科普：TLS 1.3 协议 HTTPS 加密

2025 年 12 月 22 日

TLS 1.3 协议的最大优势是遵循“密码敏捷”原则，设计了一个 TLS 支持组，使得密钥交换机制高度模块化，这为后量子密码迁移提供了灵活的算法更新机制保障，零信浏览器全球首个采用 SM2MLKEM768 算法实现了 TLS1.3 协议商密混合后量子密码 HTTPS 加密。

但是，这个非常灵活的浏览器和 Web 服务器之间的密码算法协商机制导致了原先显示商密 HTTPS 加密 **m** 标识的网站不再显示 **m** 标识，网站主和用户马上反映到客服，认为是零信浏览器的错误显示，因为别的其他国密浏览器能正常显示国密加密。看来，这个问题值得好好再次科普一下 HTTPS 加密的自适应密码算法，Web 服务器必须正确配置密码套件和密码算法支持顺序，以便浏览器能按照网站的意愿来实现密码算法选择。

一、 TLS 1.3 协议已成为 HTTPS 加密的主导协议

根据 Cloudflare 的统计数据，全球互联网流量中，TLS 1.3 协议占比 66%，成为主导协议。第二位是 QUIC 协议(谷歌开发的快速 UDP 网络连接协议)，占比 31%。TLS 1.2 协议占比接近 3%，其他不安全的 TLS 1.1 和 1.0 协议几乎忽略不计。我国目前使用的商密 SSL 协议 TLCP 对标国际标准 TLS 1.2 协议，并已经立项制定对标 TLS 1.3 的商密标准。

TLS 1.3 是 TLS 协议的最新版本，由 IETF（互联网工程任务组）制定。它简化了握手过程，并强化了加密机制。主要特点有如下三点：

- 握手过程优化：TLS 1.2 协议需要 2 个握手往返（2-RTT），而 TLS 1.3 仅需 1 个握手往返，对于重复连接支持 0-RTT（零往返），大大缩短了连接建立时间，增强了用户体验。
- 更强的加密：握手消息大部分已加密，保护协商过程不被窥探。
- 精简密码套件：仅支持现代、安全的密码算法，强制启用完美前向保密（PFS），确保即使私钥泄露，历史会话数据也无法被解密。

为什么需要升级到 TLS 1.3 协议？虽然 TLS 1.2 协议仍可安全使用，但它已发布十余年，积累了一些问题，主要有如下 4 个问题：

- 支持了许多过时且易受攻击的密码算法（如 MD5、SHA-1、CBC 模式），这些算法曾导致 POODLE、BEAST 等著名漏洞。
- 握手过程较长，增加延迟，尤其在移动网络或高延迟环境中明显。
- 部分可选功能（如静态 RSA 密钥交换）缺乏前向保密功能，私钥泄露可能危及历史数据安全。
- 旧版本（如 TLS 1.0/1.1）已被正式弃用，继续使用 TLS 1.2 也已经成为事实上被弃用。

二、 后量子密码迁移必须采用 TLS 1.3 协议

未来最大的密码威胁来自量子计算机，当前 TLS 依赖的椭圆曲线（ECDH，SM2）和 RSA 等公钥算法，可被量子算法高效破解，导致了现在就已经存在“先收集后解密”安全威胁。为应对此威胁，美国 NIST 已标准化 3 个后量子密码算法，但是直接切换到纯 PQC 算法风险较高（新算法成熟度不足）。因此，采用混合密钥交换方式：同时使用传统算法（如：X25519、SM2）和 PQC 算法（如 ML-KEM），共享密钥为两者组合。只要其中一个算法安全，整个 TLS 连接就安全。

TLS 1.3 协议为何特别适合混合 PQC 算法 HTTPS 加密？主要有如下四点：

- TLS 1.3 协议的密钥交换机制高度模块化，支持 TLS 算法扩展 - TLS 支持组。
- IETF 制定了混合算法设计标准，允许将传统密码算法+ PQC 算法组合视为一个新支持“组”，可无缝集成到 TLS 握手中。
- 由于 TLS 1.2 协议扩展混合更复杂，且握手开销更大，所以不采用。
- TLS 1.3 协议的简洁性使得添加新算法更容易，更能适合于后续增加更加安全的 PQC 算法。

根据 Cloudflare 的统计数据，全球互联网流量已有 55%采用了 TLS 1.3 协议实现了混合 PQC 算法 HTTPS 加密，一年前仅 16%，这个全球范围的快速实现后量子密码 HTTPS 加密正是得益于 TLS 1.3 协议的密码敏捷性，确保了全球互联网能平滑过渡到量子安全时代。

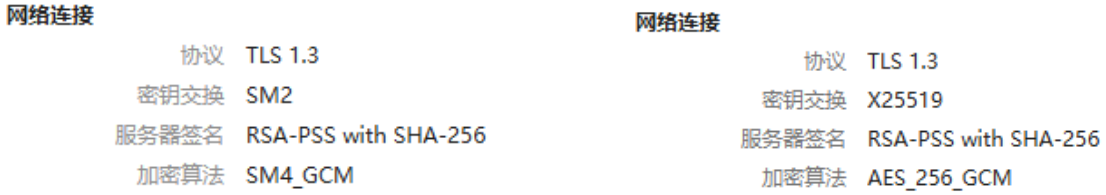
TLS 1.3 协议不仅是 HTTPS 加密的重大升级，更是互联网安全的基础设施革新。它更快、更安全，并为应对量子威胁提供了理想平台。网站运营者和开发者应尽快启用 TLS 1.3 协议，

