Public Comments for ICR 202311-1670-001

Author Full Name : Moti Gindi **Received Date :** 12/17/2023 10:19 AM

Comments Received :

Section III, clause 1

We suggest to expand clause 1 c) to cover also programmatic access key and non human identities, as following (suggested changes marked in ***):

c) *** For end-user (development, deployment etc) machines - *** Enforcing multi-factor authentication and conditional access across the environments relevant to developing and building software in a manner that minimizes security risk; *** For programmatic access keys and non-human identities - assure a continuous inventory of such keys with correlation to the sensitivity of the code and to entry points, enforcing regular rotation, implementing preventative mechanisms from leaking into source code, assure minimal exposure in delivery process, separate secure storage with minimal access and strong cryptography.***

Rationale:
A significant portion of attacks on modern applications and software supply chain results from leaked or stolen programmatic access keys (e.g. API tokens, non-human identities). This presents an blind stop and open attack surface for most software producers. We believe that the proactive identification and protection of these should be elevated to the top language of the form. This is highly aligned with PO.5.1 in the SSDF Practices and Tasks.