CNAS-CL08-A001

司法鉴定/法庭科学机构能力认可准则在电子数据鉴定领域的应用说明

Guidance on the Application of Accreditation Criteria for the Competence of Forensic Units in the Field of Digital Forensics

中国合格评定国家认可委员会

2018 年 4 月 18 日 发布　　2018 年 9 月 1 日 实施

前言

电子数据鉴定是中国合格评定国家认可委员会（英文缩写：CNAS）对司法鉴定/法庭科学机构（以下简称鉴定机构）的认可领域之一。电子数据鉴定是指在诉讼活动中鉴定人运用计算机科学与相关技术，对诉讼中涉及的电子数据领域的问题进行检测、检验、鉴别和判断并提供鉴定意见的活动。

本应用说明是 CNAS 根据电子数据鉴定领域的特性而对 CNAS-CL08:2018《司法鉴定/法庭科学机构能力认可准则》所作的进一步说明，并不增加或减少该准则的要求。因此，本应用说明采用针对 CNAS-CL08:2018《司法鉴定/法庭科学机构能力认可准则》的具体条款提出应用说明的编排方式，故章节号是不连续的。

本应用说明应与 CNAS-CL08:2018《司法鉴定/法庭科学机构能力认可准则》同时使用。

本应用说明替代 CNAS-CL27:2014《司法鉴定/法庭科学机构能力认可准则在电子物证鉴定领域的应用说明》。

司法鉴定/法庭科学机构能力认可准则
在电子数据鉴定领域的应用说明

1 范围

本应用说明适用于 CNAS 对所有从事电子数据鉴定活动的鉴定机构的认可。

2 规范性引用文件

本应用说明主要参考和引用了 CNAS-CL08:2018《司法鉴定/法庭科学机构能力认可准则》的相关内容。

3 术语和定义

本应用说明使用 CNAS-CL08:2018《司法鉴定/法庭科学机构能力认可准则》中给出的相关术语和定义。考虑到电子数据鉴定专业的特殊性，故采用以下术语和定义来描述所鉴定的检材/样本：

存储介质是指具备数据信息存储功能的电子设备、硬盘、光盘、优盘、记忆棒、存储卡、存储芯片等载体。原始存储介质是指直接来源于案件客观事实的存储介质。

电子数据是指在案件发生过程中形成的，以数字化形式存储、处理、传输的，能够证明案件事实的数据。

4 通用要求

4.1 公正性

4.2 保密性

4.3 独立性

5 结构要求

6 资源要求

6.1 总则

6.2 人员

6.2.2 授权签字人应获得电子数据鉴定领域鉴定人资格证书后在本领域鉴定工作 2 年（含）以上（或依法从事电子数据收集提取和审查判断工作 7 年以上），并具有本

专业中级及以上职称。

6.2.7 鉴定机构应根据人员岗位制定培训计划，培训内容至少应包括（但不限于）：

——鉴定方法、相关设备的操作；

——电子设备的安全保护；

——出庭质证；

——电子数据相关新技术、法律法规。

在以下情况时，鉴定机构需对相关鉴定人员进行重新培训：

——从事新的电子数据鉴定岗位工作；

——离开鉴定岗位时间超过 1 年；

——鉴定方法、关键设备发生变化。

对培训活动的有效性验证的方式包括（但不限于）：

——能力验证结果；

——内部质量控制结果；

——内外部审核；

——不符合工作的识别；

——利益相关方的投诉；

——人员监督评价和考核。

6.2.8 鉴定机构应由熟悉本专业的鉴定方法、程序、目的和结果评价的监督员，每 2 年对鉴定人以及参与鉴定工作的人员进行至少一次现场见证。结合工作岗位，见证内容应涉及设备操作、电子数据完整性校验值计算、结果的分析判断等关键技术环节。

6.3 设施和环境条件

6.3.1 鉴定机构应考虑电子数据鉴定中不同鉴定项目对设施和环境的要求。鉴定区域应采取防磁、防静电和不间断供电等措施；对手机等具有无线通信功能的检材/样本的鉴定，应在信号屏蔽或信号阻断的环境中进行。

鉴定机构应具备保护其信息网络安全的措施，包括防范计算机病毒等恶意代码、防范网络入侵和防范数据泄露等。

在特殊情况下（如恶意代码鉴定、手机等具有无线通信功能的原始存储介质联网验证时），可能需要关闭杀毒软件等安全措施或者进行无线网络连接，此时鉴定机构应评估安全风险，采取相应的措施，并保存相应记录。

