Secure management of IoT devices lifecycle through identities, trust and distributed ledgers

D3.4 DLT-based IoT Identity Manager

Document Summary Information

Grant Agreement No	101020416	**Acronym**	ERATOSTHENES
Full Title	Secure management of IoT devices lifecycle through identities, trust and distributed ledgers		
Start Date	01/10/2021	**Duration**	42 months
Project URL	www.eratosthenes-project.eu		
Deliverable	DLT-based IoT Identity Manager		
Work Package	WP3		
Contractual due date	30/06/2023	**Actual submission date**	27/06/2023
Nature	Other	**Dissemination Level**	PU
Responsible author	Jesús García Rodríguez (UMU)	**Lead Beneficiary**	UMU
Authors	Jesús García Rodríguez, Antonio Skarmeta Gómez (UMU)		
Internal reviewers	Ángel Palomares (ATOS), George Athanasiou (DBC)		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Grant Agreement No 101020416.

Revision history (including peer reviewing & quality control)

Version	Issue Date	% Complete	Changes	Contributor(s)
V0.1	02/05/2023	5%	Initial table of contents	Jesús García Rodríguez (UMU)
V0.2	04/05/2023	6%	Revised table of contents and outline	Jesús García Rodríguez, Antonio Skarmeta Gómez (UMU)
V0.3	09/05/2023	15%	Initial content in section 3	Jesús García Rodríguez (UMU)
V0.4	15/05/2023	30%	Additional content in sections 3, content in section 2	Jesús García Rodríguez (UMU)
V0.5	19/05/2023	50%	Finalize sections 3.1, 3.2.	Jesús García Rodríguez (UMU)
V0.6	26/05/2023	80%	Finalize section 3, section 4 content	Jesús García Rodríguez (UMU)
V1.0	02/06/2023	90%	Final formatting and content refinement, write section 5.	Jesús García Rodríguez (UMU)
V1.1	23/06/2023	100%	Quality Review	Ángel Palomares (ATOS), George Athanasiou (DBC), Jesús García Rodríguez (UMU)

Disclaimer

Copyright message

Table of Contents

List of Figures

List of Tables

Glossary of terms and abbreviations used

Abbreviation / Term	Description
DID	Decentralized Identifier
DLT	Distributed Ledger Technologies
Dp-ABC	Distributed Privacy-Preserving Attribute-Based Credential
IDS	Intrusion Detection System
IIoT	Industrial internet of things
IoT	Internet of Things
JSON	JavaScript Object Notation
MSPL	Medium-level Security Policy Language
MUD	Manufacturer Usage Description
NIST	National Institute of Standards and Technology
P-ABC	Privacy-Preserving Attribute-Based Credential
PoC	Proof of Concept
PS-MS	Pointcheval-Sanders Multi-Signatures
PUF	Physically Unclonable Function
TMB	Trust Manager & Broker
VC	Verifiable Credential
VP	Verifiable Presentation
XACML	eXtensible Access Control Markup Language
ZK	Zero-Knowledge

1 Executive Summary

The purpose of the current report is to document the work performed in the context of Task 3.4 "Distributed ledger-based and privacy-preserving IoT Identity Management" and its results until M21. The deliverable is of type OTHER, and in fact the main outcomes are the initial software prototypes and a research paper that has been sent for publication. This document briefly documents the initial outcomes of the task in relation to the project and is complimentary to the other results, including documentation on the software implementation design and an appendix that reflects the abstract of the research paper. Further results will be documented in deliverable D3.8.

This task has focused on the design and implementation of authentication methods based on advanced cryptographic tools, namely privacy-preserving Attribute-Based Credentials (p-ABC), which enable improved privacy and security capabilities. The solution is enabled through the use of Distributed Ledger Technologies as a public, verifiable and transparent registry that participants can access to retrieve necessary elements like public such as keys or credential schemas. Additionally, the integration into the W3C's Verifiable Credentials standard makes the approach easier to adopt, and easily combined with simpler approaches to cover scenarios where those are necessary, e.g., in very constrained devices.

2 Introduction

This document introduces and discusses the first outcomes of task 4.3.

