应用《网络设备安全保证计划》来提高电信设备的安全保障

作者：张志鹏、刘岩（atsec 中国）

2019 年 5 月

关键词：数据保护、NESAS、PCI

atsec(Beijing) information technology Co., Ltd
Floor 3, Block C, Building 1, Boya C-Center,
Beijing University Science Park, Life Science Park
Changping District, Beijing, Postcode: 102206
P.R.China
Tel +86-10-53056681
Fax +86-10-53056678
www.atsec.cn

1 为什么需要网络设备安全保证计划(NESAS)

随着移动网络安全的迅速发展，作为基础网络服务提供商的移动网络运营商也承担了更多的安全责任。在许多国家，移动运营商有责任运行可靠和强壮的移动网络，如果出现问题或将追究其法律责任。然而，移动运营商只能对运营层面进行自主的安全控制，而对于网络设备层面的安全就只能依赖于设备厂商。因此，对于移动运营商来说，如何衡量网络设备安全水平，如何选择一个安全的网络设备产品，变得尤其的重要。而对于网络设备厂商来说，如何向各个不同的网络运营商证明自己的产品安全水平，如何彰显厂商实现并保持了良好的安全标准的能力，也是一个亟需解决的问题。网络设备安全保证计划（NESAS：Network Equipment Security Assurance Scheme）就是在这个大背景下出台的一个志愿计划。所谓志愿计划，是说由移动产业内的各个运营商和设备厂商自主自愿的参与，并不强制。NESAS 不但帮助网络运营商快捷高效的确定网络产品的安全水平，挑选出来具有高安全标准的设备厂商，也帮助厂商避免了疲于应付各种不同的监管和网络运营商各自不同的安全需求。

2 什么是网络设备安全保证计划(NESAS)

网络设备安全保证计划（NESAS）是由 3GPP（3rd Generation Partnership Project）和 GSMA（Global System for Mobile Communications Assembly）共同定义的针对移动产业的志愿计划。NESAS 为运营商和厂商提供了容易落地实施的安全保证，同时为产业确定了一个通用的基线安全等级。通过这个安全基线可以验证网络设备是否满足安全需求列表，设备厂商是否按照安全标准指南进行产品开发。为了实现这个目标，NESAS 提出了以下两个方法：

- 对设备厂商的开发和产品生命周期流程的安全认证；
- 由具有资质的测试实验室通过执行定义好的和标准化的安全测试，对网络设备进行安全评估。

第一种方法允许每个设备厂商定义自己的内部流程，描述如何将安全性融入到设计、开发、实施和维护过程中。外部审核员检查这些流程，并确定这些流程是否真正落实执行。如果审核员认可，设备厂商将获得认证。该认证向外界证明，供应商能够创造安全的产品。在进行认证时，设备厂商不必向公众披露其内部流程的细节，只有审核员才能看到这些内部流程。这样，一个合格的并被认可的审核员可以保护厂商的内部机密不会被泄露给公众。

第二种方法是对实际网络设备进行安全评估。如果网络设备有一套预定义的安全测试，并且所有的网络设备都是针对这些要求进行测试，那么可以客观地测量和可视化网络设备所达到的安全级别。按照这种方法，可以评估新的网络设备以及升级后的网络设备。这些测试是由一个公认的和有能力的测试实验室进行的，这样可以保证该测试的高质量和一致性。另外一个好处是，由于测试只需要统一执行一次，设备厂商在展示其网络设备的安全性时，只需要向潜在客户们展现 NESAS 评估报告，而无需为每个客户或相关者进行重复测试，这也大大提高了设备厂商的效率且有效降低了测试成本。

这两种方法 – 流程认证和安全测试评估 – 极大的帮助移动运营商（MNO：Mobile Network Operator）确定网络产品的安全水平。非常有利于移动运营商（MNO）根据安全要求来选择厂商。

