eID 数字身份体系白皮书

（2018）

公安部第三研究所

二〇一八年四月

目录

前言

当前，数字化全面融入国民经济和社会发展各领域，数字化生产加速演进、数字化服务日益普及、数字化创新日新月异，深刻改变着经济社会的发展动力和发展方式，重塑着产业社会发展和国际竞争新格局。但同时也应该看到，我国数字化转型过程中存在着诸多瓶颈和问题，如数字资源开发利用能力不足、数字基础设施尚不完善、数字社会治理面临挑战等。

在此背景下，公安部第三研究所（以下称我所）于十二五期间承担了国家 863 计划信息安全重大专项，包括“网域空间身份管理”、“基于 eID 的典型示范应用”等科研课题，研发了“网络电子身份标识（eID）”技术并形成了相关标准体系。我所在以上科研成果的基础上，结合近年在数字身份领域的实践和理论研究，以及《电子签名法》、《网络安全法》、《民法总则》等法律法规的要求，推出《eID 数字身份体系白皮书（2018）》（以下称白皮书）。

白皮书旨在通过引入 eID 数字身份构建全国统一数字身份体系，在保护公民隐私的前提下实现多种数字身份认证方式的互通，推动数据的流通和开放，促进我国数字经济发展，建设网络强国。

白皮书所涉及的内容仅限于自然人的数字身份，所提及身份皆为自然人的身份。

1. 背景

1.1. 身份的功能

白皮书中的身份不含有阶层观念，仅从人口管理和服务的角度来讨论身份问题。一般而言，身份具有两大功能，一为区分，二为证明。

身份的区分功能服务于国家的人口管理制度。对于人口管理必须进行人口调查以及人口登记，联合国 1969 年发布的《人口登记或类似系统的方法和评估》将人口登记定义为 ：“一种个人数据的系统，即连续记录和/或协调联系一个国家常住人口的每个成员有关信息的机制，以便在特定时间间隔确定有关人口规模和特征的最新信息。”为便于人口登记，很多国家都采取一人一号的制度，比如我国通过公民身份号码对人口数据进行索引，美国采用社会保险号（Social Security Number）来作为索引记录人口数据。

身份管理的另一功能在于证明。整个社会的运行需要建立在对于社会主体一定程度的信任基础上。信任来自于对社会主体的了解，为了解决这种信任的需求，身份证明开始出现。在原始社会中，社会主体之间的交往可能仅是部落成员之间的物物交换，基于彼此的了解即可证明身份，但是随着生产力的进步，社会成员之间的互动范围不再限于熟人之间，此时需要有权威或者公信力的机构出具特定的证明来增加交往双方的信任度以完成一定的社会行为。我国的身份证即是政府为公民统一颁发的一种身份证明，在其他没有国家统一身份证明的国家，如美国，政府颁发的社会安全卡（Social Security Card）、驾照都可以作为身份证明使用。

1.2. 我国现代人口管理制度历史沿革

1958 年，我国颁布《中华人民共和国户口登记条例》，实行户籍管理制度。

1984 年 4 月 6 日国务院发布《中华人民共和国居民身份证试行条例》，并且开始颁发第一代居民身份证。

《中华人民共和国居民身份证法》经 2003 年 6 月 28 日第十届全国人大常委会第 3 次会议通过，2003 年 6 月 28 日主席令第 4 号公布；2004 年 3 月 29 日起，中国大陆正式开始为居民换发内置非接触式 IC 卡智能芯片的第二代居民身份证，相比于只具有视读功能的一代证，二代证内置了芯片作为机读存储器，并且是彩色证件，兼具有机读和视读功能。

2011 年 10 月 29 日第十一届全国人大常委会第 23 次会议《关于修改〈中华人民共和国居民身份证法〉的决定》修正 2003 年通过的《中华人民共和国居民身份证法》。最新修订的居民身份证法明确规定了“居民身份证登记的项目包括：姓名、性别、民族、出生日期、常住户口所在地住址、公民身份号码、本人相片、指纹信息、证件的有效期和签发机关”，“公民申请领取、换领、补领居民身份证，应当登记指纹信息”；还新增规定“有关单位及其工作人员对履行职责或者提供服务过程中获得的居民身份证记载的公民个人信息，应当予以保密”，“国家机关或者金融、电信、交通、教育、医疗等单位的工作人员泄露在履行职责或者提供服务过程中获得的居民身份证记载的公民个人信息，构成犯罪的，依法追究刑事责任”。

从我国现代人口管理制度的历史，可以看出人口管理的发展经历了以下几个阶段：

- 对公民实施以户为单位的户籍人口管理政策；
- 国务院发布《中华人民共和国居民身份证试行条例》，并开始发行一代身份证；
- 人大常委会正式通过《中华人民共和国居民身份证法》，开始发行具备更多防伪功能的二代身份证；
- 最新修订的《中华人民共和国居民身份证法》明确了以下事项：
  - 身份证需登记的身份基本属性信息；
  - 要求登记指纹信息，增强身份识别的准确性；
  - 对于居民身份证记载的公民个人信息，应当予以保密。

1.3. 数字身份概要

数字身份是实体社会中的自然人身份在数字空间的映射。

对于数字身份的概念，争议颇多，但普遍认为数字身份主要用于在提供数字服务时识别用户身份。我们认为数字身份是能代表主体身份属性特征集合的标记。数字身份在一定范围内用于唯一标记该主体，并将之与其他主体区分。