2.1 Mapping ERATOSTHENES Outputs

Table 1: Adherence to ERATOSTHENES GA Deliverable & Tasks Descriptions

ERATOSTHENES GA Component Title	ERATOSTHENES GA Component Outline	Respective Document Chapter(s)	Justification
DELIVERABLE			
D3.4 DLT-based IoT Identity Manager	This deliverable includes the first version of the Distributed Lerger Technologies (DLT) and privacy-preserving IoT Identity Manager as well as the applied models to the dP-ABC scheme	Section 3, 4	Section 3 covers the component and its positioning in the architecture and the relevant business challenges and project requirements. It also covers the implementation methodology, design and results, along with risks and issues and the availability of the code which is the main asset of the deliverable. Section 4 briefly relates the scientific innovation of the results, pointing to the private document with the paper for publication for more information. Note that, however, code and private document with the paper for publication cover part of the required results, as this deliverable is of type OTHER.
TASKS			
Task 3.3 Distributed ledger-based and privacy-preserving IoT Identity Management	The use of p-ABCs tools in IoT environments is not extended because they tend to be quite heavy. There are crypto schemes with good results in terms of execution time that could become a good option for the IoT scenario. This task will address the study of these cryptographic schemes in order to apply them in IoT. As long as the IoT scenarios are comprised of smart devices, equipped with constrained hardware capabilities, the need to	Section 3, 4	Section 3 covers initial version of the p-ABC component used for implementation of privacy-preserving authentication of attributes. Also, it positions it into the general ERATOSTHENES work, its architecture, requirements and business challenges. Section 4 briefly relates the scientific innovation of the results, leaving further details to the research paper whose abstract is included in Appendix A. Note that, however, the developed software and the research paper whose abstract is included in Appendix A

	optimize cryptographic protocols is increased. Most of the existing p-ABC solutions are based on the RSA/pairing based schemes of Camenisch-Lysyanskaya, although there exist alternative schemes such as the pairing based scheme of Pointcheval-Sanders (PS), which are the most efficient instantiation of p-ABCs until now. There are recent proposals that have introduced distributed (or threshold) variants of the PS scheme aimed at privacy-preserving applications. Therefore, this task will apply DLT technologies to the dP-ABC scheme while incorporating lightweight and efficient cryptography that is capable of running in IoT scenarios, allowing the IoT devices to perform the Zero-Knowledge (ZK) Proofs that are otherwise not possible with current solutions. This task also aims to study the behaviour of extremely limited devices to determine whether the application of complex cryptographic protocols is feasible given their characteristics. The outcomes will be documented in D3.4 and in the final version in D3.8		cover part of the required results, as this deliverable is of type OTHER.

2.2 Deliverable Overview and Report Structure

The deliverable is structured as follows. Section 3 positions the work in the broader context of the ERATOSTHENES architecture and the requirements of the pilots. It also describes the used development methodology and points to the availability of code. Section 4 gives a brief overview of the scientific innovation resulting from this task. Section 6 recounts the conclusions from the report. Appendix A includes the abstract of the research paper produced as outcome of the initial work in this task, which expands the results related in this document.

Additionally, we remark the following past deliverables that treat components heavily related to the documented results:

- "D1.2 Use cases, requirements and methodological framework": it was delivered in M6 and provides the requirements associated to the Trust Manager & Broker component [1].
- "D1.3 Preliminary ERATOSTHENES Architecture": provides interactions between components, specifications regarding utilized communication protocols between them, technologies to be utilized as well as an overview of the proposed platform's operations and components. This deliverable was delivered in M6 [2].
- "D3.1 Prototype of Context-aware identity and access manager": Describes the SSI components, in which the 76component is integrated to enhance privacy [3].
- "D3.3 Design of Physical Unclonable Functions for IdM": Describes PUF mechanisms, which serve as a root of trust on the identity of devices in the project's identity management solution [4].
- "D4.1 DLT-based Trust Framework": Describes initial results of tasks 4.1 and 4.2, related to the usage of DLT in ERATOSTHENES for auditable and verifiable sharing of public data, which is key in the identity management solution based on SSI [5].

3 Architecture Orientation and Industrial Requirements

In this section we position the main components related to the task at hand in the broader context of the overall architecture and align them with business needs, the different pilots of the project and their requirements. Then, we discuss the methodology for the development of these components and point to the code related to them.