NESAS 是由一系列规范文档组成，文档之间的结构关系请参见图 1。

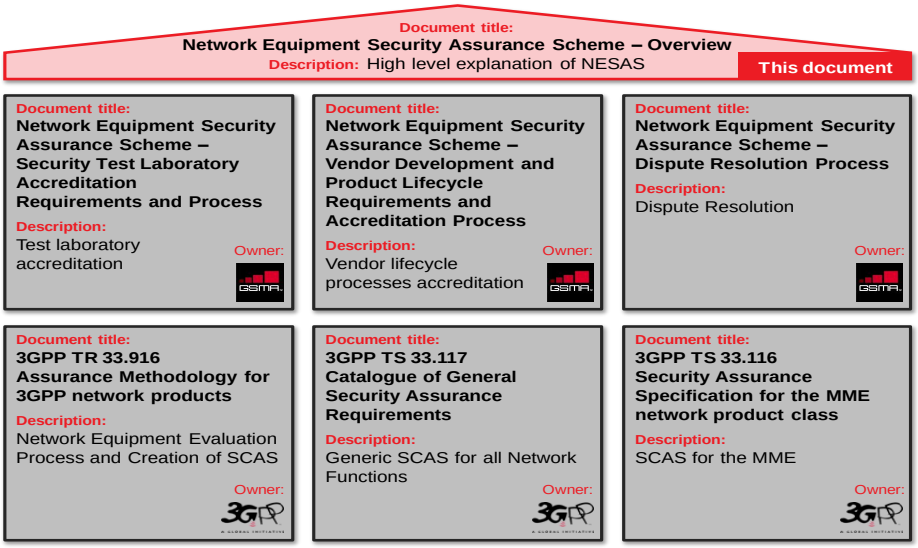

图 1　NESAS 文档概述

3 GSMA 和 3GPP 的角色

GSMA 定义和维护 NESAS 的规范，这些规范文档覆盖了对厂商开发生命周期和产品生命周期流程的评审，测试实验室的资质认可，以及网络设备的安全评估。GSMA 还定义了争议解决流程并且对整个计划进行管理。

3GPP 负责定义 SCAS，对于那些实现了一个或多个 3GPP 网络功能的网络产品，3GPP 定义了相关的安全需求和测试用例，这就是所谓的安全保证规范（SCAS：Security Assurance Specification）。

