

ARMED SERVICES BOARD OF CONTRACT APPEALS

Appeal of --)
)
URS Federal Services, Inc.) ASBCA No. 61443
)
Under Contract No. FA8108-09-D-0006)

APPEARANCES FOR THE APPELLANT: Terry L. Elling, Esq.
Amy L. Fuentes, Esq.
Holland & Knight LLP
Tysons, VA

APPEARANCES FOR THE GOVERNMENT: Jeffrey P. Hildebrant, Esq.
Air Force Deputy Chief Trial Attorney
Colby L. Sullins, Esq.
Erika L. Whelan Retta, Esq.
Trial Attorneys

OPINION BY ADMINISTRATIVE JUDGE PROUTY

Before us is a straightforward question presented by the government's pending motion to dismiss: whether the signature of appellant's Vice President, affixed to a claim through the use of a digital signature computer application that requires the use of a unique password and user identification, complies with the claim certification requirement in 41 U.S.C. § 7103(b), the Contract Disputes Act (CDA). We hold that it does and that nothing in the CDA or any of our prior cases requires the exclusive use of an ink signature or imposes standards for digital signatures that are any more stringent than those that apply to such traditionally-accepted ink signatures.

FINDINGS OF FACT

The facts material to the government's motion are relatively few, straightforward, and undisputed.

The above-captioned contract (the contract) was awarded to the predecessor of appellant, URS Federal Services, Inc. (URS) on October 3, 2008 (R4, tab 1 at 1, tab 2 (agreement changing business name of contract awardee to URS Federal Support Services)).¹ The contract incorporates by reference the standard Federal Acquisition Regulation (FAR) Disputes clause, FAR 52.233-1, DISPUTES (JUL 2002) (R4, tab 1 at 74).

¹ At some point, not clear in the Rule 4 file and not necessary to be resolved for this motion, URS dropped "support" from its name.

The Disputes clause requires that any claim exceeding \$100,000 be certified. FAR 52.233-1(d)(2)(i).

On June 30, 2017, URS submitted a demand for payment, entitled, “Certified Claim,” in the amount of \$1,232,278.54, for additional costs that were purportedly the fault of the government (R4, tab 80 at 1-8). The last page of the narrative stated:

Pursuant to the Disputes Clause of the Contract, FAR 52.233-1, and the Contract Disputes Act of 1978, as amended and codified at 41 U.S.C. §§ 7101-7109, I certify that the claim is made in good faith; that the supporting data are accurate and complete to the best of my knowledge and belief; that the amount requested accurately reflects the contract adjustment for which URS believes the Government is liable; and that I am duly authorized to certify the claim on behalf of URS.

(R4, tab 80 at 8)

Immediately underneath this statement was the following graphic representation, which we will refer to as the “digital signature” throughout the rest of this opinion:

By: **Thomas S. Walter**
Thomas S. Walter
VP, Contracts
URS Federal Services, Inc.

Digitally signed by Thomas S. Walter
DN: cn=Thomas S. Walter, o=URS,
ou=URS Federal Services, Inc,
email=tom.walter@urs.com
Date: 2017.06.30 16:47:32 -0500

(*Id.*)

Mr. Walter, whose name is reflected in the digital signature above, was the Vice President of Contracts for URS at the time the claim was submitted (*see app. opp’n*, Walter decl. ¶ 3).² As such, he had the authority to certify CDA claims on behalf of URS (*id.*). He used PDF-XChange PRO software, installed on his office computer, to create the digital signature, above, that he electronically affixed to the claim to execute the certification (*id.* at 2, ¶ 5). Prior to submission of the October 2017 claim, he had executed other contract documents for the government in the same manner, but in

² “Walter decl. ¶__” refers to a paragraph of Mr. Walter’s declaration, which is attached to Appellant’s Response to the Government’s Motion to Dismiss.

October 2017, after submission of the claim, the government requested that he cease doing so, which he did³ (*id.* at 2, ¶ 7).

According to the declaration of Charles T. Rice, the Director of Information Management (IT) for URS, the digital signature that Mr. Walter utilized from the PDF-XChange PRO software can only have been created on URS computers through Mr. Walter's use of a unique password and user identification (app. opp'n, Rice decl. ¶ 8).⁴ Mr. Rice also explained that, notwithstanding these protections, an individual using a computer external to the company's 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 (*id.* at 2, ¶ 7.C.).

The government denied URS's claim on September 14, 2017, making no reference to any alleged infirmity to Mr. Walter's signature (R4, tab 82).

As part of its reply in support of this motion, government counsel apparently sent an email to a support staff member of the software company that publishes the PDF-XChange PRO software inquiring if he could "trust the signature" (gov't reply, ex. F). The support person apparently responded by email that "you cannot trust the [digital] certificate to prove the identity of the person who applied it" (gov't reply, ex. G). This is because, without more, no outside authority has been provided a "suitable ID proving who you are" (*id.*). This email does not purport to be under oath or fit within any known hearsay exceptions⁵ although, as will be seen, we may accept it as accurate and give it consideration without changing the result of our decision in favor of URS.

