

目录

BSN实名DID服务帮助手册	1.1
第一章 BSN实名DID服务简介	1.1.1
(一) BSN个人数据实名确权服务	1.1.1.1
(二) BSN个人数据加密流转服务	1.1.1.2
(三) BSN个人隐私保护登录服务	1.1.1.3
(四) BSN自定义业务实名DID服务	1.1.1.4
(五) BSN官方个人身份证明凭证服务	1.1.1.5
(六) BSN官方个人信息信息凭证服务	1.1.1.6
(七) BSN自定义业务个人身份凭证服务	1.1.1.7
第二章 快速接入指南	1.1.2
第三章 套餐定价	1.1.3
第四章 联系我们	1.1.4

BSN实名DID服务帮助手册

version 1.1.1

修订时间：2024-3

[PDF版本下载](#)

BSN实名DID服务	区块链服务网络	BSN延安链
------------	---------	--------

Copyright 北京红枣科技有限公司

第一章 BSN实名DID服务简介

为服务国家战略，抢占区块链技术制高点，2018年，国家信息中心牵头研发和顶层设计，并联合中国移动、中国银联、北京红枣科技等单位共同发起建立了区块链底层公共基础设施——区块链服务网络（BSN）。五年来，BSN围绕关键技术开展研发和攻关，为分布式技术发展和下一代互联网构建提供了高质量的技术支撑平台和可扩展的基础设施服务，在促进技术创新、构建商业化平台并持续推动产业化应用、引领行业发展，以及开拓海外市场等方面取得了令人瞩目的成就。

2016年由国家发展改革委批准，在公安部指导下公安部第一研究所建设了国家“互联网+”行动计划重大保障支撑工程，暨“互联网+可信身份认证平台”（CTID平台），面向全社会各行各业提供“权威、安全、可信、便捷”的统一网络身份认证服务，在政务民生、交通出行、医疗健康、金融服务、数字通信等多个领域发挥了巨大作用。

从2022年底开始，BSN发展联盟联合中盾安信（厦门）、中国移动设计院等单位针对充分融合BSN区块链服务网络和CTID数字身份链两大基础设施，拓展CTID平台的中心化身份认证能力，使其同时具备分布式身份认证能力进行了探讨。经过一年的设计、研发，几家单位即将正式推出BSN实名DID服务。

在技术实现上，BSN实名DID服务由中盾安信在BSN公网的延安链上部署并管理实名DID智能合约，任何业务方采集到用户的真实身份信息（“身份证+姓名”或“身份证+姓名+面部识别”），即可通过该服务向中盾安信运营的身份链平台发送请求，经过CTID平台的身份核验后，即由中盾安信在BSN延安链上签发用户的BSN个人实名DID，并为业务方提供DID管理和更新、身份证明凭证等服务。

基于BSN实名DID服务，可以构建起多元化的实名认证体系，满足“前台匿名、后台实名”的管理要求，作为对目前中心化的身份认证体系强有力的补充，满足各种业务、各种场景的需要，并对个人数据管理体系产生重大影响，在推动数据要素合规高效、安全有序流通，提高数据要素管理水平，激活数据要素潜能等方面发挥出重要作用，为国家数据基础设施建设奠定坚实的基础。

目前，已经有民生银行、太平洋保险、中移动互联网公司、河南广电、国家卫健委等多家大型企业和政府机构参与到BSN实名DID服务的前期测试。该服务的几家发起单位也设计出了多个应用场景，这些应用场景与国家当前着力推行的释放数据要素价值、保护个人隐私、助力数字经济高质量发展战略高度一致，具体包括：

（一）BSN个人数据实名确权服务

任何软件、网站或APP等互联网应用都可以为其个人用户生成业务公私钥对（私钥可以进行托管，也可以由个人用户自行保管）。个人用户产生任何数据集时，该应用都可以为数据集生成哈希，并使用用户私钥进行签名，再通过BSN实名DID服务，经过CTID平台对个人用户的身份证、姓名、人脸等身份信息进行验证后，将用户公钥写入延安链上的BSN官方实名DID文档，并将数据集哈希、签名值、DID标识符和公钥索引上链到延安链官方存证合约，进行数据确权存证。

在数据没有发生变化的前提下，无论该数据集如何流通，任何业务方都可以通过调用个人用户在延安链上的BSN官方实名DID文档内的公钥和延安链官方存证合约里该数据集的确权存证信息（均为公开数据），验证该数据集与个人身份之间的权属关系，并可以做到“前台匿名、后台实名”。在这一服务场景内，数据集可以是任何形态的数据文件和数据格式，例如图片、文件、PDF、二进制数据包、电子邮件等。

除了为文件生成哈希并使用私钥进行签名的模式以外，该服务还支持在某些文件格式内直接嵌入私钥签名的模式（例如PDF文档），以及直接使用链账户/链钱包的公私钥对进行确权的模式。

（二）BSN个人数据加密流转服务

任何网站、APP、小程序或者软件，在与其他平台传送个人相关数据时，都要各自为自然人生成公私钥对，并通过BSN实名DID服务将公钥写入延安链上的BSN官方实名DID文档。相互传输数据的双方可以通过BSN官方实名DID文档内的公钥对数据进行相互加密，接收方必须使用对应的个人私钥才能进行解密，确保个人数据在互联网上

传输时处于高层次的加密保护下。这样的机制能够让一个业务方在传递数据前，确保另外一个业务方也掌握同一用户的基本信息，“前台匿名、后台实名”，从而降低个人数据泄露的风险。

即使在不需要强加密的数据传输场景下，一个业务方也可以使用私钥对数据进行签名，另一方收到数据时，仅通过BSN官方实名DID标识和公钥索引，在BSN官方实名DID文档内检索出对应公钥并进行签名验证，便可确保个人数据在传输过程中的完整性，达到防伪造、防篡改、防抵赖的效果。

(三) BSN 个人隐私保护登录服务

在互联网中心化的单方系统架构下，个人用户使用任何网站、APP、小程序或者软件，都必须提供自己的隐私数据，否则这些互联网应用便无法提供服务，这是全世界互联网行业的一个难题。利用BSN实名DID服务，很多业务方可以向个人用户提供“个人隐私保护登录服务”。

个人用户使用BSN实名DID服务的官方小程序或APP，经过CTID平台对个人用户的身份证、姓名、人脸等身份信息验证后，可以自行生成BSN官方实名DID，并将自己的公钥写入BSN官方实名DID文档。提供“个人隐私保护登录服务”的业务方，可以在注册界面让用户提供BSN官方实名DID标识或与之关联的BSN全网分布式域名，并使用个人私钥签名（扫码或弹出微信小程序）来验证BSN官方实名DID的归属，完成注册流程。之后用户即可使用私钥签名登录业务方系统，而业务方系统的数据库内都以BSN官方实名DID作为用户标识，并以此为基础来处理所有业务。

这样的设计实现了个人数据在业务侧完全匿名，同时满足了实名管理要求。业务方完全无法掌握个人用户信息，即使发生数据泄露，也只是业务数据。这些业务数据因为没有关联到具体的个人隐私数据，对侵入方来说也完全不具有任何意义；同时，这样的机制也能防止业务方利用销售个人数据非法牟利。

(四) BSN 自定义业务实名 DID 服务

出于安全因素考虑，在业务处理上，BSN官方实名DID文档内只能存储公钥和公钥索引。因此BSN推出了BSN自定义业务DID，作为对BSN官方实名DID的补充。

BSN自定义业务DID由业务方和BSN共同签发，申请时必须使用BSN官方实名DID文档内的公钥所对应的私钥签名，而BSN则通过使用关联的BSN官方实名DID文档内的公钥验证签名值来完成联合签发，以确保BSN自定义业务DID的实名性。业务方的DID签发公私钥对可以是任何加密算法，这也是BSN自定义业务DID的灵活性之一。业务方对BSN自定义业务DID文档的内容有绝对控制权，可以写入任何文本。当业务方在一个公共环境内（任何人都可以读取）与其他业务方针对某个具体用户进行公钥、加密数据和脱敏数据互动时，可以将BSN自定义业务DID文档作为连接器。通过这种新的信息化架构，可以打造出非常多的降本增效业务场景。

