White Paper Brief

QuantumCrypt™ True Biometric Hash
Privacy ● Revocability ● Anti-spoof

Enabling biometric technologies to eliminate biometric data storage

Biometric technology is advancing rapidly. The complex technology, people, process and policies are being addressed to secure biometric data to ensure that biometric technology will effectively continue to shape human identity authentication applications.

This white paper brief facilitates a deeper understanding of the more advanced biometric technology which will help eliminate risks, enhance security, protect the privacy and help enable biometric solutions to be more relevant in the digital identity space.

Executive Summary

Biometrics is a critical facet in the prevalence of digital identity solutions in our everyday lives. However, it also presents an immense challenge for enterprise security solution providers, biometric technology developers, integrators and OEMs, ensuring biometric data security and integrity to prevent a data breach which is costly and irreversible.

The True Biometric Hash models that Infinity has built for 2D face, fingerprint and iris can enable various biometric modalities to remove biometric data storage using advanced technology to extract only reliable and repeatable featured vectors from a biometric scan image. Not only are these same featured vectors extracted repeatedly and accurately, but the platform also collects only the reliable bits so that it doesn't compromise the overall effective biometric entropy for better security and performance.

Privacy Challenges

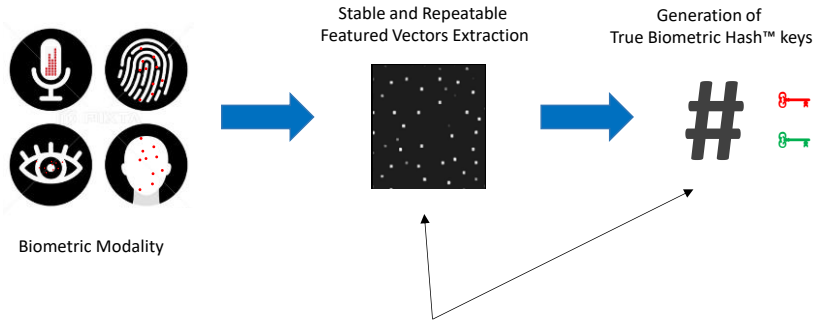
Currently, there are more biometric data or templates been generated and stored in a private server or encrypted and stored in Cloud. The growing demand for biometric privacy and data protection in the digital identity space results in various emerging technologies that securely generate a digital key from the stored biometric image or template for various authentication application.

Advancements cryptographic solutions are unable to create digital keys directly from a biometric scan due to inconsistent environmental factors affecting the biometric image capture so they have to rely on generating the digital key from a stored biometric template. These stored biometric data or template are exposed to data breaches.

Some in the industry claimed they have developed a 'hack-proof' biometric hash solution to prevent data breaches and ensure privacy. This traditional approach can produce some stable codes and some unstable codes which are weak in security. These existing solutions still rely on a protected stored biometric template to generate digital keys and backdoors remained exposed.

Solution

Infinity's QuantumCrypt™ technology generates the same stable and repeatable biometric code to create a True Biometric Hash™. The generation of stable biometric codes from varying environmental conditions and natural sensor noise during the biometric scan ensures we limit acquisition errors. As a result, the system operates with performance and good user experience. Under these varying conditions, the True Biometric Hash performs with exceptional tolerance to limit risks of having different people with some similarities and producing the same stable codes. The entropy generated by the system ensures that. Thus, using only stable bits from the biometric scan will produce automatically a stable code and it does not require a stored biometric template for authentication.