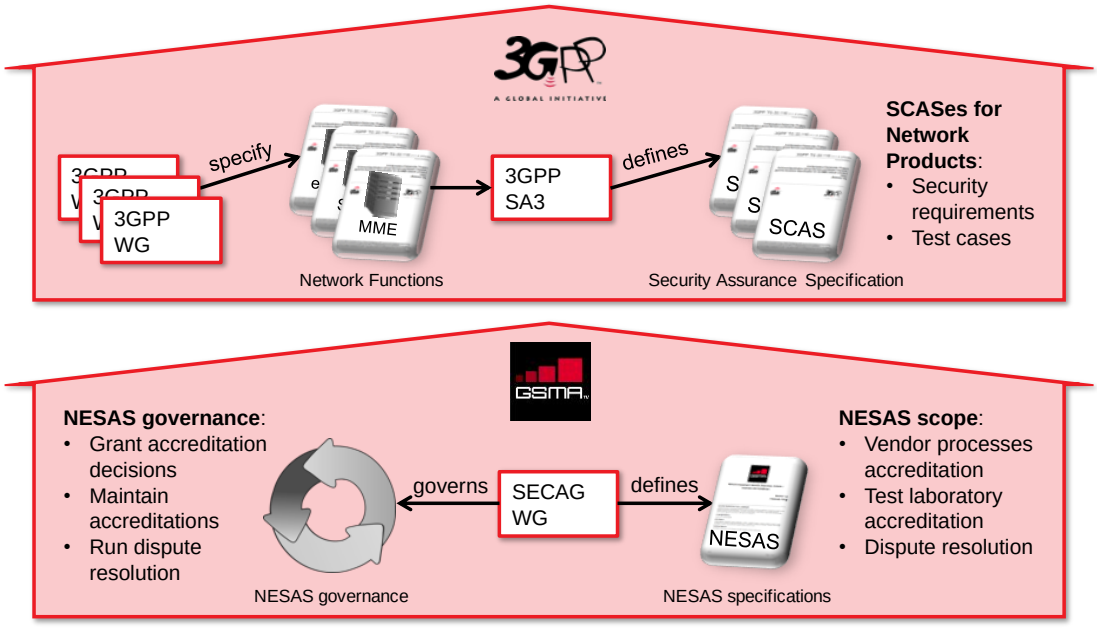

图 2　NESAS 中 3GPP 和 GSMA 的角色

4 NESAS 评估认证流程

NESAS 评估过程中有两个审核工作角色，一个是独立审核小组（IAT：Independent Audit Teams）主要负责针对流程审核，另一个是 NESAS 安全测试实验室，主要负责网络设备的安全测试。

设备厂商在 GSMA 指定的独立审核小组（IAT）中选择一个去做 NESAS 审核。审核结果会正式记录在审核报告文档中。根据 IAT 提供的审核报告中的推荐意见，GSMA 将授予设备厂商通过认证的认可。设备厂商搭建网络产品（如基站），并提交给 NESAS 安全测试实验室去做安全评估。NESAS 安全测试实验室需要由 ISO/IEC 17025 认可机构来确定该测试实验室是否有能力执行 SCAS 中描述的网络产品相关测试。NESAS 安全测试实验室根据相关的 SCAS 来评估网络产品，并验证认可的厂商开发流程已应用于被测的网络产品中。审核报告中提供了必要的信息用于验证开发流程。之后，测试实验室将产生一个评估结果报告。然后，网络产品与评估报告即可被发送到移动网络运营商客户。