鉴于数字身份具有高度识别性，且与主体的网络行为密切相关，因此，数字身份所代表的主体属性特征可能含有高度敏感的个人信息，在数字身份的注册登记和使用中必须始终考虑个人信息安全，将保障个人信息安全作为数字身份服务中关键的影响因素。

1.4. 数字身份的可识别性

身份及其识别的效力取决于身份注册登记的范围。正如“张三”在某单位具有唯一性，但是在整个中国范围内就失去了身份识别的意义。因此，身份可识别性的能力或程度与身份登记管理所服务和管理的范围密切相关。

解放后，我国延续了民国人口管理的户籍制度，直到八十年代改革开放初期，因大规模人口流动产生的管理和服务需求，开始了全国公民身份的登记管理。根据《居民身份证法》的规定 ，“**公民身份号码是每个公民唯一的、终身不变的身份代码，由公安机关按照公民身份号码国家标准编制。**”由此，公民身份号码在全国范围内确立了唯一区分身份的基础法律地位。

在网络空间，数字身份同样具有唯一性特征，其作用是要在一定范围内识别某一主体，使之与其他主体区分开来。

我国网络发展至今，一直延用了物理空间的公民身份号码作为线上公民数字身份的区分职能。但是，由于公民身份号码隐含了个人户籍所在地、出生日期、性别等个人信息，在开放的互联网上直接使用公民身份号码，无疑会对个人信息安全带来极大的隐患和危害。再则，利用大数据技术非常容易针对某个被指定了唯一公民身份号码的数据主体进行跨域数据汇集和精准画像。这一结果对于绝大多数的数据主体来说并不乐于接受。

1.5. 我国数字身份发展的突出需求

我国接入全球互联网已二十多年，国内的数字身份建设因种种原因始终未得到应有的重视。多年来的实践反复证明，仅仅使用姓名+公民身份号码代表公民的线上身份，造成了大量的个人信息泄露。大数据画像也引发了身份登记管理唯一性的要求与防止大数据技术追踪以及保护个人信息的需求之间的矛盾。此外，与线下环境身份认证方式（身份证要求本人出示，由核验方查实证件真伪及判断是否“人证合一”）不同的是，在线上填写公民身份号码既无法验证身份的真伪、也难以证明是出自本人意愿。

线上身份冒用以及电信和网络精准诈骗等诸多案件告诉我们，仅仅依靠个人信息进行数字身份建设会带来诸多安全风险。作为个人信息的重要代表，公民身份号码不宜直接作为数字身份来使用：它只起到了唯一区分的作用，而无法对个人信息进行保护。因此，结合我国现有身份管理的成就以及网络社会个人信息保护的现实需求，有必要以公民身份号码为根（唯一性），建设既能保护个人信息安全又能适应网络社会数据开放和流通需求的统一数字身份体系。

1.6. 数字身份的认证

如何认证数字身份，既是一个技术问题也是一个法律问题。技术上，目前通用的数字身份认证技术有许多，例如，基于口令的认证方式，OTP（One Time Password）和银行 U 盾的认证技术等。世界各国基于各自的电子签名相关法律推广可靠的数字身份认证，大多采用基于 PKI 的数字签名技术。

我国在 2004 年 8 月 28 日通过的《电子签名法》从法律上提供了数字身份识别的法律基础。该法第二条规定“本法所称电子签名，是指数据电文中以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容的数据”，但是电子签名法在数字身份方面并未有深入。

2. eID 数字身份定义

2.1. eID 数字身份相关主体

2.1.1. eID 数字身份签发机构

eID 数字身份签发机构是指公安部第三研究所承建的“公安部公民网络身份识别系统”，唯一负责管理 eID 数字身份体系，并签发“公安部公民网络电子身份标识（eID）”。

2.1.2. eID 数字身份凭证提供机构（Credential Service Provider，CSP）

eID 数字身份凭证提供机构是依据 eID 数字身份签发机构签发的 eID 数字身份，面向用户颁发 eID 数字身份凭证的机构。CSP 负责 eID 数字身份凭证的管理和认证器的全生命周期管理，并对 eID 数字身份提供认证服务。

2.1.3. eID 数字身份注册登记机构（Register Agent，RA）

eID 数字身份注册登记机构是对 eID 数字身份申请人进行身份证实，为其注册登记 eID 数字身份，提供 eID 数字身份凭证并绑定 eID 数字认证器的机构。RA 还对 eID 数字身份凭证和认证器提供全生命周期的服务。RA 可以由 CSP 自行担任或委托其它机构担任。

2.1.4. eID 数字身份凭证认证机构（Credential Authentication Agent，CAA）

eID 数字身份凭证认证机构是就 CSP 已颁发的数字身份凭证，基于 CSP 的授权和许可，提供数字身份认证服务的机构。CAA 可以由 CSP 自行担任或委托其它机构担任。

