可信分布式身份服务

产品介绍

文档版本 01

发布日期 2024-11-12

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目 录

1 图解可信分布式身份服务

2 产品概述

可信分布式身份服务(Trusted Decentralized Identity Service，简称TDIS)是一种基于区块链的分布式数字身份及可验证凭证的注册、签发、管理平台。符合W3C标准规范。为个人和企业用户提供统一的、可自解释的、移植性强的分布式身份标识。同时支持多场景的可验证凭证管理，细粒度的凭证签发和验证，有效解决跨部门、跨企业、跨地域的身份认证难和隐私泄露等问题。

说明

当前仅“华北-北京四”区域支持可信分布式身份服务。

基本概念

- 分布式身份(Decentralized Identity, DID)：一种新型的标识符，可实现可验证的、去中心化的数字身份。
- 可验证凭证(Verifiable Credential, VC): 一种可验证具备防篡改能力的数字化凭证。包含物理凭证可代表的所有信息，签发机构(者)相关信息、凭证类型信息(驾照、保险卡)、凭证声明属性信息(出生日期、国籍)、凭证限制相关信息(过期时间、使用条款)、凭证所有者信息(身份证号、did标识、姓名)等等。
- 签发者(Issuer): 分布式身份系统中的角色之一，根据业务逻辑验证后，负责签发可验证凭证。
- 持有者(Holder): 分布式身份系统中的角色之一，根据业务需要可向签发者申请可验证凭证，向验证者出示已持有的可验证凭证。
- 验证者(Verifier): 分布式身份系统的角色之一，可校验持有者出示的可验证凭证，用于支撑后续业务决策。

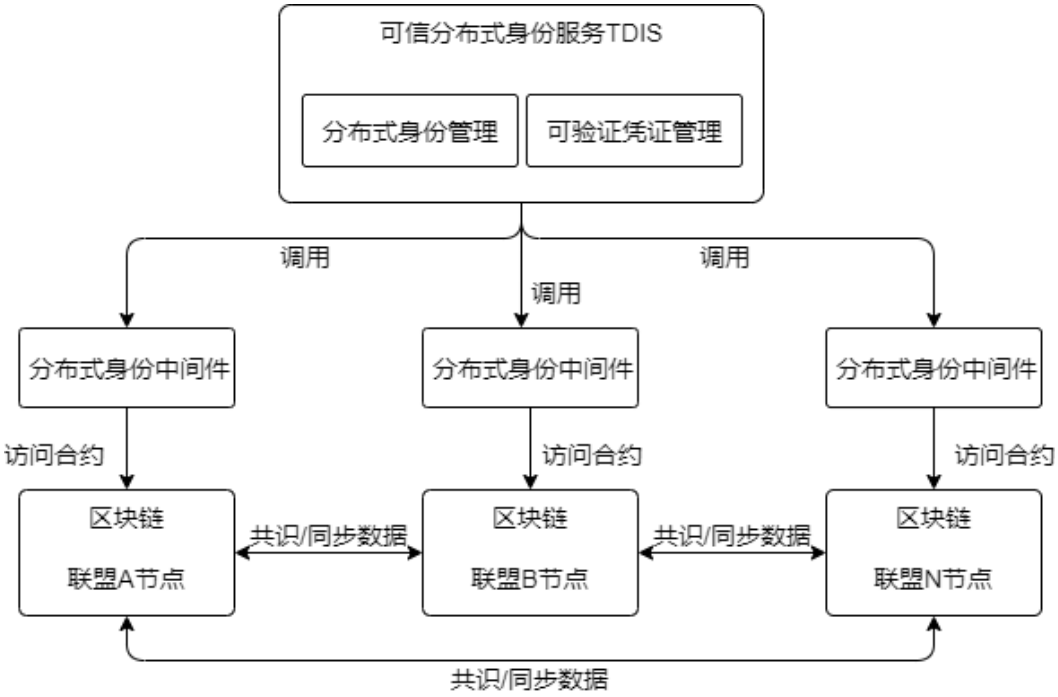
说明

每个did可以是设备、应用、组织或者个人。每个did身份可以同时是签发者、持有者或者验证者角色。

分布式身份服务调用原理

使用可信分布式身份TDIS之前，无需购买区块链和安装区块链服务，单击开通并申请免费套餐包后即可使用。用户通过TDIS服务提供的RESTful接口进行分布式身份和可验证凭证的管理。