3.1 Architectural Positioning and design decisions

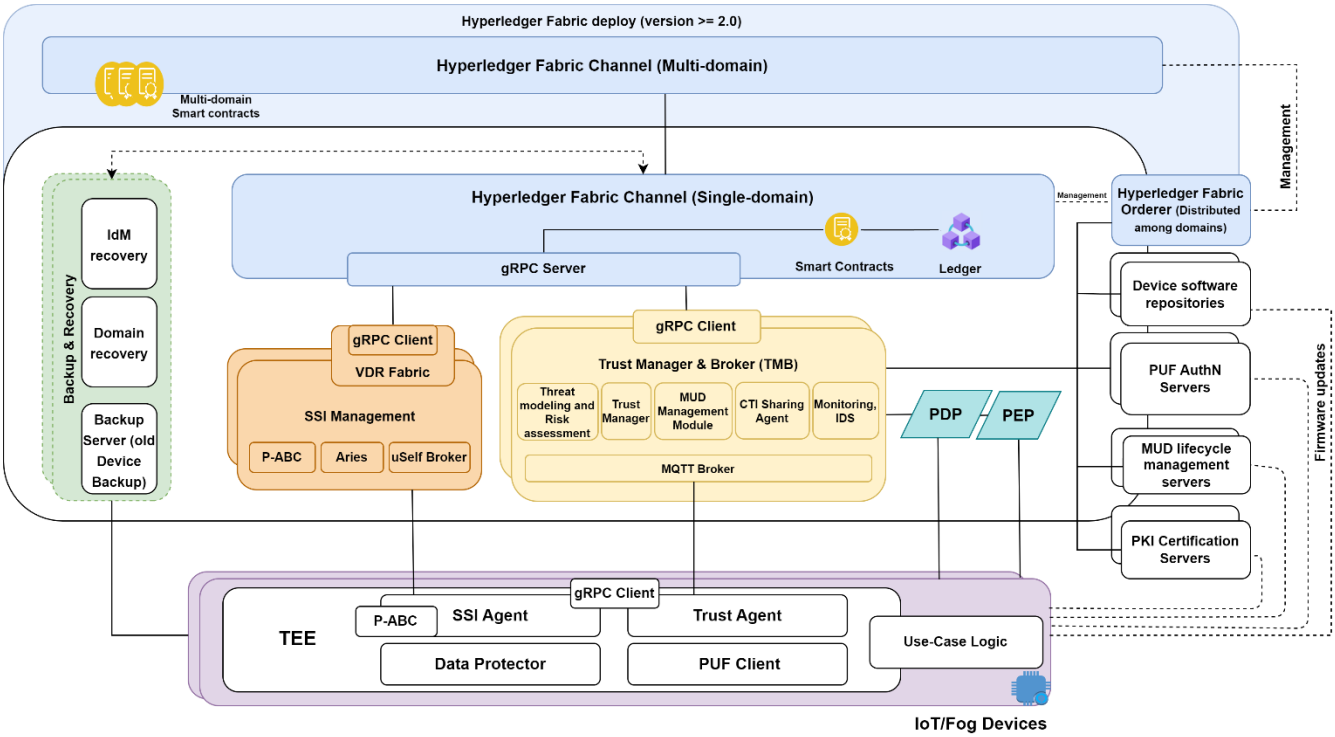

Figure 1 ERATSOTHENES instantiated architecture (modified).

Figure 1 presents the instantiated version of the architecture as of the time of this deliverable. This deliverable, and the task it is related to, deal with the privacy-preserving identity management of IoT devices supported by the DLT and cryptographic techniques. Within the architecture, the main component developed in this task is the P-ABC module. It enables the use of distributed privacy-preserving Attribute-Based Credentials based on Pointcheval-Sanders multi-signatures [11]. Thanks to this cryptographic tool, the security and privacy of the Self-Sovereign Identity (SSI) mechanisms are strengthened. Instead of showing credentials, authentication processes will involve the derivation in zero knowledge of a subset of information contained on the credential, so that minimal disclosure and unlinkability between presentations are possible.

