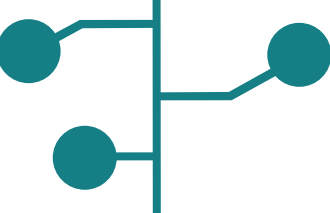


# 域名系统安全扩展

## 确保您在互联网上安全发送 DNS 信息



域名系统安全扩展 (Domain Name System Security Extensions, DNSSEC) 允许注册人对其放置在域名系统 (Domain Name System, DNS) 中的信息进行**数字签名**。此举确保了遭到 (无意或恶意) 损坏的 DNS 数据不会抵达消费者, 从而对消费者加以保护。



### 时间表



域名系统 (DNS) 在设计之时, 安全性并不是一个关注重点。攻击者可以**破坏您的 DNS 信息**, 并将您的信息重新导向至**互联网上的另一地点**, 而非您所请求的地点。



DNS 技术社群针对这个问题编制了确定性解决方案——即 DNSSEC。DNSSEC 基于**公共密钥加密**, 使用数字签名增强了 DNS 的真实可靠性。



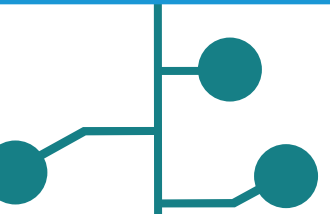
### DNSSEC 的启用



**DNSSEC 必须启动两方面的工作才可奏效。**

负责发布 DNS 信息的注册人必须**确保他们的 DNS 数据已经获得 DNSSEC 签名**。

网络运营商则需要**在其解析器上启用 DNSSEC 验证功能**, 从而应对用户发出的 DNS 查询。



### 部署 DNSSEC 的益处



有利于保护互联网、终端用户、各大企业、组织和政府。



加强应对攻击的能力。



DNSSEC 验证和保护了 DNS 数据, 使得这类数据在 DNS 以外的应用程序中也值得信赖。



**鼓励您的网络运营商启用 DNSSEC**



如需了解更多有关 DNSSEC 的信息, 请访问:

<http://go.icann.org/OCTOpublications>

<http://go.icann.org/DNSSEC>