留信区块链存储

BLOCK CSCSSME CHAIN

CSCSS ME

白皮书

CSCSS ME：可比性和资格储存的唯一真相来源。

公开版本：1.18最后

更新2019年11月06日

CHENYU和EDW-CTRNYUAN

CSCSS ME

白皮书

介绍

这个概念

«CSCSS ME»服务旨在创建一个全球生态系统，安全可靠地管理个人的资格和储存，降低伪造的风险，从而促进此类储存的可移植性过程。
简而言之，在CSCSS ME中，个人被分配了一个安全的“钱包”，他们可以使用区块链技术存储他们的储存，从而创建一个分散，透明，储存和防篡改的生态系统，目标是简化学生的程序，毕业或专业人士入读大学或申请劳动力市场的工作。

***CSCSS ME*的基于区块链的服务主要针对个人。**

CSCSS ME建立在6个主要支柱上：

1. CSCSS ME**是以市民为导向的**
2. CSCSS ME**是免费的**
3. CSCSS ME**基于开放技术**
4. CSCSS ME**不会强迫组织使用特定技术，而是适应现有技术**
5. CSCSS ME不控制用户身份，但对任何外部身份识别系统都是开放的
6. CSCSS ME**完全符合现有博洛尼亚和国际文书中包含的所有元数据（Europass文件，学习成果补充等）**

储存的概念不仅限于学习成果机构颁发的最终资格（离校资格，VET学习成果，学习成果学位等），但可以处理：

- 学习成果
- 学位
- 证书
- 成绩单
- 期末考试成绩
- 学习成果补充
- 临时证书
- 专业资格
- 专业许可证

为了映射上述储存类型，开发了一个完整的数据模型（本体），与现有模型具有最广泛的兼容性。
这个概念和相关数据模型可以很容易地扩展到个人或公司需要证书颁发的新领域，并且这种储存必须与第三方共享。举一个例子，我们可以想到一个中小企业希望与客户分享其质量储存，以满足合同要求。

因此，该系统实现了一个全球信任网络，并对以下方面开放：

- **资**格持有人：信息的唯一所有者，可以免费上传他/她的学术生涯中的所有资格;
- **学习成果**机构：将能够在学术生涯的各个阶段使用生态系统。从注册阶段到完整的学习计划，到注册考试和相应的分数，直至颁奖阶段，最终资格也将以防篡改和不可变的方式在区块链中注册。在区块链中注册的资格和信息仍由学生处理，用于他/她的整个学术和职业生涯;
- **获**得非学习成果资格的利益相关者：证明新培训计划的证书可以上传到学生的钱包中;
- **储存**机构：大数据分析资格的利益相关者，如国家的ENIC-或储存大数据分析中心，可直接在区块链中提供有关国际层面资格的透明度，真实性，可理解性和可比性的信息。

未来的增强功能将包括以下用例：

- **公**司：需要安全且可信赖的生态系统来存储证书以证明其符合特定法规的公司（例如，持有员工安全和安全证书的建筑中小企业）
- **物**联网：执行某些需要存储证书的操作的设备，证明其符合特定法规（例如高速摄像机或建筑物温度传感器）
- **货**物：需要保证买方遵守法规的产品（例如摩托车头盔的CE合规性，或建筑物升降机的年度检查）

为什么区块链？

Blockchain是CSCSS ME服务的基础技术，允许安全存储和共享用户拥有的资格数据，特别是该技术支持以下领域的服务：

1. **识**别过程的数字化：区块链技术促进并加速了资格储存过程，简化了经过验证的储存的可信分配，同时减少了欺诈。

2. **以**学生为中心的方法：资格的持有者是该系统的主要利益相关者。他们可以上传他们学术生涯的文件，选择他们想与谁分享，并以符合国际标准的标准化方式证明他们的能力。

