Schellman & Company, LLC
4010 W Boy Scout Boulevard
Suite 600
Tampa, Florida 33607

Tel: 1.866.254.0000
Fax: 1.866.971.7070

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134

January 22, 2021

RE: FEDERATION ASSURNACE LEVEL (FAL) 2 AND 3 CLARIFICATION FOR ZSCALER

To Whom It May Concern:

As you know, Schellman has performed testing as part of Zscaler's FedRAMP efforts including both the Zscaler Private Access (ZPA) and Zscaler Internet Access (ZIA) platforms.

It is my understanding that your customer has requested additional information surrounding encryption for the Security Assertion Markup Language (SAML) assertions in accordance with the digital identity requirements outlined in the National Institute of Standards and Technology (NIST) 800-63C.

Section 6.2.3 of NIST 800-63C states the following:

> *6.2.3 Encrypted Assertion*
>
> *When encrypting assertions, the IdP SHALL encrypt the contents of the assertion using either the RP's public key or a shared symmetric key. Shared symmetric keys used for this purpose by the IdP SHALL be independent for each RP to which they send assertions, and are normally established during registration of the RP. Public keys for encryption MAY be fetched by the IdP in a secure fashion at runtime, such as through an HTTPS URL hosted by the RP.*
>
> *All encryption of assertions SHALL use approved cryptography.*
>
> *When assertions are passed through third parties, such as a browser, the actual assertion SHALL be encrypted. For example, a SAML assertion can be encrypted using XML-Encryption, or an OpenID Connect ID Token can be encrypted using JSON Web Encryption (JWE). For assertions that are passed directly between IdP and RP, the actual assertion MAY be encrypted. If it is not, the assertion SHALL be sent over an authenticated protected channel.*
>
> *Note: Assertion encryption is required at FAL2 and FAL3.*

When performing FedRAMP assessments, Schellman tests encryption of the SAML assertions (when configured) as well as the encryption enforced at the transport layer for customer access paths that includes protections for SAML assertions that are exchanged between the IdP (customer managed identity provider) and RP (Relying Party).

For the latter, if the RP (Zscaler in this case) enforces encryption at the transport layer for customer access paths using TLS 1.2, the test case is accepted. This supports the above guidance around "If the actual assertion is not encrypted, the assertion SHALL be sent over an authenticated protected channel." Testing performed through third-party tools and configuration reviews of protocols allowed server side, confirmed

Zscaler's enforcement of TLS 1.2. In addition, Zscaler requires the SAML assertion responses to be signed. X509 certificates embedded within the SAML metadata files serve as the trust anchors allowing the verification of signatures, thus establishing trust in the SAML assertions that have been exchanged.

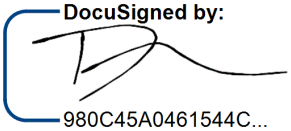
Additionally, Zscaler employs several FIPS 140-2 validated cryptographic modules in the federal environment such as the Zscaler Crypto Module (CMVP#3159), Zscaler Mobile Cryptographic Module (CMVP #3154), and the Zscaler Java Crypto Module (CMVP #3188) used for enhancing the security of customer data in transit paths. Critical software such as the Client Connector (formerly known as Z App) rely on the embedded FIPS 140-2 validated modules for establishing secure connections.

This letter is supplemental to the FedRAMP assessment performed by Schellman. The information provided in this document is "AS IS" without warranties of any kind. Schellman expressly disclaims any warranties of representations including implied warranties and fitness for a particular purpose.

Please notify Zscaler if you require any further information.

Sincerely,

DocuSigned by:



980C45A0461544C...

Douglas W. Barbin, CPA, CISSP, PCI QSA
Principal and Engagement Leader