

Immunity Verification Using Holographic Fingerprint Tags

Austrian headquartered anti-counterfeiting and authentication technologies company Authentic Vision (AV) recently launched a GDPR* compliant holographic fingerprint health tamper-proof tag that provides secure authentication of the health status of individuals in exceptional epidemiological situations such as the current coronavirus pandemic.

*GDPR – General Data Protection Regulation.

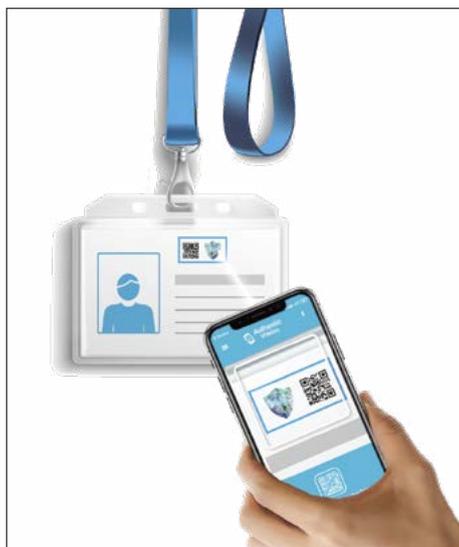


Figure 1: Authentic Vision's unique holographic fingerprint shield technology incorporated into a tamper-proof health tag that can be scanned with a smartphone.

During this pandemic there has been considerable public discussion about the need for increased immunity testing for the COVID-19 virus. Proving immunity is seen as key to opening up services, industry and travel. However, one question that continues to be asked is how will immune individuals verify their immunity as they go about their daily lives?

Immunity solution verification requirements

According to AV, an immunity verification solution must meet the following requirements:

- **Global compatibility:** it must be compatible with and work across the full range of infrastructure found around the globe;
- **Flexibility:** the solution must be flexible so that it can be implemented quickly on existing global infrastructure immediately and without changes;
- **Easy integration:** the solution must easily integrate with a wide range of existing processes and systems;
- **Ease-of-use:** the solution must not require specialised training or skills to use; and
- **Trustability:** the solution must have already demonstrated success and be trustable under the most demanding situations.

Authentic Vision's solution

AV has developed a secure and user-friendly technical solution to enable vaccinated, tested, or immune individuals to safely revert to their normal lives. This solution can be implemented immediately, ensures privacy, and guarantees data protection (GDPR compliance), which to date has been one of the stumbling blocks to other proposed solutions.

The solution involves the application of a tamper-proof tag to an existing identification document that incorporates electronic verification of immunity or vaccination. This approach provides both a visual and electronic vaccination or immunity verification that can be used in all environments – government, private sector, education, NGOs and non-profits.

The activation of the tag and the associated privileged access rights can be carried out locally by government bodies, health authorities or doctors. The required data is stored directly and in encrypted form on the health tag immediately upon issue.

With the help of this identifier, any approved health-related information can be read by another person, eg. by law enforcement authorities during a road check, employees of transport companies or security personnel during entry checks. This allows organisations of all types to quickly identify and allow citizens, employees, customers, students, patients, and others access to their facilities with the knowledge that these individuals have been vaccinated or carry immunity to the virus.

The authentication solution consists of three components:

- **AV health tag:** tamper-proof security labels in different sizes and colours;
- **AV mobile applications:** authentication using conventional smartphones and a free app;
- **AV smart portal:** management of the tags and tracking of the authenticity checks.

AV health tag

The health tag can be produced in different designs and sizes (see Figure 2). The main features and benefits are:

- Each tag has a unique identification number (alphanumeric);
- The tags are copy-protected by a unique holographic 'fingerprint';
- The tags become invalid if an attempt is made to remove them and are therefore tamper-proof.



Figure 2: AV health tag design and sizes.

AV apps

The activation of the tags can be done easily by any health authority (medical facility, hospital, or doctor's office) with the designation of privileges and access rights carried out using the free AV 'Admin' application on any smartphone.

The authenticity of the tags can be checked without specialised expertise using any smartphone and the free AV 'Authentication' app, based on *Android* or *iOS* (see Figure 3). The scan will automatically detect any previous attempts at copying or tampering.

The app can either be integrated into an existing mobile application or published as a stand-alone app in the customer's design. The message that is displayed after successful authentication can be customised to include information from health authorities and concrete recommendations for action.



Figure 3: smartphone authentication of the AV health tag.

AV smart portal

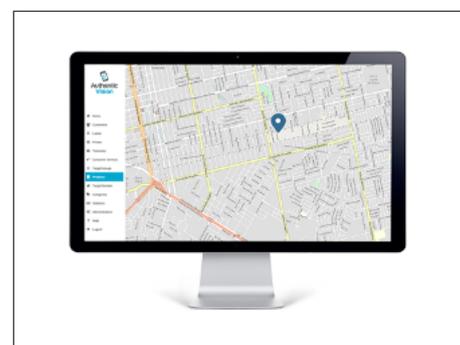


Figure 4: overview of location data in the AV smart portal.

Location data of the authentication checks are stored and evaluated using the AV smart portal (see Figure 4). The AV health tags can be managed from the web portal, eg. enabled/disabled, and individualised push messages can also be sent via the app.

This process is 100% GDPR-compliant as the connection between the user and their classification or test result is limited to the physical connection between the tag and the respective ID document. At no time is personal information stored in the label system. Only the rating or test results are stored.

www.authenticvision.com