and with an application that will work in background when asked by a web application running on the user browser.

The application has a "Setup_WebAuthentication.msi", that install the application and will perform basic initialization, like setting the application to run at Windows startup.

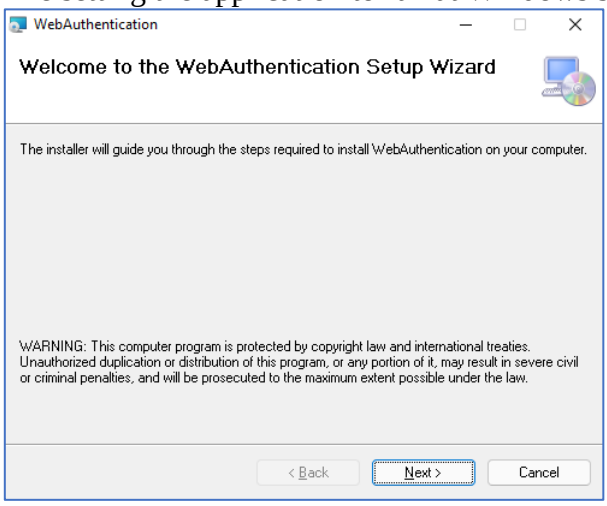

Figure 2: WebAuthentication Setup Widard

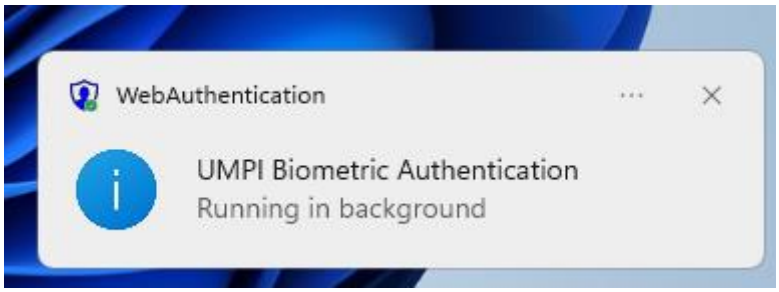

Figure 3: WebAuthentication running in background

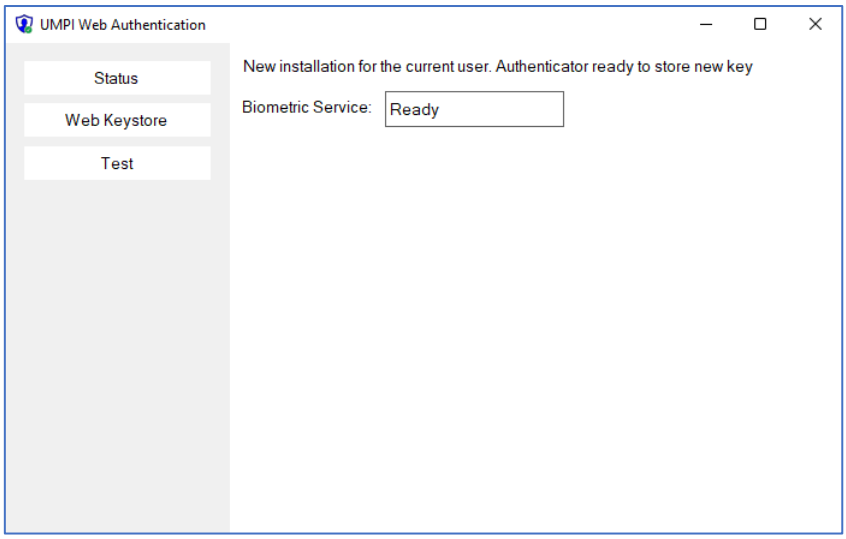

Figure 4: WebAuthentication status window

After a successful installation the WebAuthentication will start in background (Figure 3), showing its icon in the icon bar and when open will show its status (Figure 4).

Figure 5: icon bar and WebAuthentication menu

The application will run int the icon bars (Figure 5) and can be forcedly closed as any other Windows application.

2.2. WebAuthentication Test

The WebAuthentication application has a test page, where a user can be locally created and tested using a fingerprint captured with an UMPI scanner.

There are three buttons (Figure 6) :

- “Enroll”: starts a fingerprint capture (Figure 7) and store it locally as test user,
- “Verify”: capture a new fingerprint (Figure 8) and compare it with the stored fingerprint,
- “Delete”: deletes the test user and fingerprint.

Every fingerprint acquisition will show on the acquisition window with the reason of the capture (registration or verification) and the name (or http address) of the server asking for the authentication service.