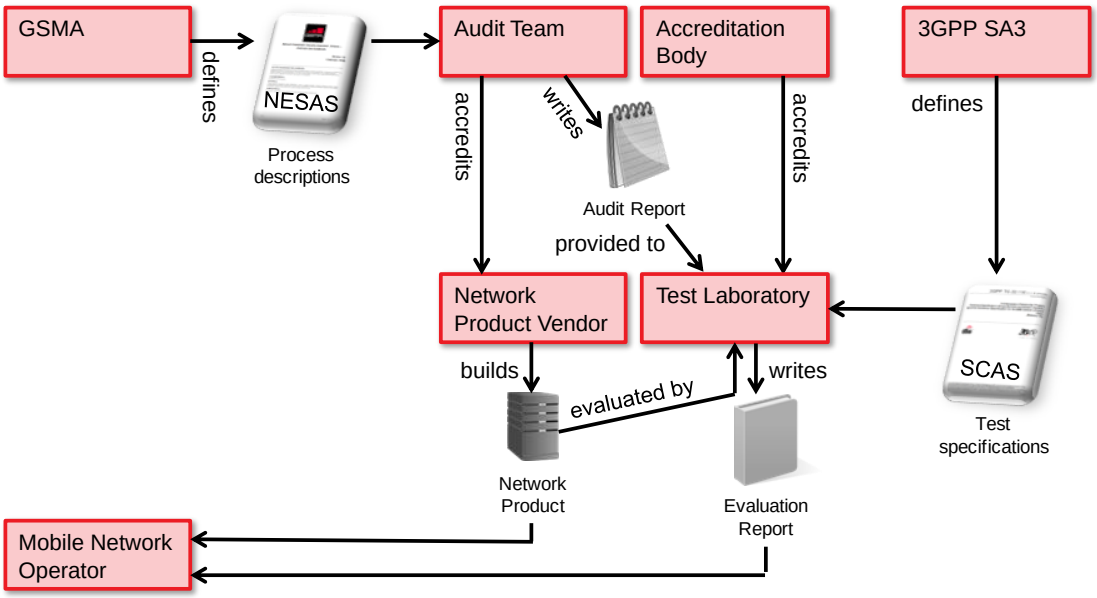

图 3　NESAS 总体流程图

下面将介绍厂商流程的资质认证和 NESAS 安全测试实验室的资质认证：

4.1 厂商流程的资质认证

对于网络产品的开发生命周期和网络产品生命周期，设备厂商需要自己来定义他们的流程。这些流程也需要定义安全性是如何融合进了生命周期的所有阶段。GSMA 指派的独立审核小组（IAT）中的某个小组对这些流程进行审核，并提交一个建议议案给 NESAS 认证委员会。NESAS 认证委员会将根据审核报告中的建议议案来确认和正式确定认证状态。NESAS 描述了如何执行认证，以及由厂商定义的过程要满足哪些要求。在 NESAS 认证委员会的提议下，GSMA 制定了具体的标准来选择和任命“独立审计小组”，以便于根据 NESAS“通用审计”的要求对网络供应商的通用流程进行审核。每三年会根据“公开招标”的结果来做出任命。

厂商流程的资质认证包括非现场流程文件审查和现场审核。最初的任命将由两家审计服务提供商组成，为厂商提供选择。根据通用审计的等级要求，审计服务提供商的数量可能会增加。审计服务提供商数量的增加也需要符合上文所述的“公开招标程序”。

为了确保各个独立审计小组的审计方法的一致性：

（i） 审计服务提供商提供的条款应该基本上与 GSMA 和认证委员会所定义的标准条款相同；

（ii） 合同关系是厂商与独立审核小组双方之间；

（iii） GSMA 应合理规范化与独立审计小组相关的审计方法和文件；

（iv） GSMA 应制定机制，以便独立审计小组之间进行比较；

（v） 认证委员会应全面负责审计质量控制。

厂商定义的流程需要确保网络产品达到所需的安全级别，这些安全要求被定义，网络产品的设计和实施必须以可理解的方式遵循这些安全要求。这正是独立审计小组在审计过程中需要重点核实的内容。独立审计小组编制一份包含审计结果的审计报告。根据审计报告及其建议提案，GSMA 可以授予认证。

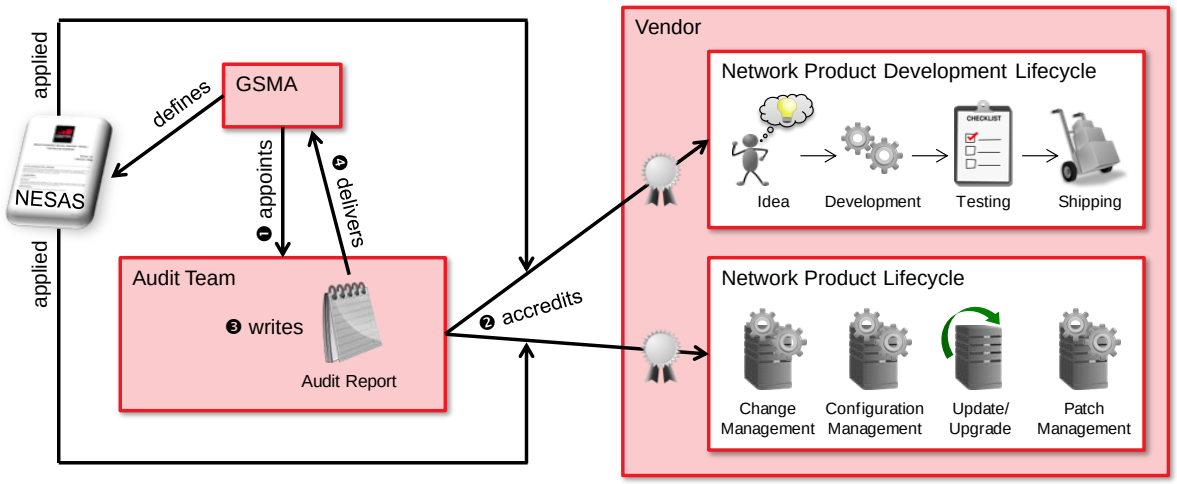

图 4 厂商流程的资质认证

参考信息

- “Network Equipment Security Assurance Scheme – Vendor Development and Product Lifecycle Requirements and Accreditation Process”定义了厂商流程认证要求和执行认证的流程。
- “Network Equipment Security Assurance Scheme – Request for Information”定义了厂商流程认证中，如何选择审计小组的标准和流程。