DECISION

The government here argues that Mr. Walter's digital signature is insufficient to comply with the CDA's claim certification requirements, largely because the government is dissatisfied that the signature can be proven to be genuine on its face (*see* gov't. mot. at 7-10). Although we have decided multiple appeals relating to "electronic signatures," in which a claimant simply typed its name, with perhaps (or perhaps not) a "/s" to distinguish it from an unsigned signature block, *see, e.g., Hawaii Cyberspace*, ASBCA

³ October 2017 is several months after Mr. Walter submitted the claim and was, in fact, after the claim was denied. The contracting officer, himself, used a similar digital signature on contract documents prior to October 2017. Walter decl. ¶ 6.

⁴ "Rice decl. ¶ __" refers to a paragraph of Mr. Rice's declaration, which is attached to Appellant's Response to the Government's Motion to Dismiss.

⁵ The government's propounding an unauthenticated unsworn document is somewhat at odds with its otherwise exacting position on authentication of signatures in this motion.

No. 54065, 04-1 BCA ¶ 32,455; *Tokyo Co.*, ASBCA No. 59059, 14-1 BCA ¶ 35,590; *NileCo General Contracting LLC*, ASBCA No. 60912, 17-1 BCA ¶ 36,862, we have not yet been presented with a digital signature of the type we see in this appeal. As discussed below, we hold that the digital signature used here meets the CDA's certification requirements and thus deny the government's motion to dismiss.

I. Standard Of Review

A challenge to the adequacy of the certification of a claim over \$100,000 is a challenge to our jurisdiction to consider the appeal. "It is well settled that certification is a jurisdictional prerequisite for this Board for contractor claims over \$100,000." *Special Operative Group, LLC*, ASBCA No. 57678, 11-2 BCA ¶ 34,860 at 171,480 (citations omitted). Although a defective certification does not deprive the Board of jurisdiction, 41 U.S.C § 7103(b)(3), the failure to certify at all does, mandating dismissal. *Special Operative Group*, 11-2 BCA ¶ 34,680 at 171,480; *CCIE & Co.*, ASBCA Nos. 58355, 59008, 14-1 BCA ¶ 35,700 at 174,816; *Baghdadi Swords Co.*, ASBCA No. 58539, 13 BCA ¶ 35,395 at 173,665.

And, as far as the law is concerned, an unsigned certification is considered to be not certified. This is because the "execution" of a CDA certification requires a "certifier to sign the claim certification," *Teknocraft Inc.*, ASBCA No. 55438, 08-1 BCA ¶ 33,846 at 167,504 (citing *Hawaii CyberSpace*, 04-1 BCA ¶ 32,455 at 160,535), thus making the failure to sign the certification language into the equivalent of "failure to certify," which may not be remedied. *Hawaii CyberSpace*, 04-1 BCA ¶ 32,455 at 160,535; *see also Tokyo Co.*, 14-1 BCA ¶ 35,590 at 174,392.

As the government correctly notes, the burden is on appellant to prove, by a preponderance of evidence, that we possess jurisdiction to consider this appeal. *See Reynolds v. Army & Air Force Exchange Service*, 846 F.2d 746, 748 (Fed. Cir.1988); *Suzan Co.*, ASBCA No. 59817, 16-1 BCA ¶ 36,474 at 177,728; *Al Rafideen Co.*, ASBCA No. 59156, 15-1 BCA ¶ 35,983 at 175,808 (burden of proof in certification case). We add that we may consider evidence outside of the pleadings to decide a jurisdictional motion, like the one here. *Suzan Co.*, 16-1 BCA ¶ 36,474 at 177,728 (citing *Land v. Dollar*, 330 U.S. 731, 735 n.4 (1947)).

II. What Is A Signature Under The CDA?

The CDA does not define "signature,"⁶ but that term is defined in the FAR 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

⁶ Recall that "execution" of the certification requires a signature. *Teknocraft Inc.*, 08-1 BCA ¶ 33,846 at 167,504.

writing. This includes electronic symbols.” FAR 2.101. Applying this definition, we have previously held that a typed but unsigned name is not sufficiently discrete or verifiable to satisfy the CDA requirement that the certification be signed. *Tokyo Co.*, 14-1 BCA ¶ 35,590 at 174,392; *RECO Rishad Engineering Construction ORG*, ASBCA No. 60444, 16-1 BCA ¶ 36,558 at 178,051-52; *ABS Development Corp.*, ASBCA No. 60022 *et al.*, 16-1 BCA ¶36,564. Thus, the legal battle over whether a symbol counts as a signature often turns (as it does here) on whether it is “discrete” and “verifiable.” These terms are not separately defined by the FAR or our case law.