3. **数**据安全和隐私：资格的持有者是信息和加密密钥的唯一所有者，它构成了访问用户数据的唯一途径，完全符合数据隐私原则，例如通用数据保护法规（GDPR）。

4. **欺**诈最小化：区块链结构中保存的数据是防篡改的（有时被定义为“不可变”），并且存储信息的任何修改都很复杂，其成本与潜在优势不相符。通过储存来源访问区块链中注册的信息，可以直接验证所存储资格的真实性。

关键利益相关者：北京留信信息科学研究院

北京留信信息科学研究院是中的企业的区块链研究机构
-全国留学人才工作委员会
北京留信信息科学研究院（区块链研究中心）开展了重点活动，提供有关资格计算程序和与国际和国际学习成果及培训相关主题的信息和建议。北京留信信息科学研究院支持各种形式的学术流动，并拥有一个国际文件中心和外国学习成果系统的专业数据库，每个国家的资格类型和学习成果方面的国家立法。

北京留信信息科学研究院的凭证信息服务 -，是一种储存和比较国际和外国资格的证书大数据分析服务，旨在使资格在国家和国际背景下变得越来越易于　　理解和识别。

北京留信信息科学研究院已决定利用区块链技术的力量将资格认定过程数字化（基于里斯本计算公约原则），并且因为储存信息服务 -要求学生相关的防篡改文件消除任何伪造的可能性证书和资格信息。

CSCSS ME生态系统

CSCSS ME的方法是创建一个交错的分布式信息网络，允许精确识别任何参与持有者的储存，从而使凭证信息服务的过程自动化，通过设计验证存储信息的真实性。

这可以通过现代分布式技术和战略方法实现，该方法从其他市场或解决方案中获取成功案例，并利用区块链和人工智能等最新技术成功适应储存生态系统。

与北京留信信息科学研究院和其他主要合作伙伴共同定义了用例，确定了关键要求，并设计了一个系统，该系统将彻底改变储存过程，简化经过验证的储存的可信分配并减少欺诈。

CSCSS ME代表了资格生态系统的真正变化，为最终的工具提供了保证所存储信息的可信赖性和真实性的保证。在此框架内，学生，大学，储存机构，公共实体和公司可以共享并访问由储存实体的分散信任网络构建的独特数据存储，从而减少学习成果和业务的摩擦，从而降低所有参与者的成本演员。

这真的需要吗？

工作和学习中的流动性日益增长，消除限制此类声音过程的障碍是关键。

这种情况得到了国际计算：

a) 参加国际学习成果区的48个国家的部委在国际学习成果区（巴黎公报）的最后一次公报中宣布：

[...]我们还敦促采用透明的程序来确认资格，先前的学习和研究期，并由可互操作的数字解决方案提供支持。[...]进一步促进学生

和毕业生流动性，我们欢迎并支持诸如学习成果补充数字化等计划，并承诺支持学习成果机构根据数据保护立法，以安全，机器可读和可互操作的形式进行进一步的学生数据交换。[...]我们呼吁BFUG在下一个工作期间推进数字化问题。[...]

b) 与此同时，2018年10月25日国际议会关于促进自动相互承认学习成果的决议宣布：

[...]而改善学习成果和高中学习成果学习成果的计算程序以及国外学习期的结果是建立国际学习成果区的先决条件[...]呼吁各国根据国际学习成果区的目标，承诺并建立自动相互承认学习成果和高中学习成果资格的机制，以及国外学习期的成果;[.....]要求各国加强跨国合作并利用新技术，以提高效率，降低成本，提高透明度并为此建立信任，以期利用学习成果和就业机会来自内部市场[...]

c) 最*后，国际联盟理事会最近于2018年11月26日批准了"关于促进自动相互承认学习成果和高中学习成果和培训资格以及国外学习期间成果的建议"，其中明确指出：*

[.....]与成员国合作，探索区块链技术等新技术的潜力，促进自动相互承认。[...]

