

国际电信联盟

ITU-T

国际电信联盟
电信标准化部门

X.1254

(09/2012)

X系列：数据网、开放系统通信和安全性
网络空间安全 – 身份管理

实体认证保证框架

ITU-T X.1254 建议书

ITU-T



ITU-T X 系列建议书
数据网、开放系统通信和安全性

公用数据网	X.1-X.199
开放系统互连	X.200-X.299
网间互通	X.300-X.399
报文处理系统	X.400-X.499
号码簿	X.500-X.599
OSI组网和系统概貌	X.600-X.699
OSI管理	X.700-X.799
安全	X.800-X.849
OSI应用	X.850-X.899
开放分布式处理	X.900-X.999
信息和网络安全	
一般安全问题	X.1000-X.1029
网络安全	X.1030-X.1049
安全管理	X.1050-X.1069
生物测定安全	X.1080-X.1099
安全应用和服务	
组播安全	X.1100-X.1109
家庭网络安全	X.1110-X.1119
移动安全	X.1120-X.1139
网页安全	X.1140-X.1149
安全协议	X.1150-X.1159
对等网络安全	X.1160-X.1169
网络身份安全	X.1170-X.1179
IPTV安全	X.1180-X.1199
网络空间安全	
计算网络安全	X.1200-X.1229
反垃圾信息	X.1230-X.1249
身份管理	X.1250-X.1279
安全应用和服务	
应急通信	X.1300-X.1309
泛在传感器网络安全	X.1310-X.1339
网络安全信息交换	
脆弱性/状态信息交换	X.1520-X.1539
事件/事故/探索法信息交换	X.1540-X.1549
政策的交换	X.1550-X.1559
探索法和信息请求	X.1560-X.1569
标识和发现	X.1570-X.1579
确保交换	X.1580-X.1589

欲了解更详细信息，请查阅 ITU-T 建议书目录。

ITU-T X.1254 建议书

实体认证保证框架

摘要

本建议书规定了四个等级的实体认证保证。（i.e., LoA 1 – LoA 4），为实现四个等级的实体认证保证确定了标准和威胁所在，它重点：

- 规定了管理实体认证水平的框架；
- 基于风险评估的结果就须用于缓解认证威胁的控制措施提供指导；
- 为向四个LoA映射其它认证保证方案提供指导；
- 为交换基于四个等级LoA的认证结果提供指导。

沿革

版本	建议书	批准日期	研究组
1.0	ITU-T X.1254	2012-09-07	17

前言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此特大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：<http://www.itu.int/ITU-T/ipr/>。

© 国际电联 2013

版权所有。未经国际电联事先书面许可，不得以任何手段复制本出版物的任何部分。

目录

	页
1 范围	1
2 参考文献	1
3 定义	1
3.1 在其它地方定义的术语	1
3.2 本建议书定义的术语	2
4 缩写词和缩略语	3
5 惯例	4
6 保证等级	4
6.1 保证等级1 (LoA1)	5
6.2 保证等级2 (LoA2)	5
6.3 保证等级3 (LoA3)	6
6.4 保证等级4 (LoA4)	6
6.5 选择适宜的保证等级	6
6.6 LoA的映射和互操作性	7
6.7 根据4个LoA等级交换认证结果	8
7 参与方	9
7.1 实体	9
7.2 证书服务提供方	9
7.3 注册机构	9
7.4 依赖方	9
7.5 验证方	10
7.6 可信任的第三方	10
8 实体认证保证框架的各阶段	10
8.1 注册阶段	10
8.2 证书管理阶段	13
8.3 实体认证阶段	15
9 管理和组织方面考虑	16
9.1 业务建立	16
9.2 法律和合同遵守	16
9.3 财务规定	17
9.4 信息安全管理与审查	17
9.5 外部服务部件	17
9.6 运营基础设施	17
9.7 衡量运营能力	17
10 威胁和控制	18
10.1 注册阶段的威胁和控制	18
10.2 证书管理阶段的威胁和控制	20

	页
10.3 验证阶段的威胁和控制	25
11 服务保证标准	29
附件A – 证书的特性.....	30
附录I – 隐私和PII的保护	31
参考文献.....	33

引言

信息通信技术系统内部或之间的许多电子交易的安全要求，都依赖于对参与实体身份的商定或规定的信任度。这种要求可能包括防止擅自使用资产和资源的措施，为此可能采用接入控制机制和/或通过对相关事件进行审计记录或为核算和计费目的实行问责制。

ITU-T X.1254 建议书提供了实体认证保证框架，其中所说的保证是指对用于确认和管理认证交易所用实体身份的所有程序、管理活动和技术的置信度。

技术		管理和组织	
注册阶段	<ul style="list-style-type: none">• 申请加入• 身份证明和身份信息验证	<ul style="list-style-type: none">• 记录/存档• 注册	<ul style="list-style-type: none">• 服务的建立• 法律和合同合规性• 财务规定
证书管理阶段	<ul style="list-style-type: none">• 证书制作• 证书预处理• 证书的发布• 证书的激活• 证书的存储	<ul style="list-style-type: none">• 证书的中止、撤销和/或销毁• 证书的恢复和/或替换• 备案	<ul style="list-style-type: none">• 信息安全管理 和审计• 外部服务要素• 可用基础设施• 测量运行能力
实体认证阶段	<ul style="list-style-type: none">• 认证• 备案		

X.1254(12)_F01

图 1 – 实体认证保证框架概述

本建议书利用四种规定的保证等级（LoA）提供有关控制技术、程序、管理活动以及保证标准的指导意见，并应为实行上述四种 LoA 而采用这些认证威胁缓解标准。它还为向规定的四个等级映射其它认证保证方案以及交换认证交易结果提供了指导意见。最后，本建议书就保护与认证程序相关的可认证个人信息（PII）提供了指导。

本建议书主要是供关注其业务的 CSP 和其它各方（如这些业务的依赖方、评估方和审计方）使用。这一实体认证保证框架（EAAF）为四个 LoA 确定了最低限度的技术、管理和程序要求，以确保不同 CSP 颁布的证书效力相等。它还提出了对实体认证保证具有影响的某些附加管理和组织考虑，但未就这些考虑规定具体标准。依赖方（RP）和其他各方可能认为本建议书有助于了解各 LoA 提供的内容。此外，也可将它适用于信任框架，为 LoA 确定技术要求。EAAF 旨在用于但不限于采用不同认证技术的基于会话和以文件为中心的使用案例。在法律/双边安排或采用同盟的情况下，直接和代理方案可同时出现。

实体认证保证框架¹

1 范围

本建议书规定了特定情境中管理实体认证保证的框架。它重点：

- 规定了四个等级的实体认证保证；
- 为实现四个等级的实体认证保证确定了标准和指导原则；
- 为向四个LoA映射其它认证保证方案提供指导；
- 为交换基于四个LoA的认证结果提供指导；以及
- 就须用于缓解认证威胁的控制措施提供指导。

2 参考文献

无。

3 定义

3.1 在其它地方定义的术语

本建议书使用了其它地方定义的术语。

3.1.1 主张[b-ITU-T X.1252]：一实体在无附带其有效性证据的情况下做出的声明。

注 – “声称”和“主张”两词通常被认为具有大体相似的含义，但又有细微差别。就本建议书而言，“主张”被认为是较“声称”更为强烈的说法。

3.1.2 认证[b-ISO/IEC 18014-2]：为实体身份提供的保证。

3.1.3 认证因素[b-ISO/IEC 19790]：用于认证或确认实体身份的信息和/或程序。

注 – 认证因素可分为四类：

- 实体之所有（如设备签名、护照、具有证书的硬件装置、私钥）；
- 实体掌握的信息（如密码、PIN）；
- 实体之性质（如生物计量特性）；
- 实体的典型工作（如行为模式）。

¹ 韩国表示对此持保留意见且不采用此建议书，因为在实体认证保证所需的四级水平和实现这四级水平的实体认证保证所用标准方面，本建议书与韩国的法规存在冲突。

3.1.4 声称[b-ITU-T X.1252]: 在不提供证据的情况下确认某事务的声明。

注 – “声称”和“主张”两字通常被认为具有大体相似的含义，但又有细微差别。就本建议书而言，“主张”被认为是较“声称”更为强烈的说法。

3.1.5 情境[b-ITU-T X.1252]: 具有实体存在和互动的确定边界条件的环境。

3.1.6 证书[b-ITU-T X.1252]: 证明声称的身份和/或权力的一组数据。

注 – 补充的证书特点见附件I。

3.1.7 实体[b-ITU-T X.1252]: 具有独立和独特存在并可在一定情境中识别的事务。

注 – 就本建议书而言，实体也用于要求得到一身份之物的具体情况。

3.1.8 身份[b-ISO/IEC 24760]: 与实体相关的一系列属性。

注 – 在具体情境中，一个身份可能具有使实体在该情境中得到唯一识别的一个或多个标识符。

3.1.9 多因素认证[b-ISO/IEC 19790]: 通过至少两个独立认证因素进行的认证。

3.1.10 非拒绝[b-ITU-T X.1252]: 防止全部或部分行动参与实体之一拒绝的能力。

3.1.11 拒绝[b-ITU-T X.1252]: 参与全部或部分行动的有关实体之一的拒绝。

3.2 本建议书定义的术语

本建议书定义了如下术语：

3.2.1 认证协议: 在实体和验证方之间确定的序列消息，可供验证方证实实体的身份。

3.2.2 权威来源: 被公认为准确和及时消息来源的数字存储器。

3.2.3 证书服务提供方 (CSP): 发布和/或管理证书的可靠参与方。

3.2.4 实体认证保证 (EAA): 在证实实体符合其身份和对它的期望的认证过程中达到的信任度。（本定义是基于[b-ITU-T X.1252]中对‘认证保证’的定义）