图 2-1 分布式身份服务调用原理

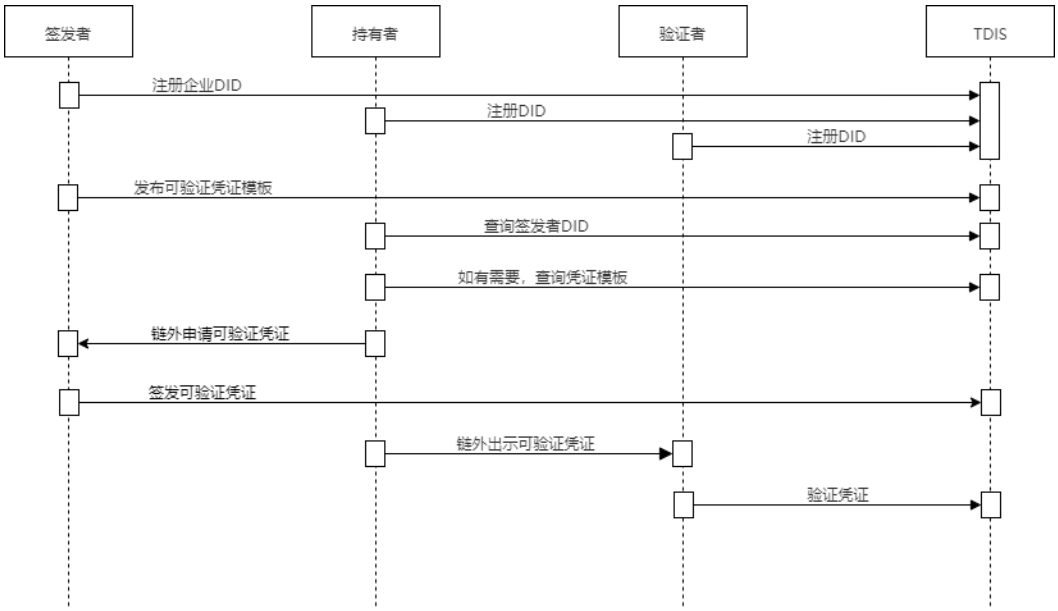


使用方式

根据持有者申请可验证凭证的方式，将可信分布式身份服务的使用分为链外申请模式和链上申请模式。

- 链外申请模式中，持有者将申请可验证凭证的身份/凭证数据直接发送给签发者。
- 链上申请模式中，持有者将申请可验证凭证的身份/凭证数据加密存储于区块链。

图 2-2 可信分布式身份使用时序图(链外申请模式)



链上申请模式中，根据持有者与签发者之间是否需要通信信道，分为在线申请和离线申请。

图 2-3 可信分布式身份使用时序图(链上申请-在线申请模式)

