RESOLUTION OF ENDORSEMENT – MINIMUM REQUIREMENTS FOR CODE SIGNING

Whereas, code signing certificates are a vital part of the internet security infrastructure, as they identify the source of new code downloaded by users and used by applications, and help prevent the spread of malicious or unknown code that can harm users, and

Whereas, to date there have been no uniform requirements for Certification Authorities (CAs) to follow when issuing code signing certificates, making it difficult for users and applications that rely on code signing certificates to evaluate the procedures followed by CAs and the strength of their code signing certificates, and

Whereas, the efforts of many CAs and applications have resulted in creation of the "Minimum Requirements for the Issuance and Management of Publicly Trusted Code Signing Certificates", version 1.1, dated September 22, 2016, as the first set of uniform, open source code signing issuance and usage requirements available to CAs, users, and applications to strengthen code signing certificates, with these Requirements to be updated on a continuous basis as appropriate in the future, and

Whereas, WebTrust audit criteria for the Minimum Requirements for Code Signing are in development to help ensure their uniform application by CAs,

Now Therefore, the following Organizations and Certification Authorities strongly **endorse** the Minimum requirements for Code Signing and pledge to follow them when issuing code signing certificates and urge others to follow these Requirements as well.

ENDORSED AND ADOPTED by the following Organizations and Certification Authorities:

CA Security Council (CASC)

Comodo

Digicert

Entrust

GlobalSign

GoDaddy

Symantec

Trustwave