注 – 信任是以实体和所称身份之间的绑定达到的信任度为依据的。

3.2.5 标识符: 用来在具体情境中以独特方式描述其特征的一个或多个属性。

3.2.6 身份信息认证: 对比发布方、数据源或其它涉及真实性、有效性、正确性和实体相关性的其它内外部资源，查验身份证明信息和证书的过程。

3.2.7 身份证明: 注册机构 (RA) 为证实一实体具有规定或认可的保证等级而捕获和确认足够信息的过程。

3.2.8 中间人攻击: 攻击者在双方不知情的情况下通过阅读、插入和修改双方消息发起的攻击。

- 3.2.9 相互认证：**向两个实体提供对方身份担保的实体身份认证。
- 3.2.10 钓鱼：**诱骗电子邮件用户披露个人或保密信息供诈骗者非法使用的一种欺诈行为。
- 3.2.11 注册机构（RA）：**向证书服务提供方（CSP）确认和/或担保实体身份的可信任的参与方。
- 3.2.12 依赖方（RP）：**依赖于身份主张和声称的参与方。
- 3.2.13 盐（salt）：**散列程序使用的非保密但通常随机的数值。
注 – 它亦称为沙。
- 3.2.14 共享秘密：**认证使用的只为实体和验证方所知的秘密。
- 3.2.15 时戳：**代表与共同参考相关的时间点的可靠时间变量参数。
- 3.2.16 交易：**实体和业务提供方之间支持业务或计划用途的离散事件。
- 3.2.17 信任框架：**供交换身份信息各方使用的一系列要求和执行机制。
- 3.2.18 可信赖第三方（TTP）：**就安全相关行动可为其他参与方所信任的机构或其代理（例如，与安全相关的活动）。
注 – 可信赖第三方在认证过程中受到实体和/或验证方的信任。
- 3.2.19 有效期：**身份或证书可用于一项或多项交易的时间段。
- 3.2.20 认证过程：**通过将提供的信息与过去确证的信息进行比较的信息检验过程。
- 3.2.21 验证方：**验证身份信息的参与方。
注 – 验证方可参加EAAF的多个阶段并能够执行证书认证和/或身份信息认证。

4 缩写词和缩略语

本建议书采用了如下缩写词和缩略语：

CA	认证机构
CSP	证书服务提供方
EAA	实体认证保证
EAAF	实体认证保证框架
ICT	信息通信技术
IdM	身份管理
IP	互联网协议
LoA	保护等级
LoAs	（多个）保护等级
MAC	媒体接入控制
NPE	非法人实体

PDA 个人数字助理
PII 可确认的个人信息
PIN 个人识别码
RA 注册机构
RP 依赖方
SAML 安全断言标记语言
TCP/IP 传输控制协议/互联网协议
TLS 传输层安全
TPM 可信平台模块
TTP 可信第三方
URL 统一资源定位器

5 惯例

本建议书适用于以下描述方式表达的规定：

- a) “Shall” 表示要求；
- b) “Should” 表示建议；
- c) “May” 表示允许；
- d) “Can” 表示可能性和能力。

6 保证等级

这个实体认证保证框架（EAAF）为实体认证确认了四个保证等级（LoA）。每个 LoA 描述了对直至和包括认证程序本身的程序的置信度，从而保证使用一具体身份的实体实际是被赋予该身份的实体。就本建议书而言，LoA 是过程和技术控制措施的函数，而证书服务提供方（CSP）根据第 10 款规定的标准对每个 EAAF 阶段实施了技术控制措施。实体认证保证（EAA）受到管理和组织考虑的影响，但本建议书没有为这些考虑提供明确的规范性标准。实体可以是人或非法人实体（NPE）。

例如，一个网络的 LoA 可以是所有网络组成部分的函数，并包括 NPE 或可模仿实体的端点装置（如移动电话、PDA、机顶盒、笔记本电脑）。有些情况下，端点设备可模仿合法实体。因此，以一定的可信度区分可信与欺诈设备是 EAA 的根本。

LoA1 为最低等级的保证，而 LoA4 则是最高等级的保证。确定一特定情况下的适用 LoA 取决于多种因素。确定必要的 LoA 主要以下述风险为依据：认证错误和/或证书的错误使用产生的后果，由此产生的损坏和影响及其出现的可能性。较高的 LoA 应用于较高的认知风险。

EAAF 为四个 LoA 当中的每一等级提供了要求和实施指导，重点为执行以下阶段的程序提出了要求：

- a) 注册（如身份证明、身份信息验证、登记）；

- b) 证书管理（如证书颁发、证书激活）；
- c) 认证。

它还为影响实体认证保证的管理和组织方面的考虑（如法律合规性、信息安全管理）提供了指导。

定义的 LoA 见表 6-1。

表 6-1 – 保证等级²

等级	说明
1 – 低	对主张或声称的身份不甚或没有信任
2 – 中	对主张或声称的身份部分信任
3 – 高	对主张或声称的身份高度信任
4 – 极高	对主张或声称的身份极度信任

本框架包括为各实体认证保证框架阶段取得所需 LoA 的要求。利用此框架达到的 LoA 将是最低的 LoA 阶段等级。

6.1 保证等级1 (LoA1)

在 LoA1 一级，对主张或声称的实体身份仅有最低限度的信任，但对于该实体为连续认证事件中的同一实体表示部分信任。这一 LoA 被用于认证错误相关风险最低的情况。未对采用的认证机制提出具体要求；只要求它提供某种最低限度的保证。包括与较高 LoA 相关的证书在内的广泛现有技术，可以满足对这一 LoA 的认证要求。此级别无需使用加密方法（例如，基于加密的挑战应答协议）。

例如，LoA1 可能适用的认证情况是，一实体为创建客户化网页向商业网络提供了自行注册的用户名或密码，或参与了需为利用新闻或产品记录等资料和记录材料而登记网址的交易。

例如，LoA1 一级的媒体接入控制（MAC）地址可满足一项设备认证要求。但无法有把握地禁止另一设备使用同一个 MAC 地址。

6.2 保证等级2 (LoA2)

在 LoA2 一级，对主张或声称的实体身份有了部分信任。这一 LoA 适用于中等认证错误相关风险，并可以接受单因素认证。成功认证将取决于实体通过安全认证协议证明它对证书具有控制。应利用控制手段降低窃听者和在线猜测攻击的有效性，并采取控制手段防范对存储证书的攻击。

例如，服务提供商可能运行令其客户能够更改其记录地址的网站。受益人可更改其记录的交易，可被视为 LoA2 认证交易。此项交易涉及造成不便的中等风险。由于有关支付数额、账户状态和更改记录的正式通知被发送到受益人的记录地址，此项交易又增加了擅自发布 PII 的中等风险。因此，服务提供商应至少先得到某种认证保证，再允许开展这一交易。

² LoA是过程、管理活动和技术控制措施的函数，而CSP根据第10款规定的标准对每个EAAF阶段实施了技术控制措施。

6.3 保证等级3 (LoA3)

在 LoA3 一级，对主张或声称的实体身份具有高度信任。这一 LoA 适用于与错误认证相关的较高风险，并应采用多因素认证。在认证协议中交换的所有保密信息都应在交换和休息过程中予以加密保护（尽管 LoA3 不需要基于加密的挑战应答协议）。对证书的生成或存储没有提出要求；可在通用计算机或专用硬件上存储或生成。

例如，专利律师以电子方式向专利和商标局提交证书的交易可能需要 LoA3 认证交易。不当的披露可能带来巨大的财务损失风险。其它 LoA3 交易实例包括允许实体实施某些金融交易的在线接入账户，或第三方合同商利用远程系统访问潜在敏感性的客户个人信息。

6.4 保证等级4 (LoA4)

在 LoA4 一级，对主张或声称的实体身份极度信任，这一 LoA 适用于与认证错误相关的高风险。LoA4 提供了本建议书的最高等级的实体认证保证。LoA4 与 LoA3 相似，但它增加了针对人员实体的个人身份证明和利用防篡改硬件装置存储所有秘密或私人加密密钥的要求。此外，认证协议中的所有 PII 和其它敏感数据都应在交换和休息过程中受到加密保护。

例如，在认证失败情况下，其使用可能存在很高风险或极有可能出现灾害的业务，可能 LoA4 的保护。责任方需完全确保相应实体可提供关键信息，如果责任方未能确认相关信息，其甚至可能会承担刑事责任。最后，批准可能造成高风险财务损失的交易，可能也是 LoA4 等级的交易。

在 LoA4 一级，数字证书（如 ITU-T X.509、卡校验（CV）证书）可能被用于 NPE 的认证，其中包括笔记本电脑、移动电话、打印机、传真机和其它连网设备。例如，智能电话的注册程序可能需要将数字证书嵌入智能电话。此外，为了防止未经授权的电网使用，可在智能仪表技术的部署工作中采用数字证书。

6.5 选择适宜的保证等级

选择适用 LoA 的依据是对实体接受认证后开展的交易或业务所作的风险评估。通过向 LoA 映射影响等级，所有认证交易参与方都可以确定他们所需的 LoA，购置服务并相应地依靠有保证的身份。表 6-2 说明了各认证等级的认证失败可能带来的后果和影响。

表 6-2 – 各保证等级的潜在影响

认证失败可能造成的后果	按保证等级划分的潜在认证失败影响			
	1	2	3	4
造成不便、危险或有损于地位或名声	最低*	中等	较高	极高
财务损失或机构赔偿责任	最低	中等	较高	极高
有损于组织、其计划或公共利益	未提供	最低	中等	极高
擅自发布敏感信息	未提供	中等	较高	极高
个人安全	未提供	未提供	最低 中等	较高 极高
民事或刑事违法行为	未提供	最低	较高	极高
* Min=最低; Mod=中等; Sub=较高; High=极高				