2.1.5. eID 数字身份依赖机构（Relying Party，RP）

eID 数字身份依赖机构是具体应用 eID 数字身份，并基于对 CAA 认证结果的信赖提供数字服务的机构。

2.1.6. 申请人

申请人是向 eID 数字身份注册登记机构申请 eID 数字身份凭证的主体。

2.1.7. 注册用户

申请人经过 RA 的身份证实并取得 eID 数字身份凭证和认证器后，即成为拥有 eID 数字身份的 CSP 注册用户。

2.1.8. 声明人

声明人（或称发起认证的请求人）是在进行 eID 数字身份认证时，声称具有 eID 数字身份凭证所指向身份的主体。声明人有可能与注册用户不一致。

2.1.9. 用户

白皮书中的用户包含申请人、注册用户、声明人。

2.2. eID 数字身份基本概念

2.2.1. eID 数字身份

eID 数字身份是以公民身份号码为根，由“公安部公民网络身份识别系统”基于密码算法统一为中国公民生成的数字标记。

eID 数字身份既可以保证签发给每个公民的数字标记的唯一识别性，又可以减少公民身份明文信息在互联网上的传播，又可以实现不同应用中公民 eID 数字身份有条件的互通。

eID 数字身份是实体社会中自然人身份在数字空间的映射，是自然人在数字空间获取数字服务时代表其主体身份的数字标记的集合。

eID 数字身份由唯一的公民 eID 数字身份和用户 eID 数字身份组成。对应公民个人在不同的数字服务机构中的用户 eID 数字身份是不同的，但在某一数字服务机构中是唯一的。用户 eID 数字身份既可以在某一数字服务机构唯一区分某一用户，又可防止该用户在不同数字服务机构中的个人信息被串联、追踪、汇集和画像。

2.2.2. 认证因子（Authentication Factor）

认证因子是用于认证身份的某种因子，主要分为三类：你所知道的认证因子（What you know），你所拥有的认证因子（What you have）和你所与生俱来的认证因子（What you are）。认证因子及其组合多用作 eID 数字身份认证器。

你所与生俱来的认证因子（What you are）包括生理特征（例如面部、声纹、指纹、虹膜等）的测量和行为特征（例如笔迹、步态、唇语、打字节奏等）的测量。这两类都被认为是生物识别，具有不可撤销性，如果在网上被不安全应用，会带来被泄露及被冒用的风险，在用于认证时须有限制地使用。

2.2.3. eID 数字身份认证器（Authenticator）

eID 数字身份认证器，是由声明人拥有和控制的，在认证 eID 数字身份时用于核验声明人与 eID 数字身份凭证所指向身份主体一致性的工具。

认证器可以视为一种认证因子或者多种认证因子的组合，声明人通过其持有的

认证器向 CAA 请求认证身份。例如声明人可以通过使用加载 eID 的金融 IC 卡或 SIM 卡并输入口令向 CAA 证明其拥有并能控制上述认证器，以此来进行身份认证。虽然注册用户拥有 eID 数字身份认证器，但是认证器的有效性由 CSP 管理。

2.2.4. eID 数字身份凭证

eID 数字身份凭证，是指出于身份认证的目的、由 CSP 面向注册用户提供的、与注册用户认证器关联的一系列数据。基于 eID 数字身份凭证，RP 可以向 CAA 请求认证注册用户的身份。

2.2.5. eID 数字身份认证

eID 数字身份认证是由 CSP 提供的数字身份认证。CSP 基于 eID 数字身份注册登记时向注册用户颁发的 eID 数字身份凭证和 eID 数字身份认证器，在声明人凭其所控制的认证器进行数字身份认证请求时，向 RP 发出声明人与注册用户一致或不一致的断言，以便于 RP 判断是否向声明人提供相应的数字服务。

2.2.6. eID 数字身份凭证颁发等级（Credential Issuance Level，CIL）

为确定某个申请人是 eID 数字身份所声明身份的可靠性，CSP 在颁发 eID 数字身份凭证时会采取特定的流程以保证申请人与 eID 数字身份所声明身份的一致性。不同 eID 数字身份凭证颁发等级代表的 eID 数字身份风险也各自不同。例如，经过现场面签而颁发的 eID 数字身份凭证与在线认证颁发的 eID 数字身份凭证，前者发生身份冒用的风险低且易追责。白皮书中对 eID 数字身份凭证颁发流程进行分级，不同的 RP 应对自己提供的数字服务进行评估，进而决定采用何种 eID 数字身份凭证颁发等级的 eID 数字身份凭证。

2.2.7. eID 数字身份凭证认证等级（Authentication Assurance Level，AAL）

eID 数字身份凭证认证等级是指 eID 数字身份认证过程中的声明人与 eID 数字

身份凭证所述身份之间的一致性的可靠性等级。不同的认证方式以及认证过程中所采取的措施会直接影响到 eID 数字身份认证结果的可靠性，对于 eID 数字身份认证结果可靠性要求高的 RP 必然要求使用可靠性更高的 eID 数字身份凭证认证过程。因此，对 eID 数字身份凭证认证过程的可靠性进行分级对于 RP 具体应用 eID 数字身份具有重要意义。

3. eID 数字身份服务原则

3.1. 用户自愿原则

应允许用户选择是否申请 eID 数字身份凭证或使用 eID 数字身份凭证进行身份识别或认证。

3.2. 个人信息保护原则

eID 数字身份应用于互联网环境，能识别网络行为主体并获取到个人敏感信息，并且在应用中会逐渐积累起与之关联的大量个人信息。收集、使用、流通此类个人信息必须在法律要求的范围内进行，因此，eID 数字身份应当将个人信息安全作为贯彻全程的首要考虑因素，不得侵犯个人信息主体的生活安宁、财产和人身安全。

3.3. 个人信息收集最小化原则

对个人信息的收集应该遵循最小化原则、适当性原则，并与所提供的服务相匹配，不得收集服务所需以外的、不必要的个人信息，用户应该能够对其被收集的个人信息进行控制。

3.4. 便利和互操作原则

相关机构应注重用户体验及用户便利性，如服务响应速度、操作便捷性及应用间切换流畅度等。

CSP 依据统一的 eID 数字身份颁发 eID 数字身份凭证，因此，即使是不同 CSP 颁发的 eID 数字身份凭证也能实现 eID 数字身份的唯一识别性，鼓励不同 CSP 之

