IETF安全域介绍

夏靓

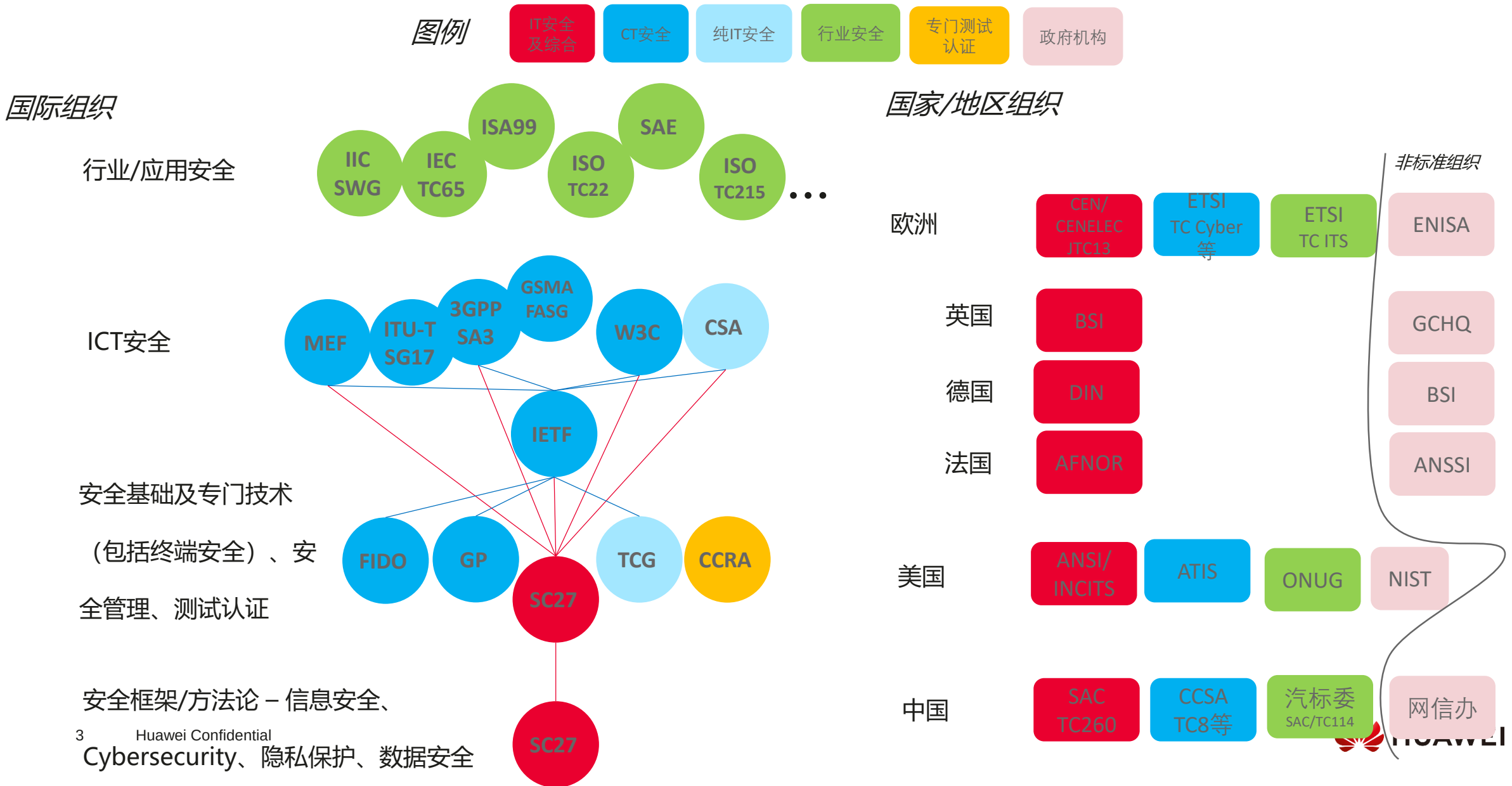
华为技术

Security Level:

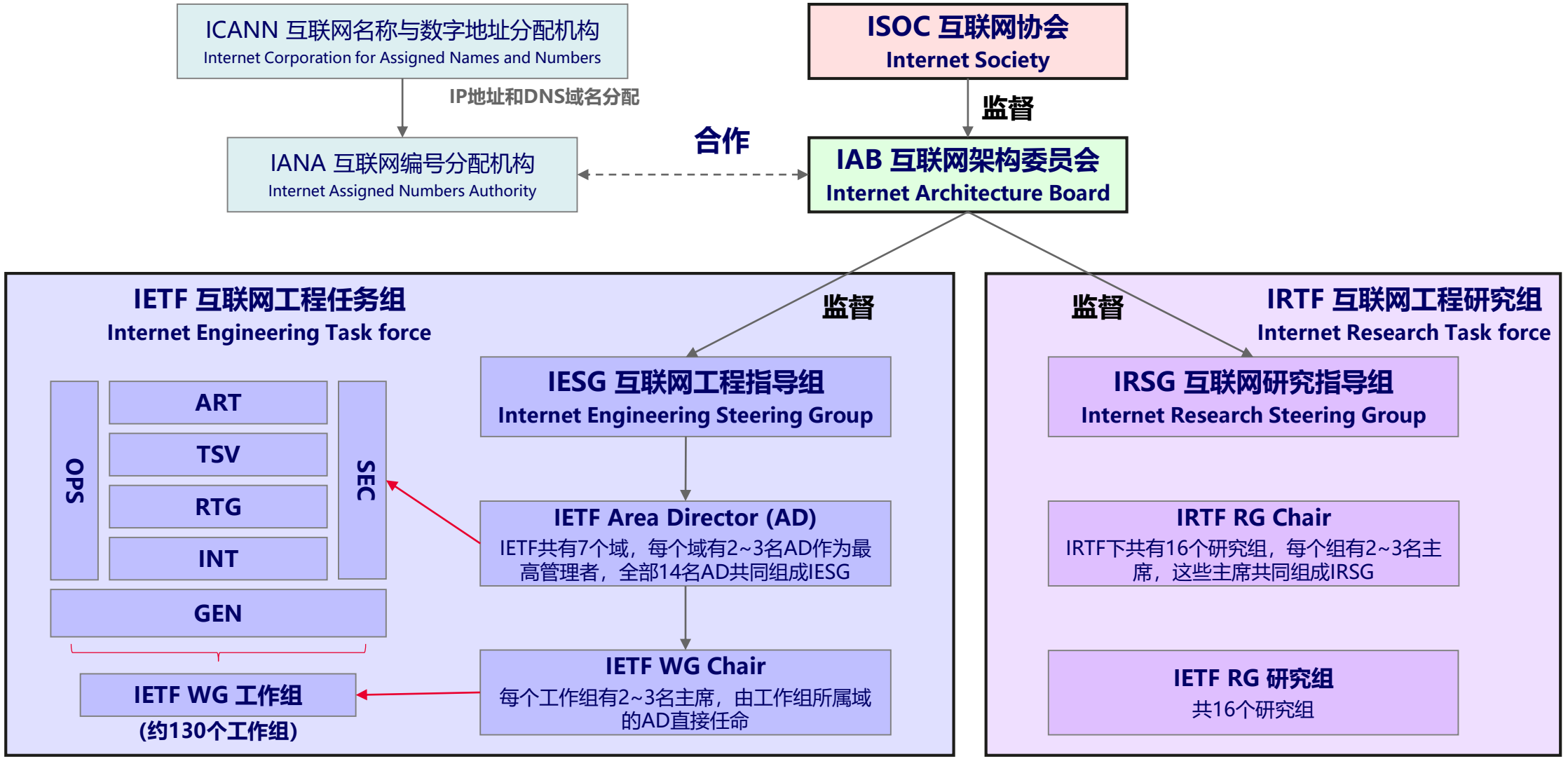
HUAWEI

目录

安全标准组织沙盘：以JTC1 SC27为根，高度分散到不同领域



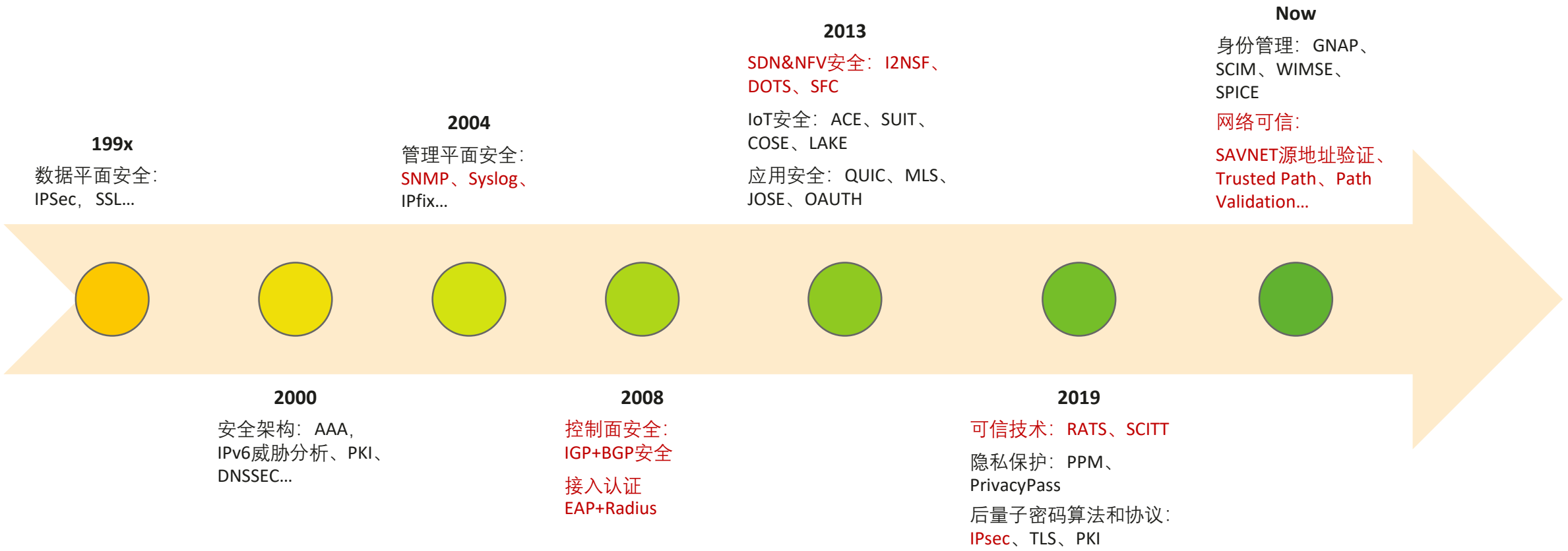
IETF标准与组织流程简介



HUAWEI

IETF安全标准的过去、现在与未来

华为参与



IETF安全技术标准发展脉络

TCP/IP协议、网络基础设施安全 → SDN&NFV、IoT和应用安全 → 设备可信，隐私保护，后量子安全 → 新一代身份管理，网络可信 → …

HUAWEI

IETF安全相关工作组

➢ 安全基础-密码算法

工作组	工作组全称、工作内容简介	主要玩家
CFRG	Crypto Forum：密码算法研究组 • 讨论和审查加密机制在IETF中的使用，通过Informational RFC推动互联网社区（即IETF）对密码机制的理解和使用 • **CFRG为IETF中使用的密码机制进行背书。**	• 主席：Alexey Melnikov（英国 Isode）、Stanislav Smyshlyaev（俄罗斯 CryptoPro）、Nick Sullivan（美国 Cloudflare） • 参与厂商：Cisco、Vigil Security、DFINITY Foundation、University of Bristol、IBM、NCC、Qualcomm、CryptoNext Security, Sorbonne University等