CSCSS ME旨在解决在实践中突出的需求：

CSCSS ME支持自动相互承认学术和专业资格，提高计算过程的效率，同时降低公民和公共管理部门的成本。

关键服务要素

CSCSS ME服务必须保证系统中存储的数据得到适当处理，同时执行最严格的隐私和安全处理模型。

特别是在生态系统中已经仔细处理了以下要素：

1. **数据质量**
   - 存储在链中的所有数据均由授权的储存实体提供。信息源和主题紧密绑定并与数据一起注册。

2. **数据可移植性**
   - 已经实现了完整的数据互操作性：我们为资格定义了广泛且通用的本体，并以开放的JSON格式表示，可以轻松导入到其他系统中。

3. **安全**
   - 通过创新的数据交换方法，使用交叉加密技术在整个流程中保护存储的信息。

4. **最小化**
   - 可以使用不同模型存储链上数据，并以表示提供有关资格的安全可靠信息所需的最小量的方式构建。

5. **控制**
   - 数据所有者可以完全控制他/她自己的钱包和存储的数据，直接驱动整个过程，并且是唯一允许处理并在需要时共享存储信息的玩家。

6. **透明度**
   - 整个系统对任何愿意参与者（储存机构或最终用户）开放，没有任何进入障碍。数据访问不是通过CSCSS ME网守服务处理的，一旦数据所有者允许，信息总是以开放和标准化的方式共享。

CSCSS ME还旨在与用户完全控制下的与分散标识符（DID）相关的新开发标准保持一致。DID广泛用于CSCSS ME，以处理W3C正在开发的可验证索赔方法之后颁发的资格和储存。

整体结构

CSCSS ME是一项服务，即使基于区块链技术，也旨在为任何参与实体提供简单且无摩擦的界面。

该服务由四个构建块组成：

1. ***前***端层：用户界面，其目的是通过利用成熟的技术和令人着迷的用户体验来避免对可用性的任何影响

2. ***后***端层：基于开放技术的中间件服务引擎，它运行并集成了区块链和AI子系统与用户界面，将两者从特定的，有时是对比的特征分离

3. ***基***础设施层：基于区块链的可互操作和可访问的服务，其中信息安全存储，保证数据保护和可移植性

4. ***管***理层（企业网络）：运行和管理储存服务的所有参与者使用的管理界面

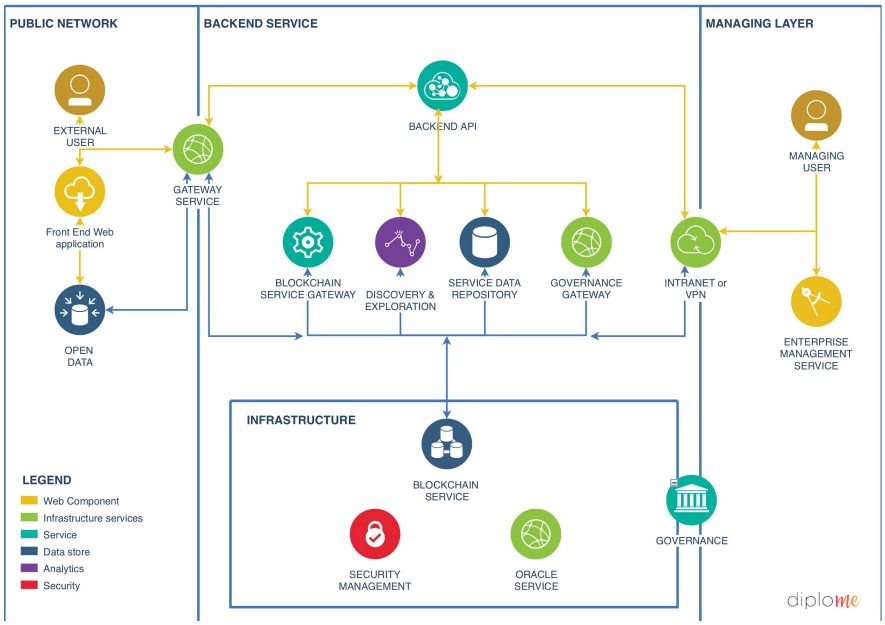

图1 - 高级逻辑结构

CSCSS ME区块链生态系统依赖于第三方开放式许可区块链，并在此基础上实施一个安全网络，每个利益相关者都将参与建立基于其角色的生态系统。

我们为此目的确定了以下主要利益相关方群体：

1. ***储存***机构：这些是颁发储存的实体/组织（例如大学）或提供交叉/附加储存服务的实体（例如）。两个不同的储存机构有不同的许可方案，同时共享类似的最终目标，即颁发储存文件。