间积极采取措施进行 eID 数字身份认证的互通。

3.5. 充分告知原则

eID 数字身份对于自然人主体而言并不易于理解。因此，相关机构在进行与 eID 数字身份有关业务的操作时，应尽量用易于理解的语言向有关主体做出充分的信息披露，应保证有关主体能充分了解所进行的与 eID 数字身份有关的操作，并在需要有关主体进行涉及具体权利、义务、责任的操作时予以充分的提醒。

3.6. 风险控制原则

eID 数字身份依据其注册登记、签发、认证、应用的流程以及具体应用的场景，都会存在不同程度的风险，其中主要风险是面临个人信息泄露、身份被冒用和账户被盗用等。在提供 eID 数字身份服务以及具体应用 eID 数字身份的过程中，有关机构应根据具体情况评估相应的风险因素，并预先做出控制。

4. eID 数字身份特点

eID 数字身份有以下特点：

- eID 数字身份以公民身份号码为根生成；
- eID 数字身份基于密码算法产生，从 eID 数字身份无法逆推出公民身份号码原文；
- eID 数字身份采用碎片化方法生成：对于不同的 CSP，同一注册用户的 eID 数字身份并不相同；对于同一 CSP 的不同 RP，同一注册用户的 eID 数字身份也不相同；
- eID 数字身份由“公安部公民网络身份识别系统”统一管理，碎片化处理后的 eID 数字身份在“公安部公民网络身份识别系统”内可实现与公民身份号码的关联。

为保护个人信息，我国不仅在 2015 年《中华人民共和国刑法修正案（九）》中明确了对于侵犯公民信息罪的定罪量刑标准，也在 2017 年通过的《中华人民共和国民法总则》中明确了自然人的个人信息受法律保护。《中华人民共和国网络安全

法》作为网络安全方面的专门法，在第二十四条规定“国家实施网络可信身份战略，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认”，第四十二条规定“网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告”。eID 数字身份不仅可以将公民身份信息转化为特定的不具备识别性的碎片化的个人标记，有效减少公民的身份信息在互联网上的传播，从而最大化的保护个人信息，还可基于 eID 数字身份的统一管理框架，在“公安部公民网络身份识别系统”将碎片化处理后的个人标记与公民身份号码进行关联，实现不同数字身份认证之间的互通。

eID 数字身份不仅可用于线上的身份识别和个人信息保护，在线下也有丰富的应用场景。例如在某些安防领域，无需出示身份证件，eID 数字身份的注册用户也能通过与国家权威身份信息源安全连接的身份核验设备完成身份核验。