PQUIP	Post-Quantum Use In Protocols：在协议中使用PQC算法 • 新工作组；不定义新协议、不更新现有协议；不定义新密码机制或评估特定密码机制是否能抵抗量子计算攻击。 • 为IETF相关协议、文档中密码机制的后量子迁移**提供操作和工程方面的指导。**	• 主席：Paul Hoffman（美国 ICANN）、Sofia Celi（葡萄牙 Brave Software） • 参与厂商：Cisco、Nokia、DigiCert、VeriSign、Amazon、Cloudflare、Entrust、AirBus、Siemens、MIT、MITRE、英国NCSC等

➢ 安全基础-PKI/证书

工作组	工作组全称、工作内容简介	主要玩家
ACME	Automated Certificate Management Environment • 自动化证书管理，在线自动签发DV域名验证证书	• 主席：Deb Cooley（美国 NSA）、Yoav Nir（以色列 DELL） • 参与厂商：Cisco、Google、DigiCert、Entrust、Comcast、安永、DELL、Neustar、Internet Security Research Group
LAMPS	Limited Additional Mechanisms for PKIX and SMIME • PKIX证书相关扩展，CMP证书管理协议，电子邮件安全S/MIME扩展。 • **PKIX证书向PQC后量子密码演进**	• 主席：Tim Hollebeek（美国 DigiCert）、Russ Housley（美国 Vigil Security） • 参与厂商：Cisco、Ericsson、Nokia、DigiCert、Entrust、美国NSA、Siemens、Cloudflare、Red Hound、Red Hat、Amazon、AWS、Adobe等