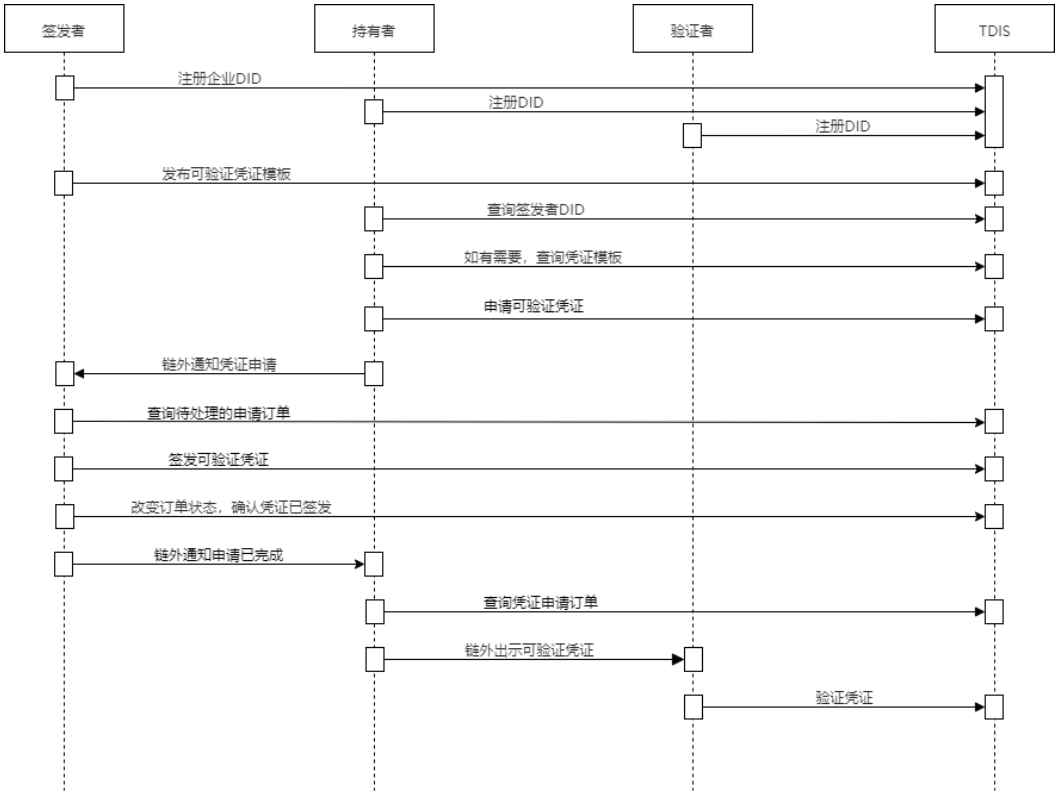
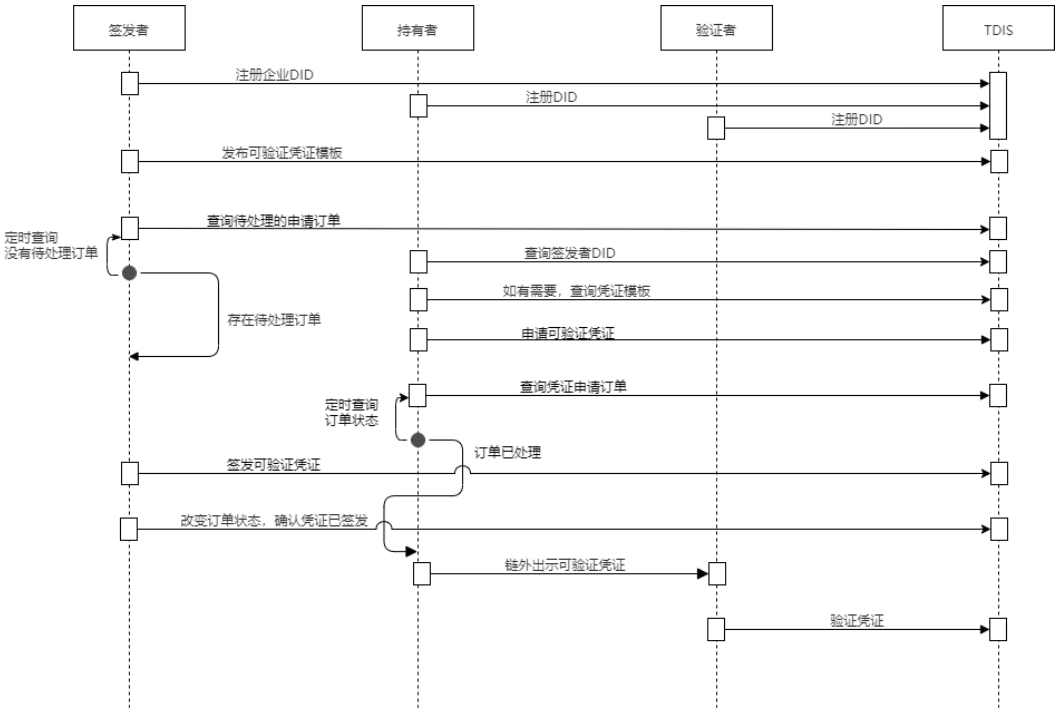


