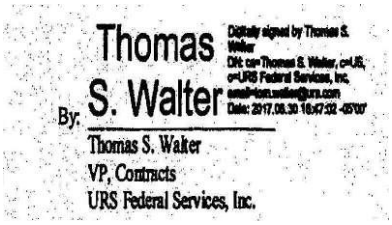
DIGITAL SIGNATURE CERTIFICATION VALID

In a 2017 blog titled "How to Sign Your Claim and Certification" (November 28, 2017), this author discussed some of the pitfalls in claim signatures and certification, and recommended that contractors "not type "signed" or anything else on a claim or certification, but rather insert a real, live signature of a person authorized to bind your company." As of a recent Armed Services Board of Contract Appeals ("ASBCA") decision, the Government should now accept digital signatures that meet the same standards as traditionally accepted ink signatures. *URS Fed. Servs., Inc.* ASBCA No. 61443, Oct. 3, 2019. Specifically, the digital signature is acceptable if it requires the use of a unique password and user identification, and is fully compliant with the claim certification requirement in 41 USC § 7103(b) of the Contract Disputes Act ("CDA").

URS submitted a claim for $1.2 million for costs that were purportedly the fault of the government. The last page of the claim included the required certification, and the following "digital signature:"



Mr. Walter, the certifier was the Vice President of Contracts and had the authority to certify claims. He used PDF-Xchange PRO software to create the digital signature that he affixed to his claim and certification. The Director of Information Management of URS stated that this digital signature could only have been created on URS computers through Mr. Walters' use of a unique password and unique identification.

The Government asserted that Mr. Walter's digital signature was insufficient to comply with the CDA's claim certification requirements, primarily because the signature could not be proven to be genuine on its face.

The Board noted prior appeals relating to "electronic signatures" in which a claimant simply typed its name, sometimes adding a "/s" to distinguish it from an unsigned signature block. All of these were held to be an insufficient signature. Here is a list of cases found by this author, previously discussed in the 2017 blog:

(1) *NileCo Gen'l Contracting,* LLC, ASBCA No. 60912, Sept. 22, 2017. The contractor merely used a typewritten signature block ("Anwar Ahmed Director"). The Board dismissed the claim even though the contractor claimed there had been a course of dealing permitting use of the typewritten signature block. The Board noted that the parties could not override the jurisdictional requirement of an executed certification

through a course of dealing—and could not confer jurisdiction by agreement of the parties.

(2) *ABS Dev. Corp.,* ASBCA No 60022 et al., Nov. 17, 2016. For some of the claims in the appeal, the contractor used several typewritings of a name (presumably typewritten by electronic means) purporting to be signatures. "A typewritten name, even one typewritten in Lucida Handwriting font, cannot be authenticated and therefore is not a signature. [also] The typewritten "//signed//" is not a signature because it cannot be authenticated. Anyone can type a person's name, there is no way to tell who did so from the typewriting itself." These documents were dismissed as unsigned certifications.

(3) *Tokyo Co,* ASBCA No. 59059, April 23, 2014. The claim was stamped "TOKYO COMPANY For general contracting & services Baghdad-Iraq Build 23 St. Al-Karadaa" above the typed words "General Manager of Company BENIAMEN MONADHIL." The Board held that a stamp bearing the company name, explaining what it does, and its address and the typed but unsigned name of the general manager "are not particularized and do not specifically identify the person executing the certification." Again, the claim was dismissed.

(4) *Teknocraft, Inc.*, ASBCA No. 55438, April 3, 2008. The company marked its certification as follows:

> //signed//Sam Kuma
>
> President, Technocraft, Inc.

The Board stated that the notation "//signed//" in the signature block was tantamount to being void of a signature, and was a fatal defect. "The computer generated nonspecific notation is not a discrete verifiable symbol which can be authenticated. As we discussed in *Hawaii Cyberspace, citing Youngdale & Sons Const. Co v. United States,* 27 Fed. Cl. 516, 561, n. 87 (1993), the necessity to sign the certification is to hold the signer 'accountable for any falsities contained therein.' Without a signature, the purported author of the certification could just as easily disavow the certification because "//signed//" cannot be authenticated. Proper execution of the certification is fundamental, going to the essence of the requirement."

The Board then analyzed Mr. Walter's electronic signature, nothing that although the CDA does not define "signature," the FAR defines it as "the discrete, verifiable symbol of an individual that, when affixed to a writing with the knowledge and consent of the individual, indicates a present intention to authenticate the writing. This includes electronic symbols." FAR 2.101.

The question was whether the electronic signature is discrete and verifiable, and the Board found as follows:

> Discrete: simply means "separate and distinct."
>
> Verifiable means the same as the dictionary definition—establishing the truth, accuracy or reality of.

The government contended that to be verifiable, the electronic signature must be authenticated with a validated, trustworthy certificate underlying the signature. The Board rejected this requirement out of hand, because neither the text of the FAR or CDA supported it. Furthermore, the Board noted that

> any common sense examination of …an ink signature informs a less onerous interpretation of 'verifiable' than the government demands. No ink signature, on its face, includes any way for the reader to know who executed it unless that reader already possesses an intimate familiarity with the certifier's handwriting…In our experience we have NEVER seen an appeal where the government successfully argued that the ink signature certifying a clam was inadequate or facially belonged to someone else.

The Board then stated that it would continue to allow ink signatures to satisfy certification requirements, and would not impose draconian demands on digital signatures not required to be met for their ink counterparts. "If one can later establish that a mark is tied to an individual, it is verifiable. This is also consistent with the more open policy towards allowing electronic signatures reflected in the Electronic Signature in Global and National Commerce Act ("ESIGN") 15 U.S.C. §§ 7001-06."

Finally, the Board held that the claim, including the original signature, originated from Mr. Walter's email account, and was inserted by him since it required a password and user identification unique to him. This was sufficient for the Board to conclude that Mr. Watler's signature could be verified, even though there was no underlying certificate submitted to the Board. (The Board noted the URS Director of Information Management had stated in his declaration that a person using a computer outside the URS network would not normally be able to access the "certificate" attesting to the validity of the digital signature because making such a certificate publicly available would be contrary to information security protocols and allow for the disclosure of sensitive, nonpublic information.)

Takeaway: the Board will accept for CDA certification a digital signature that requires the use of a unique password and user identification (provided all other CDA requirements are met). It should also be noted that FAR 4.502(d) explicitly states that "Agencies may accept electronic signature and records in connection with Government contracts." And finally, many government contractors have received contract awards, contract modifications, and other signed contract documents from contracting officers that use the same type of digital signature that Mr. Walter used—all of which have been accepted. See, e.g. *Pond Constructors, Inc.,* B-414307, May 1,

2017"); *PricewaterhouseCoopers LLP; IBM U.S. Federal,*. B-409885, September 05, 2014 (Although a memorandum was not signed the digital signature of the contracting officer contains the date of the signature); By letter dated September 13, 1991, the Director, Computer Systems Laboratory, National Institute of Standards and Technology (NIST), asked whether federal agencies can use Electronic Data Interchange (EDI) technologies, such as message authentication codes and digital signatures, to create valid contractual obligations that can be recorded consistent with 31 U.S.C. § 1501. [W]e conclude that agencies can create valid obligations using properly secured EDI systems. *Nat'l Inst. of Standards & Tech.-Use of Elec. Data Interchange Tech. to Create Valid Obligations,* 71 Comp. Gen 109 (Dec. 13, 1991.