The vision of identity management in ERATOSTHENES will be supported by this module, along with, of course, the close collaboration with other parts of the architecture. The p-ABC module will be integrated in the SSI management components so that the enabled operations are used in the ERATOSTHENES identity management flows. Also, the DLT will be a key component to facilitate the usage of p-ABCs and credentials in the ERATOSTHENES ecosystem. The DLT provides a public registry, transparent and with a fully verifiable history, enabling the trustworthy sharing of keys and necessary metadata (e.g., credential schemas) in a decentralized way. In fact, inter-DLT technologies make it possible to use credentials across domains when necessary. Other tools like Physical Unclonable Functions (PUF) and Advance Data Protection (ADP) mechanism will improve the general security of the identity management solution, by providing a root of trust for the device identity and a secure way to manage the cryptographic elements, respectively. These components are the focus of other deliverables, such as D4.1, D3.1, D3.2 or D3.3.

3.2 Business, Industrial Positioning and End-User Requirements

The identity management solution of the ERATOSTHENES project, following a self-sovereign approach, addresses the business challenge of secure authentication and identification of devices in IoT scenarios, while also tackling privacy concerns. The different pieces are used to ensure a secure and automatized management of identity, with PUF serving as a trust anchor during bootstrapping and enrolment, and the usage of wallets and credentials enabling fine-grained authentication of attributes for access control. The whole process is made trustworthy and transparent through the usage of DLTs. Particularly, the p-ABC component that is the focus of this document enhances security and privacy of authentication processes, by allowing the derivation of zero-knowledge proofs over the identity credentials, so that holders can disclose fine-grained information without revealing the complete credential, thus protecting the credential information and enabling the privacy goals of minimal disclosure and unlinkability, while ensuring formal guarantees of the authenticity of the data presented to the verifier. The integration into the emerging W3C's Verifiable Credentials standard, whose importance in the current landscape of Self-Sovereign Identity is unquestionable, makes the solution easier to adopt in many ecosystems, even those that would not take advantage of the whole technology stack of ERATOSTHENES.

The initial requitements for ERATOSTHENES projects were identified in Deliverable D1.2. In this section we present the coverage of the requirements specifically by the p-ABC component in the context of Task 3.3. To identify the related requirements, we have examined the initial requirements presented in D1.2 and the Component-Requirement mapping presented in Deliverable D1.3. The results of our coverage analysis are presented in the following table. For each requirement displayed in the tables, we present its description and importance (from D1.2), along with the Coverage Role and Rationale. The Coverage Role aims to depict the role of the components described in this deliverable in satisfying the requirement. It can be *Direct*, which means that the components are of prime importance in satisfying the requirement, or *Supporting*, when the components support the achievement of the requirements in a more indirect way, complementing other components responsible for satisfying the requirement. Lastly, Coverage Rationale explains the reasoning on these claims, and how the solution actually helps cover the requirement.

Table 2: Requirement coverage of the p-ABC module

Req. ID	Description	Impor--tance	Coverage Role	Coverage Rationale
P1_FR_11	Sender/Receiver devices must identify each other	M	Supporting	When identification requires authentication of additional identity attributes p-ABCs
P1_NFR_10	Accuracy of implemented integrity and authenticity checks	M	Supporting	p-ABCs provide formal authenticity assurance of attribute claims (i.e., computationally infeasible to forge, so that selecting security parameters properly ensures <<1% probability)
P1_OR_01	Protection of personal identifiable information w.r.t GDPR	M	Supporting	One of the protection goals of GDPR is minimal disclosure during operations, which is fully enabled through the zero-knowledge proofs used in p-ABCs
P1_OR_02	Pilot supports the privacy protection goal of unlinkability	C	Direct	The zero-knowledge property of p-ABCs implies, in particular, formal unlinkability between authentication processes (of course, unless identifying information is consciously revealed)

