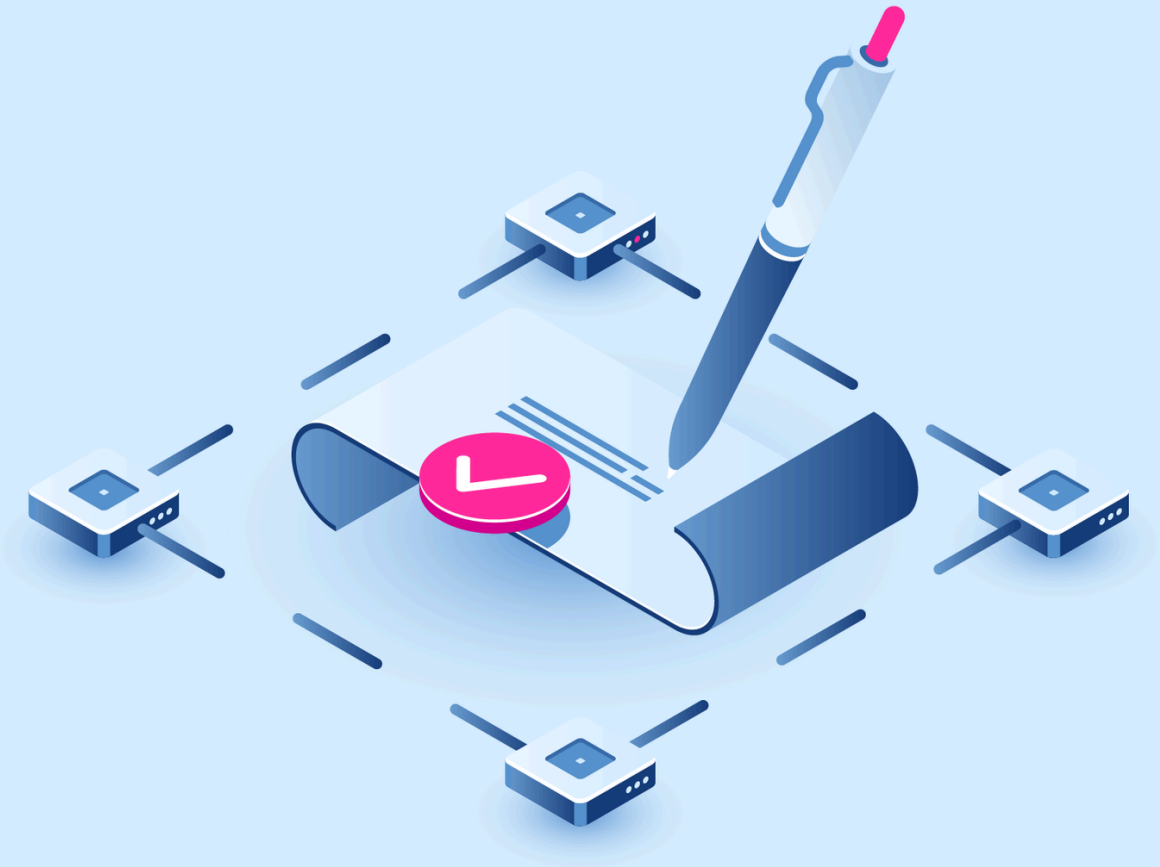
WHAT IS TO BE HEEDED WHEN ENTERPRISES USE PUBLIC DIGITAL SIGNATURES?

LE HAI LINH



The promulgation of the Law on E-Transactions 2023 has created a new legal framework for e-signatures including public digital signatures which are now widely used by enterprises in procedures relative to tax, customs, and social insurance and in signing e-contracts. Accordingly, public digital signatures are digital signatures used in public activities and secured by public digital signature certificates. Guiding public digital signatures, Decree 23/2025/ND-CP regulating e-signatures and trust services (**Decree 23**) will take effect from April 10, 2025, replacing Decree 130/2018/ND-CP guiding the regulations of the Law on Electronic Transactions on digital signatures and digital signature authentication services, amended and supplemented by Decree 48/2024/ND-CP (**Decree 130**). In this Legal Newsletter, NHQuang&Associates will analyze certain contents of businesses' concerns related to public digital signatures in Decree 23.

Firstly, Decree 23 regulates public digital signature certificates. Public digital signature certificates are provided by organizations providing public digital signature authentication services *to verify that the authenticated agency, organization, or individual is the signer of the public digital signature.* A public digital signature certificate provides the name of the organization issuing the digital signature certificate, the validity period of the digital signature certificate, the purpose and scope of use of the digital signature certificate, etc. The validity period of a public digital signature certificate is 3 years in maximum and can be extended under the procedures in Article 39 of Decree 23 before the expiration date of the certificate. According to Decree 130, the maximum validity period of a public digital signature certificate is 5 years for the initial issuance and a maximum of 3 years for the renewal, and organizations and individuals must renew the certificate at least 30 days before the expiration date.

To be issued a public digital signature certificate, individuals and organizations shall prepare a set of application documents according to Article 34, Decree 23. For organizations, the application documents include the certificate of business registration or investment registration, identity documents of the organization's legal representative such as the citizen identity card, etc. After receiving the application documents, the organization providing public digital signature authentication services checks and reviews the documents, enters into a contract with the subscriber and issues the public digital signature certificate to the subscriber. Compared to the provisions of Decree 130, the process of issuing public digital signature certificates prescribed in Decree 23 is more detailed and specific, creating a transparent process and favorable conditions for individuals and organizations involved in registering and using public digital signatures.

Secondly, Decree 23 stipulates the obligations of signers before using digital signatures, specifically:

- Checking the status of digital signature certificates, including the status of their digital signature certificates on the information system of the agency or organization that generates and issues that digital signature certificates, and the status of the digital signature certificate of organization that generates, issues their digital signature certificates on *the trust service authentication system of the National Electronic Authentication Center* instead of "*the technical system of the National Digital Signature Authentication Service Provider*" as prescribed in Decree 130.
- Using digital signature software that complies with technical standards for digital signatures on data messages, with functions such as authenticating the signer and digital signature, and storing and deleting information attached to digitally signed data messages. This is the new content of Decree 23 compared to Decree 130.

Thirdly, Decree 23 stipulates recipients' obligations when receiving digitally signed data messages. Accordingly, a recipient has to check the information such as the status of the digital signature certificate, scope of use, limits of liability, and information on the digital signature certificate of the signer. The status of digital signature certificates must be checked according to the procedure in clause 2, Article 16, Decree 23; for example, for a public digital signature certificate issued by a public digital signature authentication service provider, the recipient has to check the status of the public digital signature certificate of the organization that issues the certificate at the time the signature is digitally signed on the trust service authentication system of the National Electronic Authentication Center. In addition, the recipient must use the digital signature verification software that meets relevant technical standards.

Decree 23 has provided more detailed regulations on e-signatures in general and public digital signatures in particular, which are consistent with the Law on Electronic Transactions 2023, while meeting development requirements of the society, creating favorable conditions for individuals and organizations in the use of e-signatures, but also ensuring the legal validity of e-signatures. Enterprises should update and study the provisions of Decree 23 and other guiding documents that may be promulgated in the near future to use public digital signatures in accordance with legal regulations, ensuring the legal validity of public digital signatures. Should you need more information about the legal regulations and the use of e-signatures and digital signatures in practice, kindly contact NHQuang&Associates for legal support and advice.