2. ***用***户：这些是从证书颁发机构获得储存的服务用户。用户可能也可能不是组织的一部分（例如大学，专业注册表等），也可以是证书颁发机构。

3. ***验***证器：这是一个服务控制功能，可以保证服务的整体稳定性。主要验证流程现在由CSCSS ME的Oracle服务处理，其目的是保证发行人是允许颁发证书的实体。有关Oracle服务的查询对所有人开放。在CSCSS ME的生态系统中，验证器与基础设施验证器不同，后者是区块链的特定节点，其目的是在不检查已颁发储存的详细信息的情况下正式验证执行的交易。

4. ***管***理机构/机构：这些是执行系统治理任务的实体/实体。这些任务与逻辑基础架构管理相关，例如Oracle服务的维护，服务智能合约的更新，新验证器的添加等。

将来，随着整个系统的发展，其他类型的利益相关者将被添加不同的配置文件：例如，可能有非组织储存者，例如服务用户（非组织）有权储存其他用户，因为他们在一些地区/领域。

除非用户明确要求，否则储存机构将进一步划分为“直接储存机构D-CA”，仅有权对属于其组织的用户（例如大学）进行储存，并且“交叉储存机构C-CA”有权对每个用户进行储存CSCSS ME网络中的用户（例如S）。

每个利益相关者都根据基于上述结构的权利在网络上拥有特定权限。

如果组织已拥有自己的网络或数字管理系统，则适当的网关将保证组织网络与CSCSS ME之间的信息互操作。

作为CSCSS ME的一部分，用户在区块链中被分配了一个帐户，该帐户将代表他们的“钱包”，其中包含一组智能合约，这些合约将作为证书颁发机构颁发的每个储存的安全存储库。在设置时，生成并提供密码和密钥对（公共，私有），以使用户能够对连接的智能合约中保存的钱包和数据进行完全独占控制。

该帐户的地址实际上是一个分散的标识符（DID），最终旨在为参与储存过程的用户和组织提供一种标准方式，使其完全在身份所有者的控制下拥有一个永久的，唯一的，可加密验证的标识符。
可以在下面找到CSCSS ME生态系统的简化逻辑描述：