HUAWEI

IETF安全相关工作组

➢ 网络安全-接入认证

工作组	工作组全称、工作内容简介	主要玩家
EMU	EAP Method Update • EAP认证方法的增强与更新，包括**IoT轻量级认证方法** • **EAP-AKA、EAP-AKA'**	• 主席：Joseph Salowey（美国 Venafi）、Peter Yee（美国 AKAYLA） • 参与厂商：Ericsson、Cisco、FreeRADIUS、CableLabs、HP、CMCC、Huawei、DFN、University of Murcia、University of Oviedo
KITTEN	Common Authentication Technology Next Generation • 对GSS-API和Kerberos认证系统的扩展及增强	• 主席：Alexey Melnikov（英国 Isode）、Benjamin Kaduk（美国 Akamai） • 参与厂商：Red Hat、MIT、Painless Security、Shibboleth Consortium
RADEXT	• RADIUS EXTensions RADIUS协议扩展，包括RADIUS over TLS/DTLS	• 主席：Valery Smyslov（俄罗斯 ELVIS-PLUS）、Margaret Cullen（美国 Painless Security） • 参与厂商：FreeRADIUS、DFN、Cisco、RESTENA

➢ 网络安全-安全传输

工作组	工作组全称、工作内容简介	主要玩家
IPSECME	IP Security Maintenance and Extensions • IPsec协议/IKE协议更新与扩展，包括：**IKEv2协议向PQC后量子演进的扩展方案；组播IPsec；IKEv2扩展**	• 主席：Tero Kivinen（芬兰 INSIDE Secure）、Yoav Nir（以色列 DELL） • 参与厂商：俄罗斯ELVIS-PLUS、Cisco、Nokia、**Huawei**、Apple、Aiven、Red Hat、secunet Security Networks AG
TLS	Transport Layer Security • TLS/DTLS协议更新与扩展，包括：**TLS协议和算法更新；TLS向PQC后量子演进的扩展方案；TLS支持PSK（QKD）**	• 主席：Joseph Salowey（美国 Venafi）、Sean Turner（美国 Sn3rd）、Christopher Wood（美国 Cloudflare） • 参与厂商：Mozilla、ARM、Google、Apple、Cloudflare、Ericsson、Cisco、**Huawei**、Salesforce、Facebook、Akamai、AWS、IBM
UTA	Using TLS in Applications • TLS/DTLS的应用相关，例如IoT中使用TLS/DTLS的Profile定义、TLS/DTLS的推荐安全使用等	• 主席：Orie Steele（美国 Transmute）、Valery Smyslov（俄罗斯 ELVIS-PLUS） • 参与厂商：ARM、Akamai、Venafi
QUIC	QUIC • 新的传输层安全协议QUIC	• 主席：Lucas Pardue（美国 Cloudflare）、Matt Joras（美国 Meta） • 参与厂商：Google、Mozilla、Microsoft、Alibaba、Akamai、Meta、Cloudflare、Ericsson、Protocol Labs、Fastly

IETF安全相关工作组

➢ 网络安全-可信相关

工作组	工作组全称、工作内容简介	主要玩家
RATS	Remote Attestation Procedures • 远程证明的架构、交互、接口等。 • **1）远程证明消息接口逐步标准化；** • **2）对远程证明结果的应用**	• 主席：Nancy Cam-Winget（美国 Cisco）、Kathleen Moriarty（美国 CIS）、Ned Smith（美国 Intel） • 参与厂商：Cisco、Juniper、**Huawei**、Nokia、Microsoft、Intel、ARM、Qualcomm、德国Fraunhofer
SCITT	Supply Chain Integrity, Transparency, and Trust • 软件供应链完整透明可信	• 主席：Hannes Tschofenig（ARM）、Jon Geater（英国 RKVST） • 参与厂商：Microsoft、ARM、MITRE、德国Fraunhofer
TEEP	Trusted Execution Environment Provisioning • TEE可信执行环境中可信应用的管理	• 主席：Nancy Cam-Winget（美国 Cisco）、Tirumaleswar Reddy（印度 Nokia） • 参与厂商：Microsoft、ARM、Qualcomm、德国Fraunhofer