对形成最低、中等、较高和极高风险的认定，取决于机构利用本建议书为每种可能的后果确定的风险标准。此外，可能存在多种影响情况（例如，后果可能包括对机构造成的伤害，以及擅自披露敏感信息）。在多种影响情况下，应使用与后果相对应的最高等级 LoA。

每个 LoA 都取决于 CSP 在各 EAAF 阶段对其业务提供采用的控制措施与程序的力度和严格性。EAAF 确定有必要在每个 LoA 等级为 CSP 制定运行服务保证标准。第 11 款这一标准作了介绍，但具体要求超出了本建议书的范围。

在利用风险评估结果确定可行的 LoA 时，或许还需要考虑到安全范围以外的其它业务相关因素。其中可能包括：

- a) 机构的残余风险管理方法；
- b) 机构在表6-2显示的影响方面的风险偏好；
- c) 为服务确定的商业目标（如机构拥有缓解诈骗行为的程序并能够泰然接收诈骗风险，采用以密码为证书的较低LoA可能更有利于旨在提高采用率的服务）。

交易的风险评估可以作为机构总体信息安全风险评估（如 ISO/IEC 27001）的一部分，并应着重考虑到进行交易的具体安全需求。风险评估应解决与 EAA 相关的风险。应将风险评估的结果与四个 LoA 等级相比较，并选择最能满足风险评估要求的 LoA。

当预计存在多个交易等级时，可对每项交易或交易组使用不同的 LoA。换言之，单一机构可根据涉及的具体交易采用多个 LoA。

6.6 LoA的映射和互操作性

不同域可产生不同的 LoA 定义。这些 LoA 不一定支持本框架涉及的四级 LoA 的一对一映射。例如，一个域可能采用 4 级模式，而其它域则采用 5 级模式。必须分别定义并广泛通报不同认证模式采用的不同标准。

为实现不同 LoA 模式的互操作性，每个域都须通过以下方法说明其映射方案是怎样与本建议书定义的 LoA 相关联的：

- a) 制定一个定义清晰的实体认证保证方法，其中包括妥善定义的LoA类别；以及
- b) 广泛公布这一方式，使那些希望与它们达成综合类型协议的机构能够明确了解相互采用的程序和术语。

LoA 方式应从风险评估角度考虑和明确定义 LoA，而风险评估则在以下方面进行了说明和量化：

- a) 预计的威胁；
- b) 倘若威胁真的来临，其影响（如min、mod）；
- c) 确定必须在各LoA控制的威胁；
- d) 就为在各LoA实行控制措施采用的安全技术和程序提出建议，例如对硬件所附证书（如智能卡）作出详细说明或明确证书生成和存储的要求；
- e) 确定不同认证因素组合等值的标准，同时考虑到身份证明和相关证书。

解决不同 LoA 模式之间映射/桥接的方式之一或许是利用本文件定义的四级模式，并向它映射 n 等级的其它模式。这一方法可以利用不同认证保证模式实现身份综合，并映射到四级模式。映射将确定怎样处理未经映射的 LoA，既可以完全忽略它们，也可将它们有效地映射到下一个最低等级（因为如果未事先予以具体确定，就没有采用较高 LoA 的依据）。

6.7 根据4个LoA等级交换认证结果

参与认证交易的各方（如 CSP、RP）可能需要为完成交易或活动交换信息。

采取的各种行动包括但不限于以下几种：

- a) 允许RP表明它希望实体实现认证的LoA；
- b) 使实体或CSP能够在回复中说明实际的LoA；
- c) 使实体或CSP公布被证明能够满足该LoA相关要求的那些LoA。

认证参与方应就交换信息的协议、语义学、格式和机构达成一致。RP 可能需要指明是否接具体请求以外的其它认证响应。

虽然数字证书是传递证书相关保证信息的既定方式，元数据正在越来越多地被用作通报交换方保证要求的方式。例如以统一资源定位器（URI）形式出现的‘安全主张标记语言’（SAML）认证‘情境类别’，是各方表达有关认证要求和主张的认证保证等级的著名机制。例如，一身份提供方提出的典型主张可传达的信息包括“此用户是 John Doe，其电子邮件地址为 john.doe@example.com，他通过认证并利用密码机制进入此系统。”

本框架的其余部分论及了确定服务程序和需求的结构，以及与身份认证相关的威胁和影响。它在结尾部分对照可能评估的服务对服务保证标准进行了综述，以确保为实现充分的证书服务而分配适用的 LoA。

7 参与方

EAAF 的参与方包括 CSP、RA、RP、验证方和 TTP。他们既可能属于单一机构，也可能属于不同机构。一系列机构可能提供不同类型的关系和能力，包括共用或互动组件、系统和服务。

7.1 实体

实体可使其身份得到认证。认证实体的能力取决于多种因素。根据本框架的上下文，实体认证能力意味着该实体已经注册，得到了 CSP 颁发的相应证书，并确定了认证协议。在认证过程中，该实体可自行证明其身份，也可由他方作为其代表进行认证。

7.2 证书服务提供方

证书服务提供方（CSP）负责颁发和/或管理证书、硬软件以及可用于制作证书的相关数据。密码和生物计量特性均为 CSP 可能颁发和管理证书的实例。而具有私钥的智能卡，则是 CSP 可能颁发和管理的硬件及（可用于证书制作的）相关数据。CSP 也可能发布和管理可用于认证证书的数据。如果密码被用作证书，这一数据可能是密码单向功能的等值物。如果证书是基于数字签名的信息，CSP 可能形成能为验证方所用的公共密钥证明。CSP 发布和支持的证书以及实行的保护手段，是确定在一具体认证交易（亦见第 10.3 款）期间达到哪一级 LoA 的关键因素。

每一实体都会发布一份或多份证书或证书制作手段，以便在晚些时候进行认证。通常只有在实体注册后期的注册程序成功完成后，才能发布证书或证书制作手段。

7.3 注册机构

注册机构（RA）向一 CSP 确定和/或验证并担保一实体的身份。RA 应获得 CSP 的信任才能履行与注册阶段相关的程序，并以能够使 CSP 随后分配证书的方式进行实体注册。

每个 RA 都需根据规定的程序开展某种形式的身份证明和身份验证。为将一实体同其它实体区分开来，通常要向该实体分配一个或多个标识符，使该实体能够在随后适用的情境下得到识别。

7.4 依赖方

依赖方（RP）最初依赖于身份主张或要求，并可能需要多种用途的认证身份，如账户管理、接入控制、授权决定等。依赖方可自行从事实体认证工作，也可将这项工作委托第三方。

7.5 验证方

验证方是负责验证身份信息的一方。验证方可参加 EAA 的多个阶段，执行证书验证和/或身份信息认证。

7.6 可信任的第三方

可信任的第三方（TTP）是在与某些活动中得到其它参与方信赖的机构或其代理（例如，与安全相关的活动）。就本框架而言，实体和/或验证方信任 TTP 的验证工作。负责实体验证的 TTP 的实例包括认证机构（CA）和时戳机构。

8 实体认证保证框架的各阶段

此条款提供了 EAA 的阶段和程序模式。虽然某些 EAA 模式可能不同于本模式的结构，符合本模式需要完全达到本框架规定的要求的功能。本框架具有技术中立性。

采用此框架的机构制定的政策、程序和能力，可提供必要的支持程序并达到本框架规定的要求。这些因素会随具体机构选择的作用而有所不同，机构提供证书的 LoA 便是一个例子。例如，机构可能需要遵循：

- a) 代表与具体LoA相关的机构或其代理采取具体行动的要求；
- b) 外部或第三方在EAAF范围内评估一机构的运作能力的要求；
- c) 对采用这一框架的机构提供的程序、服务和能力建立信任所需的政策、行动和能力。

8.1 注册阶段

注册阶段包括四个程序：申请加入、身份证明、身份验证及存档/记录。这些程序可完全由单一机构执行，也可能包括一系列机构提供的多种关系和能力，包括共用或互动组件、系统和服务。

必要程序可能视适用的 LoA 所需的严格程度而有所不同。当一实体在 LoA1 一级注册时，这些程序应为最低限度程序（如个人可点击网页的“新用户”按键，以创建用户名和密码）。在其它情况下，注册程序可能比较繁冗。例如，LoA4 等级的注册需要实体和 RA 的当面会晤和广泛的身份证明。

8.1.1 申请加入

注册阶段可以多种方式启动。例如，它可根据试图亲自获得具体证书（如一个新的网站用户希望获得用户名和密码）的实体提出的要求启动。代表实体的第三方或 CSP 自身（如政府颁发的身份卡、雇员胸牌）也同样可以启动注册程序。例如，只有在实体获得第三方赞助的情况下才会受理较高等级的 LoA 申请。

在任何情况下，人员注册阶段的启动程序都会包括填写申请表。这份表格应记录足够信息，以确保在一情境（如通过记录完整名称、出生日期和地点）中对实体进行唯一确认。对于移动装置等 NPE 而言，注册可能需要通过装置内置证书予以启动，这将使装置能够得到唯一识别，并通过加密的配置参数文件接收定制的设备设置。

CSP 将规定提供注册服务和使用注册相关服务的条件。可根据可信任的框架制定注册相关服务条件。实体可酌情在继续注册程序之前接受或由他方代为接受免责声明或其它法律规定。