(五) BSN 官方个人身份证明凭证服务

BSN官方个人身份证明凭证经由CTID数字身份链平台签发，使用固定的凭证模板。任何网站、APP、小程序或者软件，都可以为其个人用户申请BSN官方个人身份证明凭证。申请时，需要经过CTID平台对个人用户的身份证、姓名、人脸等身份信息进行验证，并使用BSN平台方DID内的公钥所对应的私钥进行签名，以及使用CTID数字身份链平台的公钥进行加密。CTID数字身份链平台生成BSN官方个人身份证明凭证并返回给业务方，业务方可以在不同场景内使用该凭证进行业务处理。该凭证具有两套模板，一套为标准模板，另一套在标准模板之上增加了个人的BSN官方实名DID标识。

BSN官方个人身份证明凭证通常用于与第三方的业务相互认证。第三方收到该凭证后，可以验证凭证是否由CTID数字身份链平台签发、是否由合作企业申请，以及可以通过由身份证、姓名等身份信息生成的哈希对个人身份进行验证，以达到对个人相关的业务数据或事项进行相互验证的目的，并且可以做到“前台匿名、后台实名”。BSN官方个人身份证明凭证可以下载到本地设备内，包括手机或者电脑浏览器等，并进行本地验证。

(六) BSN 官方个人身份信息凭证服务

BSN官方个人身份信息凭证服务由CTID数字身份链平台提供。该凭证直接向个人用户颁发，可以作为个人身份信息的载体。该凭证的签发流程非常严格，任何APP如需申请该凭证，必须使用CTID数字身份链平台移动端SDK。该凭证以及凭证关联的私钥由用户自行管理，业务方无法取得。

个人用户持有该凭证，可以在一定程度上作为“前台匿名、后台实名”的个人身份信息载体使用。在需要验证用户个人身份的场景，如果业务方拥有能够支持该凭证的设备，即可直接从用户手机上读取该凭证进行验证。

(七) BSN 自定义业务个人身份凭证服务

BSN自定义业务个人身份凭证由业务方签发，是BSN官方个人身份证明凭证的补充，具有很强的业务灵活性。业务方可以自定义面向个人用户的业务凭证模版，并将其上传到延安链。凭证模版内可以包含BSN官方实名DID标识、公钥索引、BSN平台方DID签名值和灵活的业务数据字段等数据域。

业务方在签发BSN自定义业务个人身份凭证时，可以使用BSN官方实名DID文档内已有的公钥所对应的私钥签发，并将凭证哈希上传到延安链官方存证合约。第三方进行业务凭证验证时，可以根据BSN官方实名DID标识或与之关联的BSN全网分布式域名，调出相应的BSN官方实名DID文档，并使用索引找到公钥，对凭证的实名性进行验证后，再根据业务数据字段进行业务处理。

BSN自定义业务个人身份凭证完全由业务方签发，凭证模板也完全由业务方定义，因此上述格式仅作为参考。业务方可以自由组合，例如可以使用BSN平台方DID内的公钥所对应的私钥进行签发，并将个人用户的BSN官方实名DID文档内的公钥所对应的私钥签名写入凭证。业务方甚至可以自行完成关联了BSN官方实名DID的自定义凭证的签发，完全不使用本服务。本服务主要提供了模板的公示和验证，以及凭证哈希的公示和验证服务。

需要强调的是，BSN 实名 DID 服务作为一项底层技术逻辑，它的潜在的应用范围是非常广阔的。在上述应用场景之外，我们也希望能有更多的合作伙伴和业务平台方，设计出更多的应用场景，让这项技术能够发挥出更多价值，为社会治理和经济发展做出更多贡献。

尽管分布式身份认证目前还是一个相对前沿的概念，但是从目前了解到的情况来看，这项技术在全世界范围内得到广泛应用已经是不可逆的技术发展趋势，最终将为整个 IT 行业带来革命性的变化，对各个领域、各行各业产生广泛而深远的影响。欧洲目前已经推出个人数字身份和 DID 的相关立法，但是预计 2026 年才会启动具体的建设。BSN 实名 DID 服务的推出，不仅标志着中国在这一领域占据了领先地位，引领了全球技术发展路线，还意味着未来我们有机会让中国的技术体系成为全球范围内的分布式实名数字身份标准。

与此同时，对于 BSN 自身而言，作为一项底层技术公共基础设施，BSN 已经在全世界范围内赢得了广泛认可。而 BSN 实名 DID 服务标志着 BSN 向基础能力和应用场景层面的迈进，随着这一服务得到广泛应用，必定能够促使人们在分布式网络基础设施的固有认知之外，进一步提高对 BSN 的理解，进而推动 BSN 的发展迈上一个新的台阶。

备注：数据安全说明

- 所有终端用户的个人敏感信息均由业务方进行加密后，才通过BSN实名DID服务API接口发送到CTID数字身份链平台，并最终在延安链上生成BSN官方实名DID。在整个过程中，BSN各方无法接触、收集或存储任何个人信息；
- 延安链由国家信息中心、中国移动集团设计院、CTID数字身份链平台运营方、信通院云大所和红枣科技通过各自建立验证节点来进行共治共管，以确保没有任何单独一方可以对链环境进行重构或者修改；
- BSN实名DID服务相应的智能合约由CTID数字身份链平台部署并管理，任何其他公司和人员都无法对该合约进行干扰和修改，以确保合约本身的安全性和权威性；
- BSN官方实名DID由权威的CTID数字身份链平台生成，其签发私钥对应的公钥是公开的，任何人都可以通过公钥来验证BSN官方实名DID的生成方为合法并具有公信力的机构。

(一) BSN个人数据实名确权服务

1. 产品说明

任何软件、网站或APP等互联网应用都可以为其个人用户生成业务公私钥对（私钥可以进行托管，也可以由个人用户自行保管）。个人用户产生任何数据集时，该应用都可以为数据集生成哈希，并使用用户私钥进行签名，再通过BSN实名DID服务，经过CTID平台对个人用户的身份证、姓名、人脸等身份信息进行验证后，将用户公钥写入延安链上的BSN官方实名DID文档，并将数据集哈希、签名值、DID标识符和公钥索引上链到延安链官方存证合约，进行数据确权存证。

在数据没有发生变化的前提下，无论该数据集如何流通，任何业务方都可以通过调用个人用户在延安链上的BSN官方实名DID文档内的公钥和延安链官方存证合约里该数据集的确权存证信息（均为公开数据），验证该数据集与个人身份之间的权属关系，并可以做到“前台匿名、后台实名”。在这一服务场景内，数据集可以是任何形态的数据文件和数据格式，例如图片、文件、PDF、二进制数据包、电子邮件等。

除了为文件生成哈希并使用私钥进行签名的模式以外，该服务还支持在某些文件格式内直接嵌入私钥签名的模式（例如PDF文档），以及直接使用链账户/链钱包的公私钥对进行确权的模式。

2. 场景案例

• 场景一

数码相机软件或手机照相软件可以在用户注册时，在后台或设备内为用户生成公私钥对，经过CTID平台对个人用户的身份证、姓名、人脸等身份信息进行验证后，将公钥写入延安链上的BSN官方实名DID文档。之后每次在用户拍照时，都可以为照片在后台生成哈希，并使用用户私钥进行签名，再自动上传到延安链官方存证合约内。这相当于为用户拍摄的所有照片都打上了“实名水印”，并带有时间戳，可以在照片流通后随时证明其实名所属权。软件提供商可以将这一实名确权服务作为增值服务推出。该案例是为文件生成哈希并使用私钥进行签名的模式。

• 场景二

提供PDF文件类服务的网站（如电子合同签署），同样可以在后台为用户生成公私钥对（也可以由用户生成并自行掌管私钥，完全由网站决定）。处理任何PDF文件时，都可以将私钥签名直接写入PDF文件相应的数据域内（甚至不使用哈希），经过CTID平台对个人用户的身份证、姓名、人脸等身份信息进行验证后，再将对应公钥写入延安链上的BSN官方实名DID文档。无论文件如何流通，都可以通过私钥签名和公开的BSN官方实名DID文档内的公钥来证明其所属权或签名权。该案例是将私钥签名直接写入某些支持该操作的文件类型的模式。