➢ IoT/轻量化安全

工作组	工作组全称、工作内容简介	主要玩家
ACE	Authentication, Authorization for Constrained Environments • 轻量化OAUTH：协议及相关扩展很丰富，基本完成。未来会成为IoT安全关键技术集	• 主席：Daniel Migault（加拿大 Ericsson）、Loganaden Velvindron（毛里求斯 cyberstorm.mu） • 参与厂商：Ericsson、Microsoft、ARM、Cisco
COSE	CBOR Object Signing and Encryption • CBOR对象签名加密，美国公司在这个工作组集中推进PQC算法融合	• 主席：Mike Jones（美国 Microsoft）、Matthew Miller（美国 Mozilla）、Ivaylo Petrov（瑞士 Google） • 参与厂商：August Cellars、Microsoft、Ericsson、IBM
LAKE	Lightweight Authenticated Key Exchange • 轻量认证密钥交换	• 主席：Stephen Farrell（爱尔兰 都柏林圣三一大学）、Malisa Vucinic（法国 Inria） • 参与厂商：Ericsson
SUIT	Software Updates for Internet of Things • IoT固件的安全更新：ARM主推的标准，未来有可能成为主流应用技术	• 主席：Russ Housley（美国 Vigil Security）、Dave Thaler（美国 Microsoft）、David Waltermire（美国 NIST） • 参与厂商：ARM、Fraunhofer
DANCE	DANE Authentication for Network Clients Everywhere • 基于DNS的轻量级身份体系。DNS域名作为IoT终端轻量级身份，用DNSSEC代替PKI	• 主席：Wes Hardaker（美国 南加州大学）、Joey Salazar（哥斯达黎加 Alajuela） • 参与厂商：Saleforce

IETF安全相关工作组

➢ 应用层安全

工作组	工作组全称、工作内容简介	主要玩家
JOSE	Javascript Object Signing and Encryption • JSON对象签名加密，主要是基于W3C Verifiable Credentials诉求定义JSON-based selective disclosure and zero-knowledge proofs	• 主席：John Bradley（智利 Yubico）、John Preuss Mattsson（瑞典 Ericsson）、Karen O'Donoghue（美国 Internet Society） • 参与厂商：Microsoft、Ping Identity、Transmute、mesur.io
MLS	Messaging Layer Security • 应用层加密，CGKA连续性群组密钥管理协议	• 主席：Nick Sullivan（美国 Cloudflare）、Sean Turner（美国 Sn3rd） • 参与厂商：Cisco、Mozilla、Google、Twitter、Facebook
OHAI	Oblivious HTTP Application Intermediation • 通过HTTP Proxy保护Client身份不泄露	• 主席：Richard Barnes（美国 Cisco）、Shivan Kaul Sahib（加拿大 Brave Software） • 参与厂商：Mozilla、Apple、Cloudflare
SECEVENT	Security Events • HTTP安全事件信息分发相关	• 主席：Dick Hardt（美国 Hellō）、Yaron Sheffer（加拿大 Intuit） • 参与厂商：Amazon、Microsoft、Google、Cisco、Oracle
PPM	Privacy Preserving Measurement • 利用多方计算，实现保护用户隐私的数据收集协议	• 主席：Benjamin Schwartz（美国 Google）、Samuel Weiler（美国 W3C/MIT） • 参与厂商：Mozilla、Cloudflare
MASQUE	Multiplexed Application Substrate over QUIC Encryption • 应用层协议over QUIC	• 主席：Christopher Wood（美国 Cloudflare）、Eric Kinnear（美国 Apple） • 参与厂商：Google、Apple、Ericsson、Cloudflare、Alibaba

➢ Web授权

工作组	工作组全称、工作内容简介	主要玩家
OAUTH	Web Authorization Protocol • OAUTH2.0扩展更新：OAuth是面向于解决第三方应用授权问题的开放协议	• 主席：Hannes Tschofenig（ARM）、Rifaat Shekh-Yusef（加拿大 Auth0） • 参与厂商：IBM、Microsoft、Ping Identity、ARM
GNAP	Grant Negotiation and Authorization Protocol • 解决OAUTH2.0不能解决的Web授权场景	• 主席：Yaron Sheffer（加拿大 Intuit）、Leif Johansson（瑞典大学计算机网络） • 参与厂商：Bespoke Engineering、acert.io
PRIVACYPASS	Privacy Pass • 能实现隐私保护的Web授权协议	• 主席：Benjamin Schwartz（美国 Google）、Joseph Salowey（美国 Venafi） • 参与厂商：Google, Cloudflare