8.1.2 身份证明和身份信息验证

身份证明是捕获和验证充足信息的过程，以便在规定或商定的保证等级上进行实体认证。身份信息验证是指对比发布方、数据源或其它涉及真实性、有效性、正确性和实体相关性的其它内外部资源，查验身份证明信息和证书的过程。根据情境，由权威机构发布或批准的各种身份信息（如政府的身份卡、驾照、生物计量信息、基于机器的认证、出生证明）可满足身份证明要求。为达到身份证明要求而提供的实际的身份信息会随 LoA 的等级不同而变化。

身份证明可能包括对提交的身份证件的物理检查，以检测可能的欺诈、篡改或伪造行为。身份证明还可能包括确保身份可用于其它情境（如得到其它 RA 验证）的检查。LoA 等级越高，身份证明要求就要越加严格。此外，对远程身份的主张和声称（如通过在线渠道）的身份证明程序，应比当地的身份主张或要求（如亲自会晤 RA）更为严格。

身份证明要求的严格性，是以必须为每一个 LoA 等级达到的目标为依据。在 LoA1 等级，唯一的目标是确保身份是预期情境中的唯一。该身份不应同时与两个不同实体相关。而在 LoA2 等级上需要达到两个目标。首先该身份应是该情境中的唯一。其次，与身份相关的实体应为客观存在，这意味着该身份不应是为诈骗目的虚构或有意伪造的。³例如，LoA2 的人员身份证明可能包括对出生和死亡等级的检查，以便在一定程度上保证确有出处（虽然它不能证明拥有出生证明的实体就是出生证明涉及的实体）。与之相似，LoA2 等级的 NPE 身份证明可能包括利用序列号码溯查制造商的工作。

LoA3 包括 LoA1 和 LoA2 的目标，也可以达到通过外部数据库等一个或多个权威来源验证身份信息的目的。身份信息验证可显示在用身份及其与实体的联系。然而，这并不能保证身份信息处于身份拥有者的实际或合法的掌握之中。对人员而言，LoA4 给 LoA3 附加的一项目标是，为防止假冒而要求亲眼看到该实体。

更高等级的 LoA 身份证明程序应囊括较低等级的 LoA 程序。例如，LoA3 身份证明作出的假设是，LoA1 和 LoA2 身份证明的检验结果合格。

³ 这并不排除使用假名。

表8-1 – 将身份证明目标用于LoA

LoA	说明	目标	控制措施	处理方法 ⁴
LoA1 – 低	对主张或声称的身份不甚或没有信任	使身份成为情境中的唯一	自我主张或声称	本地或远程
LoA2 – 中	对主张或声称的身份部分信任	身份是情境中的唯一，而且身份所属实体客观存在	通过使用权威来源提供的身份信息证明身份	本地或远程
LoA3 – 高	对主张或声称的身份高度信任	使身份成为情境中的唯一，身份所属实体客观存在，身份得到验证并用于其它情境	通过使用权威来源提供的身份信息进行身份证明和验证	本地或远程
LoA4 – 极高	对主张或声称的身份极为信任	使身份成为情境中的唯一，身份所属实体客观存在，身份得到验证并用于其它情境	通过利用多个权威来源提供的身份信息进行身份证明+身份信息验证+亲临现场 ⁵	仅限本地

应利用第 10.1.2 款列出的管控措施确定保护注册免受威胁所需使用的 LOA 控制手段。

EAAF 的落实工作完全依赖于供预期的实体和/或 RA（一个子集的）使用的身份信息和来源。

这些证书、身份信息和来源的可靠性和准确性，决定了注册阶段提供的实际保证。因此，EAAF 的实施方应在决定依靠哪些证书、身份信息和/或来源进行身份证明和验证时，审慎考虑不同来源和发布方使用的身份（管理）基础设施提供的保证。EAAF 的所有实施工作都包括文件的发布（如第 10.1.2.1 提及的身份证明政策），该文件概述了支持注册阶段所依靠的身份信息、来源和/或发布方。

⁴ 远程身份证明是通过网络完成的，因而无法实际看到实体，而本地身份证明则是以要求实际看到实体的方式完成的。

⁵ 目睹本人的管控措施仅适用于人员实体。

8.1.3 备案 – 记录

这是实体完成注册的程序，即生成注册记录的注册阶段的备案程序。这项记录应包括采集的（和可能得到保留的）信息和记录、身份验证程序信息、这些措施的结果及其它相关数据。随后对是否接受、拒绝或将注册提交进一步审议或其它后续工作做出决定并记录在案。

8.1.4 登记

登记是实体申请使用服务或资源的程序。虽然登记程序通常被认为是注册程序的一部分，因为它处于注册程序的末尾，而且可能在晚些时候履行。与其它可能只需一次的注册程序不同，登记是实体申请首次使用每项服务或资源都必须履行的程序。

8.2 证书管理阶段

证书管理阶段包括与用户得以参与活动或情境的证书或证书全周期管理相关的所有程序。证书管理阶段可能涉及以下部分或全部程序：证书的初建、证书或证书制作手段的发布、证书或证书制作手段的激活、证书的存储、证书或证书制作手段的撤销和/或销毁、证书或证书制作手段的恢复和/或替换和备案。其中的一些程序取决于证书是否由硬件设备承载。

8.2.1 证书的初建

证书初建程序包括首次创建证书或证书制作手段所需的所有程序，其中可能包括预处理、初始化和绑定程序。

8.2.1.1 证书的预处理

某些证书或证书制作手段须经预处理才能发布，例如证书需要根据实体身份量身定制的个性化预处理。个性化视证书的不同而呈现不同形式。例如，拥有证书的智能卡的个性化可能包括未来持卡实体的打印（在卡外侧）或书写（在卡的芯片上）名称。密码一类证书无需个性化处理。

8.2.1.2 证书初始化

证书初始化包括确保证书制作手段能够随后支持它计划支持的功能的所有措施。例如，智能卡芯片计算出随后支持生成数字签名所需的加密密钥对。此外，智能卡可能以“锁定”状态发行，并需要在初始化程序期间使用 PIN。

8.2.1.3 证书绑定

绑定是在证书、证书制作手段和其发放实体之间建立联系的程序。完成绑定的方式和对绑定关系的信任度会随 LoA 的不同而有差异。例如，在将一实体的持续假名标识符与实体的客户记录进行绑定的在线情况下，首次“激活码”可能是经安全信道内的仅限会议的加密标签（cookie）载过绑定程序的。此外，在这一程序的末尾，一俟实体至持续标识符绑定步骤完成，可能需要为持续标识符与客户记录的绑定发出激活码提示。

8.2.2 证书的颁发

证书的颁发是向实体提供具体证书或证书制作手段或将实体与具体证书或证书制作手段相结合的程序。此程序的复杂度会随 LoA 的要求而变化。对较高的 LoA 而言，这可能包括亲自递送拥有证书的硬件设备（如智能卡）；在 LoA 较低的情况下，该颁发程序可以简单到向实体的物理或电子邮件地址发送密码或 PIN。

对于设备等 NPE 而言，每当设备制造商针对每份数字证书向证书服务提供方（CSP）提供唯一的设备识别号码表而大量预定数字证书时，通常是启动较高 LoA 颁发程序的时间。CSP 的反映是以加密格式向制造商提供证明和私钥。在制作过程中，制造商可能在每台设备中嵌入生成唯一设备标识符的数字证书。

8.2.3 证书激活

证书激活是证书或证书制作手段做好投入使用准备的程序。激活程序可视证书的情况包括多种措施。例如，为防止临时错误使用，证书或证书制作手段在初始化到向实体颁发之间可能处于“锁定”状态。在这种情况下，启动可能涉及证书“解锁”（如利用密码）。证书或证书制作手段也可以在临时中止其有效性的暂停期之后激活。

8.2.4 证书的存储

证书存储是将证书或证书制作手段以防范擅自披露、使用、修改或销毁的方式安全存储的程序。证书存储涉及与证书相关的实体以及防范擅自使用证书所需的行动。

在用于检证书合法性的信息不是证书一部分的情况下，证书存储不一定包括对该信息的保护。较高的 LoA 需要对认证所需的散列密码表等信息加以保护。

8.2.5 证书中止、作废和/或销毁

作废是证书的有效性被永久性终止的过程。中止则是证书的有效性临时停止的相关过程。在许多不同的情况下，作废可能是适当的。作废须出现在以下的情况中：

- a) 已报告某一证书，或生成证书的方法已经丢失、被窃或受到损害；
- b) 证书已过期；
- c) 证书赖以存在的基础已不复存在（如员工已离开其单位）；
- d) 证书被用于未经许可的用途；或
- e) 已发放了另一个证书取代所述证书。

通知需要作废的事件与完成作废过程之间的时限由组织政策决定。在更高的保证等级，允许用于作废的时间通常更短。智能卡上的证书等一些证书可在作废时进行物理的销毁。但是，与证书有关的信息并非总可以销毁。

8.2.6 证书更新和/或更换

更新是延长现有证书有效期的过程。更换则是向某个实体发放新证书、或某种生成证书的方式以替换先前发放的、已作废证书的过程。当 CSP 向实体的电子邮件地址发送临时密码，使得该实体可以在提供临时密码后创建新密码即是更换的一个示例。另一示例为 PIN 解锁码，该码应被视作 PIN 处理。证书更新和更换过程的严格程度根据保证等级的不同而变化。