5. eID 数字身份模型简述

eID 数字身份模型中的主体间逻辑关系如下图所示：

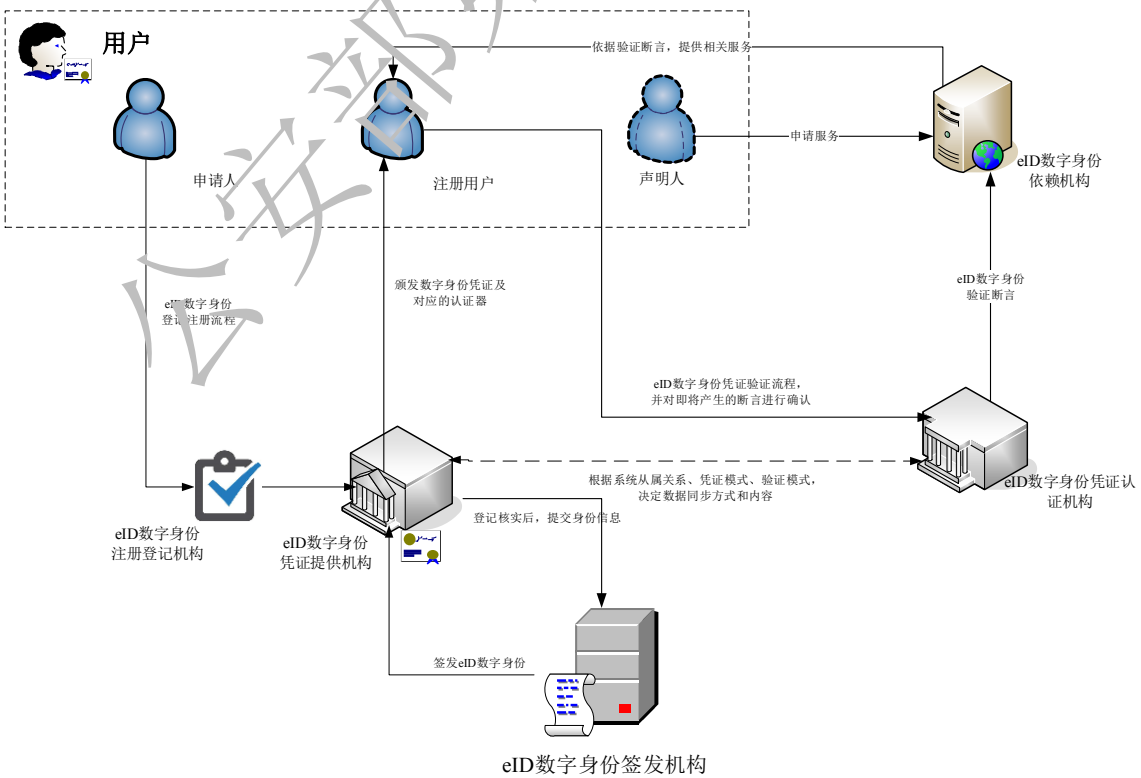

图 5-1 eID 数字身份模型

eID 数字身份模型可以分为两个部分：申请人注册登记和声明人认证。其中申请人注册登记包括以下步骤：

- 申请人向 eID 数字身份注册登记机构（RA）申请 eID 数字身份凭证提供机构（CSP）的 eID 数字身份凭证；
- eID 数字身份注册登记机构（RA）完成对申请人的实体身份证实后，申请人成为 eID 数字身份凭证提供机构（CSP）的注册用户；
- eID 数字身份注册登记机构（RA）向 eID 数字身份凭证提供机构（CSP）为注册用户申请 eID 数字身份、eID 数字身份凭证和 eID 数字身份认证器，并向注册用户进行颁发。由 eID 数字身份凭证提供机构（CSP）负责维护注册用户 eID 数字身份凭证的生命周期并收集相关信息，由注册用户保管和维护自己的 eID 数字身份认证器。

声明人认证包括以下步骤：

- 声明人通过认证协议向 eID 数字身份凭证认证机构（CAA）证明其对 eID 数字身份认证器的掌控；
- eID 数字身份凭证认证机构（CAA）向 eID 数字身份凭证提供机构（CSP）核实与声明人的 eID 数字身份认证器相关联的 eID 数字身份凭证，并从 eID 数字身份凭证提供机构（CSP）获得声明人的身份信息；
- eID 数字身份凭证认证机构（CAA）向 eID 数字身份依赖机构（RP）提供身份认证断言，eID 数字身份依赖机构（RP）根据该断言对注册用户进行服务访问授权；
- 声明人从 eID 数字身份依赖机构（RP）获取认证授权的服务。

eID 数字身份模型中主体交互的关键两个步骤是 eID 数字身份注册登记机构（RA）对申请人实体身份的证明以及 eID 数字身份凭证认证机构（CAA）对声明人的认证。根据风险管理的需求，在申请人实体身份证实和声明人身份认证阶段必须采用一定的技术措施和策略去消除某种程度的风险。因此，根据要消除的风险程度可以为实体身份证实和 eID 数字身份凭证认证分别划分不同的等级以满足风险管理需要。

eID 数字身份签发机构通过“五位一体”的 eID 服务体系对外提供 eID 数字身

份及其服务，eID 服务体系具体内容见 eID 官网（www.eid. cn）介绍。

6. eID 数字身份服务流程

6.1. eID 数字身份的签发

eID 数字身份签发机构根据 CSP 提供的申请人姓名和公民身份号码签发 eID 数字身份。

6.2. eID 数字身份的注册登记

eID 数字身份是在线操作行为主体身份的标记。eID 数字身份在正式签发之前必须完成对于申请人的身份证实。

6.2.1. 身份证实

身份证实流程可以分为三个基本环节: 身份区分、身份证明真实性的核验以及人证合一认证。因此，身份证实的预期结果可以分成如下几个层次：

- 在某项数字服务的注册用户群体内，将已声明的身份确定为单个、唯一的身份；
- 确认所有提供的证明是正确和真实的（例如，不是伪造或盗用的）；
- 确认所声称的身份与提供身份证明的真实主体相一致。

在完成身份证实之后，申请人即成为注册用户，RA 代表 CSP 向注册用户颁发 eID 数字身份凭证和认证器，由 CSP 维护注册用户 eID 数字身份凭证的生命周期并收集相关信息，由注册用户保管和维护自己的 eID 数字身份认证器。

6.2.1.1. 身份区分

身份区分的目标是在一个给定的人群或背景下唯一区分每一个人。eID 数字身份能对拥有中华人民共和国公民身份号码的公民进行唯一性的区分。它为 eID 数字身份体系的整体身份证实过程提供了一个重要的起点。

6.2.1.2. 身份证明的核验

身份证明的核验目的是从申请人那里收集最合适的身份证明（如身份证或其它 eID 数字身份凭证），并确定其真实性、有效性和准确性。

6.2.1.3. 人证合一认证

人证合一认证的目标是确认和建立声称的身份与提供证明的真实主体之间的联系。eID 数字身份在进行身份证实过程中，需要证明申请人与身份证明所列身份主体的一致性。

6.2.2. 到场

到场指的是申请人本人亲自到达指定场所完成身份证实的过程。指定场所一般是 RA 的营业场所，具备一定的安防监控条件，到场的身份证实相对于非到场的身份证实风险控制更为严格且能保留更多的身份证实记录，能更有效地减少身份冒用风险或者对冒用者进行责任追溯。

6.2.3. 面签

基于风控要求或法律要求，颁发较高等级的 eID 数字身份凭证时要求面签。面签是由专人对于申请人进行面对面的身份核验，分为受监督的面对面互动和受监督的远程互动两种。进行面签操作的业务员须查看申请人的生物特征（例如手指、脸部等）是否存在非天然材料，并确保生物特征数据是从申请者那里收集的，而不是另一个主体。