6.3.4 应实施、监控并定期评审设施的控制措施，这些措施应涉及但不限于：

a) 鉴定机构的办公区域与鉴定区域应进行有效的隔离；

d) 当鉴定活动对人身健康有危害时，应配备保障人身安全的设施和防护装备。

6.4 设备

6.4.4 对鉴定结果有效性有影响的鉴定设备版本或配置发生改变时，应重新进行功能核查。核查的措施可包括：

——对同一检材/样本进行重复鉴定，审查鉴定结果的可复现性；

——将核查结论与另一个鉴定机构的核查结论进行比对；

——将核查结论与预期结果进行比对，列出已知的缺陷。

6.4.13 对鉴定结果有影响的电子数据鉴定设备的记录，除准则中所列内容之外，还应包括：

——设备核查的记录；

——设备的配置情况；

——软件的名称和升级后的版本号。

6.5 计量溯源性

6.6 外部提供的产品和服务

6.6.2 c) 对于涉及内网、敏感终端、服务器、大数据的外部技术支持或服务，应当制定相关的保密措施。

7 过程要求

7.1 委托受理

7.1.1 i) 在接收原始存储介质时，应当检查原始存储介质的相关信息，必要时，查阅封存记录；具有无线通信功能的，应当检查是否采取了信号屏蔽、信号阻断或者切断电源等措施；在接收电子数据时，应计算、核查电子数据的完整性校验值，必要时，核查提取电子数据过程的记录；

注 3：适用时，应对原始存储介质的拆封过程和重新封存过程进行录像。

注 4：准则中相关信息是指原始存储介质的封存状态、其是否完好、唯一性标识等信息。

j) 因鉴定活动可能对原始存储介质造成损坏或改变的，应向委托方说明并进行书面确认。

7.2 方法的选择、验证和确认

7.3 抽样/取样

7.3.5 当鉴定工作涉及现场取样时，应记录取样人及取样的时间、地点、设施和联网状况等信息。

7.4 检材/样本的处置

7.4.1 鉴定机构应制定检材/样本的处置程序，保证检材/样本的完整性，包括：

——计算、核查电子数据的完整性校验值，并进行备份；

——适用时，应通过写保护设备对检材/样本进行鉴定；

——适用时，应对检材/样本制作电子数据备份，对备份文件进行检验；

——无法使用写保护设备且无法制作备份时，应尽可能减少对检材/样本中的电子数据造成改变；如不可避免对检材/样本中的电子数据造成影响鉴定结果的改变，应征得客户的同意，书面注明原因，记录操作过程并对操作过程进行录像。

7.4.4 鉴定机构应有专门防磁、防静电存储措施以保护检材/样本。

7.5 记录/档案

7.5.1 电子数据鉴定记录应能够追溯到鉴定人员的操作过程和鉴定方法，应能够支持当鉴定人不在时其他鉴定人可以评估鉴定过程并解释这些数据。应记录所有使用的关键设备的操作参数，包括方法中未指定的参数；应记录检出数据的完整性校验值。当出现异常数据时（如硬盘坏道等存储介质故障、超过方法可接受的范围），应记录原因。

7.5.4 当使用电子数据鉴定设备实时生成的电子日志作为原始记录时，电子日志应满足准则中技术记录、数据控制和信息管理等有关要求。

7.6 测量不确定度的评定

7.7 确保结果的有效性

7.7.1 鉴定机构的质量控制活动应优先考虑以下方式：

——不同人员对同一检材/样本进行检验；

——不同厂商同类型设备对同一检材/样本进行检验。

当鉴定机构持续 1 个月未开展鉴定活动时，电子数据鉴定机构应实施至少一次监控鉴定结果有效性的活动。

7.7.2 在认可证书有效期内，鉴定机构参加能力验证活动应覆盖认可能力范围内的鉴定项目/参数，对于无法获得能力验证的项目/参数，至少进行一次实验室间比对。

7.8 鉴定文书

7.8.1 总则

7.8.1.2 当鉴定机构以硬拷贝或电子数据传输的方式发布鉴定文书时，应采取措施保证鉴定文书的完整性。必要时，采用加密方式传输。

7.8.2 鉴定文书的通用要求

7.8.2.1 电子数据鉴定文书的格式和包含的信息应符合法规或行业所规定的要求。鉴定文书的信息除准则所列内容外，还应满足：

g) 原始存储介质的描述应包括原始存储介质的封存状况、异常状态；适用时，应核查电子数据的完整性校验值。

h) 适用时，应提供取样人及取样的时间、地点；

m) 鉴定结果中应包括检出数据的完整性校验值；

q) 鉴定设备的信息（含版本号）。

7.9 投诉

7.10 不符合工作

7.11 数据控制和信息管理

7.11.6 适用时，应通过比对电子数据完整性校验值对数据转移进行核查。

8 管理体系要求

8.1 方式

8.2 管理体系文件化（方式 A）

8.3 管理体系文件的控制（方式 A）

8.4 记录控制（方式 A）

8.5 应对风险和机遇的措施（方式 A）

8.6 改进（方式 A）

8.7 纠正措施（方式 A）

8.7.1 在电子数据鉴定中出现异常时，分析潜在的原因除了注释中所列之外还应包括计算机病毒等恶意代码的影响、计算机内运行的其它软件的影响、计算机运行的网络环境的影响等。

8.8 内部审核 (方式 A)

8.9 管理评审（方式 A）