True Biometric Hash in the Cryptographic space

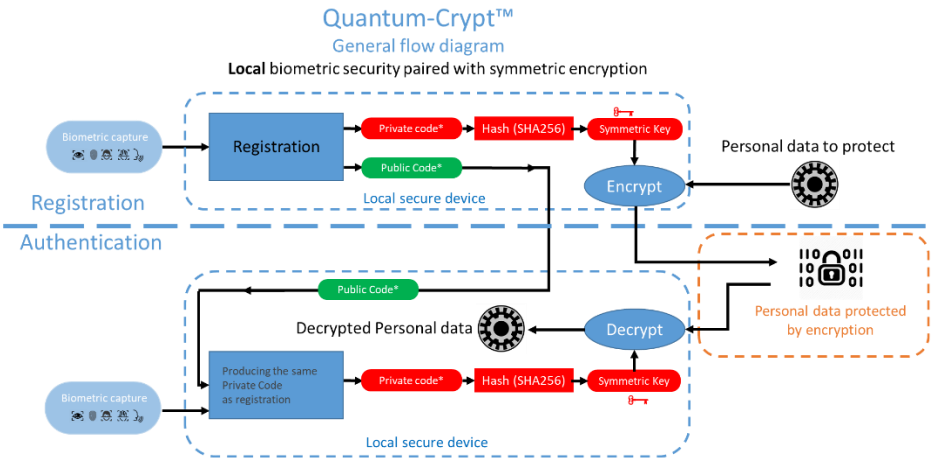
Registration Process

- Biometric scan captures the image
- QuantumCrypt™ technology identifies, extracts stable and repeatable featured vectors from image
- Public/Private Code is generated. Private code is hashed
- Symmetric or asymmetric cryptographic Keys are issued from the biometric generated hash code
- In the case of asymmetric cryptographic keys, Public Key is stored, Private Key is erased from the system. No biometric data stored in any case.

Verification

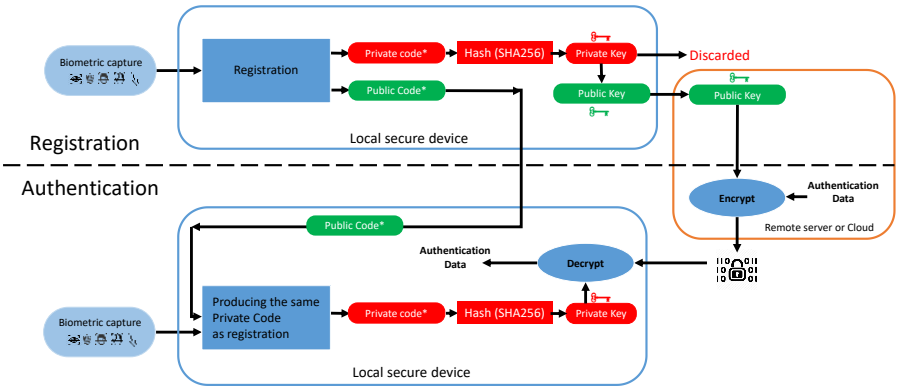
- Biometric scan captures the image
- QuantumCrypt™ technology extracts the same stable features as during registration
- The Public Code will tell the system 'where are the features' to look for building the Private Code
- The same Private Code is generated, same hash key and same cryptographic Keys are issued for authentication

1. Flow diagram with Symmetric Cryptographic Keys (for local data protection or verification)



No biometric data stored.

2. Flow diagram with Asymmetric Cryptographic Keys (to enable remote secure data transfer of verification)



No biometric data stored.

How we do it

Infinity's QuantumCrypt™ enabling technology is designed to work with various existing biometric algorithms to generate repeatable biometric codes at all times. The algorithm collects and resamples the biometric signals on a repeatable basis.

The introduction of the public code is the innovation making it possible to collect stable data while not carrying out any biometric information or any sensitive data. The public code answers to the question "Where is the data to collect?", but it doesn't allow guessing what any bit value of the Private Code. For that, the presence of the biometric scan is necessary to get the Private Code.

The Public Code structure allows the building of revocable codes. By changing the selection of features referenced in the Public Code, we can build a different Private Code and consequently different cryptographic keys while keeping same biometric source and without exposing any biometric data.

Using the iris modality as an example, it involves exposing the iris to the camera with minimum co-operation from users. On face capture, a requirement would be stable illumination, good controls of tilt and face, and stable landmarks detection. These user experience are inherent with most of the existing biometric algorithms in the market today.

The technology can select and isolate those featured vectors with good reliability and repeatability in each amplitude. This is important to ensure 100% repeatable bits are readable.

Conclusion

Infinity's QuantumCrypt™ technology solves the industry's key pain points of privacy concerns relating to biometric data security and integrity. It enables cancellation of the database in the event of a data breach and also supports most 3rd party anti-spoof solutions. Eliminating any biometric data or template storage keeps fraud at bay and paves the way for broader biometric inclusion that can help solve complex challenges in the digital identity foundation for the e-commerce market.

Infinity Optics is awarded the "Frost & Sullivan 2020 Best Global Biometric New Product Innovation"

To learn more:
enquiry@infinityoptics.com.sg