8.2.7 保存记录

应在证书的整个有效期内保存适当的记录。至少须保存记录以下信息：

- a) 生成证书的事实；
- b) 证书的标识符（适用时）；
- c) 证书发放的对象实体（适用时）；
- d) 证书的状态（适用时）。

须保存证书管理阶段涉及的各（适用）流程的记录。当向人员实体发放证书时，记录保存有可能涉及 PII 的处理。见附件 I。

8.3 实体认证阶段

在实体认证阶段，实体采用其证书向 RP 证实其身份。认证程序仅涉及（是否）信任身份的主张或声称，与依赖方在主张或声称基础上可选择采取的行动无关。

8.3.1 验证

验证程序包括采用协议显示拥有并/或控制证书，以便建立对某个实体的信任。验证协议要求根据可适用 LoA 的不同而变化。例如，对于低级的 LoA，认证可涉及密码的使用。对于更高级的 LoA，认证可能涉及采用基于密码的挑战-应答（challenge-response）协议。更高级的 LoA 需要采用多因素验证。并非所有的验证因素均提供相同的强度，采用多因素来增强确信度。见第 10 节。

8.3.2 保存记录

出于提供服务、合规性、问责和/或法律要求等各种目的，可能需要在验证阶段对事件进行监控并保存记录。

当涉及人类实体时，这些记录中包含的信息可能包括敏感信息。这些记录应按照考虑保护要求和将 PII 最小化的方式进行管理。亦参见附录 I。

9 管理和组织方面考虑

EAA 不仅只来自于技术因素，也与监管、协议合同以及如何管理与组织提供服务方面的考虑有关。一个技术上严密但没有合格管理和运作的解决方案可能在提供 EAA 时在安全性方面充分发挥其潜力。

本节用于提供信息并描述了影响到 EAA 的组织和管理方面的考虑。它并未提供各种 LoA 的具体标准。管理和组织方面考虑的具体标准和合规性评估并不属于本建议书的范围，而应在信任框架中提供。

9.1 业务建立

业务建立涉及业务提供商的法律地位以及功能性业务提供的地位问题。例如，知道身份管理和认证服务的提供商是经过注册的法律实体，使人确信 CSP 是在其运营的司法体系下一家真实可靠的企业。当业务组成部分由不同的法律实体运作时（如作为一项单独功能的注册），这变得更为重要。

尽管所有 LoA 的基本要求是相同的，但更高级的 LoA 应更依赖于业务提供的完成和可靠。例如，在 LoA3 及以上，也应从其合作关系的了解以及对其在操作中允许的独立水平的了解中获得业务提供的更多保证。

9.2 法律和合同遵守

所有 EAAF 参与者均应了解并遵守其所负有的、与业务运营和交付有关的法律要求。这意味着（但不限于）可寻求的信息类型、如何进行身份验证以及可保留何种信息。处理 PII 尤其是一项法律关注（见附录 I）。应考虑到参与者运营所在的所有司法制度。在 LoA2 及更高等级，也应确定具体的政策和合同要求。

9.3 财务规定

当服务的长期可用性成为实体和依赖方的预期考虑时，应显示出财务稳健性，足以确保业务的持续运营并承担所伴随的责任风险。对于 LoA1 服务和依赖，此类规定不太可能会考虑，而在 LoA2 和更高等级支持更重要交易的服务应满足此类要求。

9.4 信息安全管理与审查

在 LoA2 和更高等级，EAAF 参与者应具备备有证明文件的信息安全管理法则、策略、风险管理方法以及其他经过认可的控制机制，以便保证具备有效的做法。对于 LoA3 和更高等级，应采用正式的信息安全管理系统（如 b-ISO/IEC 27000）。

根据法律、合同和技术合规性协议的不同，各参与者应确保各方承诺遵守并在发生不遵守的情况下提供校正手段。在 LoA2 和更高等级，该确保应由内部和外部安全审查以及安全地保留重大事件（包括这些审计）的记录加以支持。可采用审查的方法检查各方的做法是否符合已经达成的一致。可将争端解决服务用于解决分歧。

9.5 外部服务部件

当一个组织依赖于第三方提供其一部分服务时，如何指挥这些各方的行为并对其进行监管将有助于业务提供的整体保证。安排的性质和范围应与所需的 LoA 以及采用的信息安全管理系统相对应。在 LoA1，此保证应影响最小，但从 LoA2 起，这些措施有助于所给出的整体保证。

9.6 运营基础设施

要实现大规模的信任网络，可采用信任框架。在信任框架中，参与者支持相互间的信息交流。根据协议的不同，可要求这些额外参与者确保所有各方承诺遵守并提供不遵守情况下的纠正手段。

9.7 衡量运营能力

决策者规定信任网络的技术和合同要求。技术要求可包括产品版本等级、系统配置、设置和协议，而合同要求则可调整为恰当的信息做法。决策者在确定这些要求时，应包括可衡量潜在信任框架实体的标准。决策者可利用专家们已经取得的成果（如本建议书），而不是自己制定标准。决策者越是更多地采用不同信任框架的标准，各实体就更容易地理解和一致地应用这些标准。此外，指定的标准集可作为各种 LoA 时要求或能力的不同严格程度或类型的表达方式。

10 威胁和控制

本节描述 EAAF 各阶段的威胁，并提供 LoA 要求的控制。

10.1 注册阶段的威胁和控制

10.1.1 注册阶段的威胁

表 10-1 确定并描述了登记阶段的威胁。

表 10-1 – 登记阶段的威胁

威胁	示例
冒名 (Impersonation)	某个实体通过伪造的驾驶证非法使用另一个实体的身份信息，或某个设备采用虚假的媒体访问控制 (MAC) 地址在网络中注册。

10.1.2 保护不受注册阶段威胁影响所需的 LoA 控制

表 10-2 确定了根据 LoA 注册阶段所需的控制。

表 10-2 – 各 LoA 的注册阶段控制

威胁	控制	所需控制			
		LoA1	LoA2	LoA3	LoA4
冒名 (Impersonation)	身份验证 (IdentityProofing)：是否符合政策 (PolicyAdherence)	#1	#1	#1	#1
	身份验证：本人	/	/	/	#2
	身份验证：授权信息	#3	#4	#5	#6

注 – 上表中，标识符 #1 – #6 相当于在各 LoA 提供保护的具体控制。这些控制中的每一个详述于 10.1.2.1 节中。表格中单元格内的对角线表示在所示的 LoA，各个控制不适用。

10.1.2.1 注册阶段威胁的控制

以下注册阶段威胁的控制相当于表 10-2 中 #1 – #6。

身份验证：是否符合政策

#1. 公布身份验证政策并根据其公布的身份验证政策进行所有的身份验证。

身份验证：本人

#2. 须对人采用本人的身份验证。

身份验证：授权信息

#3. 身份信息可为自我宣称或自我主张。

#4. 以下控制适用：

- 自 #3 起的所有控制
以及：
- 实体须提供至少来自一个符合规定的身份信息政策权威来源的身份信息。
 - a) 对于人

- i) 本人：
 - 确保实体拥有至少来自一份符合规定的政策权威来源并附有与实体外貌相符的拥有者照片的身份文件；且
 - 确保所出示的身份文件在使用时看起来像真实的文件，签发正确且有效。
- ii) 非本人：
 - 实体须提供证据，证明他/她具有符合政策的个人身份信息。（可接受的身份信息可包括驾照或护照）；且
 - 所提供证据的存在和有效性须根据政策要求进行确认。
- b) 对于 NPE：
 - 一个权威身份信息来源的记录信息，如通用名称、描述、序列号、MAC地址、拥有者、位置、生产厂商等。

#5. 以下控制适用：

- 自#4起的所有控制。

此外：

a) 对于人：

i) 本人：

- 通过根据在身份文件中所列的联系信息与实体进行联系来验证其准确性；
- 根据相关权威来源的登记至少验证一份身份文件（如证明出生、婚姻或移民的文件）；
- 根据可用的权威信息来源并（在可能时）根据来自其他渠道、足以确保唯一身份的来源证实个人信息；并
- 验证此前实体提供的信息或可能只有实体知晓的信息。

ii) 非本人：

- 确保由一个可靠的第三方检查实体从权威来源向目前拥有LoA3（或更高）证书提供的主张/声称；和/或
- 验证此前实体提供的信息或可能只有实体知晓的信息。

b) 对于 NPE：

- 须在LoA3采用可靠的硬件（如TPM）；
- 对于已经使用的NPE，NPE须采用人发放的LoA3证书进行物理注册并附有设备RA。当使用可靠的硬件时，应予以激活；

- 尚未采购的NPE应采用LoA3人类验证或数字签名进行预订，以确认正在订购的实体经过授权，可以预订NPE。生产厂商的RA须注册NPE，启动一切可靠的硬件并控制NPE的发布和个性化。可靠硬件将在连入网络后启动；
- 对于非电脑的NPE，设备、所有者、网络或通信运营商与RA之间的绑定应按照与可靠硬件电脑类似的方式加密；且
- 当使用软件时，编码须根据LoA3人类发放证书在发放前进行数字签名并须由RA联署，作为使用前予以接受的证据。

#6. 以下控制适用：

- 自#5起的所有控制。

此外：

a) 对于人：

- 实体须通过至少一家其它遵循政策的权威来源提供身份信息。

b) 对于 NPE：

- 应在发布时登记连接到电脑、智能手机或类似处理器的其他设备并加密绑定到定位器设备上（如装有可靠硬件的设备、生物测定阅读器、智能卡、GPS地理验证器等）；
- 设备间绑定协议的任何变更须通过RA管理。在可能时，网络管理能力应提醒RA或网络管理设备关系发生的任何变化以及采取的校正行动；
- 须具备防止任何被更改的设备关系开始工作的能力；以及
- LoA4软件码须采用LoA4人类发放证书在发放前进行数字签名并须由RA联署，作为使用前予以接受的证据。