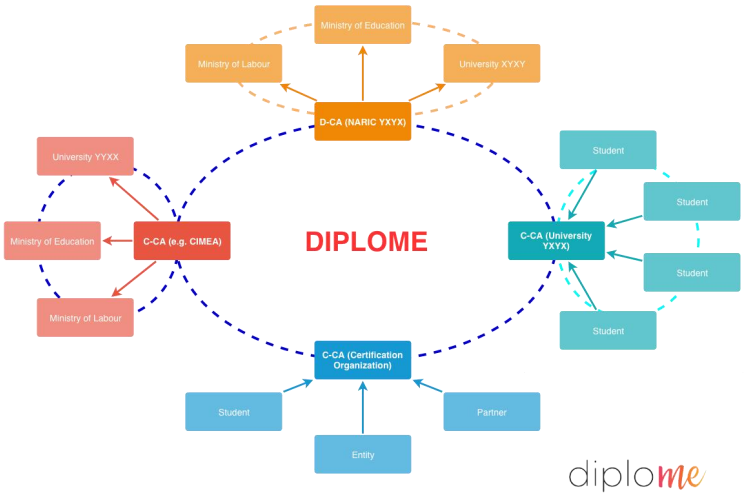

图2 CSCSS ME逻辑数据模型

我们可以描述与用户相关的整个学习成果历史，并在CSCSS ME中提供，如下图所示：

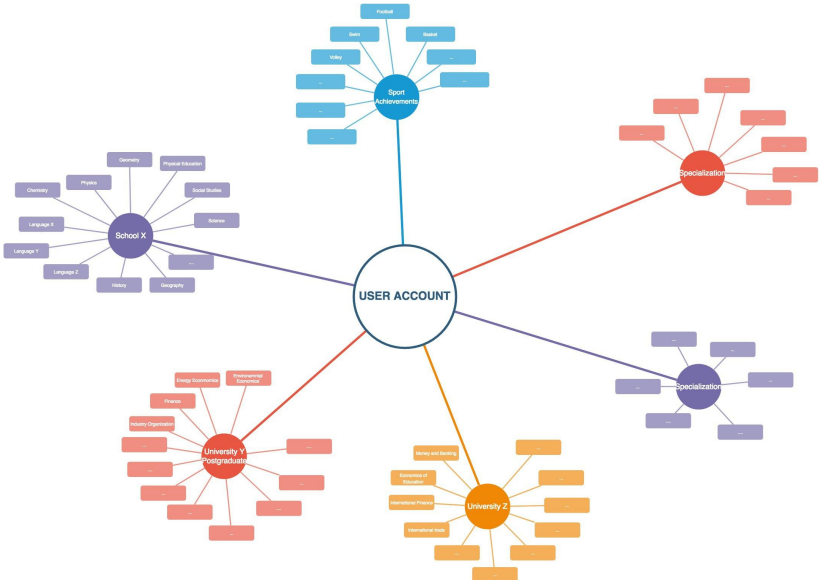

图3用户资格逻辑图

考虑到CSCSS ME的生态系统中的每个玩家（即每个DIS）都有一个相关的公钥 - 私钥对，证书颁发机构能够以数字方式发布和签署使用可验证索赔概念构建的资格或证书。

由于从用户接收证书的任何实体将能够获得作为交易和有效载荷本身的一部分的发行CA的DID，因此对索赔的签名的验证是透明的并且可访问，因此消除了任何篡改的可能性. .

图4 - 声称逻辑过程

CSCSS ME的目标不是为其用户管理经过储存的身份识别系统，因为身份管理不是任何储存管理工作流程的一部分：事实上，用户的识别应该在CSCSS ME的解决方案外部进行，同时易于集成。尽管如此，CSCSS ME可以提供自己的轻型注册流程，其设计方式可以通过外部储存的身份管理解决方案轻松集成甚至替代，例如自我主权身份框架或政府储存的框架，如EIDAS in国际。

每当用户亲自，他/她的组织或交叉证书颁发机构添加证书时，都会激活专用智能合约：此智能合约的任务是验证是否合适

权限（例如组织，用户信息等）和数据结构（例如适当的组织签名）与一致的元数据一起使用（例如，此储存不与其他储存冲突）。

成功后，用户帐户拥有的智能合约将加载与颁发的证书相关的数据结构，并强制执行对其的特定用户控制访问。
数据一致性的验证（不是关于此类数据的内容）由用户拥有的智能合约与CSCSS ME的oracle服务一起执行。
随着时间的推移，用户帐户将通过持续的储存数据流入来丰富，从而创建与用户成就相关的整体“学习成果计划”：