图 2-4 可信分布式身份使用时序图(链上申请-离线申请模式)



与区块链服务 BCS 的关系

区块链服务（Blockchain Service简称BCS）是面向企业及开发者提供的区块链技术服务平台，它可以帮助您快速部署、管理、维护区块链网络，降低您使用区块链的门槛，让您专注于自身业务的开发与创新，实现业务快速上链。

分布式身份服务TDIS依赖区块链服务BCS。用户无需在区块链服务BCS购买区块链，可直接开通TDIS服务使用基于BCS服务构建的可信分布式身份服务。实现分布式身份和可验证凭证的生成、申请、签发等管理能力，以及数据的发布、授权、分享、解密等能力。

3 产品功能

可信分布式身份服务支持以下功能：

表 3-1 功能说明

功能	说明
套餐包管理	支持申请套餐包，查看套餐包状态、剩余量、购买时间等。
服务监控	支持查看接口调用情况，例如总调用量、调用成功量、调用失败量等。
身份管理接口	支持以RESTful API的方式调用分布式身份和可验证凭证的管理功能。例如，身份创建、更新，可验证凭证申请、签发、验证等功能。

4 产品优势

- **分布式身份系统**

  遵循W3C的 Decentralized Identifiers(DIDs)v1.0 和 Verifiable Credentials(VC)v1.0 标准规范实现。系统扩展性强，支持身份和可验证凭证的全流程链上管理能力。

- **强数据隐私保护**

  可验证凭证支持基于属性级别的细粒度出示，凭证使用者可根据隐私保护需要，任意组合出示凭证中的属性给验证者完成验证，最大程度保护用户隐私，同时解除了已签发凭证对应用业务场景的限制。 凭证申请和签发的相关材料全链路加密存储，使数据可用不可见。