10.2 证书管理阶段的威胁和控制

10.2.1 证书管理的威胁

表 10-3 列出了证书管理阶段的威胁。

表 10-3 – 证书管理威胁

威胁	示例
证书生成（CredentialCreation）： 篡改（Tampering）	攻击者在信息从登记程序转向证书生成程序时修改信息。
证书生成：非法生成 （UnauthorizedCreation）	攻击者使得CSP在虚假身份基础上生成一个证书。
证书发放（CredentialIssuance）： 披露（Disclosure）	在证书建立过程中，当CSP为某个实体生成的证书从CSP向实体传送时，被攻击者复制。

威胁	示例
证书激活（CredentialActivation）： 非法拥有（Unauthorized Possession）	攻击者获得不属于其的证书并假装为合法实体，使得CSP激活证书。
证书激活： 无效（Unavailability）	1 与证书或生成证书的手段有关的实体不处于通常的位置并无法充分向CSP证明其身份。 2 证书或生成证书的手段交付延误，无法在规定期限内激活。
证书存储（CredentialStorage）： 披露（Disclosure）	公布存储在系统中的证书。例如，攻击者将对用户名和密码的存储记录做出评估。
证书存储：篡改（Tampering）	将用户名映射到证书的文件被破坏，导致映射被修改，现有证书被攻击者可以存取的证书所替代。
证书存储：复制（Duplication）	攻击者采用存储的信息生成一份可为非指定实体使用的复制证书（如通过复制可以生成证书的智能卡）。
证书存储：实体披露 （DisclosureByEntity）	实体在可由其他人访问的地方保留一份用户名和密码的书面记录。
证书作废（CredentialRevocation）： 作废延误（DelayedRevocation）	作废信息发布不及时，导致在证书验证人在更新有关最新作废信息前仍在使用作废的证书，进而造成对相关实体的威胁。
证书作废：除名后使用 （UseAfterDecommissioning）	当员工离开公司后，用户帐户未删除，导致旧账号可能被未经授权人员滥用。 – 在存储在硬件设备中的证书的密钥被作废后使用该证书。
证书更新（CredentialRenewal）： 披露（Disclosure）	CSP为实体更新的证书，在传送时被攻击者复制。
证书更新：篡改（Tampering）	实体生成的新密码在提交给CSP，以取代过期密码时被攻击者修改。
证书更新：非法更新 （UnauthorizedRenewal）	攻击者可利用有缺陷的证书更新协议扩展当前实体的证书有效期。 攻击者欺骗CSP为当前实体发放新证书，且新证书将当前实体的身份绑定到攻击者提供的证书上。对于NPE实体，在系统组件（如RAM）被使用后重新将其标注（重新发放）为新部件即是一个实例。
证书记录（CredentialRecordkeeping）： 否认（Repudiation）	实体主张或断言一个合法证书是虚假的或包含有不正确信息，以便虚假地否认曾使用过证书。

10.2.2 保护不受证书管理阶段威胁影响所需的 LoA 控制

表 10-4 确定了根据 LoA 证书管理阶段所需的控制。

表 10-4 – 各 LoA 的证书管理控制

威胁	控制	所需控制			
		LoA1	LoA2	LoA3	LoA4
证书生成：篡改	合适的证书生成 (AppropriateCredentialCreation)	#1	#1	#2	#2
	仅硬件 (HardwareOnly)	/	/	/	#3
	状态锁定 (StateLocked)	/	/	/	#4
证书生成：非法生成	跟踪目录 (TrackedInventory)	#5	#5	#5	#5
证书发放：披露	合适的证书发放 (AppropriateCredentialIssuance)	#6	#7	#7	#8
证书激活：非法拥有 证书激活：无效	由实体激活 (ActivatedByEntity)	#9	#9	#10	#11
证书存储：披露 证书存储：篡改 证书存储：复制 证书存储：实体披露	证书安全存储 (CredentialSecureStorage)	#12	#13	#14	#15
证书作废：作废延误 证书作废：除名后使用	证书安全废止和销毁 (CredentialSecureRevocation &Destruction)	#16	#16	#16	#16
证书更新：披露 证书更新：篡改 证书更新：非法更新	证书安全更新 (CredentialSecureRenewal)	#17	#17	#18	#19
证书记录：否认	记录保留 (RecordRetention)	#20	#20	#21	#21

注 – 上表中，标识符#1 – #21相当于在各LoA提供保护的具体控制。这些控制中的每一个详述于10.2.2.1节中。表格中单元格内的对角线表示在所示的LoA，各个控制不适用。

10.2.2.1 证书管理阶段的威胁控制

以下证书管理阶段的威胁控制对应于#1 – #21 表 10-4 中的数字。

合适的证书生成

#1. 以下控制适用：

- 须将正式和明文记录的程序用于证书生成。
- 最终将证书绑定到某实体前，CSP必须充分保证该证书正在且始终将与正确的实体绑定在一起。

#2. 以下控制适用：

- 自#1起的所有控制。

此外：

- 证书绑定应采用以下方式之一，提供篡改保护：
 - a) 数字签名；或
 - b) 对于硬件设备上的证书，在“状态锁定”一节中所述的机制。

仅硬件

#3. 证书须包括在硬件安全模块中。⁶

状态锁定

#4. 硬件设备上的证书须在生成流程结束时置于锁定状态。

跟踪目录

#5. 如果某个证书，或生成证书的方法处于硬件设备上，那么硬件设备须完全安全地保存并跟踪目录。例如，非个性化的智能卡应保存在安全的地方并记录其序列号，以免被盗并随后被试图生成非法的证书。

合适的证书发放

#6. 证书发放须采用正式和明文记载的程序。

#7. 以下控制适用：

- 自#6起的所有控制。
此外：
- 发放程序须包括确保向合适的实体提供证书的机制。如果证书不是当面交付，须采用某种机制检查交付地址存在且与实体是合法相关的。

#8. 以下控制适用：

- 自#7起的所有控制。
此外：
- 如果证书不是当面交付，须采用安全渠道交付且实体或实体的代表须签收，告知已收到证书。

由实体激活

#9. 须存在某种程序，确保证书或生成证书的方法只有在目标实体的控制下时才被激活。对此程序没有具体的要求。

#10. 须存在某种程序，确保证书或生成证书的方法只有在目标实体的控制下时才被激活。该程序须确认在将要激活证书的互动中实体身份信息的有效性（例如，挑战 – 应答协议）。

#11. 须存在某种程序，确保证书或生成证书的方法只有在目标实体的控制下时才被激活。该程序须：

- a) 验证实体与证书激活绑定（例如，挑战-应答协议）；以及
- b) 仅允许在策略决定的期限内进行激活。

⁶ ISO/IEC 19790:2012中定义的硬件安全模块的边界。

证书安全存储

#12. 以下控制适用：

- 基于共享秘密的证书通过访问控制，仅限需要访问的主管部门和应用访问的方式给予保护；以及
- 须在向实体提供的、与使用这些证书有关的文件中描述存储证书的保护策略。

#13. 以下控制适用：

- 自#12起的所有控制。
此外：
- 此类共享的保密文件不得包含明码文本的密码或机密；可采用变通方法保护共享秘密。

#14. 以下控制适用：

- 自#13起的所有控制。
此外：
- 共享秘密应通过访问控制，仅限需要访问的主管部门和应用访问的方式给予保护。此类共享秘密须加密。共享秘密的密钥自身须加密并存储在密码模块（硬件或软件）中。共享秘密的密钥须只在验证运作立即需要时才进行解码；以及
- 须要求实体或实体的代表确认他们知道这些要求并同意根据这些要求保护证书。

#15. 以下控制适用：

- 自#14起的所有控制。
此外：
- 须要求实体或实体的代表签署一份文件，承认他们了解证书存储的要求并同意相应地保护证书。

证书安全废止和销毁

#16. CSP 须在规定的时限内废止或销毁（如可能）组织策略所定义的各 LoA 的证书（包括那些共享秘密的证书）。

证书安全更新

#17. 以下控制适用：

- CSP须制定证书更新和更换的适当策略；
- 在CSP允许更新和/或更换之前，实体须在CSP允许更新并/或更换之前展示当前未过期证书的持有证据；
- 密码须满足有关密码强度和再使用的最低CSP策略要求；
- 当前证书过期后，不得允许更新；
- 须在受保护渠道进行所有互动。

#18. 以下控制适用：

- 自#17起的所有控制。
此外：
- 根据第10.1.2.1节（身份验证：是否符合政策、身份验证：授权信息）进行LoA2身份验证。

#19. 以下控制适用：

- 自#17起的所有控制。
此外：
- 根据第10.1.2.1节（身份验证：是否符合政策、身份验证：授权信息）进行LoA3身份验证。

记录保留

#20. CSP 须保留每个证书登记、历史和状态的记录（包括作废）。保留期限须由 CSP 策略规定。

#21. 以下控制适用：

- 自#20起的所有控制。
- 须为每个记录的保护链制定正式和明文记录的程序。

10.3 验证阶段的威胁和控制

10.3.1 验证阶段的威胁

验证阶段的威胁包括与验证过程中证书使用有关的威胁以及验证的一般性威胁。验证的一般性威胁包括但不限于：恶意软件（如病毒、木马、键盘记录软件）、社交工程（如偷窥、盗窃硬件和个人识别号）、用户错误（如密码较弱、未能保护验证信息）、不真实的否认、在数据传输过程中非法截获和/或修改验证数据、拒绝服务以及程序性缺陷等。除使用多因素验证外，验证一般性威胁的控制不属于本建议书的范围。本节侧重于与使用证书进行验证有关的威胁，描述了这些威胁并列出了每种威胁类型的控制。