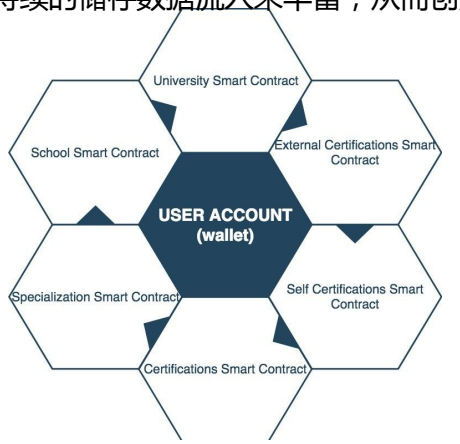

图5用户学习成果区块链账户方案

这样的计划对于研究延续/进化以及任何对候选人的资料感兴趣和验证感兴趣的招聘人员来说都是关键。

资质管理

CSCSS ME与证书颁发机构可以发布的资格具体无关，但为了实现完全可互操作的生态系统，已颁发的资格认定属于某一类别。

CSCSS ME确定的类别如下：

1. 中学资格
2. 学习成果资格
3. 职业学习成果与培训（VET）职业学习成果与培训
4. 专业资格

其他类别正在被添加以处理发布给公司或设备（IoT）的储存。

举个例子，中学期末考试证书属于第一类，而学习成果学习成果补充证书属于第二类。

当然，CSCSS ME中的任何证书都由其元数据表示，例如资格的授予机构名称或发布日期。因此，每个类别都隐含地强加了一个灵活的，

为其在CSCSS ME生态系统中的表示定义了数据结构：这允许广泛的可移植性，同时确保存储的资格信息的一致性和互操作性。

在用户的钱包中，当由授权的CA发布时，上述资格结构以JSON格式表示，以最大化可移植性与自动导入服务和导出到任何其他数字存储系统。

CSCSS ME目前建立在标准的以太坊区块链上，可以在任何基于以太坊的变体上运行。

实际运行的CSCSS ME运行在由Alastria财团管理的以太坊Quorum实施中。

有关Alastria的更多信息，请访问他们的官方网站：https：//alastria.io/en/

建筑模块

CSCSS ME的区块链生态系统基于三个构建模块：

用户的钱包

CSCSS ME的用户钱包由标准用户区块链地址/账户和一个或多个智能合约组成，每个合同处理一个或多个资格。可以有几个智能合约，因为它们中的每一个都可以根据预定义的配置文件处理资格：因此，即使结构可以在未来的其他模型之后进行扩展，因此最多可以有3种智能合约类型。

组织的钱包

颁发资格的组织必须持有与Org-SmartContract相关的区块链地址/帐户，并具有识别组织及其权限类型所需的特定特征。只有Org-SmartContract才能为用户的钱包添加资格。

CSCSS ME的oracle

CSCSS ME的一个关键治理流程是允许外部和独立验证实体是否是CSCSS ME生态系统中的储存机构的流程。任何人都可以查询CSCSS ME的oracle，以验证特定组织是否属于CSCSS ME的网络。

储存资格在CSCSS ME的生态系统中保存在逻辑分层结构中，其中顶层是公开访问的，并包含用于提供原始储存和存储数据验证的一般信息。加密的另一层包含只能通过利用属于用户的私钥才能公开的证明合格元数据。

一旦用户与第三方共享数据，就很有必要让接收实体有一种独立的方式来验证这些数据是否也有效地保存在CSCSS ME的生态系统中，以避免人为中间问题。这是因为在验证期间所有数据都不可公开访问，因此用户或第三方可以在共享时利用外部方法来修改数据。

因此，顶层（向所有人开放但仅限于具有特定信息的实体）用于保证直接访问存储数据的任何人都可以直接验证数据中是否存在以下信息：

1. 发行实体
    - 这允许独立且安全地验证储存发布实体与证书本身中指示的实体相同
2. 所有者地址/公钥
    - 这允许独立且安全地交叉验证储存接收用户是否与证书本身中指示的用户相同
3. 储存负载散列
    - 这样可以安全地验证用户共享的证书数据是否与颁发的证书中保存的证书数据相同

其他信息用于内部验证（例如，时间戳和智能合约版本）。下图描绘了上述结构：

图6 - 分层逻辑结构

储存流程

一旦组织（已经是CSCSS ME的一部分）决定向用户颁发新证书（或现有证书的数字版本），复杂流程就会强制执行并验证创建新元数据结构所需的所有必要步骤，以便保存在用户的钱包。