4.2 NESAS 安全测试实验室的资质认证

NESAS 安全测试实验室可以由厂商自己拥有，也可以是外部独立的第三方。无论何种情况，他们都需要按照 ISO/IEC 17025 的要求进行资质认证，认证的内容包括测试程序、文件体系、流程的维护和评审、能力、独立性和公正性。

由于 ISO/IEC 17025 是一个通用的认证机制，而测试实验室的资质认证总是会涉及到某个测试领域的一些附加的标准作为认证标准的一部分。对于 NESAS 来说，这意味着 NESAS 安全测试实验室需要在 ISO/IEC 17025 认证中证明他们能够执行 NESAS 和 SCAS 中描述的测试，并且符合适用于 NESAS 的附加要求。

应测试实验室的要求，官方认可的 ISO/IEC 17025 认证机构对测试实验室进行审核。如图 6 所示，对测试实验室进行 NESAS 和 SCAS 的场景下的 ISO/IEC 17025 审核。主题专家与 ISO/IEC 17025 认可机构合作执行审核，因为主题专家可以将网络设备安全领域所需的专业知识带到审核中。一旦审核成功完成，所有要求都得到满足，测试实验室将成为经过认证的 NESAS 安全测试实验室。

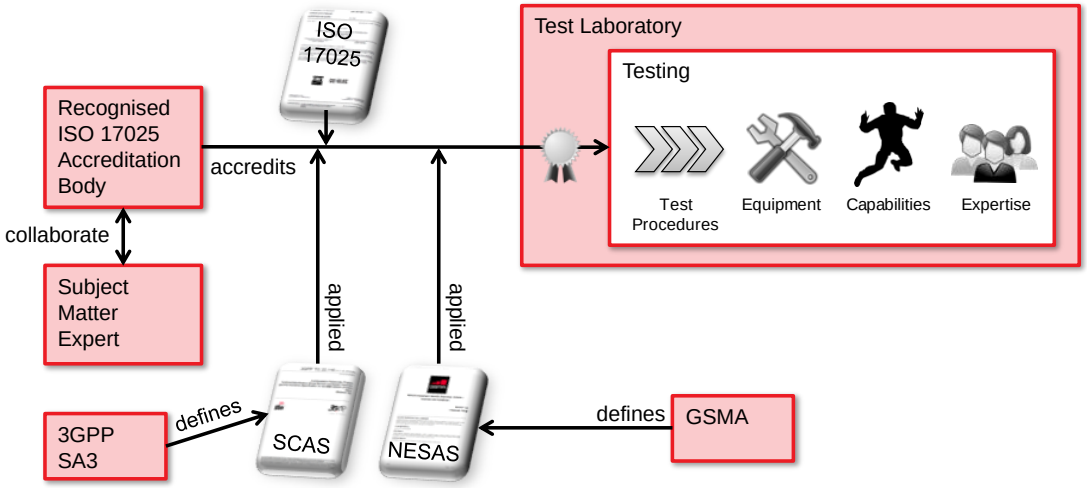

图 5　NESAS 安全测试实验室的资质认证

参考信息

- “ Network Equipment Security Assurance Scheme – Security Test Laboratory Accreditation Requirements and Process”定义了测试实验室资质认证的要求和执行资质认证的流程。
- NESAS 安全测试实验室必须有能力执行 3GPP 的 SCAS 中包含的测试规范。（3GPP TS 33.117 Catalogue of General Security Assurance Requirements 和 3GPP TS 33.116 Security Assurance Specification for the MME network product class）
- 在 3GPP 规范 TR 33.916（Security Assurance Methodology for 3GPP network products）中描述了如何创建和维护 SCAS 的方法论。

4.3 网络产品评估流程

在设备厂商和 NESAS 安全测试实验室都已经完成认证后，网络设备产品可以被执行评估。

网络产品由设备厂商生产后，提供给 NESAS 安全测试实验室。该 NESAS 安全测试实验室从相应的 SCAS 中找出需要的测试规范，并从中得出详细的测试案例来进行网络产品测试。所有测试的结果将记录在评估报告中。