受监督的远程面签还须满足以下两个要求：

- RA 须保证整个身份证实过程处于监控之中，过程中申请人不得离开；
- RA 须保证至少有一个现场业务员与申请人远程参加整个身份证实过程。

6.3. eID 数字身份的认证

eID 数字身份认证过程主要由 RP、CAA 以及数字身份声明人参与。

基于认证因子的不同，认证过程会分为单因子认证和多重因子认证。一般认为，采用的认证因子越多，身份认证的结果就越可靠。

6.3.1. 认证过程

认证过程开始于声明人通过身份认证协议向 CAA 证明，声明人拥有和控制其所声称的 eID 数字身份所绑定的 eID 数字身份认证器。一旦证明声明人对 eID 数字身份认证器的拥有和控制，即表明通过对 eID 数字身份凭证的认证完成了对 eID 数字身份的认证。

6.3.2. eID 数字身份凭证生命周期管理

发生在注册用户 eID 数字身份凭证生命周期里的一系列事件影响着 eID 数字身份凭证和认证器的使用。本部分内容描述了针对这些事件采取的处理措施。

6.3.2.1. 绑定

绑定是指在注册用户的 eID 数字身份凭证与认证器之间建立关联关系，使认证器可用于 eID 数字身份认证。eID 数字身份认证时可使用多个认证器。

6.3.2.1.1. 注册登记时绑定

在颁发 eID 数字身份凭证时，CSP 通过 RA 会将特定的认证器与注册用户的 eID 数字身份凭证相绑定。

6.3.2.1.2. 注册登记后的绑定

注册登记后认证器与 eID 数字身份凭证的绑定可能包括以下情况：

- 现有 eID 数字身份凭证绑定新的认证器，新的认证器有可能提升 eID 数字身份凭证的认证等级；
- 现有认证器中增加新的认证因子，新增加的认证因子有可能提升 eID 数字

身份凭证的认证等级。

6.3.2.1.3. 挂失及补办

eID 数字身份认证器有可能丢失、被盗或被他人不当占有，此时注册用户可要求 RA 对原有的 eID 数字身份凭证进行挂失，并通过补办业务绑定新的 eID 数字身份认证器与 eID 数字身份凭证。

6.3.2.1.4. 重置

注册用户有可能遗忘 eID 数字身份认证器的口令，无法完成对 eID 数字身份凭证的认证，此时注册用户可要求 RA 重置认证器而无需改变 eID 数字身份凭证。

6.3.2.2. 过期

一旦 eID 数字身份凭证到期，将不再具有 eID 数字身份认证的功能。

6.3.2.3. 更新

当现有 eID 数字身份凭证在过期前进行更新时，其有效期将根据 CSP 的生命周期管理政策进行相应延长。

6.3.2.4. 注销

注册用户可以主动要求注销 eID 数字身份凭证。

当 eID 数字身份认证器被采取措施停止使用（包括但不限于销毁、废止、收回等）时，eID 数字身份凭证应被注销。

7. eID 数字身份凭证颁发等级（Credential Issue Level, CIL）

eID 数字身份凭证颁发等级意味着注册用户与 eID 数字身份凭证所声明身份一致的可靠程度。基于 eID 数字身份凭证的颁发流程，不同的 eID 数字身份凭证可能代表不同的身份可靠程度。eID 数字身份凭证的目的是保证申请人是他们所声称的身份，从风险控制角度，eID 数字身份业务流程中的各个机构应根据 eID 数字身份

凭证颁发等级的不同，而采取不同的风险处理措施。且这个颁发可靠程度需要达到规定等级，即 eID 数字身份凭证颁发等级（CIL）。根据监管或者提供服务的需要，CSP 可以选择不同的颁发等级。下文列出了对 CSP 在颁发 eID 数字身份凭证时的通用要求以及不同 CIL 的 eID 数字身份凭证颁发要求。

7.1. 通用要求

对于管理 eID 数字身份凭证的 CSP 和 RA 而言：

- 颁发 eID 数字身份凭证时所依据的公民身份信息**必须**真实存在
- 颁发 eID 数字身份凭证时**必须**留存申请人有效的联系方式
- 收集用以身份证明的个人信息**必须**遵循最小化原则。
- 收集个人信息时**必须**明确通知申请人信息收集的目的和保存身份属性对于身份证实的必要性，包括这些属性在完成身份证实过程中是自愿提供还是强制性的，以及不提供属性的后果。
- 除了提供服务或者因司法程序需要，**不得**在未经用户同意的情况下将收集和保存的身份属性用作其它用途，且除非必要情况**不得**把同意授权作为为用户提供服务的前置条件。
- **必须**建立投诉解决机制。
- **必须**妥善保护注册过程中收集的所有个人信息，并注明信息来源。
- 整个证明流程**必须**在安全连接的受保护通道上进行。
- 如果停止进行 eID 数字身份有关服务，**必须**妥善处理或销毁所有敏感数据。

7.2. eID 数字身份凭证颁发等级 1（CIL1）

注册登记 CIL1 的 eID 数字身份凭证时，CSP 必须确保身份信息真实存在，并留存有效的联系方式。如果用户同意，只要求 CIL1 凭证的 RP 应当接受 CIL2 及以上等级的 eID 数字身份凭证。

7.3. eID 数字身份凭证颁发等级 2（CIL2）

在 CIL2 中，CSP 要求用户提供一定强度等级的身份证明，并对身份证明进行

确认和核验。

以下部分是 CIL2 在注册登记环节的具体要求。

7.3.1. CIL2 身份证明收集要求

CSP 须从申请人那里收集身份证明以确定申请人身份；身份证明是法律法规中要求的身份证件或更高 CIL 级别的 eID 数字身份凭证。

7.3.2. CIL2 身份证明确认要求

CSP 在对身份证明进行确认时，必须确保身份证明所列信息真实存在，且对身份证明的真实有效性采取了核验措施。

7.3.3. CIL2 联系方式确认

用户绑定认证器之前，CSP 必须通过申请人所持有的、经之前线下面签核验身份后存留的已知联系方式（例如手机号码、电子邮箱或住址等）取得确认，但此种方式应设定一定时效。