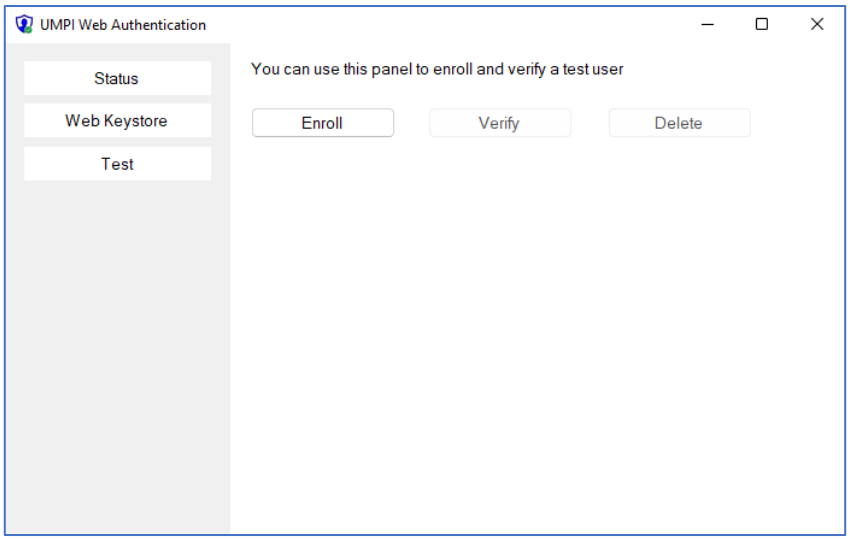

Figure 6: WebAuthentication Test page

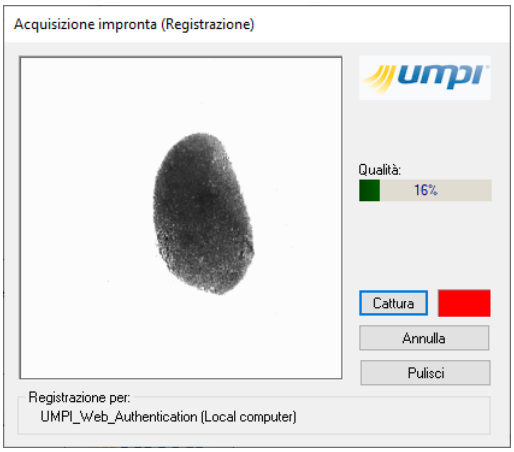

Figure 7: Enrollment window

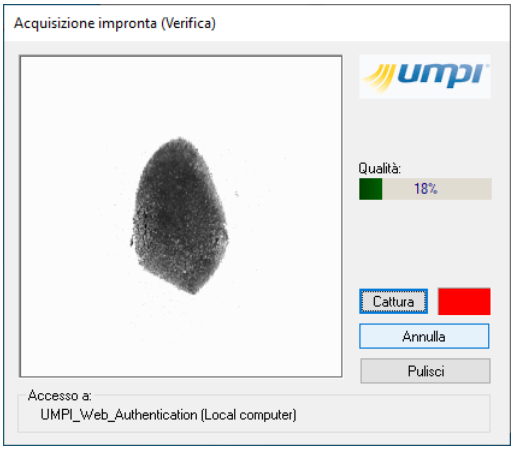

Figure 8: Verification Window

2.3. WebAuthentication KeyStore

In the KeyStore page (Figure 9) there is the list of user accounts stored on the computer and available to the current user.

Users are identified with a user name, or *USERNAME*, that is a string representing the registered user, and the account is identified with the *Server Name*.

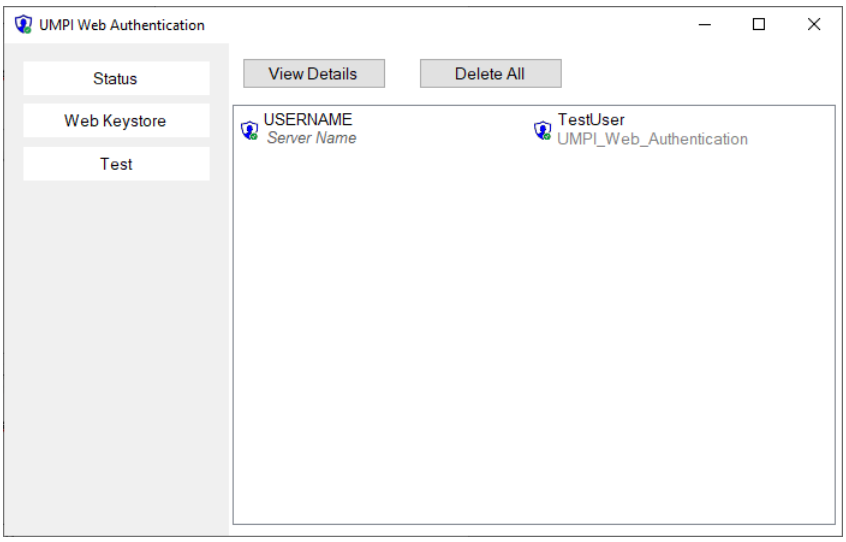

Figure 9: WebAuthentication KeyStore window

The visualization can be toggled between “Details” and “Icons”. In “Details” the list reports for each account the security level of the key type (RSA1024 or other type) used for authentication by the server.

2.4. App disinstallation

The app can be removed from the computer using the standard Windows procedure to remove apps.

Please stop the execution (from the icon bar) before removing. Also note that the application will be removed also for other users, while accounts data is still retained in users data folders:

“C:\Users\[USERNAME]\AppData\Roaming\UMPI\”