以保护用户数据安全并提升用户体验。未来，随着 PQC 算法的不断成熟，混合方案将在 TLS 1.3 协议上全面绽放，让 HTTPS 加密在量子时代继续坚不可摧。

三、 零信浏览器优先采用 TLS 1.3 协议支持 PQC 算法和 SM2 算法

目前，大多数浏览器和服务器都已默认支持 TLS 1.3 协议，零信浏览器优先采用 TLS 1.3 协议，这是导致有些已经完成国密改造的网站，使用零信浏览器旧版本可以显示“m”标识，但是使用现在的新版本由于 Web 服务器支持 TLS 1.3 协议但不支持 TLS 1.3 协议的商密算法，所以不再显示“m”标识。零信浏览器新版本为显示“m”标识设置了更高的要求：必须是密钥交换算法、服务器签名算法和加密算法都是采用商密算法(SM2/SM3/SM4)。如下图三种情况所示，第一种情况是采用 TLS 1.3 协议的商密算法和后量子密码算法混合算法-SM2MLKEM768，第二种情况是采用了 TLS 1.3 协议的全套商密算法，第三种情况是采用了传统 SMSSL 协议，这三种情况都会显示“m”标识。

某部委官网部署了国密 SSL 证书，支持 SMSSL 协议，零信浏览器以前版本由于不支持 TLS 1.3 协议实现商密 HTTPS 加密，所以优先采用 SMSSL 协议（第三种情况）实现商密 HTTPS 加密，所以零信浏览器会显示“m”标识，但是由于新版本的零信浏览器优先采用 TLS 1.3 协议，而并非优先采用 SMSSL 协议，因为零信浏览器优先支持后量子密码算法，这个网站现在的网络连接方式如下左图所示，密钥交换采用 SM2 算法、加密算法采用 SM4 算法，但是服务器签名采用 RSA 算法，因为该网站虽然同时部署了 RSA 算法 SSL 证书和 SM2 算法 SSL 证书，但同零信浏览器握手时并没有提供商密 SSL 证书，只提供了 RSA 算法 SSL 证书，不满足 3 种算法都必须采用商密算法的原则，所以不能显示“m”标识，这个网站只需改进服务器配置，支持 TLS 1.3 协议 SM2 算法，就可以实现上述第二种情况的全栈商密算法。如果使用谷歌浏览器访问这个网站，如下右图所示，也是采用了 TLS 1.3 协议，密钥交换采用了 X25519 算法、服务器签名采用了 RSA 算法，加密算法采用了 AES256 算法。



鉴于 TLS 1.3 协议密码算法协商机制非常灵活，大家可以使用零信浏览器访问各种网站看到各种各样的密码算法组合，下图列出 3 个常见的组合，第一个是使用了国际算法混合 PQC 协议实现密钥交换，零信浏览器会显示后量子密码“**Q**”标识，但由于只有加密算法采用了 SM2 算法，所以不会显示“**m**”标识。第二个仅加密算法采用了 SM4 算法，第三个是使用 ECC 算法实现服务器签名，也不能显示“**m**”标识。

协议	TLS 1.3
密钥交换	X25519MLKEM768
服务器签名	ECDSA with SHA-256
加密算法	SM4_GCM

协议	TLS 1.3
密钥交换	X25519
服务器签名	ECDSA with SHA-256
加密算法	SM4_GCM

协议	TLS 1.3
密钥交换	SM2
服务器签名	ECDSA with SHA-256
加密算法	SM4_GCM

零信浏览器和零信 HTTPS 加密自动化网关优先采用商密混合 PQC 算法-SM2MLKEM768，实现了密钥交换算法、服务器签名算法和加密算法都是采用商密算法，所以，用户使用零信浏览器访问零信官网会同时显示“**Q**”标识和“**m**”标识，如下左图所示，使用开发者工具查看会显示密钥交换算法采用 SM2MLKEM768 算法，所以显示“**Q**”标识，而其他两项也都是采用商密算法，如下右图所示，所以零信浏览器会同时显示“**m**”标识。

网络连接

协议	TLS 1.3
密钥交换	SM2MLKEM768
服务器签名	SM2 with SM3
加密算法	SM4_GCM

零信技术秉承用户至上原则，不增加用户费用的前提下，为用户提供同时完成商密合规改造和后量子密码迁移的完整解决方案，实现了一次技改就能同时解决 SSL 证书自动化管理、商密改造和后量子密码迁移三大 HTTPS 加密改造难题，满足我国关基用户的证书自动化管理、商密合规和后量子密码迁移安全保障应用需求，这是省钱、省时、省事的首选方案。

王高华

2025 年 12 月 22 日于深圳

欢迎关注零信技术公众号，实时推送每篇精彩 CEO 博客文章。
已累计发表中文 245 篇(共 72 万 5 千多字)和英文 105 篇(14 万 2 千多单词)。