TrustStamp

In collaboration with CWAG and the Alliance Partnership, Trust Stamp has built a proof of concept model that is being run between the Attorneys General of New Mexico and Guanajato Mexico.

This project is using Trust Stamp **Facial Matching** and **Hashing Systems** to create a means for the two Attorneys General offices to share hashes related to the victims of human trafficking. The mechanism allows investigators to be notified of "matches" without the complications of sharing personally identifiable information. This system of utilizing hashes has resolved a longstanding issue for law enforcement operations when it comes to inter-jurisdictional data sharing. In the past, warrants were required prior to the sharing of any information which often caused delays or the need for specific legislation in certain jurisdictions. By utilizing the biometric hash, no personal information is shared and privacy as well as data security protocols are maintained across jurisdictions. This is a game changing action and the Attorney General of New Mexico has opined to that effect.

The technology was announced by General Balderas at the international Biometric Institute conference in NYC in June, 2018.

Trust Stamp's primary focus has been developing AI-powered identity authentication systems focused on facial biometrics.

Trust Stamp's R&D and development expenditure has been based upon the dual thesis that over the next 5-years facial biometrics will become the dominant authentication methodology for online transactions and that, as usage expands, so will the investment by criminals in attacks upon the methodologies.

In response, they have developed and patented multiple AI approaches to identify and defend against presentation attacks for both still and video images. Once they have proven a live and unadulterated facial image they use:

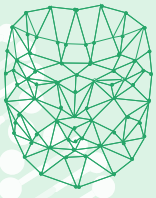
forensically examined scans of government issued ID

data mining social media

other online and proprietary resources

to attach a legal identity to the biomnetric hash.

In parallel, TrustStamp has also patented, an "evergreen" encrypted biometric hash that can be **server** or **blockchain** based and function as a digital DNA for an individual.



The hash is currently created from a still photograph or video by extrapolating measurements from a virtual 3-D mask that their software creates, but it can evolve over time and be based on, or can embed, and/or be a pivot point to, multiple biometric factors and other data points. As a hash, the data can never be reverse engineered and does not constitute personally identifiable information for both U.S. and GDPR purposes.

A major distinguishing feature of Trust Stamp's methodologies is their patented hashing process that allows them to compare every new biometric hash to every other hash that they have ever seen and their proprietary AI which calculates the probability that two hashes were generated from the same human face. Although traditional siloed KYC processes often "pass" synthetic and stolen identities that supported by credit files and ID documents, this process has identified numerous synthetic identities (and fraudsters with multiple identities) and there is less than a one in a billion chance of the hash matching more than one face.

As a second implementation in August, Trust Stamp will enroll staff in each of the AG's offices in a biometrically encrypted communication systems that will allow them to exchange encrypted messages and files that can only be decrypted with the live facial biometrics of an authorized user. The system does not use private keys, user names or passwords removing most opportunities for compromise.