IETF安全标准为什么重要：安全根技术标准集中

- **可信根：**
  - **RATS工作组：**基于可信根，进行网络设备和IoT设备的**远程证明**，保证设备完整性不被破坏，设备安全态势良好。进一步，在E2E加密之外，构建**E2E可信路径**，保证关键业务的安全可信传输；
  - **TEEP工作组：**对终端和设备的**可信执行环境**进行**远程管理**，包括应用安装部署等；
  - **SCITT工作组：软件供应链完整透明可信**，IETF安全可信领域由单机和网络的远程证明向软件BOM全生态可信发展
- **密码技术：**
  - **CFRG研究组：**密码研究组。讨论和审查**加密机制在IETF中的使用。**比如：PAKE，AEGIS，混合密钥推导，AEAD等
  - **PQUIP工作组**：为IETF相关协议、文档中密码机制的后量子迁移**提供操作和工程方面的指导**
- **数字证书：**
  - **LAMPS工作组： PKIX证书**相关扩展，**CMP**证书管理协议， PKIX证书向PQC**后量子密码演进**
  - **ACME工作组：自动化证书管理**，在线自动签发DV域名验证证书
- **路由安全：**
  - **SIDROPS工作组：**防止BGP路由泄露和劫持，RPKI，ROA等；
  - **SAVNET工作组：**源地址验证协议体系；
- **安全传输：**
  - **IPSECME工作组： IPsec协议/IKE协议更新与扩展**，包括：IKEv2协议向PQC后量子演进的扩展方案；组播IPsec；IKEv2扩展
  - **TLS工作组： TLS/DTLS协议更新与扩展**，包括：TLS协议和算法更新；TLS向PQC后量子演进的扩展方案；TLS支持PSK（QKD）
  - **QUIC工作组：新的传输层安全协议QUIC**
  - **MASQUE工作组：应用层协议over QUIC，**给QUIC引入Datagram帧，使能QUIC 成为互联网通用传输加密隧道Tunnel（HTTP/UDP/IP over QUIC）

HUAWEI

IETF安全标准为什么重要：安全新技术标准涌现

- **隐私保护：**
  - **OHAI工作组：**通过HTTP Proxy保护**Client身份不泄露**；
  - **PPM工作组：**利用多方计算，实现**保护用户隐私的数据收集协议**；
  - **PRIVACYPASS工作组：**能实现**隐私保护的Web授权协议。**
- **身份管理：**
  - **OAUTH工作组：**OAUTH2.0扩展更新。OAuth是面向于解决**第三方应用授权**问题的开放协议；
  - **ACE工作组：轻量化OAUTH。**协议及相关扩展很丰富，基本完成；
  - **GNAP工作组：**GNAP的目标是设计一个**细粒度的Web授权协议**，可以看作是对OAuth协议的演进，除了传统的对申请访问资源进行授权外，还支持**对身份标识相关信息的访问授权；**
  - **SCIM工作组：跨域用户身份管理，**主要用于**企业SaaS服务场景；**
  - **WIMSE BOF：** 给云计算中的**微服务赋予身份，workload identity**的协议实现；
  - **SPICE BOF：**数字凭证**定义和使用。**
- **数据安全：**
  - **SATP工作组：安全资产转移协议。**目标是开发一种在**两个网关之间**运行的标准协议，目的是在网络或系统之间**转移数字资产；**
  - **TIGRESS：终端之间**的**数字凭证**交换和颁发协议。
- **远程证明的广泛应用：for TLS，for PKI, for OAUTH…**
- **去中心化，支持审计的透明化（Transparency）技术：**证书透明CT、供应链透明SCITT、密钥透明KeyTrans等；

HUAWEI

IETF安全标准为什么重要：主流IT和CT厂商广泛参与

CT厂商	IT厂商	研究/监管机构
• **设备商：** HUAWEI，Cisco，Ericsson，Nokia • **运营商：** Comcast，CMCC，Orange，Telefonica • **芯片商：** ARM，Qualcomm，Broadcom，Intel	• **传统IT厂商：** IBM，Oracle，Red Hat • **互联网和云服务提供商：** Microsoft，google，Facebook，Amazon，Akamai，Cloudflare，Mozilla，Alibaba • **终端厂商：** apple，Huawei	• **研究机构：** 清华、MIT、Fraunhofer SIT • **监管机构：** CNNIC, NCSC、MITRE、NSA，CIS

HUAWEI

IETF安全标准热点分享一：后量子密码算法和协议

- **随着NIST开始进行PQC后量子密码算法公开筛选，协议和证书等支持PQC算法成为IETF安全域热点。2021年起，多个工作组中均出现相关的提案，但推动者多为美国厂商机构，缺乏中国声音**：
  - **LAMPS工作组**：AWS、Cloudflare、Entrust、IBM、NSA等推动近10篇PKI证书支持PQC相关文稿，**目前工作组已接纳4篇。**
    - Using SPHINCS+ in CMS（链接）、Using KYBER in CMS（链接）、Using Dilithium in Certificates（链接）、Using KYBER in Certificates（链接）等。
    - 混合证书（Hybrid Certificate）相关：单证书多算法（Composite） vs 单算法多证书（Non-Composite）
  - **TLS工作组**：Cisco、Amazon、滑铁卢大学推动TLS混合使用PQC算法和传统算法进行密钥交换的文稿（链接），**目前已被工作组接纳。**
  - **COSE工作组**：Google、IBM、NXP等推动PQC签名算法的JSON和CBOR序列化编码文稿（链接），**目前已被工作组接纳。**
  - **SSH协议相关**：AWS、University of Waterloo提出SSH协议使用PQC算法和传统算法进行密钥交换的文稿（链接）。
  - **CFRG研究组**：美国Cisco、Entrust、Cloudflare等厂商和美国NIST、德国BSI等监管机构共同推动多篇PQC算法文稿；
- **Post-Quantum Use In Protocols （PQUIP）工作组于2022年底正式成立**
  - 讨论与IETF工作相关的PQC过渡、迁移过程中的运营和工程问题和经验，以及无工作组的协议与PQC相关的问题。
  - 记录支撑PQC过渡、迁移的相关设计指南等文档。
  - 不会更新现有协议、制定新协议、定义新密码机制或评估给定密码机制是否能抵抗量子计算攻击。
  - 现有文稿：英国NCSC牵头起草PQC迁移的术语文稿；美国DigiCert牵头PQC for Engineers指南文稿；整理PQC算法和协议支持PQC算法的现有标准和文稿清单（链接）