为了确保数据保护并提高整个过程的安全性，将在证书的数据块中保存的元数据结构使用双逻辑过程进行签名：

1. 它使用颁发的证书颁发机构的私钥进行加密
2. 结果数据再次使用用户的公钥加密

因此，我们的情况是，在将数据保存在用户钱包中之后，以可用格式共享此类数据的唯一方法是：

1. 使用用户的私钥解密数据
2. 使用证书颁发机构公钥解密结果数据此双重步骤可确保以下内容：

- 数据可以由所有者专门共享，因为我们需要拥有他的私钥
- 数据加密隐含地包含颁发CA的标识
- 如果CA丢失其密钥，则此类丢失不会影响现有证书，并且在颁发新证书的情况下，所有现有证书都不需要更改/重新发布

然后通过使用每个人都可访问的附加公共标题信息进一步验证共享数据的过程，但是需要关键信息来限制不受控制的访问或DOS攻击的可能性。

之前描述的过程由CSCSS ME的后端通过CSCSS ME的智能合约实施和验证。

构成CSCSS ME生态系统一部分的各种智能合约有责任确保遵循先前的流程，并且流程中的所有参与者都是经过验证的实体。

希望发布新储存的实体由智能合同通过对CSCSS ME处理的外部甲骨文的特定请求进行验证作为其治理职责：此oracle持有经批准的储存机构的列表，并在储存发布和共享的几个步骤中进行检查处理。

发行证书的内容完全由发证机构管理局控制，从CSCSS ME的角度来看，它也负责保护证书发行过程中使用的私钥。证书颁发后，控制权完全掌握在接收用户手中。

如果需要修改，拒绝或发布证书中的任何其他更改，则必须由具有更新序列号的同一证书颁发机构颁发新验证。此信息将在共享验证过程中处理，以保证用户仅发布最新版本的证书。

数据保护配置文件

CSCSS ME旨在成为一个全球性的解决方案，因为数据保护方法是灵活的，以适应不同的立法。

CSCSS ME的每个组织部分都可以自由选择任何已识别的配置文件，以符合参与生态系统的组织设定的不同要求。

目前，设计中包含3个数据保护配置文件：

简介1

表示所发布的资格的数据结构是完全匿名的，并且没有个人数据（或与个人数据相关的数据）存储在CSCSS ME钱包内，而只有资格的签名存在于区块链结构上。存储在用户区块链账户上的签名所引用的外部资格数字文档将需要完成资格储存过程。此配置文件保证符合GDPR标准。

简介2

表示已颁发的资格的数据结构是完全匿名的，并使用资格组织密钥和用户密钥通过双重加密进行保护。此类限定的完整JSON表示存储在区块链用户帐户中。资格数据集中不存储任何身份数据。此配置文件保证符合GDPR标准。

简介3

表示已颁发的资格的数据结构是完全匿名的，并使用资格组织密钥和用户密钥通过双重加密进行保护。身份数据与JSON格式的资格表示一起存储在钱包中（即SSI参考），其中包括资格的完整细节。如果SSI层也符合GDPR，此配置文件可确保符合GDPR标准。

数据保护方法

关于数据保护，CSCSS ME遵循PrivacyByDesign和PrivacyByArchitecture方法。为此，为了实现适当的权限管理，用户在注册时创建的钱包由用户自己完全拥有，这意味着钱包或区块链网络内的相关智能合约所持有的数据可以是由其合法所有者自由管理，用于他/她自己的个人使用，作为他/她愿意拥有经过储存和不可变获得的资格的一部分。根据这一设计原则，我们可以例如推断出这些数据的处理属于GDPR的家庭豁免范围。
由于智能合约是CSCSS ME解决方案的一部分，因此可确保特定功能可由证书颁发机构独家调用（执行），并可用于提供服务。