• 场景三

大学、公司或任何机构在向个人用户发放数字证明文件时（如毕业证、资格证书、工作证、票证等），均可按照上述案例中的流程，在软件或者APP内生成公私钥对，为该数字文件生成哈希并使用私钥进行签名，经过CTID平台对个人用户的身份证、姓名、人脸等身份信息进行验证后，再将公钥写入延安链上的BSN官方实名DID文档。之后在任何时间，都可以通过BSN官方实名DID文档内的公钥、BSN官方实名DID对应的个人身份和哈希签名来验证该数字证明文件的真实性，以及签发单位的真实性。该案例是为文件生成哈希并使用私钥进行签名的模式。

• 场景四

对于某些链上数据（如数字资产），业务方如果持有这些数据的链账户或钱包地址的公私钥对，也可以在经过CTID平台对个人用户的身份证、姓名、人脸等身份信息进行验证后，将其对应公钥写入延安链上的BSN官方实名DID文档。验证方可以根据该数字资产的链账户私钥签名交易信息，以及BSN官方实名DID文档内的公开

公钥，确定该数字资产与某个人用户的个人身份之间的权属关系。该案例是利用链账户/链钱包的公私钥对进行确权的模式。

3. 技术流程

- 访问BSN-DDC官方门户网站<https://ddc.bsnbase.com>，注册成为业务平台方，并购买相应套餐；
- 业务平台方根据《BSN实名DID服务技术接口文档》（接口文档）在系统后台服务集成BSN实名DID服务的SDK，通过调用接口文档“7.4.6-计算文件哈希值”或“7.4.7-计算字符串哈希值”方法为个人用户的数据集生成哈希，并通过调用“7.4.1-生成公私钥对”方法为个人用户生成业务公私钥对。也可以自己在本地进行公私钥的生成和哈希计算；
- 业务平台方使用上述生成的用户公钥，经过CTID平台对个人用户的身份证、姓名、人脸等身份信息进行验证后，调用接口文档“7.2.1-申领DID”方法（需要消耗BSN官方实名DID服务套餐）申领BSN官方实名DID，得到个人用户的BSN官方实名DID文档；
- 业务平台方使用上述生成的用户私钥和数据集哈希，调用接口文档“7.4.4-签名”方法计算数字签名值，之后调用“7.3.19-自定义数据的存证”方法（需要消耗能量值）将数字签名值、数据集哈希和DID标识这些数据信息提交到BSN延安链的公共存证服务内，通过官方存证合约进行存证；
- 第三方验证：验证方需访问BSN-DDC官方门户网站<https://ddc.bsnbase.com>，注册成为业务平台方，开通“接入DDC网络”并购买能量值套餐。之后调用接口文档“7.4.6-计算文件哈希值”或“7.4.7-计算字符串哈希值”方法为需要验证的数据集生成哈希，并根据用户DID标识或关联的BSN全网分布式域名调用接口文档“7.2.2-查询下载DID文档”方法（需要消耗能量值），查询该用户的BSN官方实名DID文档，取得BSN官方实名DID文档内的相应公钥。再调用接口文档“7.3.21-核验自定义的存证数据”方法，传入数据集哈希、DID标识和获取到的公钥，最终得到核验结果。其中公钥会对BSN延安链上的数据集哈希进行签名值的验签。

4. 所需套餐

- 需要购买BSN官方实名DID服务套餐（每次实名核验（姓名+身份证）/真人核验（姓名+身份证+人像）+生成或更新BSN官方实名DID文档大约需要花费0.75-1.2元人民币），套餐详细内容请点击[查看](#)；
- 需要购买BSN-DDC基础网络能量值套餐（每次下载BSN官方实名DID文档需要花费0.04元人民币，调用BSN延安链官方存证合约需要花费约0.06元人民币），套餐详细内容请点击[查看](#)。

5. 与BSN全网分布式域名关联

BSN实名DID服务可以关联BSN全网分布式域名服务。每个购买了BSN实名DID服务套餐的业务平台方，都会获赠一个自有品牌的“.did”一级域名（例如bsn.did），业务平台方可以将每个个人用户的实名DID与该一级域名下的二级域名或三级域名直接关联，以方便后续的业务处理，例如查询、公钥获取等。

业务平台方也可以为个人用户注册“.com”“.web3”或“.bsn”的一级域名，并关联到对应的实名DID标识上，以便于个人用户可以随时在其他业务APP或网站内，自行输入域名并关联到自己的实名DID文档。具体详情请访问[BSN全网分布式域名官网](#)。

6. 数据安全说明

- 所有终端用户的个人敏感信息均由业务方进行加密后，才通过BSN实名DID服务API接口发送到CTID数字身份链平台，并最终在延安链上生成BSN官方实名DID。在整个过程中，BSN各方无法接触、收集或存储任何个人信息；
- 延安链由国家信息中心、中国移动集团设计院、CTID数字身份链平台运营方、信通院云大所和红枣科技通过各自建立验证节点来进行共治共管，以确保没有任何单独一方可以对链环境进行重构或者修改；
- BSN实名DID服务相应的智能合约由CTID数字身份链平台部署并管理，任何其他公司和人员都无法对该合约进行干扰和修改，以确保合约本身的安全性和权威性；
- BSN官方实名DID由权威的CTID数字身份链平台生成，其签发私钥对应的公钥是公开的，任何人都可以通过公钥来验证BSN官方实名DID的生成方为合法并具有公信力的机构。

(二) BSN个人数据加密流转服务

1. 产品说明

任何网站、APP、小程序或者软件，在与其他平台传送个人相关数据时，都要各自为自然人生成公私钥对，并通过BSN实名DID服务将公钥写入延安链上的BSN官方实名DID文档。相互传输数据的双方可以通过BSN官方实名DID文档内的公钥对数据进行相互加密，接收方必须使用对应的个人私钥才能进行解密，确保个人数据在互联网上传输时处于高层次的加密保护下。这样的机制能够让一个业务方在传递数据前，确保另外一个业务方也掌握同一用户的基本信息，“前台匿名、后台实名”，从而降低个人数据泄露的风险。

即使在不需要强加密的数据传输场景下，一个业务方也可以使用私钥对数据进行签名，另一方收到数据时，仅通过BSN官方实名DID标识和公钥索引，在BSN官方实名DID文档内检索出对应公钥并进行签名验证，便可确保个人数据在传输过程中的完整性，达到防伪造、防篡改、防抵赖的效果。

2. 场景案例

• 场景一

合同签署平台可以为每个签署人在BSN官方实名DID文档内生成本地公私钥对（个人掌握私钥）。在签署合同时，平台不仅可以为合同（PDF文件）打上私钥签名水印，在明确了下一个签署人后，平台前端同时还可以使用下一个签署人在BSN官方实名DID文档内的公钥对合同进行加密，并在平台内传递给下一个签署人，该签署人可以在平台前端通过本地私钥解密，并进行后续的签署和传递操作。这样的机制可以在平台内传递合同时，实现签署人到签署人的端到端加密，确保合同的保密性，可以从技术上实现连平台管理者都无法查看合同内容。这是在同一平台下个人用户之间进行信息加密传输的案例。

• 场景二

电子邮件服务商（例如企业级服务）可以在开户时为自然人用户生成公私钥对，并将公钥写入BSN官方实名DID文档（私钥由用户自行保管）。多个电子邮件服务商只要互相了解BSN官方实名DID文档内的公钥索引，即可提供相互之间的邮件加密服务。发件人在输入收件人的邮件地址时，同时输入其BSN官方实名DID标识或与之关联的BSN全网分布式域名，邮件服务器即可使用对应公钥索引下的公钥对邮件进行加密，收件人收到加密邮件后，可以使用自己的私钥在本地解密阅读。这样可以实现邮件在互联网上的完全加密传输，甚至邮件服务商也无法接触到邮件内容。这是跨平台个人用户之间进行信息加密传输的案例。

• 场景三

医疗机构的系统可以为患者和医生生成关联BSN官方实名DID的公私钥对（个人掌握私钥，公钥写入BSN官方实名DID文档）。当患者访问医疗网站并向医生发送个人病历时，医疗系统的前端通过该医生的公钥对患者病历进行前端加密，并将密文病历通过互联网传输至医疗网站的后端系统，确保只能由该医生使用其私钥进行解密才能得到患者的原始病历资料。