HUAWEI

IETF安全标准热点分享二：远程证明的广泛应用

- 将远程证明应用在身份鉴别机制中，在传统通过密码学验证Client是谁的基础上，需要再验证Client的其他属性，例如“设备可信”或者叫“设备安全”属性。身份鉴别是可以通过密码学保证可信，传统上并没有可信的机制来传递“设备安全”属性，如今通过TPM、TEE等硬件可信根可以实现可信传递”设备安全“属性。

- **Using Attestation in TLS and DTLS**
  - https://datatracker.ietf.org/doc/draft-fossati-tls-attestation/，Hannes Tschofenig (Siemens)、ARM

- **Use of Attestation with Certification Signing Requests**
  - https://datatracker.ietf.org/doc/draft-ounsworth-csr-attestation/，Mike Ounsworth (Entrust)、Hannes Tschofenig (Siemens)
- **Attestation Attributes for Use with Certification Signing Requests**
  - https://datatracker.ietf.org/doc/draft-stjohns-csr-attest/，NthPermutation Security
- **A Standard Format for Key Compromise Attestation**
  - https://datatracker.ietf.org/doc/draft-mpalmer-key-compromise-attestation/，pwnedkeys.com
- **Nonce-based Freshness for Attestation in Certification Requests for use with the Certification Management Protocol**
  - https://datatracker.ietf.org/doc/draft-tschofenig-lamps-nonce-for-cmp/，Siemens
- **Automated Certificate Management Environment (ACME) Device Attestation Extension**
  - https://datatracker.ietf.org/doc/draft-acme-device-attest/，Google

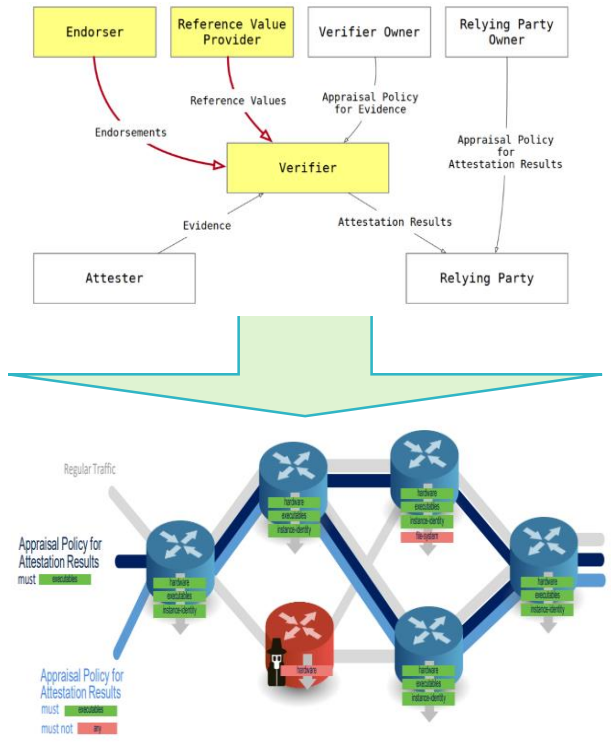
- **Attestation in OpenID-Connect**
  - https://datatracker.ietf.org/doc/draft-sh-rats-oidcatt/，Intel、MIT
- **The Use of Attestation in OAuth 2.0 Dynamic Client Registration**
  - https://datatracker.ietf.org/doc/draft-tschofenig-oauth-attested-dclient-reg/，Siemens
- **OAuth 2.0 Attestation-Based Client Authentication**
  - https://datatracker.ietf.org/doc/draft-looker-oauth-attestation-based-client-auth/，MATTR、Bundesdruckerei GmbH