除将多因素验证用于 LoA 3 和 4 的要求外，在验证阶段的 LoA 方面描述具体的控制并不妥当。一些控制也许不适合所有的情况。例如，对于访问在线杂志订阅用户的验证控制也许有别于医生读取病历的控制。因此，随着利用风险和结果越来越严重，建议 CSP 应深入考虑安全，即分层设定适合于运营环境、应用和 LoA 的控制。应由系统审计商在风险分析的基础上决定如何以及何时、以哪种组合采用这些控制。

用于验证的证书面临着多种威胁。表 10-5 列出了证书使用威胁的一些种类并提供了说明威胁的具体实例。

表 10-5 – 验证阶段证书使用威胁的摘要

威胁	示例
一般性威胁	验证的一般性威胁包括对于任意类型ICT常见的多种安全威胁。一些示例包括键盘记录软件、社交工程和用户错误。除使用多因素验证外，这些威胁的控制不属于本建议书的范围。请注意，多因素验证无法防止所有可能的一般性威胁。
在线猜测 (OnlineGuessing)	攻击者通过猜测证书可能数值的方式，不断试图登录。
离线猜测 (OfflineGuessing)	<p>利用分析方法，在验证处理之外暴露与证书生成有关的秘密。密码破解常常依赖于暴力破解方法，如采用字典攻击。在字典攻击中，攻击者采用某个程序，重复一部字典（或不同语言的多部字典）中所有的词，计算每个词的哈希（hash）值并根据数据库检查得到的哈希值。</p> <p>采用彩虹表（rainbow table）是另一种秘密破解方法。彩虹表为预先计算的明文/哈希值表格。彩虹表速度快于暴力破解攻击，因为采用了减项函数来减少搜索空间。一旦生成或获得以后，攻击者可反复使用彩虹表。</p>
证书复制 (CredentialDuplication)	实体的证书或生成证书的方式已被非法复制。非经授权复制私钥即是一例。
网络钓鱼 (Phishing)	实体被引诱与假冒的验证者往来并被骗提供了其秘密或可用来伪装成实体的敏感个人信息。当实体收到一封电子邮件，将其导向一个欺诈网站并要求用户以其用户名和密码登录的网站即是一例。
偷听 (Eavesdropping)	攻击者被动窃听验证处理，以获取可在后续主动攻击中用来伪装成实体的信息。
重放攻击 (ReplayAttack)	攻击者可重放先前截获的（合法实体与RP之间的）讯息，作为实体向RP验证。
会话劫持 (SessionHijack)	攻击者可在实体和验证者成功进行验证交换之后将其插入到这两者之间。攻击者可向依赖方伪装成实体或相反的情况，以控制会话数据交换。攻击者可通过窃听或预测用来标记实体所发送的、HTTP请求的验证cookie值，控制一个已经过验证的会话。
中间人 (ManInTheMiddle)	攻击者将其置于实体和依赖方之间，以便其可以拦截并改变验证协议讯息的内容。通常攻击者在实体面前伪装成依赖方并同时向验证者面前伪装成实体。与双方同时进行主动交换可使攻击者使用一个合法方发送的验证讯息并成功地向另一方进行验证。
证书盗窃 (CredentialTheft)	生成或包含已被攻击者偷窃证书的装置。

威胁	示例
伪装和假装 (SpoofingAndMasquerading)	伪装和假装指攻击者伪装成另一个实体，以使攻击者可开展一个原本无法实施的行动（如获取一个原先无法获得的资产）的情况。可采用实体的证书或假装成一个实体（如通过伪造证书）实现此目的。其中一些示例包括：伪装成某个实体的攻击者通过制作一个“拙劣的”、与实体样式匹配的手指伪造一项或多项生物特征；攻击者通过其设备广播属于另一个设备、可访问某个特定网络的MAC地址来伪装某个MAC地址；或攻击者装作合法的、负责下载在线软件应用和/或更新的软件发布商等。

10.3.2 保护证书使用不受威胁影响所需的 LoA 控制

表 10-6 确定了根据 LoA 应对证书使用威胁所需的控制。

表 10-6 – 每种 LoA 的证书使用威胁控制的摘要

威胁	控制	所需控制				
		LoA*	LoA1	LoA2	LoA3	LoA4
一般性**	多因素验证				#1	#1
在线猜测	强力密码 (StrongPassword) 证书锁定 (CredentialLockOut) 默认账户使用 (DefaultAccountUse) 审查和分析 (AuditAndAnalyze)	#2 #3 #4 #5				
离线猜测	加盐哈希密码 (HashedPasswordWithSalt)	#6				
证书复制	反伪造 (AntiCounterfeiting)	#7				
网络钓鱼	探测钓鱼来自何方的讯息 (DetectPhishingFromMessages) 通过反钓鱼做法 (AdoptAntiPhishingPractice) 互认证 (MutualAuthentication)	#8 #9 #10				
窃听	不传送密码 (NoTransmitPassword) 加密验证 (EncryptedAuthentication) 不同验证参数 (DifferentAuthenticationParameter)	#11 #12 #13				
重放攻击	不同验证参数 时戳 (Timestamp) 物理安全 (PhysicalSecurity)	#13 #14 #15				
会话劫持	加密会话 (EncryptedSession) 修补TCPIP缺陷 (FixTCPIP_Vulnerabilities) 加密互握手 (CryptographicMutualHandshake)	#16 #17 #18				
中间人	互认证 加密会话	#10 #16				

表 10-6 – 每种 LoA 的证书使用威胁控制的摘要

威胁	控制	所需控制				
		LoA*	LoA1	LoA2	LoA3	LoA4
证书盗窃	证书激活 (CredentialActivation)	#19				
伪装和假装	码数字签名 (CodeDigitalSignature) 实时发现 (LivenessDetection)	#20 #21				
LoA* – 应根据风险评估确定的必要性应用这些控制。 一般性** – 多因素验证无法阻止全部一般性威胁。						

注 – 上表中, 标识符 #1 – #21 对应着各种 LoA 时提供保护所需的具体控制。每个控制详述于 10.3.2.1 节。

10.3.2.1 验证阶段证书使用威胁的控制

以下验证阶段证书使用威胁的控制对应于 #1 – #21 表 10-6 所列的号码。

多因素验证

#1. 须采用两种或多种应用不同验证因素的证书 (如某些与你熟知的事物组合而成的事物)。

强力密码

#2. 须采用强力密码 (如复杂、包含大小写、数字和特殊符号的非字典字符串)。

证书锁定

#3. 应在一定次数密码尝试失败后采用锁定或减速机制。

默认账户使用

#4. 不得采用默认的账户名和密码 (如生产厂商的设定)。

审查和分析

#5. 须采用登录失败的审查跟踪, 以分析企图在线猜测密码的模式。

HashedPasswordWithSalt

#6. 须采用加盐值的哈希密码, 以阻止暴力攻击和彩虹表攻击。

反伪造

#7. 装有证书的设备上须采用反伪造措施 (如全息、缩微相片等)。

探测网络钓鱼来自何方的讯息

#8. 须采用专门设计用来探测网络钓鱼攻击的控制 (如贝叶斯过滤器、IP 黑名单、URL 过滤器、启发和指纹识别方法等)。

通过反网络钓鱼方法

#8. 须采用禁止图像、禁止不受信任来源的超文本链接以及在电子邮件客户中提供视觉提示等方法保护实体不受网络钓鱼的攻击。

互认证

#9. 须采用相互认证。

不传送密码

#11. 须采用不通过网络传送密码的认证机制（如 Kerberos 协议）。

加密验证

#12. 如果需要通过网络进行验证，那么数据须加密传输。

不同的验证参数

#13. 每种验证处理须采用不同的验证参数（如一次性的密码、会话证书等）。

时戳

#14. 每个讯息须以不可伪造的时戳标注时间。

物理安全

#15. 须采用物理安全机制（即篡改证据、发现和响应）。

加密会话

#16. 须采用加密会话。

修补 TCP/IP 缺陷

#17. 须采用修补 TCP/IP 缺陷的平台补丁。

加密互握手

#18. 须采用基于加密（如 TLS）的互握手交换。

证书激活

#19. 须要求具备激活特性，以使用证书（如向包含证书的硬件设备中输入 PIN 码或生物信息）。

码数字签名

#20. 须将数字签名与受信任来源进行比对，以应对软件下载被非经授权方篡改。

实时发现

#21. 须采用实时发现方法确定虚假生物特性的使用（如伪造的指纹）。

11 服务保障标准

寻求遵循本框架的信任框架运营商须制定满足其准备支持的每个 LoA 要求的具体标准，并须根据那些标准对表示遵循该框架的 CSP 进行评估。与此类似，CSP 须通过评估其整体业务流程并根据具体标准评估技术方法来确定其业务遵循该框架所在的 LoA。

附件A

证书的特性

(本附件是本建议书的一个组成部分。)

- a) 证书是数据。

证书并不包含任何装有数据的物理容器或设备，也不包括构成证书的数据的生成器。因此，通行码生成器从不是证书的一部分，可以签名数据的智能卡、生成数字签名的软件、可以书写的纸等也不是证书的一部分。
- b) 证书必须包含是身份和/或资格证据的数据。

此类证据的示例有：

 - 1) 已知事物（如静态密码）；
 - 2) 生物特征或同一事物的再现；或
 - 3) 经过处理的某事物生成的数据（如由通行码生成器生成的一次性通行码、由硬件或软件通过假定由某个实体所有的密钥数字签名过的数据）。
- c) 证书可与其他有利于验证和识别进程，但不是实际证书一部分的数据联合。

这种数据的示例包括实体的名称和公共密钥证书。实体或资格证明并不需要这些，但它们对认证协议是有用的。将实体名称关联到证书可确认身份。将公共密钥证书关联到证书可提供有助于测试证据的信息并可提供有关实体身份或资格的信息。
- d) 证书亦可为推导得出的证书。

