Is the notarized document encrypted/secure?

Every document notarized on the Blue Notary platform is encrypted using X.509 PKI (Public Key Infrastructure) technology for securing digitally signed documents. This ensures each finalized notarized document is tamper-evident.

PKI is a system that governs the issuance of digital certificates that protect sensitive data and secure end-to-end communications. Digital certificates provide unique digital identities to users, applications, and devices in an online world.

PKI is a critical part of the IT strategic backbone. PKI is important because the certificate-based technology helps organizations establish trusted signature, encryption, and identity between people, systems, and things.

All Digital Certificates (Blue Notary and others) are built by an entity generating what is known as a key pair – a private key that remains confidential and a public key that is widely distributed. The private key is used for creating digital signatures and decrypting messages, while the public key is used by others to verify these signatures and encrypt messages to the key owner. The X.509 standard is based on Abstract Syntax Notation One, an interface description language which binds an identity -- such as an individual or hostname -- to a public key with a digital signature.