此外，设备厂商创建了所谓的证据，其中需要包含一个原理阐述，NESAS 安全测试实验室通过这个原理阐述可以评估和理解厂商是否在建设网络产品时，按照已经通过认证的内部流程来生产该网络产品的。

在设备厂商的资质认证过程中产生的审计报告，会指导 NESAS 安全测试实验室如何评估证据。证据评估的结果将被添加到评估报告中。证据评估把网络产品和已认证的厂商流程联系了起来，这也是为什么包含了两个结果（来自于网络产品的评估结果和来自于证据评估的结果）的评估报告对 MNO（移动网络运营商）有着重要的意义。

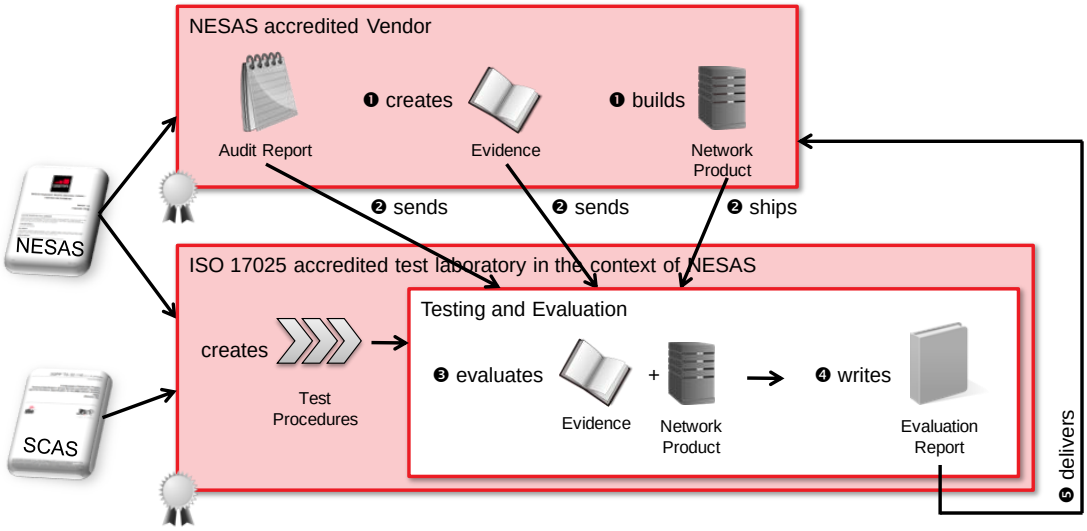

图 6　网络产品的评估流程

完成后的评估报告会被移交给设备厂商，设备厂商可以在供货时，把网络产品连同这个评估报告一起提交给任何相关的 MNO。

最终，MNO 会决定评估报告中网络产品达到的安全等级是否充分满足移动网络部署的要求。评估报告中的信息，使得 MNO 可以衡量和查看该网络产品的安全性和相应的开发生命周期的安全性。

参考信息

- “Network Equipment Security Assurance Scheme – Vendor Development and Product Lifecycle Requirements and Accreditation Process”定义了哪些用于评估的证据是厂商必须提供给 NESAS 安全测试实验室的。
- NESAS 安全测试实验室必须有能力执行 3GPP 的 SCAS 中包含的测试规范。（3GPP TS 33.117 Catalogue of General Security

Assurance Requirements 和 3GPP TS 33.116 Security Assurance Specification for the MME network product class）

- 在 3GPP 规范 TR 33.916（Security Assurance Methodology for 3GPP network products）中描述了如何创建和维护 SCAS 的方法论。

4.4 争议解决

网络设备安全保障方案争议解决委员会（NESAS DRC：Network Equipment Security Assurance Scheme – Dispute Resolution Committee）作为一个公正的解释机构用来处理那些出现在某些情形下的争议，这些情形包括关于审计程序的争议，评估程序的争议和当 NESAS 官方文档中不同部分出现不一致时的争议解释。除上述情况，如果有一个争议涉及到两个或两个以上机构关于审计程序、评估程序或 NESAS 官方文件解释的分歧，必须联系 NESAS DRC 来解决。