3. 技术流程

- 数据传输双方访问BSN-DDC官方门户网站<https://ddc.bsnbase.com>，注册成为业务平台方，并购买相应套餐和能量值；
- 数据传输双方根据《BSN实名DID服务技术接口文档》（接口文档）在系统后台服务集成BSN实名DID服务SDK，通过调用接口文档“7.4.1 生成公私钥对”方法为个人用户分别生成业务公私钥对；
- 业务方使用上述生成的用户公钥，经过CTID平台对个人用户的身份证、姓名、人脸等身份信息进行验证后，通过调用接口文档“7.2.1-申领DID”方法（需要消耗BSN官方实名DID服务套餐）申领BSN官方实名DID，得到个人用户的BSN官方实名DID文档；
- 传输方使用用户的BSN官方实名DID标识调用接口文档“7.2.2 查询下载DID文档”方法（需要消耗能量值），查询该用户的BSN官方实名DID文档，使用接收方在BSN官方实名DID文档里存储的上述自己生成的公私钥对中

的公钥，调用接口文档“7.4.2 加密”方法对用户个人数据进行加密，随后把加密数据传输给接收方；如果需要传输明文数据，传输方对用户数据用上述自己生成的私钥调用“7.4.4 签名”方法进行签名，把用户数据、签名数据、公钥索引一起传输给接收方；

- 接收方收到加密数据后使用上述自己为用户生成的公私钥对中的私钥调用接口文档“7.4.3 解密”方法进行解密，获取传输过来的用户明文数据；如果接收到明文数据，则使用用户的BSN官方实名DID标识调用接口文档“7.2.2 查询下载DID文档”方法（需要消耗能量值）查询该用户的BSN官方实名DID文档，检索公钥索引对应的公钥调用接口文档“7.4.5 验签”方法对签名数据进行验签。

4. 所需套餐

- 需要购买BSN官方实名DID服务套餐（每次实名核验（姓名+身份证）/真人核验（姓名+身份证+人像）+生成或更新BSN官方实名DID文档大约需要花费0.75-1.2元人民币），套餐详细内容请点击[查看](#)；
- 需要购买BSN-DDC基础网络能量值套餐（每次下载BSN官方实名DID文档需要花费0.04元人民币），套餐详细内容请点击[查看](#)。

5. 与BSN全网分布式域名关联

BSN实名DID服务可以关联BSN全网分布式域名服务。每个购买了BSN实名DID服务套餐的业务平台方，都会获赠一个自有品牌的“.did”一级域名（例如bsn.did），业务平台方可以将每个个人用户的实名DID与该一级域名下的二级域名或三级域名直接关联，以方便后续的业务处理，例如查询、公钥获取等。

业务平台方也可以为个人用户注册“.com”“.web3”或“.bsn”的一级域名，并关联到对应的实名DID标识上，以便于个人用户可以随时在其他业务APP或网站内，自行输入域名并关联到自己的实名DID文档。具体详情请访问[BSN全网分布式域名官网](#)。

6. 数据安全说明

- 所有终端用户的个人敏感信息均由业务方进行加密后，才通过BSN实名DID服务API接口发送到CTID数字身份链平台，并最终在延安链上生成BSN官方实名DID。在整个过程中，BSN各方无法接触、收集或存储任何个人信息；
- 延安链由国家信息中心、中国移动集团设计院、CTID数字身份链平台运营方、信通院云大所和红枣科技通过各自建立验证节点来进行共治共管，以确保没有任何单独一方可以对链环境进行重构或者修改；
- BSN实名DID服务相应的智能合约由CTID数字身份链平台部署并管理，任何其他公司和人员都无法对该合约进行干扰和修改，以确保合约本身的安全性和权威性；
- BSN官方实名DID由权威的CTID数字身份链平台生成，其签发私钥对应的公钥是公开的，任何人都可以通过公钥来验证BSN官方实名DID的生成方为合法并具有公信力的机构。

(三) BSN个人隐私保护登录服务

1. 产品说明

在互联网中心化的单方系统架构下，个人用户使用任何网站、APP、小程序或者软件，都必须提供自己的隐私数据，否则这些互联网应用便无法提供服务，这是全世界互联网行业的一个难题。利用BSN实名DID服务，很多业务方可以向个人用户提供“个人隐私保护登录服务”。

个人用户使用BSN实名DID服务的官方小程序或APP，经过CTID平台对个人用户的身份证、姓名、人脸等身份信息验证后，可以自行生成BSN官方实名DID，并将自己的公钥写入BSN官方实名DID文档。提供“个人隐私保护登录服务”的业务方，可以在注册界面让用户提供BSN官方实名DID标识或与之关联的BSN全网分布式域名，并使用个人私钥签名（扫码或弹出微信小程序）来验证BSN官方实名DID的归属，完成注册流程。之后用户即可使用私钥签名登录业务方系统，而业务方系统的数据库内都以BSN官方实名DID作为用户标识，并以此为基础来处理所有业务。

这样的设计实现了个人数据在业务侧完全匿名，同时满足了实名管理要求。业务方完全无法掌握个人用户信息，即使发生数据泄露，也只是业务数据。这些业务数据因为没有关联到具体的个人隐私数据，对侵入方来说也完全不具有任何意义；同时，这样的机制也能防止业务方利用销售个人数据非法牟利。

2. 场景案例

• 场景一

某短视频APP，在遵守了中国互联网实名制要求的前提下，在业务上对个人信息没有任何依赖，因此可以选择为用户提供基于BSN实名DID服务的隐私保护注册和登录服务。当用户注册时选择隐私授权注册，通过BSN实名DID服务，利用官方小程序或APP存储的BSN官方实名DID标识（或与之关联的BSN全网分布式域名）与私钥，调用BSN实名DID服务验证用户私钥签名，验签后平台完成用户实名注册，并存储BSN官方实名DID信息和公钥信息，之后用户只需在本地验证私钥签名即可完成登录。这一服务可供隐私保护意识较强的用户自主选择。BSN实名DID服务作为个人隐私数据的防火墙，实现了“前台匿名、后台实名”，在业务侧完全匿名，同时满足实名管理要求。

• 场景二

对于某些基于区块链技术的服务，在用户通过平台或者APP界面生成链账户或钱包时，可以通过BSN实名DID服务小程序直接使用已经关联BSN官方实名DID的公私钥对，并在验证私钥签名后，将BSN官方实名DID标识和相应公钥存入业务系统，完成链账户注册，用户不需要提供任何隐私信息。用户使用链账户或钱包进行链上业务处理时，一般情况下均需使用私钥签名，区块链服务平台使用保存的公钥进行验签即可。这一隐私保护逻辑可以应用在任何需要链账户或钱包地址触发的区块链场景中，包括数字藏品、数字资产交易等。

• 场景三

对于深度涉及个人隐私的体检机构，应提供匿名体检服务。个人用户在体检机构的网站或APP内申请注册时，使用BSN官方实名DID进行隐私保护注册；在体检现场，通过电脑或手机端扫描二维码，使用私钥签名验证身份，并由体检机构系统保存对应公钥，在匿名情况下完成体检；出具体检报告后，系统自动使用用户的公钥进行加密，通过网站、邮件或者其他方式发送给用户，用户使用自己的私钥解密并查看具体报告，实现了体检报告的加密传递。整个流程从最大程度上保护了用户的健康隐私。

3. 技术流程

- 个人用户登录BSN实名DID服务的官方小程序或APP，经过CTID平台对个人用户的身份证、姓名、人脸等身份信息进行验证后，生成个人BSN官方实名DID（小程序费用规则），个人的公私钥对会加密存储在官方小程序或APP中，并提供导出或恢复功能；