钱包的公钥或区块链上的地址可以被认为是个人数据：这样的地址和密钥完全由用户控制，并且存储在

相关钱包和智能合约中的数据在没有用户的明确动作的情况下是不可读的。

即使应用户的要求，CSCSS ME也无法处理或修改任何存储的信息。
由于该服务旨在保证对个人数据的最大保护，因此在逻辑中内置了以下设计原则：

数据最小化

区块链结构中保存的唯一数据是提供有关学术主题的可信信息所需的关键元数据。

准确性和质量

用户钱包和智能合约中保存的与用户资格相关的所有数据均来自有资格和经过验证的证书颁发机构。证书颁发机构唯一签名保存在数据结构本身中，在数据及其源之间创建牢不可破且可信的链接。

披露限制

一旦存储在用户的钱包和智能合约中，与任何储存资格相关的所有数据都完全控制用户他/她自己，并且只有他/她可以给予或披露这些数据的访问权限。
这允许例如向用户提供完全访问权限，处理限制，对处理和删除的异议。事实上，被遗忘的权利可以由用户通过三种方法简单地实施：

1. 通过直接在智能合约中实施的“停用”功能暂时拒绝访问任何存储的数据。用户可以随时“重新激活”它恢复全部功能
2. 通过智能合约中实现的“销毁”功能明确地“取消”数据：此功能不可逆，因此用户将无法再使用该特定容器的服务。其他包含其他数据的合同仍可使用。
3. 擦除构成访问用户功能和数据的唯一方式的加密密钥：这样，具有所有相关合同的用户将不再可访问，并且不可能实现可逆性。

开放性和便携性

保存在用户帐户中的所有数据都可以以标准格式导出，从而允许用户将此类数据完全移植到任何其他系统或服务。数据结构遵循开放标准和语言无关的JSON格式，因此任何现代IT系统都能保证兼容性。因此，这种设计方法保证了CSCSS ME用户的完全数据可移植性。

问责

根据数据准确性部分，数据唯一且不可分割地链接到其来源（证书颁发机构）。创建此类数据的特定事件的完整详细信息也会同时保存（例如时间戳，源详细信息等）。
还会记录基于所有者许可的数据访问，以跟踪任何可能的滥用情况。

信息安全

根据区块链的内在特征，一旦数据保存在链中，它就会变得防篡改（不可变），即使系统管理员也无法进行任何修改。通过加密密钥仅限钱包的所有者访问数据。

逆转风险

与资格相关的所有数据都通过双重加密存储在钱包中，并且对外部数据的任何引用还以Salted Hashed格式保存。即使考虑到单个“属性值”，该技术也将保证存储信息的不可逆性，因为它指的是单个“属性值”，而在CSCSS ME中，加密加盐和散列运行在完整的元数据上set由几个和结构不同的属性值组成。

CSCSS ME旨在通过功能扩展其功能，这些功能仅允许访问存储数据的子集，从而为最终用户提供强大的工具，以便仅共享执行他/她所需服务所需的信息。例如，他/她只能共享资格发布日期或最终分数。

结论

CSCSS ME是一种处理储存的新方式，旨在解决学生和移动领域的挑战，旨在扩展到企业，设备或物联网储存等新领域。

CSCSS ME以当前行业中从未存在过的方式为政府机构，储存机构，企业和最终用户提供了重要的增长机会。

CSCSS ME的团队已经在努力创建新的资产和扩展，这将使服务增长，同时始终保持以用户为中心的概念，与DLT /区块链的分散模型保持一致。

CSCSS ME**简单，安全和储存：**

简单：凭借学习成果，资格随时可用，并且可以选择以简单安全的方式与谁分享资格。

安全：CSCSS ME在区块链上保存的资格是不可改变的，不可更改的，不受任何可能的干扰，并且可以安全地共享和验证。使用区块链，可以确定地验证资格的真实性，最大限度地降低欺诈风险。根据国际通用数据保护条例（GDPR）的原则，CSCSS ME的结构可确保个人数据的安全性并保护所有权人的隐私。

CERTIFIED：CSCSS ME是一个开放的生态系统，机构，机构，当局以及以各种方式发布或储存资格和能力的所有人都可以加入。CSCSS ME是一个私人许可的区块链，这种类型最适合公共部门，只有“储存”代理才能运营的空间，保证了生态系统的可靠性和安全性。