Mozilla Root Store
331 E. Evelyn Avenue
Mountain View, CA
94041 USA

25 February 2019

Attention: Wayne Thayer; Kathleen Wilson.
REF: Bugzilla ID= 1427262

To the respective Roots Programs,

I am writing to provide DarkMatter Group’s position on a recent media article about the UAE that referenced security and intelligence matters. It also mentioned DarkMatter with misleading information about who we are and what we do. Similar claims have been raised in the Mozilla Policy Group where Forum members have been urged to take action against DarkMatter Group, seeking to derail a two-year process to have our Roots included in their Trust Store. We believe this is grossly unfair and has no basis in fact.

I want to assure you that DarkMatter’s work is solely focused on defensive cyber security, secure communications and digital transformation. We have never, nor will we ever, operate or manage non-defensive cyber activities against any nationality.

Our purpose and vision are very clear, and it is publicly communicated: DarkMatter exists to enable businesses and governments to become smart, safe and cyber resilient. We are proud of our contribution to our clients’ efforts in securing their organisations. Furthermore, as a large player in the cyber security field, we work with our government clients in their quest to protect their nations. We operate in strict adherence and compliance with both the letter and spirit of relevant national laws and all employees are required to abide by local and relevant laws without exception.

We cannot and do not comment on work that we simply do not do, nor can we comment on the practices of government entities and other companies mentioned in a media report. What we can say is what DarkMatter does - all our products, solutions and services are on our website in full view for anyone to see. And just as important is the way we do this work transparently with our clients.

A good example of this is the way DarkMatter has conducted itself where, in the spirit of transparency, we have published all our public trust TLS certificates to appropriate CT log facilities (including all our OV certificates) before this was even a requirement. We have been entirely transparent in our operations and with our clients as we consider this a vital component of establishing and maintaining trust.
Where an issue is raised with us (and we welcome this feedback), we immediately open an investigation. For example, we have used FIPS certified HSMs as our source of randomness in creating our Certificates Authority (CAs - both ECC-based and RSA-based authorities), so we opened an investigation based on Corey Bonnell’s earlier post regarding serial numbers and will produce a corresponding bug report on the findings. In fact, we have finalized this investigation on the raised entropy issue in less than 24 hours. Our conclusion is that our serial numbers in certificates are being generated in accordance with the required Baseline Requirements. Regarding points raised on cryptographic subversion, we do not have access to our clients’ private keys nor to their Key Management and Key Generation infrastructures. We limit our activities to X.509 certificates generation over clients’ public keys, certificate management, and certificate revocation only. Moreover, we recommend best practices with respect to cryptographic algorithms, key sizes in use, and respective implementation.

DarkMatter Group acknowledges that cyber security is still a nascent field and its underlying discourse is increasingly polarised today. As cyber security emerges as one of the most challenging aspects of the 21st century, public-private partnerships is the only manner for governments and companies such as DarkMatter to tackle some of the traditional and non-traditional security threats facing the world today. We want to not only be a part of the discourse but take the lead in developing and shaping public awareness and readiness on how to build cyber resilient societies, economies and institutions. But we believe such discussions should be based on facts, not sensationalized media reports that do this industry a disservice.

We strive to make DarkMatter the most transparent company in the industry where, for example, we make all source code of the technology we develop and build auditable to our clients whether private or government sector. This journey is a long and challenging path, but it is the right one and we are committed to enabling secure digital societies.

We look forward to seeing you in two weeks’ time at our scheduled meeting and hope this letter assuages any questions raised within the Forum.

Yours sincerely,

Karim Sabbagh
Chief Executive Officer
DarkMatter Group

P.O.Box: 27625
Dubai - U.A.E.