- 业务平台方访问BSN-DDC官方门户网站<https://ddc.bsnbase.com>，注册成为业务平台方，并购买能量值套餐，根据《BSN实名DID服务技术接口文档》（接口文档）在系统后台服务集成BSN实名DID服务SDK；
- 个人用户在业务平台注册登录时，业务平台调用并跳转到BSN实名DID服务的官方APP或者小程序（或者二维码扫码方式），用户在跳转的官方APP或者小程序内对业务平台进行访问授权，业务平台从官方APP或者小程序获取用户的BSN实名DID标识、公钥索引、签名值和用户私钥签名数据，平台方调用接口文档“7.2.2 查询下载DID文档”方法（需要消耗能量值）查询该用户的BSN官方实名DID文档，使用公钥索引检索公钥信息调用接口文档“7.4.5 验签”方法对用户的签名授权数据进行验签；
- 平台方将用户的BSN官方实名DID标识、公钥（或关联的BSN全网分布式域名）与业务内部账户绑定，在后续登录时，用户可使用BSN官方实名DID标识（或关联的BSN全网分布式域名）和私钥签名登录，平台方只需本地验签用户的签名数据即可。

4. 所需套餐

- 小程序费用规则：包含DID、一组公私钥对、一个bsn.did的二级域名一次性收费2元人民币，绑定自定义全网域名和datahub的费用推出后另行提供；
- 业务平台方需要购买BSN-DDC网络能量值套餐（每次下载DID文档需要花费0.04元人民币），套餐详细内容请点击[查看](#)。

5. 与BSN全网分布式域名关联

BSN实名DID服务可以关联BSN全网分布式域名服务。每个购买了BSN实名DID服务套餐的业务平台方，都会获赠一个自有品牌的“.did”一级域名（例如bsn.did），业务平台方可以将每个个人用户的实名DID与该一级域名下的二级域名或三级域名直接关联，以方便后续的业务处理，例如查询、公钥获取等。

业务平台方也可以为个人用户注册“.com”“.web3”或“.bsn”的一级域名，并关联到对应的实名DID标识上，以便于个人用户可以随时在其他业务APP或网站内，自行输入域名并关联到自己的实名DID文档。具体详情请访问[BSN全网分布式域名官网](#)。

6. 数据安全说明

- 所有终端用户的个人敏感信息均由业务方进行加密后，才通过BSN实名DID服务API接口发送到CTID数字身份链平台，并最终在延安链上生成BSN官方实名DID。在整个过程中，BSN各方无法接触、收集或存储任何个人信息；
- 延安链由国家信息中心、中国移动集团设计院、CTID数字身份链平台运营方、信通院云大所和红枣科技通过各自建立验证节点来进行共治共管，以确保没有任何单独一方可以对链环境进行重构或者修改；
- BSN实名DID服务相应的智能合约由CTID数字身份链平台部署并管理，任何其他公司和人员都无法对该合约进行干扰和修改，以确保合约本身的安全性和权威性；
- BSN官方实名DID由权威的CTID数字身份链平台生成，其签发私钥对应的公钥是公开的，任何人都可以通过公钥来验证BSN官方实名DID的生成方为合法并具有公信力的机构。

(四) BSN自定义业务实名DID服务

1. 产品说明

出于安全因素考虑，在业务处理上，BSN官方实名DID文档内只能存储公钥和公钥索引。因此BSN推出了BSN自定义业务DID，作为对BSN官方实名DID的补充。

BSN自定义业务DID由业务方和BSN共同签发，申请时必须使用BSN官方实名DID文档内的公钥所对应的私钥签名，而BSN则通过使用关联的BSN官方实名DID文档内的公钥验证签名值来完成联合签发，以确保BSN自定义业务DID的实名性。业务方的DID签发公私钥对可以是任何加密算法，这也是BSN自定义业务DID的灵活性之一。业务方对BSN自定义业务DID文档的内容有绝对控制权，可以写入任何文本。当业务方在一个公共环境内（任何人都可以读取）与其他业务方针对某个具体用户进行公钥、加密数据和脱敏数据互动时，可以将BSN自定义业务DID文档作为连接器。通过这种新的信息化架构，可以打造出非常多的降本增效业务场景。

2. 场景案例

• 场景一

某元宇宙公司向个人用户提供创建元宇宙内虚拟人的服务，可以先通过BSN实名DID服务为用户建立实名分布式身份，然后利用BSN自定义业务DID的灵活性，为用户创建的每个虚拟人创建业务DID身份。在这样的体系下，一个BSN官方实名DID可以关联无数个BSN自定义业务DID，并且可以在BSN自定义业务DID文档内写入每个虚拟人的建模数据，根据授权开放给其他元宇宙平台和游戏平台使用。这样的技术体系可以让实名用户拥有的每一个虚拟人具有一个永久身份ID和与之对应的BSN全网分布式域名地址，并且根据公开的建模信息，让同一个虚拟人在每个平台展示出来的形象都是一致的，真正实现所有元宇宙内容相互连通的场景。

• 场景二

需要提供个人公示信息的网站或者APP，也可以利用BSN自定义业务DID服务实现更透明、更具实名保证的信息公示。例如教育机构在为下属教师生成BSN官方实名DID后，可以将教师的业务信息存储在另行生成的BSN自定义业务DID文档中，例如教师资格证、专业领域、从业年限、各类证书等，并允许其他业务方从延安链上读取该BSN自定义业务DID文档。任何需要获取教师身份和资格的场景，只要使用教师的基本身份信息，就可以直接检索到由教育机构公示的所有信息，并且可以通过签名验证教育机构的真实性和教师个人身份的真实性。

• 场景三

在Web3时代，个人用户也可以利用BSN自定义业务DID来建立自己的Web3个人主页。将来会出现提供建立个人Web3主页的专业服务：对个人用户进行BSN官方实名DID认证后，再生成BSN自定义业务DID，允许个人用户在关联的BSN自定义业务DID文档内写入HTML格式内容，并且将文档开放给其他平台，可以自由从延安链上读取。个人用户可以在所有Web2时代的网站内录入自己的BSN自定义业务DID地址或与之关联的BSN全网分布式域名，则这些网站，包括各类Web3元宇宙平台、游戏平台、区块链浏览器等，都可以调取BSN自定义业务DID文档内的HTML内容，将个人Web3页面内容展示在各类前端设备上（电脑、手机、头显、3D成像等）。未来个人用户只需要维护一个Web3的BSN自定义业务DID文档，就能够对无数个Web2和Web3平台内的个人内容进行自动更新，这种模式将实名DID技术可以链接各平台内容的功能发挥到了极致。

3. 技术流程

- 访问BSN-DDC官方门户网站<https://ddc.bsnbase.com>，注册成为业务平台方，并购买相应套餐；
- 业务方根据《BSN实名DID服务技术接口文档》（接口文档）在系统后台服务集成BSN实名DID服务SDK，当个人用户需要进行BSN自定义业务DID的申领时，如果用户没有BSN官方实名DID，业务方需首先调用接口文档“7.2.1 申领DID”方法（需要消耗BSN官方实名DID服务套餐）为该用户完成BSN官方实名DID申领；随后业务平台方调用接口文档“7.3.1 申领DID”方法为个人用户完成BSN自定义业务DID的申请，得到包含BSN签名值

的BSN自定义业务DID文档（SDK已提供SM2算法，如需其他算法可自行实现）（需要消耗BSN业务DID服务套餐）；

- 当第三方需要核验BSN自定义业务DID文档的BSN签名时，可通过BSN实名DID服务公钥自行（不需要在BSN-DDC基础网络注册）对BSN自定义业务DID文档中的BSN签名进行核验；也可以调用接口文档“7.3.3 核验DID文档”方法对BSN自定义业务DID文档中的BSN签名值进行核验（需要核验的BSN自定义业务DID文档可以通过BSN自定义业务DID标识调用接口文档“7.3.5 查询下载DID文档”方法进行获取）（消耗能量值），通过BSN自定义业务DID文档能够获取自定义文本信息并进行业务处理。

4. 所需套餐

- 需要购买BSN官方实名DID服务套餐（每次实名核验（姓名+身份证）/真人核验（姓名+身份证+人像）+生成或更新实名DID文档大约需要花费0.75-1.2元人民币），套餐详细内容请点击[查看](#)；
- 需要购买BSN业务实名DID服务套餐（每次业务实名DID的生成、销毁DID文档大约需要花费0.35-0.5元人民币），套餐详细内容请点击[查看](#)；
- 需要购买BSN-DDC网络能量值套餐（每次更新业务实名DID文档大约需要花费0.05元人民币，下载业务实名DID文档需要花费0.04元人民币），套餐详细内容请点击[查看](#)。