在此情况下，此类推导出的证书可以从一系列证书中推导得出的批量信息，通常由某实体创建并发送，用于证书认证方的验证。例如，对于某些类型的匿名验证，实体将CSP发布的证书转换为用于验证工作的推导证书。
- e) 并非构成证书的所有数据均需要保密。
- f) 证书可用于实体的验证、识别或授权，或三者的组合。
- g) 证书在被接受为真实可信，可用于其具体用途（如验证、识别、授权）之前必须验证。
- h) 证书验证必须通过几个步骤。这些步骤包括：
 - 1) 核对证书的真实性，以确保其来自于所宣称的发布者；
 - 2) 确认证书的合法性和可信度，（如确定是否存在从证书发布者至受信来源的直接链接）；
 - 3) 确认数学/密码的计算精确度。
- i) 证书可能会是真实的，但不一定在所有情况下有效（如在预付费电话芯片卡等智能卡上的证书，是真实的，但可能只能采用发行者的设施才能呼叫）。

附录I

隐私和PII的保护

(本附录是本建议书的一个组成部分)

用于特定用途的特定验证方法的合适性将不仅取决于对验证有效性的评估，也取决于所涉组织面临的风险和风险容忍程度。滥用实体 PII 或 PII 保护不足为组织带来了重大风险，包括声誉影响和问责的暴露。因此，PII 用于验证目的及其保护需要谨慎权衡和考虑。本节提供了与一些组织在决定采用并实施某种验证方法时应考虑在内的一些隐私考虑有关的信息指导。

当实体为个人时，绝大多数验证方法将涉及以下一个或多个过程中的 PII 处理：

- a) 当收集、证明并验证身份和其他与实体有关的信息时，在注册过程中；
- b) 在实体证书的生成、发放和管理过程中；
- c) 在实体使用证书以及依赖方和验证方进行验证的过程中。

不可能同时实现强力验证和绝对隐私。有着多种强力加密验证方法，这些方法对隐私的不利影响有限（如匿名证书、分组签名）。此外，应注意到，保证等级的增强（如 LoA4 相对于 LoA2）可能但不一定对个人隐私产生负面影响。很大程度上取决于所选的验证方法以及如何实施。在做出这些决定时，除有必要保护其资源和在非法活动中对实体进行问责外，每个组织应仔细考虑保护实体 PII 的必要性。

绝大多数验证方法涉及到采用有区别的标识符，在一个验证的情况下明确地将一个实体与其他可能的实体区别开来。对于各种其他目的（如账户管理和适当的审查跟踪的维护），采用有区别的标识符经常也是必要的。与使用区分标识符有关的主要隐私关注并不涉及如此使用区分标识符，而是在许多不同情况下重复使用相同的标识符。例如，通常认为指定用于一种目的的帐号敏感度低于用于多个用途（如税收、医疗、退休）的政府行政参考号码。在某些司法制度中，也可能存在限制使用特定标识符的法律。

鉴于前述的考虑，各组织应采用有效的安全保护，在本 EAAF 所涉的各个阶段和过程中保护实体的 PII。特别是，所选的验证方法应按照通常将 PII 处理降低到最低限度进行设计和实施。此外，采用在其他情况下或领域内也可使用的可区分标识符应限于有必要使用且相关法律允许使用的情况。

可在两个来源查询 ISO/IEC 其他保护 PII 的导则：

- a) [b-ISO/IEC 29100]描述了在三个主要因素方面的基本隐私要求：(1) 保护个人隐私和保护其PII的法律和规章要求，(2) 具体的业务和使用情况要求，以及(3) PII实体的个人隐私偏好。[b-ISO/IEC 29100]描述了以下基本隐私原则：同意和选择；目的说明；收集限制；使用、保留和披露限制；数据最小化；精确度和质量公开；透明和通知；个人参与和访问；问责；安全控制和合规。除进行风险评估，分析各种威胁外，各组织应对其验证方法进行隐私影响评估，评估其系统的哪些部分将需要在隐私保护措施方面特别注意。
- b) [b-ISO/IEC 29101]提供了负责处理PII的ICT系统架构。若干关切点和结构观点对此构架框架结构进行了介绍。现已为应用ICT系统处理PII提供了一批组件。该框架意在构建遵守[b-ISO/IEC 29100]中所述隐私原则的系统框架。

关于与保护 PII 有关的要求、原则和系统设计的详细指导，读者可参考上述标准。

参考文献

- [b-ITU-T X.1252] Recommendation ITU-T X.1252 (2010), *Baseline identity management terms and definitions*.
- [b-ITU-T Y.2702] Recommendation ITU-T Y.2702 (2008), *Authentication and authorization requirements for NGN release 1*.
- [b-ITU-T Y.2720] Recommendation ITU-T Y.2720 (2009), *NGN identity management framework*.
- [b-ITU-T Y.2721] Recommendation ITU-T Y.2721 (2010), *NGN identity management requirements and use cases*.
- [b-ITU-T Y.2722] Recommendation ITU-T Y.2722 (2010), *NGN identity management mechanisms*.
- [b-ISO/IEC 9798] ISO/IEC 9798:2010, *Information technology – Security techniques – Entity authentication*.
- [b-ISO/IEC 18014-2] ISO/IEC 18014-2:2009, *Information technology – Security techniques – Time-stamping services – Part 2: Mechanisms producing independent tokens*.
- [b-ISO/IEC 19790] ISO/IEC 19790:2012, *Information technology – Security techniques – Security requirements for cryptographic modules*.
- [b-ISO/IEC 19792] ISO/IEC 19792:2009, *Information technology – Security techniques – Security evaluation of biometrics*.
- [b-ISO/IEC 27000] ISO/IEC 27000:2012, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.
- [b-ISO/IEC 27001] ISO/IEC 27001:2005, *Information technology – Security techniques – Information security management system – Requirements*.
- [b-ISO/IEC 29100] ISO/IEC 29100:2011, *Information technology – Security techniques – Privacy framework*.
- [b-ISO/IEC 29101] ISO/IEC 29101, *Information technology – Security techniques – Privacy architecture framework*.
- [b-ISO/IEC 24760-1] ISO/IEC 24760-1:2011, *Information technology – Security techniques – A framework for identity management – Part 1: Terminology and concepts*.
- [b-ISO/IEC 19790] ISO/IEC 19790:2012, *Information technology – Security techniques – Security requirements for cryptographic modules*.
- [b-NIST SP800-36] NIST Special Pub 800-36 (2003), *Guide to Selecting Information Technology Security Products*.
<<http://csrc.nist.gov/publications/nistpubs/800-36/NIST-SP800-36.pdf>>
- [b-NIST SP800-63] NIST Special Pub 800-63 (2006), *Electronic Authentication Guideline Version 1.0.2*.
<http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf>
- [b-AGGPKI] *Australian Government Gatekeeper Public Key Infrastructure*.
<http://www.gatekeeper.gov.au/>
- [b-DuD] Van Alsenoy B., and De Cock, D. (2008), 'Due processing of personal data in eGovernment? A Case Study of the Belgian electronic identity card', *Datenschutz und Datensicherheit*, Vol.32, No.3, pp.178-183.

- [b-EoI] New Zealand Standard: *Evidence of Identity Standard Version 2.0, 2009.*
<<http://www.dia.govt.nz/EoI/pdf/EoIv2.0.pdf>>
- [b-ENISA] ENISA, *Mapping (Interoperable Delivery of European e-government services to public Administrations, Businesses and Citizens) IDABC Authentication Assurance Levels to SAML v2.0.*
- [b-IAF] *Kantara Initiative Identity Assurance Framework v2.0.*
<<http://kantarainitiative.org/confluence/display/GI/Identity+Assurance+Framework>>
- [b-MOV] Menezes, A., van Oorschot, P., and Vanstone, S. (1997), 'Handbook of Applied Cryptography', pp. 3-4.
<<http://www.cacr.math.uwaterloo.ca/hac/>>
- [b-NeAF] *The National e-Authentication Framework.*
<<http://www.finance.gov.au/e-government/security-and-authentication/authentication-framework.html>>
- [b-OECD] OECD (2007), *OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication.*
<<http://www.oecd.org/dataoecd/32/45/38921342.pdf>>
- [b-OMB] OMB M-04-04 (2003), *e-Authentication Guidance for Federal Agencies*
<<http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>>
- [b-PEA] Industry Canada (2004), *Principles for Electronic Authentication: A Canadian Framework.*
<http://strategis.ic.gc.ca/epic/site/ecic-ceac.nsf/en/h_qv00240e.html>

ITU-T系列建议书

A系列	ITU-T工作的组织
D系列	一般资费原则
E系列	综合网络运行、电话业务、业务运行和人为因素
F系列	非话电信业务
G系列	传输系统和媒质、数字系统和网络
H系列	视听及多媒体系统
I系列	综合业务数字网
J系列	有线网络和电视、声音节目及其它多媒体信号的传输
K系列	干扰的防护
L系列	电缆和外部设备其它组件的结构、安装和保护
M系列	电信管理，包括TMN和网络维护
N系列	维护：国际声音节目和电视传输电路
O系列	测量设备的技术规范
P系列	电话传输质量、电话设施及本地线路网络
Q系列	交换和信令
R系列	电报传输
S系列	电报业务终端设备
T系列	远程信息处理业务的终端设备
U系列	电报交换
V系列	电话网上的数据通信
X系列	数据网、开放系统通信和安全性
Y系列	全球信息基础设施、互联网协议问题和下一代网络
Z系列	用于电信系统的语言和一般软件问题