这些争议可能发生在两个或两个以上 NESAS 参与者之间（例如网络运营商，设备供应商，测试实验室，以及审计师），关于 NESAS 审计和评估流程和官方 NESAS 文档的争议，NESAS DRC 将针对这个事项公布客观裁决。

该 NESAS DRC 是一个常设委员会，由 NESAS 认可委员会的成员们组成。这个常设委员会必须由多于 6 个 GSMA 会员代表组成，这些 GSMA 会员代表必须是精通 NESAS 所有事务的专家。

该 NESAS DRC 将仅管理以下方面相关的事项：

(i) 审计小组是否遵循了规定的审计程序，是否已经能够从设备厂商处获得所有用于执行审计程序的必要信息；

(ii) NESAS Security Test Laboratory 是否遵循了规定的评估程序，是否已经能够从设备厂商处获得所有用于执行审计程序的必要信息；

(iii) 审计团队和 NESAS 安全测试实验室是否已经正确地解释了 NEAS 文档。

NESAS DRC 不会对审计报告和评估报告的事实，结论和建议做裁定。

在申请 NESAS DRC 裁定前，争议各方应利用一切可能的合理资源去解决争议。所有参与的各方应提前识别争议问题，以便于大家对此争议问题有一个共同的理解。参与争议的所有各方应达成一致的 NESAS DRC 调用的措辞，包括引发争议问题的时间。

所述 NESAS DRC 必须根据“Network Equipment Security Assurance Scheme – Dispute Resolution Process”中描述的争议解决流程进行处理，并且在认为必要的情况下，可以提供附加准则和/或定义进一步的议程。该 NESAS DRC 将采用合理的商业努力寻求尽快解决纷争，不得无故拖延解决纠纷（通常会在通知后的 10 天内）。采用少数服从多数的方法，由 NESAS DRC 成员选出最后的决定。

该 NESAS DRC 裁决/决定对争议的各方具有约束力，该裁决/决定一旦做出， 对当前的争议和未来的此类争议有效。


参考信息

- “Network Equipment Security Assurance Scheme – Dispute Resolution Process”定义了 NESAS 争端解决流程。提出争议的利益相关者需要遵循这个流程。

4.5 NESAS 范围

如上所示，NESAS 的重点专注于网络设备的安全性。该方案解决了行业的需求和挑战，并通过采取以下多层面的方法：

- 厂商的产品开发流程的认证；
- 厂商的产品生命周期过程的认证；
- 对网络设备产品的评估，由具备能力的 NESAS 安全测试实验室执行 3GPP 定义的和标准化的安全测试。

为了使移动产业的各个相关厂商达成一致的认识，请关注以下对 NESAS 范围的重要说明：

- 没有官方认可的授权组织为网络设备颁发通过认证的证书；
- 没有关于网络设备不存在某些功能（例如后门）的证明；
- 该计划不能代替现有的经营者或国家的要求；
- 该计划不包括网络设备之间的接口的安全性；
- 该计划并没有解决端对端的安全需要。

4.6 管理

NESAS 由 SECAG（Security Assurance Group）Doc 005 管理。SECAG Doc 005 与任何其他 NESAS 中的条款有冲突的情况下，以 SECAG Doc 005 为准。

5 NESAS 优势

NESAS 对于移动行业相关者、监管机构和广大用户具有重大价值。

由于有了 NESAS，网络设备所达到的安全保障等级是可测量的、可见的、具有可比性并且是一目了然的。这让移动网络运营商受益颇多，因为它引入了透明度，帮助移动网络运营商确定各个厂商的网络设备是否符合移动网络运营的安全要求。对于厂商来说，它提供了一个平台，以彰显厂商的实现/保持良好的安全标准的能力。

NESAS 推动大部分厂商给出确保产品的开发和维护流程的安全承诺。这对移动网络运营商在选择厂商时是很有益处的，因为它增加了厂商的可信度和移动网络运营商做决定的信心。另一方面，它也在鼓励和促进厂商加强产品的安全性，并且从设计之初就将安全融入到产品之中，在设备厂商界形成一个良好的安全产品文化。