5. 与BSN全网分布式域名关联

BSN实名DID服务可以关联BSN全网分布式域名服务。每个购买了BSN实名DID服务套餐的业务平台方，都会获赠一个自有品牌的“.did”一级域名（例如bsn.did），业务平台方可以将每个个人用户的实名DID与该一级域名下的二级域名或三级域名直接关联，以方便后续的业务处理，例如查询、公钥获取等。

业务平台方也可以为个人用户注册“.com”“.web3”或“.bsn”的一级域名，并关联到对应的实名DID标识上，以便于个人用户可以随时在其他业务APP或网站内，自行输入域名并关联到自己的实名DID文档。具体详情请访问[BSN全网分布式域名官网](#)。

6. 数据安全说明

- 所有终端用户的个人敏感信息均由业务方进行加密后，才通过BSN实名DID服务API接口发送到CTID数字身份链平台，并最终在延安链上生成BSN官方实名DID。在整个过程中，BSN各方无法接触、收集或存储任何个人信息；
- 延安链由国家信息中心、中国移动集团设计院、CTID数字身份链平台运营方、信通院云大所和红枣科技通过各自建立验证节点来进行共治共管，以确保没有任何单独一方可以对链环境进行重构或者修改；
- BSN实名DID服务相应的智能合约由CTID数字身份链平台部署并管理，任何其他公司和人员都无法对该合约进行干扰和修改，以确保合约本身的安全性和权威性；
- BSN官方实名DID由权威的CTID数字身份链平台生成，其签发私钥对应的公钥是公开的，任何人都可以通过公钥来验证BSN官方实名DID的生成方为合法并具有公信力的机构。

(五) BSN官方个人身份证明凭证服务

1. 产品说明

BSN官方个人身份证明凭证经由CTID数字身份链平台签发，使用固定的凭证模板。任何网站、APP、小程序或者软件，都可以为其个人用户申请BSN官方个人身份证明凭证。申请时，需要经过CTID平台对个人用户的身份证、姓名、人脸等身份信息进行验证，并使用BSN平台方DID内的公钥所对应的私钥进行签名，以及使用CTID数字身份链平台的公钥进行加密。CTID数字身份链平台生成BSN官方个人身份证明凭证并返回给业务方，业务方可以在不同场景内使用该凭证进行业务处理。该凭证具有两套模板，一套为标准模板，另一套在标准模板之上增加了个人的BSN官方实名DID标识。

BSN官方个人身份证明凭证通常用于与第三方的业务相互认证。第三方收到该凭证后，可以验证凭证是否由CTID数字身份链平台签发、是否由合作企业申请，以及可以通过由身份证、姓名等身份信息生成的哈希对个人身份进行验证，以达到对个人相关的业务数据或事项进行相互验证的目的，并且可以做到“前台匿名、后台实名”。BSN官方个人身份证明凭证可以下载到本地设备内，包括手机或者电脑浏览器等，并进行本地验证。

2. 场景案例

• 场景一

在线金融服务应用场景中，银行A的用户希望进行身份验证，以在银行A关联的证券公司B开通某项证券服务。用户通过银行A平台申请BSN官方个人身份证明凭证，提供身份证、姓名、人脸等身份信息后，银行A将身份验证请求通过BSN实名DID服务接口发送至CTID数字身份链平台，生成个人身份证明凭证。用户收到凭证后，将其下载到手机等本地设备内，之后用于在证券公司B的服务流程中进行本地验证。证券公司B可通过验证凭证的CTID数字身份链平台签名、银行A的DID签名等，确保用户的个人身份得到了CTID平台和银行A的认证，从而安全、便捷地为用户提供证券服务。

• 场景二

任何组织和单位如果要证明其员工的在职身份或学生的在校身份，均可使用BSN实名DID服务来开具相应的BSN官方个人身份证明凭证。第三方可以通过该凭证来验证该组织的真实性（通过注册时颁发的BSN平台方DID）、员工信息的真实性、隶属关系的真实性等，从而避免使用纸质文档或者非验证的电子文档，通过技术手段来完全避免造假的风险。

3. 技术流程

- 访问BSN-DDC官方门户网站<https://ddc.bsnbase.com>，注册成为业务平台方，并购买相应套餐；
- 平台方在系统后台服务根据《BSN实名DID服务技术接口文档》（接口文档）“7.1 使用说明”适配BSN实名DID服务SDK；
- 平台方要求个人用户提供身份证、姓名、人脸等身份信息；
- 平台方可以使用两套模板为用户生成个人身份证明凭证：
 - 使用标准模板，通过调用接口文档“7.2.4 申领身份认证结果凭证”方法为个人用户申领带有CTID数字身份链平台签名的身份认证结果凭据密文和生成的存证哈希（需要消耗BSN官方实名身份凭证服务套餐）；
 - 使用带有个人的BSN官方实名DID标识的模板，先调用接口文档“7.2.7 查询凭证模板”方法查询想要使用的身份证明凭证的模板信息，然后调用接口文档“7.2.6 申领证明型凭证”方法，输入模板信息，为个人用户申领带有CTID数字身份链平台签名的身份证明存证凭据（需要消耗BSN官方实名身份凭证服务套餐）
- 平台方获取到用户的密文身份证明凭证信息，使用平台方自己在安信CTID数字身份链平台登记的公钥对应的私钥，调用接口文档“7.4.3 解密”方法将用户的密文身份证明凭证信息进行解密后发送给验证方；
- 验证方拿到用户身份证明凭证后使用CTID数字身份链平台的公钥对用户身份证明凭证的CTID数字身份链平台签名进行验签；

- 验证方根据身份证明凭证明文信息中的通过身份证、姓名生成的哈希对个人身份进行验证；CTID数字身份链平台的签名证明该凭据的有效性及其对应自然人的实名认证结果；
- 验证方也可以访问BSN-DDC官方门户网站<https://ddc.bsnbase.com>，注册成为业务平台方，开通“接入DDC网络”；在自己的业务系统中根据接口文档“7.1 使用说明”适配BSN实名DID服务SDK，参考接口文档“7.2.9 核验凭证”方法核验用户身份证明凭证。

4. 所需套餐

- 需要购买BSN官方实名身份凭证服务套餐（每次实名核验（姓名+身份证）/真人核验（姓名+身份证+人像）+生成或更新身份凭证大约需要花费0.75-1.2元人民币），套餐详细内容请点击[查看](#)。

5. 数据安全说明

- 所有终端用户的个人敏感信息均由业务方进行加密后，才通过BSN实名DID服务API接口发送到CTID数字身份链平台，并最终在延安链上生成BSN官方实名DID。在整个过程中，BSN各方无法接触、收集或存储任何个人信息；
- 延安链由国家信息中心、中国移动集团设计院、CTID数字身份链平台运营方、信通院云大所和红枣科技通过各自建立验证节点来进行共治共管，以确保没有任何单独一方可以对链环境进行重构或者修改；
- BSN实名DID服务相应的智能合约由CTID数字身份链平台部署并管理，任何其他公司和人员都无法对该合约进行干扰和修改，以确保合约本身的安全性和权威性；
- BSN官方实名DID由权威的CTID数字身份链平台生成，其签发私钥对应的公钥是公开的，任何人都可以通过公钥来验证BSN官方实名DID的生成方为合法并具有公信力的机构。

Copyright 北京红枣科技有限公司

(六) BSN官方个人信息凭证服务

1. 产品说明

BSN官方个人信息凭证服务由CTID数字身份链平台提供。该凭证直接向个人用户颁发，可以作为个人身份信息的载体。该凭证的签发流程非常严格，任何APP如需申请该凭证，必须使用CTID数字身份链平台移动端SDK。该凭证以及凭证关联的私钥由用户自行管理，业务方无法取得。

个人用户持有该凭证，可以在一定程度上作为“前台匿名、后台实名”的个人信息载体使用。在需要验证用户个人身份的场景，如果业务方拥有能够支持该凭证的设备，即可直接从用户手机上读取该凭证进行验证。