7.4. eID 数字身份凭证颁发等级 3（CIL3）

以下部分是 CIL3 在注册登记环节的具体要求。

7.4.1. CIL3 身份证明收集要求

CSP 须从申请人那里收集身份证明以确定申请人身份；身份证明是法律法规中要求的身份证件或更高 CIL 级别的 eID 数字身份凭证（同 CIL2）。

7.4.2. CIL3 身份证明确认要求

CSP 在对身份证明进行确认时，须确保身份证明所列信息为真实存在，且对身份证明的真实有效性采取了**可靠的**核验措施，例如使用专用的身份证明验证设备辅

助。

7.4.3. CIL3 联系方式确认

用户绑定认证器之前，CSP 必须通过申请人所持有的、经之前线下面签核验身份后存留的已知联系方式（例如电话手机号码、电子邮箱或住址等）取得确认，但此种方式应设定一定时效。

7.4.4. CIL3 人证合一认证要求

申请人持之前线下面签核验身份后办理的、与公民身份信息相关的认证器在线下指定场所进行身份核验，CSP 依据核验结果签发凭证。

7.4.5. CIL3 到场要求

应要求申请人亲自到 CSP 指定场所完成身份核验。

7.5. eID 数字身份凭证颁发等级 4（CIL4）

以下部分是 CIL4 在注册登记环节的具体要求。

7.5.1. CIL4 身份证明收集要求

CSP 须从申请人那里收集身份证明以确定申请人身份；身份证明应是法律法规中要求的身份证件。

7.5.2. CIL4 身份证明确认要求

CSP 在对身份证明进行确认时，须确保身份证明所列信息为真实存在，且对身份证明的真实有效性采取了**可靠的**核验措施，例如使用专用的身份证明验证设备辅助（同 CIL3）。

7.5.3. CIL4 联系方式确认

用户绑定认证器之前，CSP 必须通过申请人所持有的、经之前线下面签核验身份后存留的已知联系方式（例如手机号码、电子邮箱或住址等）取得确认，但此种方式应设定一定时效。

7.5.4. CIL4 人证合一认证要求

CSP 基于申请人凭有效身份证件到场面签的结果进行人证合一认证，面签方式应当符合白皮书 6.2.3 的要求。

7.5.5. CIL4 到场要求

注册登记 CIL4 的 eID 数字身份凭证时，申请人必须亲自到 CSP 指定场所完成身份核验。

7.5.6. CIL4 颁发记录留存要求

留下核验过程的影像、申请人照片及本人签名以防抵赖并便于追溯。

8. eID 数字身份认证等级（Authentication Assurance Level, AAL）

成功的身份认证可以向 RP 提供合理的风险防护，即提供了请求数字服务的声明人拥有并控制颁发给注册用户的认证器的可靠性保证。eID 数字身份凭证认证等级（AAL） 分类描述了这种可靠性保证的可信度。

RP 可以根据风险状况，以及攻击者控制认证机构和访问机构系统造成的潜在危害，选择三种等级的 AAL 选项。这三种 AAL 的等级衡量了身份认证过程的强度。

8.1. eID 数字身份凭证认证等级 1（AAL1）

AAL1 为声明人拥有并控制颁发给注册用户的认证器的可靠性提供了一些保证。AAL1 需要使用广泛的可用身份认证技术进行单因子身份认证。成功的身份认证要求声明人通过安全的认证协议证明对认证器的拥有和控制。

8.1.1. AAL1 允许的认证器类型

可使用以下类型的认证器：

- 用户记忆的口令
- 查找密码表
- 带外设备（“带外设备”是指使用独立认证通道的设备，相对应地，“带内设备”是指共享请求认证通道的设备）
- 单因子一次性密码（OTP）设备
- 多因子一次性密码设备
- 单因子密码软件
- 单因子密码设备
- 多因子密码软件
- 多因子密码设备

8.1.2. AAL1 要求的安全控制措施

在适用的情况下，在操作系统中运行的、基于软件的认证器应该尝试检测用户端的风险（例如是否存在恶意软件），并且当检测到这样的危害时不应该继续运行。

声明人和校验设备（使用带外认证器的主要通道，例如，桌面终端发起验证，通过手机短信确认）之间的通信必须经由安全连接的受保护通道进行，以确保认证器输出的机密性并防御中间人攻击。

RP 应在有限时间内依据用户所持有认证器的认证结果提供服务。如果用户长时间不活动，或者超出了认证有限期，RP 需要对用户重新认证或者停止提供服务。

8.2. eID 数字身份凭证认证等级 2（AAL2）

AAL2 为注册用户声明人拥有并控制了颁发给注册用户的认证器的可靠性提供了较高的保证。通过安全的身份认证协议，需要两个不同的身份认证因子的持有和控制证明。AAL2 及以上等级需要使用经认可的的密码技术。