由具备资质认可的测试实验室执行网络设备评估，可以让移动网络运营商在部署设备之前，就能够确定该设备的安全等级。 此外，NESAS 也为厂商，移动网络运营商，相关监管机构和国家主管部门，减少了大量安全性测试的负担，大大提高了效率。

尽管移动网络运营商可以自由地设置自己的个人安全需求，但是 NESAS 可以确保基线安全级别并提供一套通用的适用于所有客户和市场的安全要求。在报价和合同谈判环节，供应商和移动网络运营商针对安全需求可以节省大量工作，不需要再列出大量安全需求，进行逐一讨论。它对于设备厂商的好处更加明显，厂商不再需要为不同的运营商去通过多种安全认证。

有了 NESAS，设备厂商只需要完成这一个审计即可，而不用为不同的运营商和监管者去满足不同的审计要求。从厂商侧，这会大大节省成本、降低开销、提高效率，最终会体现在网络设备的价格降低。

NESAS 启用高效成熟的认证模式，在提高安全水平的同时，保证各个相关厂家的工作量和开销都是在可控范围之内。

6 NESAS 发展现状与展望

2017 年 7 月，有关 NESAS 的概念，流程和文档处于试点测试阶段。在 2017 年，所做的试点工作主要是学习和评估方案在实践中是如何工作的，并解决所有出现的问题，该计划在 2018 年全面启动。

NESAS 被设计为迭代改进。从试点学到的所有经验教训将被反馈到 NESAS 的官方初始版。此后，更新版本将定期发布，并将考虑和采纳来自各利益相关方的反馈。这种方式有利于鼓励利益相关者参与进来，帮助发展该计划以满足他们的需求，同时获得认证的厂商和更安全的网络设备也更加有利于整个移动生态系统。

当前 NESAS 的发展状态和 NESAS 文件的最新版本可以从 GSMA 公司网站的 NESAS 入口获得。https://www.gsma.com/aboutus/leadership/committees-and-groups/working-groups/fraud-security-group/network-equipment-security-assurance-scheme

如果将来认为有必要，NESAS 的范围可以扩展，并且额外的安全要求可以添加到现有的 SCAS 中。通过开发和批准新的相应的 SCAS，可以将新的网络设备类型加进该计划。此外，如果有必要将增加或修改要求来扩展厂商流程认证和测试实验室认证。从本质上说，NESAS 是一个不断自我发展，自我完善的计划，将随着时间不断的演进，2017 年的试点工作标志着该行业重要的第一步。

atsec 从 GSMA NESAS 体系建设的最初便积极参与到相关的技术工作。目前，atsec 作为 GSMA 的试点项目的独立审核小组，已经开展了与大型通信公司的 NESAS 审计合作。atsec 希望长期致力于 NESAS 的发展，并为未来通讯行业的信息安全做出自己的贡献。

7 参考文献

[1] 3GPP TR 33.916 Security Assurance Methodology for 3GPP network products

[2] 3GPP TS 33.116 Security Assurance Specification for the MME network product class

[3] 3GPP TS 33.117 Catalogue of General Security Assurance Requirements

[4] FS.14 Network Equipment Security Assurance Scheme – Security Test Laboratory Accreditation Requirements and Process

[5] FS.15 Network Equipment Security Assurance Scheme – Vendor Development and Product Lifecycle Requirements and Accreditation Process

[6] FS.16 Network Equipment Security Assurance Scheme – Dispute Resolution Process

[7] GSMA NESAS WI 4a Doc Network Equipment Security Assurance Scheme – Request for Information; to be published in April 2016

[8] GSMA NESAS WI 4b Doc Network Equipment Security Assurance Scheme – Request for Proposal; to be published in June 2016

[9] GSMA NESAS WI 5 Doc Network Equipment Security Assurance Scheme – Pilot Proposal

[10] RFC 2119 “Key words for use in RFCs to Indicate Requirement Levels”, S. Bradner, March 1997. Available at http://www.ietf.org/rfc/rfc2119.txt