2. 场景案例

• 场景一

BSN官方个人信息凭证可以视为经过加密的个人信息载体。例如，用户在酒店办理入住时，利用集成了CTID数字身份链平台移动端SDK的业务APP或小程序（酒店认可即可，如携程等），经过CTID平台对个人用户的身份证、姓名、人脸等身份信息进行验证后，生成BSN官方个人信息凭证，储存在手机里并生成相应二维码，即可以在不用携带或出示实体身份证的情况下办理入住。在法律允许的前提下，可以实现个人用户在不向酒店暴露过多个人的身份信息的同时完成实名入住，有效保护了个人隐私，还可以遏制酒店贩卖住宿用户信息的灰色产业。

• 场景二

在医院实名制挂号场景中，可以将BSN官方个人信息凭证服务嵌入到挂号APP内，经过CTID平台对个人用户的身份证、姓名、人脸等身份信息进行验证后，为用户生成BSN官方个人信息凭证。用户可以直接使用自助终端机对该凭证或相应的二维码进行验证，并完成取号、缴费、打印报告等各项操作，其安全程度要远远大于普通二维码，降低了造假风险。同时，用户可以授权该凭证在其他关联医院使用，实现一码通用，甚至可以通过该凭证关联用户在多家医院的医疗信息。

3. 技术流程

- 访问BSN-DDC官方门户网站<https://ddc.bsnbase.com>，注册成为业务平台方，并购买相应套餐；
- 平台方移动端APP内集成CTID数字身份链平台移动端SDK（IOS/安卓版），个人用户在APP中完成BSN官方实名DID的申领（需要消耗BSN官方实名DID服务套餐）；
- 个人用户在平台方移动端APP中完成BSN官方个人信息凭证申领（需要消耗BSN官方实名身份凭证服务套餐），申领完成后该凭证加密保存在APP中；
- 个人用户在使用BSN官方个人信息凭证时，需要通过自主授权后方能使用并进行个人信息的选择性披露，具体步骤参考“CTID数字身份链平台移动端SDK技术文档”。

4. 所需套餐

- 需要购买BSN官方实名DID服务套餐（每次实名核验（姓名+身份证）/真人核验（姓名+身份证+人像）+生成或更新BSN官方实名DID文档大约需要花费0.75-1.2元人民币），套餐详细内容请点击[查看](#)；
- 需要购买BSN官方实名身份凭证服务套餐（每次实名核验（姓名+身份证）/真人核验（姓名+身份证+人像）+生成或更新身份凭证大约需要花费0.75-1.2元人民币），套餐详细内容请点击[查看](#)；

5. 数据安全说明

- 所有终端用户的个人敏感信息均由业务方进行加密后，才通过BSN实名DID服务API接口发送到CTID数字身份链平台，并最终在延安链上生成BSN官方实名DID。在整个过程中，BSN各方无法接触、收集或存储任何个人信息；

- 延安链由国家信息中心、中国移动集团设计院、CTID数字身份链平台运营方、信通院云大所和红枣科技通过各自建立验证节点来进行共治共管，以确保没有任何单独一方可以对链环境进行重构或者修改；
- BSN实名DID服务相应的智能合约由CTID数字身份链平台部署并管理，任何其他公司和人员都无法对该合约进行干扰和修改，以确保合约本身的安全性和权威性；
- BSN官方实名DID由权威的CTID数字身份链平台生成，其签发私钥对应的公钥是公开的，任何人都可以通过公钥来验证BSN官方实名DID的生成方为合法并具有公信力的机构。

Copyright 北京红枣科技有限公司

(七) BSN自定义业务个人身份凭证服务

1. 产品说明

BSN自定义业务个人身份凭证由业务方签发，是BSN官方个人身份证明凭证的补充，具有很强的业务灵活性。业务方可以自定义面向个人用户的业务凭证模版，并将其上传到延安链。凭证模版内可以包含BSN官方实名DID标识、公钥索引、BSN平台方DID签名值和灵活的业务数据字段等数据域。

业务方在签发BSN自定义业务个人身份凭证时，可以使用BSN官方实名DID文档内已有的公钥所对应的私钥签发，并将凭证哈希上传到延安链官方存证合约。第三方进行业务凭证验证时，可以根据BSN官方实名DID标识或与之关联的BSN全网分布式域名，调出相应的BSN官方实名DID文档，并使用索引找到公钥，对凭证的实名性进行验证后，再根据业务数据字段进行业务处理。

BSN自定义业务个人身份凭证完全由业务方签发，凭证模板也完全由业务方定义，因此上述格式仅作为参考。业务方可以自由组合，例如可以使用BSN平台方DID内的公钥所对应的私钥进行签发，并将个人用户的BSN官方实名DID文档内的公钥所对应的私钥签名写入凭证。业务方甚至可以自行完成关联了BSN官方实名DID的自定义凭证的签发，完全不使用本服务。本服务主要提供了模板的公示和验证，以及凭证哈希的公示和验证服务。

2. 场景案例

• 场景一

BSN自定义业务身份凭证的模板可以由业务方自行定义，比上述两种官方凭证的固定格式在业务处理上要灵活很多。例如，拍卖行需要参拍方提供多份不同银行的存款证明后才能进行参拍身份的确定，每个银行可以自定义自己的存款证明模版，并且签发自己银行的存款证明凭证，存款证明凭证中包含BSN官方实名DID标识、公钥索引、BSN平台方DID签名值、存款金额等数据。银行签发存款证明凭证时，可以使用用户的BSN官方实名DID文档内已有的银行公钥所对应的私钥签发，并将凭证哈希上传到延安链官方存证合约。拍卖方可以通过读取存款证明凭证内容完成资格审核，如果需要更加严谨，则通过延安链上的BSN官方实名DID文档内的银行签发时对应的公钥对每个凭证进行验证，最终判断是否具有参拍资质。

• 场景二

学信网可针对各大高校学生定义凭证模版，模版内可以定义学生的BSN官方实名DID数据域属性、公钥索引数据域属性、签名值数据域属性，以及高校毕业证书、考研证书、四六级证书等证书详情，便于学生统一管理自身证书。学生可以通过访问学信网申请签发个人业务身份凭证，网站系统通过学生的身份证、姓名、人脸等身份信息，验证学生的BSN官方实名DID标识，并写入自己的签发凭证所用私钥对应的公钥。当学生在不同公司就业时，相关公司可以通过凭证签发方学信网公示的公钥对凭证的签名进行验证，证明凭证内包含的学历、学位和证书信息是由学信网提供并背书的。如果需要更严谨，公司也可以根据学生的BSN官方实名DID标识或与之关联的BSN全网分布式域名，查询学信网公示的公钥是否在BSN官方实名DID文档内，证明学生的实名身份，以及与学信网的业务关系。

3. 技术流程

- 访问BSN-DDC官方门户网站<https://ddc.bsnbase.com>，注册成为业务平台方，并购买相应套餐；
- 业务平台方根据《BSN实名DID服务技术接口文档》（接口文档）在系统后台服务集成BSN实名DID服务SDK；随后业务平台方调用接口文档“7.3.1 申领DID”方法（需要消耗BSN业务实名DID套餐）完成BSN官方业务DID的申领，接着调用接口文档“7.3.7 注册发证方”方法完成发证方信息上链，最后调用接口文档“7.3.9 上传凭证模版”方法进行BSN自定义业务个人身份凭证模版上传（需要消耗能量值）；
- 业务平台方为用户申请业务个人身份凭证签发时，如果用户没有BSN官方实名DID，需要调用接口文档“7.2.1 申领DID”方法（需要消耗BSN官方实名DID套餐）为该用户完成BSN官方实名DID的申领，随后业务平台方调用接口文档“7.3.11 查询凭证模版”方法获取业务个人身份凭证模版，调用接口文档“7.3.13 签发凭证”方法完成

签发业务个人身份凭证(SDK已提供SM2算法, 如需其他算法可自行实现); 平台方也可以选择调用接口文档"7.3.17凭证哈希存证"方法将该凭证哈希上传到延安链官方存证合约内 (需要消耗能量值) ;