8.2.1. AAL2 允许的认证器类型

当使用多因子认证器时，可以使用以下任何一种认证器：

- 多因子 OTP 设备
- 多因子密码软件
- 多因子密码设备

当使用两个单因子认证器的组合时，它必须包括一个口令和一个认证器（基于所有物，即“你所拥有的”），如下所示：

- 查找密码表
- 带外设备
- 单因子 OTP 设备
- 单因子密码软件
- 单因子密码设备

8.2.2. AAL2 要求的安全控制措施

- 在适用的情况下，在操作系统中运行的、基于软件的认证器应该尝试检测用户端危害（例如，通过恶意软件），并且当检测到这样的危害时不应该继续运行。至少有一个 AAL2 使用的认证器必须具有防止重放的特性。AAL2 认证必须至少从一个认证器证明认证意图。
- 声明人和认证器之间的通信（在有带外认证器的情况下是主要通道）必须经由安全连接的受保护通道进行，以确保认证器输出的机密性并防御中间人攻击。
- 当在认证过程中使用智能手机等设备时，对该设备的解锁（通常使用 PIN 码或生物特征建模后本地比对）不得被作为认证因子之一。一般来说，认

证方不可能知道设备已被锁定，或者解锁过程是否符合相关认证器类型的要求。

- RP 应在有限时间内依据用户所持有认证器的认证结果提供服务。如果用户长时间不活动，或者超出了认证有限期，RP 需要对用户重新认证或者停止提供服务。

8.3. eID 数字身份凭证认证等级 3（AAL3）

AAL3 为声明人拥有并控制了颁发给注册用户的认证器的可靠性提供了非常高的保证。AAL3 的认证基于拥有密码协议的密钥。AAL3 类似于 AAL2，但是需要 “基于硬件的、不可复制的”密码认证器来提供对抗身份冒用的能力。为了在 AAL3 进行认证，声明人应通过安全认证协议证明拥有和控制两种不同的认证因子。其中，经过认可的密码技术是一个必需的条件。

8.3.1. AAL3 允许的认证器类型

AAL3 认证必须使用认证器组合中的一种进行。可能的组合是：

- 多因子密码设备
- 与口令一起使用的单因子密码设备
- 与单因子密码设备一起使用的多因子 OTP 设备（软件或硬件）
- 与单因子密码软件一起使用的多因子 OTP 设备（仅限硬件）
- 与多因子密码软件一起使用的单因子 OTP 设备（仅限硬件）
- 与单因子密码软件和口令一起使用的单因子 OTP 设备（仅硬件）

8.3.2. AAL3 要求的安全控制措施

- 声明人与认证器之间的通信必须经由安全连接的受保护通道进行，以确保认证器输出的机密性并抵抗中间人攻击。AAL3 中使用的所有认证器必须具有防止身份冒用的特性，以及防止重放的特性。AAL3 的所有认证和重新认证过程都必须至少从一个认证器展示认证意图。
- AAL3 认证器必须对至少一个认证因子满足防止危害的特性。AAL3 中的

基于硬件的认证器和认证方应该可以抵制相关的旁路攻击（例如定时和功耗分析）。相关的旁路攻击必须由认证方进行风险评估确定。

- 当在认证过程中使用智能手机等设备时，对该设备的解锁不得被作为认证因子之一。一般来说，认证方不可能知道设备已被锁定，或者解锁过程是否符合相关认证器类型的要求。
- RP 应在有限时间内依据用户所持有认证器的认证结果提供服务。如果用户长时间不活动，或者超出了认证有限期，RP 需要对用户重新认证或者停止提供服务。

9. eID 数字身份与个人信息安全

9.1. 个人信息的收集

各有关机构须在收集用户个人信息时，明确通知用户收集信息的目的和保存身份信息对于证明身份的必要性，包括这些信息在完成身份证实过程中是自愿提供还是强制性的，以及不提供信息的后果。注册登记过程中收集的所有个人信息都须得到妥善保护，以确保其机密性、完整性，并注明信息来源。即使在需要全面识别的情况下，也尽可能限制所收集个人信息的数量。

9.2. 个人信息的使用

需使用加密或专有方法保护个人信息，或者同时使用上述两种方法，并且这些方法可以确保个人信息的完整性。

9.3. 个人信息的存储

个人信息的存储除了便于提供 eID 数字身份服务的考虑外，更应注意个人信息的存储安全，是否有可能泄露或被人不当取得。

9.4. 个人信息的管理

CSP 须保存管理记录，该记录包括了审计日志、申请人身份核验及声明人身份

认证的所有步骤，以及证明过程所用的身份证明类型。CSP 须实施风险管理流程，包括确定对隐私和安全风险的评估。

9.5. 个人信息的流通

确需向第三方提供个人信息时，转让方还应：

- 取得信息主体的同意或对个人信息进行处理使其无法识别特定个人且不能复原；
- 通过合同等法律文书明确双方的安全责任；
- 确保受让方的安全措施不低于转让方的安全措施；
- 采用安全措施确保个人信息以安全的方式转让给受让方；
- 准确记录和保存个人信息的转让情况，包括转让日期、规模、目的、受让方的名称等；
- 受让方发生个人信息安全事件对个人信息主体造成损害时，转让方有责任帮助个人信息主体追究受让方责任，或给予个人信息主体适当赔偿；
- 帮助个人信息主体了解受让方对个人信息的存储、使用等情况，包括个人信息主体的权利，例如访问、更正、删除、注销账户等；
- 个人信息主体请求删除其个人信息时，转让方应同时通知受让方及时删除；
- 当个人信息控制者被第三方收购、兼并、重组或发生其他控制权变更情况后，新的个人信息控制者应继续履行原个人信息控制者的责任和义务,变更个人信息使用目的时，应重新取得个人信息主体的明示同意。