bpi BITS
Business
Innovation
Technology
Security

February 21, 2019

Via Electronic Delivery

Donna Dodson, Chief Cybersecurity Advisor, NCCoE
National Institute of Standards and Technology

Re: **Comments on SP 1800-16, Securing Web Transactions: TLS Server Certificate Management**

Dear Ms. Dodson,

The Bank Policy Institute ("BPI") through its technology policy division BITS ("BITS") respectfully submits this comment letter to the National Institute of Standards and Technology's ("NIST") National Cybersecurity Center of Excellence ("NCCoE") in response to the NCCoE's notice for comments regarding Transport Layer Security (TLS) Server Certificate Management.

BITS shares the NCCoE's view articulated in the preliminary drafts of SP 1800-16 that TLS Server Certificate Management is of the utmost importance to the security and operations of public and private sector organizations with an online presence due to its ubiquitous nature in securing web transactions and other communications on internal networks.

BITS commends the NCCoE for documenting and defining best practices for large and medium enterprises, taking into full consideration the unique challenges inherent to organizations with tens of thousands of certificates and keys requiring significant management of inventories, ownership tracking, continuous monitoring, rapid migration, and automation. Further, BITS praises the NCCoE for recognizing that improper management of TLS certificate can cause significant harm to business operations and, in some cases, to the nation and public at-large.

In recent years, BITS has been tracking the development and evolution of encryption protocols such as TLS 1.3. A particularly noteworthy trend in these protocols is the move to provide "Forward Secrecy" through ephemeral cipher suites that employ an ephemeral Diffie-Hellman (DH) or Elliptic Curve Diffie-Hellman (ECDH) key pair.

Last year, the Internet Engineering Task Force (IETF) TLS Working Group finalized TLS 1.3, which effectively removed RSA Key Exchange, and other static key options, limiting implementations to "Forward Secrecy" only. This decision caused much controversy since it disrupts numerous security and diagnostic tools relied upon for over twenty years with previous versions of the TLS protocol.

In response to these actions, the European Telecommunications Standards Institute (ETSI), a global standards body headquartered in France, finalized a key management specification to be used in conjunction with TLS 1.3 called ETSI TS 103 523-3, also known as Enterprise Transport Security (ETS), in October 2018. This standard allows enterprises the discretion to use static DH and ECDH key pairs across multiple sessions, or a single session, allowing flexibility to choose the number of decryption keys to manage while retaining the ability to continue using services provided by an established ecosystem of security and diagnostic tools. Importantly, ETS remains fully compatible with TLS 1.3 clients.

This choice is particularly significant within the financial services industry where internal networks are predominately encrypted. Firms with large, complex network infrastructure must comply with relevant regulations and perform appropriate risk management with respect to troubleshooting, network security monitoring, fraud monitoring and other functions where passive, out-of-band inspection is often the most prudent and scalable solution.

BITS recognizes the NCCoE references the need for these inspection capabilities in draft SP 1800-16B, "*Methods for Gaining Visibility into Encrypted Communications"* and extols the authors for observing the intrinsic server certificate management challenges around key management, including secure key portability. BITS encourages further attention to enterprise key management use cases and the development of automated, product agnostic and interoperable solutions. Establishing new key management standards, to include passive inspection enterprise use cases, would provide significant value and attenuate risk within complex network environments and data centers.

On the basis of the operational and cybersecurity enterprise need, BITS is willing to support and engage in the appropriate NCCoE public-private partnership to address this crucial challenge.

Thank you for your consideration.

Yours truly,

Chris Feeney

Chris Feeney
Executive Vice President & President, BITS
Bank Policy Institute