- 当第三方需要核验业务个人身份凭证时, 利用业务平台方提供的公钥对业务个人身份凭证进行自行核验 (不需要在BSN-DDC基础网络注册) 。

4. 所需套餐

- 需要购买BSN官方实名DID服务套餐 (每次实名核验 (姓名+身份证) /实人核验 (姓名+身份证+人像) +生成或更新实名DID文档大约需要花费0.75-1.2元人民币) , 套餐详细内容请点击[查看](#);
- 需要购买BSN业务实名DID服务套餐 (每次业务实名DID的生成、销毁DID文档大约需要花费0.35-0.5元人民币) , 套餐详细内容请点击[查看](#);
- 需要购买BSN-DDC网络能量值套餐 (每次上传BSN自定义业务个人身份凭证模板消耗约0.2元人民币, 调用BSN延安链官方存证合约需要花费约0.06元人民币) , 套餐详细内容请点击[查看](#)。

5. 数据安全说明

- 所有终端用户的个人敏感信息均由业务方进行加密后, 才通过BSN实名DID服务API接口发送到CTID数字身份链平台, 并最终在延安链上生成BSN官方实名DID。在整个过程中, BSN各方无法接触、收集或存储任何个人信息;
- 延安链由国家信息中心、中国移动集团设计院、CTID数字身份链平台运营方、信通院云大所和红枣科技通过各自建立验证节点来进行共治共管, 以确保没有任何单独一方可以对链环境进行重构或者修改;
- BSN实名DID服务相应的智能合约由CTID数字身份链平台部署并管理, 任何其他公司和人员都无法对该合约进行干扰和修改, 以确保合约本身的安全性和权威性;
- BSN官方实名DID由权威的CTID数字身份链平台生成, 其签发私钥对应的公钥是公开的, 任何人都可以通过公钥来验证BSN官方实名DID的生成方为合法并具有公信力的机构。

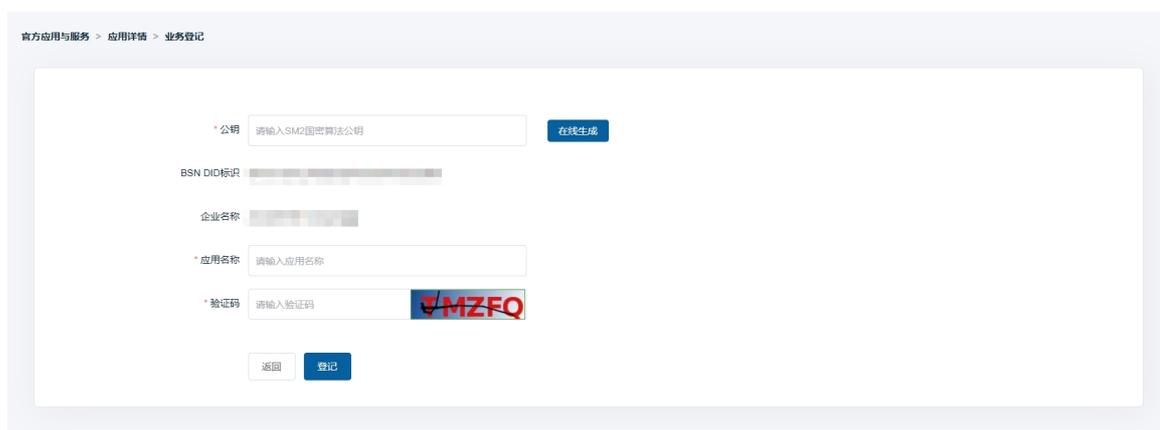
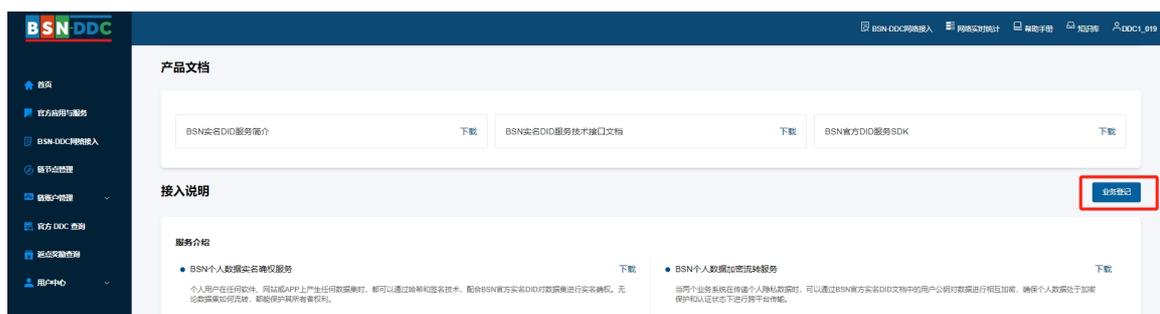
第二章 快速接入指南

接入BSN-DDC网络

- 企业机构需要访问 ddc.bsnbase.com 注册为业务平台方。
- 企业机构需要登录BSN-DDC官方门户，生成BSN平台方DID。详情请参见 [BSN-DDC帮助手册](#)。

业务登记

- 企业机构按照标准SM2国密算法生成公私钥对；
- 企业机构需要登录BSN-DDC官方门户，在BSN实名DID服务的应用详情页面，点击【业务登记】按钮，将生成的公钥、BSN平台方DID标识符、企业名称、应用名称（可以是网站名称、业务系统平台名称等）信息进行登记；
- BSN客服人员完成初审后，将上述信息发送给中盾安信进行业务机构登记（1-3个工作日）；
- BSN客服人员以邮件通知方式向您回复登记结果。



购买套餐

企业机构需在“BSN-DDC官方门户 - 官方应用与服务 - BSN实名DID服务 - 购买套餐”，购买相关套餐。（[了解套餐定价](#)）

第三章 套餐定价

购买套餐请前往[BSN-DDC官方门户](#)。

服务名称	操作	核验方式	套餐名称	调用次数	单价	优惠单价 (截止2024年6月30日)	套餐金额
BSN官方实名DID服务 签发方、合约部署方：CTID数字身份链平台	生成、更新（增加业务公钥）、 二要素查询DID标识	实名核验(姓名+身份证)	二项核验DID套餐一	10,000次	2元/次	1元/次	10,000元
			二项核验DID套餐二	120,000次	2元/次	0.83元/次	100,000元
			二项核验DID套餐三	400,000次	2元/次	0.75元/次	300,000元
		实人核验(姓名+身份证+人像)	三项核验DID套餐一	8,333次	2.5元/次	1.2元/次	10,000元
			三项核验DID套餐二	100,000次	2.5元/次	1元/次	100,000元
			三项核验DID套餐三	340,000次	2.5元/次	0.88元/次	300,000元
BSN业务实名DID服务 签发方：业务方+BSN联盟 合约部署方：BSN联盟	生成、更新（不扣除调用次数，仅消耗能量值）、销毁	使用BSN官方实名DID中的业务公钥对应的私钥签名+嵌入实名DID标识	业务实名DID套餐一	20,000次	1元/次	0.5元/次	10,000元
			业务实名DID套餐二	230,000次	1元/次	0.43元/次	100,000元
			业务实名DID套餐三	850,000次	1元/次	0.35元/次	300,000元
BSN官方实名身份凭证服务 签发方、合约部署方：CTID数字身份链平台	生成、更新	实名核验(姓名+身份证)	二项核验凭证套餐一	10,000次	2元/次	1元/次	10,000元
			二项核验凭证套餐二	120,000次	2元/次	0.83元/次	100,000元
			二项核验凭证套餐三	400,000次	2元/次	0.75元/次	300,000元
		实人核验(姓名+身份证+人像)	三项核验凭证套餐一	8,333次	2.5元/次	1.2元/次	10,000元
			三项核验凭证套餐二	100,000次	2.5元/次	1元/次	100,000元
			三项核验凭证套餐三	340,000次	2.5元/次	0.88元/次	300,000元

Copyright 北京红枣科技有限公司

第四章 联系我们

如果您有任何问题，请联系我们：

客服电话：400-071-8215

客服邮件：support@bsnbase.com

BSN官方门户：bsnbase.com

BSN-DDC基础网络门户：ddc.bsnbase.com

BSN微信公众号二维码：



Copyright 北京红枣科技有限公司