“Discrete,” though paired with “verifiable,” turns out to be a relatively unimportant term in the definition. We read it to mean separate and distinct, *see, e.g., Webster’s Ninth New Collegiate Dictionary* (1986)⁷, which is easily met by the digital signature we see here.

For “verifiable,” we, again, turn to the dictionary, which yields a definition of “capable of being verified,” with “verify” meaning “establish the truth, accuracy, or reality of.” *Webster’s Ninth New Collegiate Dictionary*.

Consistent with its view that the authorship of an electronic signature must be immediately demonstrated on its face, the government argues that, to be verifiable, an electronic signature must be capable of being authenticated with a “validated, trustworthy certificate underlying the digital signature” (gov’t mot. at 10). We reject this definition out of hand because it is not supported by the text of the FAR or CDA.⁸ Moreover, any common sense examination of what we accept in 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—and even that knowledge can be overcome by the simple expedients of tracing or photo-shopping such a mark. In our experience, we have NEVER seen an appeal where the government successfully argued that the ink signature certifying a claim was inadequate or facially belonged to somebody else.

We have no intention of revisiting the practice by which we generally allow ink signatures to satisfy certification requirements, but we are certainly not going to impose draconian demands on digital signatures, not required to be met for their ink counterparts. In particular, if there is no way to require an ink signature to be certainly identifiable as

⁷ Though we reference one particular dictionary, these definitions are relatively consistent across the board.

⁸ The government relatedly argues that certain International Standards Organization (ISO) standards impose particular requirements upon digital signatures (*see* gov’t mot. at 4-5, 8). Since these standards are neither part of the contract, nor the CDA, nor the FAR, they are simply immaterial.

originating from the purported signatory at a glance, we will not require a digital signature to be instantly linked to some immediate form of proof of its veracity.

With the common practice involving ink signatures in mind and looking to the straightforward dictionary definition of verifiable, we conclude that, 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” Act), 15 U.S.C. §§ 7001-7006.⁹

III. The Digital Signature Here Meets The FAR’s Definition of Signature

Although, as noted above, the government expresses dismay that it cannot immediately link the digital signature here to a digital certificate (gov’t mot. at 10), that is not the test for whether a signature is considered valid for CDA certification purposes. The test is whether the mark acting as a signature can be ultimately tied to the signatory, and we find the digital signature here can.

First, it is plain that the claim document, including the digital signature, originated from Mr. Walter’s email account with appellant. This, to us, reflects evidence that he was the author and creator of the digital signature. Second, the evidence from Mr. Rice, URS’s IT manager, also indicates that the digital signature originated with Mr. Walter since it required password and user identification unique to him.

Against this evidence that supports a finding that Mr. Walter executed the digital signature (*i.e.*, that it is verifiable), the government argues that even the software maker concedes that the certificate available does not prove that Mr. Walter executed it (gov’t reply at 6-8). Even if we were to consider this “evidence” from the government, of which we are dubious because it is not authenticated in any way, it would not change our decision. The software company’s purported response was completely consistent with the declarations from Mr. Walter and Mr. Rice, and thus consistent with our finding that the authorship of the signature could be verified—just not with the attached certificate.¹⁰

⁹ The parties have argued extensively over whether the ESIGN Act applies to the digital signature here (*see* app. resp. at 6-7, 21-23; gov’t reply at 8-17. We need not decide the applicability of the ESIGN Act, finding, as we do, that the digital signature before us is compliant with the FAR and CDA on its own terms.

¹⁰ Thus, the facts of this decision are distinguishable from such prior opinions as *ABS*, 16-1 BCA ¶ 36,564, cited by the government, in which we rejected a typed name as a signature because “anyone can type a person’s name.” *ABS*, 16-1 BCA ¶ 36,564, at 178,099 (quoted by gov’t mot. at 10). Here, the evidence is that only Mr. Walter could have made the digital signature.

CONCLUSION

There is sufficient evidence before us to determine that Mr. Walter's digital signature on the claim certification was, in fact, his and is verifiably so. The government's motion to dismiss is denied.

Dated: October 3, 2019



J. REID PROUTY
Administrative Judge
Vice Chairman
Armed Services Board
of Contract Appeals

I concur



RICHARD SHACKLEFORD
Administrative Judge
Acting Chairman
Armed Services Board
of Contract Appeals

I concur



LIS B. YOUNG
Administrative Judge
Armed Services Board
of Contract Appeals

I certify that the foregoing is a true copy of the Opinion and Decision of the Armed Services Board of Contract Appeals in ASBCA No. 61443, Appeals URS Federal Services, Inc., rendered in conformance with the Board's Charter.

Dated:

PAULLA K. GATES-LEWIS
Recorder, Armed Services
Board of Contract Appeals