HUAWEI

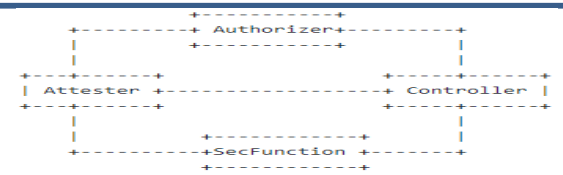
IETF安全标准热点分享三：可信网络标准体系开始构建

IETF中正在不同维度定义可信网络需求、架构、特性、能力等

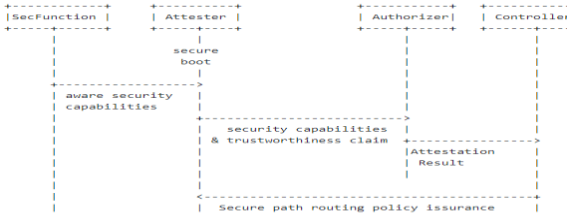
IETF RATS 定义远程证明框架与协议，CISCO，Juniper等公司在IETF提出了基于远程证明的可信网络构建方法，其核心思想就是通过远程证明确认对端路由器的可信性并通过**信任扩展的方式构建一个逻辑可信网络**并建立相应的转发路径



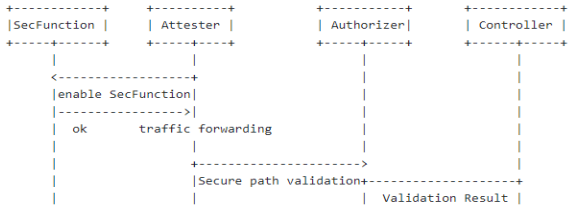
中国移动在IETF提出secure path需求和架构文稿，描述需要整个网络提供：可信路径—基础设施原生安全+安全特性加固、add-on的安全产品或服务、业务路经验证。从而提供可信网络整体解决方案，重点在于安全可视化和和可信SLA保证。



架构

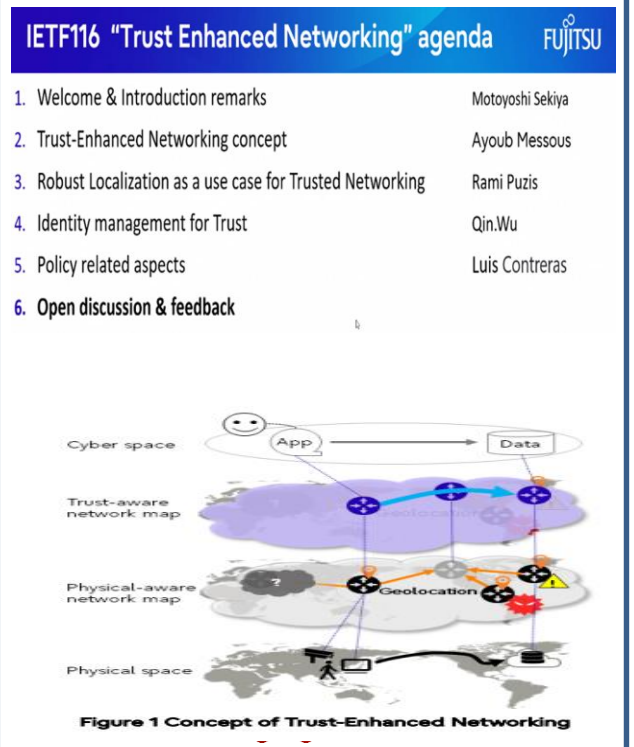


设备可信和安全能力通告



业务路径验证

富士通在IETF116举办Trust Enhanced Networking Side Meeting, 为成立工作组预热。 Fujitsu前期白皮书中使用了**Quality of trust、trust map、trust enhanced networking**等概念，强调要对网络进行信任测量与分级，但是强调基于**设备真实地理位置**来衡量可信度



个人对IETF组织和工作方法的一些心得

- IETF安全值得参与：TCP/IP与Internet安全相关根技术研究、应用与改进，新技术的制定、引领与推广的核心舞台；

- IETF是工程师文化，强调场景、问题、技术方案、具体实现和商业价值，做标准需要围绕并服务于这些目的。这些工作做扎实了，标准是水到渠成和相辅相成；

- IETF是开放与合作的，欢迎任何人带着新的问题和想法来参与，来讨论和贡献。强调合作与妥协，推崇和而不同，斗而不破，实现产业的整体发展。

HUAWEI

Thank you.

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home and organization for a fully connected, intelligent world.

Copyright©2018 Huawei Technologies Co., Ltd.
All Rights Reserved.

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product portfolio, new technology, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.

HUAWEI