- **丰富的扩展组件**

  提供凭证模板管理、链下凭证签发、密钥托管等扩展功能组件，帮助用户基于分布式身份快速构建应用，无须购买和管理区块链资源。

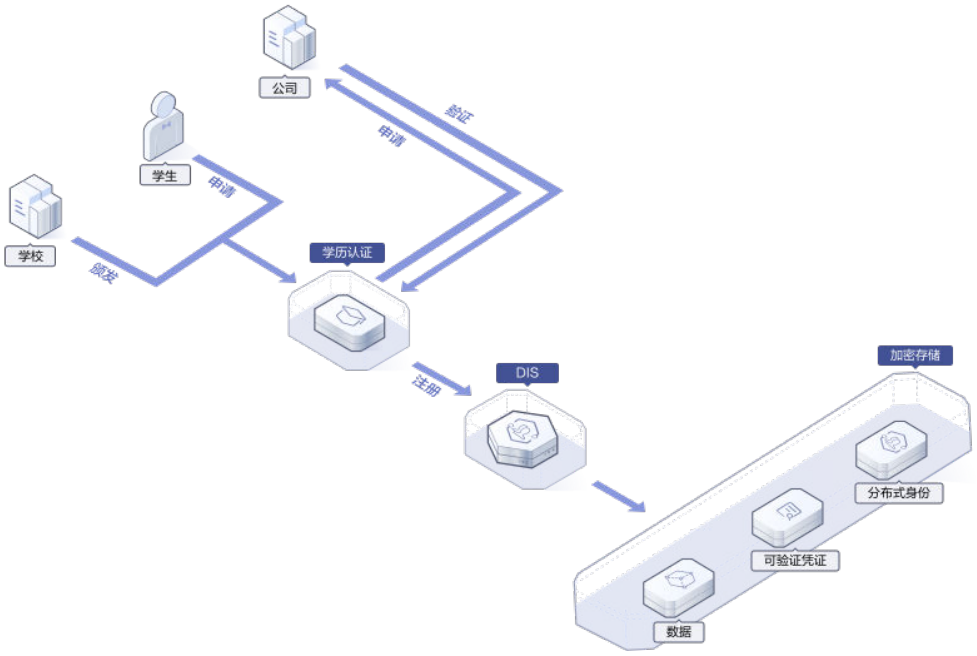
5 应用场景

基于可信分布式身份构建电子证照应用平台。

行业痛点

解决公众办事证照多、核验慢、难追溯、证照使用难审计、难监管等痛点。同时保护用户隐私，增强身份凭证自主可控。

方案架构



方案优势

- **完备的身份和认证管理**

  随着数字社会的发展，数字身份得到越来越多的使用。传统的身份管理中，身份颁发和获取依赖中心化的第三方，无法实现身份的自主可控、自解释。同时身份的可移植性差。TDIS服务可提供完备的身份管理和认证凭证管理。

- **强数据隐私保护**

分布式场景下用户通过出示凭证获得相应的权限和权益。但凭证出示粒度较粗，隐私保护能力较差，在出示验签的过程中导致用户无关属性暴露。TDIS服务提供强数据隐私保护能力，保障证照应用中的证照数据可用不可见。

- **丰富易用的扩展组件**

  证照应用中凭证多种多样，难于管理和维护。凭证模板管理组件可以提将证照统一化、标准化。屏蔽底层区块链用户接入门槛，可快速集成分布式身份构建业务。

6 权限管理

如果您需要对华为云上购买的TDIS资源，给企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制华为云资源的访问。

通过IAM，您可以在华为云账号中给员工创建IAM用户，并使用策略来控制他们对华为云资源的访问范围。例如您的员工中有负责软件开发的人员，您希望他们拥有TDIS的使用权限，但是不希望他们拥有删除TDIS等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用TDIS，但是不允许删除TDIS的权限策略，控制他们对TDIS资源的使用范围。

如果华为云账号已经能满足您的要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用TDIS服务的其它功能。

IAM是华为云提供权限管理的基础服务，无需付费即可使用，您只需要为您账号中的资源进行付费。

TDIS 权限

默认情况下，新建的IAM用户没有任何权限，您需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

TDIS部署时通过物理区域划分，为项目级服务。授权时，“作用范围”需要选择“区域级项目”，然后在指定区域（如华北-北京4）对应的项目（cn-north-4）中设置相关权限，并且该权限仅对此项目生效；如果在“所有项目”中设置权限，则该权限在所有区域项目中都生效。访问TDIS时，需要先切换至授权区域。

如下表所示，包括了TDIS的所有系统权限。

表 6-1 TDIS 系统权限

系统权限	权限描述	权限类别	说明
Tenant Administrator	全部云服务管理员（除IAM权限）	系统角色	详情请参考**系统权限**。
Tenant Guest	全部云服务只读权限（除IAM管理权限）	系统角色	

操作步骤

步骤1 管理员登录统一身份认证服务控制台。

步骤2 创建用户并授权，详细操作请参考**创建IAM用户**和给**IAM用户授权**。

步骤3 创建用户组并授权，请参考**详细操作**。

步骤4 用户组添加2创建的用户，使用户具备用户组的权限，实现用户的授权。请参考**详细操作**。

----结束

相关链接

IAM产品介绍

7 计费说明

本服务目前处于公测试运行阶段，用户可以开通服务后申请免费套餐包进行使用。

服务公测期间数据不承诺保存，正式商用后数据会清空。

GET 类型的RESTful API调用，不会扣除套餐包的调用次数。

8 约束与限制

限制项	说明
使用区域	只支持“华北-北京四”区域。
套餐包	目前仅支持申请1个免费套餐包，包含2000次调用。 **说明** 如果需要使用超过2000次的调用次数，请联系技术支持人员开通。