P2_FR_04	Devices can be enrolled in the system and associated to user identity	M	Supporting	The p-ABC cryptography will be used to issue Verifiable Credentials that include identity information that will be used to interact with ERATOSTHENES after enrolment.
P2_FR_12	Sender/ Receiver Devices should be able to identify each other	M	Supporting	When identification requires authentication of additional identity attributes p-ABCs
P2_OR_02	Protection of personal identifiable information w.r.t GDPR	M	Supporting	One of the protection goals of GDPR is minimal disclosure during operations, which is fully enabled through the zero-knowledge proofs used in p-ABCs
P2_OR_03	Pilot supports the privacy protection goal of unlinkability	C	Direct	The zero-knowledge property of p-ABCs implies, in particular, formal unlinkability between authentication processes (of course, unless identifying information is consciously revealed)
P3_FR_05	Sender/ Receiver Devices should be able to identify each other	M	Supporting	When identification requires authentication of additional identity attributes p-ABCs
P3_OR_02	Protection of personal identifiable information w.r.t GDPR	M	Supporting	One of the protection goals of GDPR is minimal disclosure during operations, which is fully enabled through the zero-knowledge proofs used in p-ABCs
P3_OR_03	Pilot supports the privacy protection goal of unlinkability	C	Direct	The zero-knowledge property of p-ABCs implies, in particular, formal unlinkability between authentication processes (of course, unless identifying information is consciously revealed)
EXT_FR_04	The infrastructure must enable enrolment of devices coming from different domains	M	Supporting	Verifiable Credentials, and consequently p-ABCs, can be used to authenticate identity data that will be useful for using identity information from the original domain when enrolling in the new one
EXT_FR_06	The infrastructure must enable one-off interactions across domains	M	Supporting	Verifiable Credentials, and especially those that support zero-knowledge proofs, are suitable for one-off interactions where formal guarantee of authenticity of identity claims is needed and privacy is important

EXT_NFR_04	Protection against replay attacks in identification processes	M	Direct	The implemented p-ABC showings can be easily protected from replay attacks by using a one-time use (e.g., time based) message for the signature of knowledge that occurs in a showing.
EXT_NFR_06	Avoid forgery of identity assertions	M	Direct	p-ABCs provide formal authenticity assurance of attribute claims (i.e., computationally infeasible to forge, so that selecting security parameters properly ensures <<1% probability)

3.3 Methodology

3.3.1 Implementation methodology

The development of the p-ABC technology is, as with other project components, incremental and prototype or pilot-driven.

Some of the steps resulting from this iterative approach are:

- Initial design of the library interfaces, and implementation in C of the main ZK functionalities, along with unit testing
- Design and initial implementation of the integration (only issuance/verification of credentials) of the C library into the project's identity management framework through a Go wrapper and the modification of the Go Hyperledger ARIES component.
- Initial unit and integration testing as part of PoC.
- Second version of the integrated component into ARIES, that includes the whole process of zero-knowledge presentation based on the W3C's Verifiable Credentials standard.

Additionally, the work has been included in the general WP3 agreed methodology, based on Agile Scrum. Thus, the task has participated in the following meetings:

- Sprint Planning meeting: monthly periodical meeting for defining the user stories to be developed each sprint
- Sprint Review meeting: this meeting is devoted to reviewing the status of the different user stories

Collaboration tools:

- Backlog Repository: Tool devoted for defining/list the user stories defined by the Product Owners
- Backlog Board: Scrum Board that allows the Consortium to see the status of the different user stories
- Slack channels: using slack for direct communications and daily sprint meetings
- Microsoft Teams meetings
- E-Mails
- GitLab (branches, merge-request)

3.3.2 Implementation design and development decisions

The implementation of the p-ABC module has been focused on the case of distributed privacy-preserving Attribute-Based Credentials (dp-ABC) based on Pointcheval-Sanders Multi-Signatures [11]. With this, we gain the usual advantages of many p-ABC systems: selective disclosure, unlinkability and advanced disclosure techniques (e.g., range proofs). It also leads to the usual limitations: p-ABC are more expensive than plain signatures in terms of computation

resources, and they are not a widely implemented solution. However, these limitations are palliated by the work in this project. The p-ABC module establishes an integration of the cryptographic primitive into W3C's Verifiable Credentials (VC) [9], which is an emerging standard gaining lots of traction in identity management solutions, especially those based on SSI. The standard establishes a model for representing digital credentials in an interoperable and machine-verifiable way, with the key property of being cryptographically secure. Verifiable Credentials play an equivalent role to physical identity credentials, consisting of information related to the subject of the credential (identity attributes such as name), information that identifies the issuing authority, and other metadata (expiration dates, type of credential…). Verifiable Credentials will be generated and signed by an issuer, and the holder will have complete control over them from that point. Holders will carry out authentication processes directly against verifiers. For that, they can use their VCs derive Verifiable Presentations, which are a tamper-evident way to gather and share identity information from the credentials for a presentation process.

In our case, the p-ABC technology will be used to modify the signed VC so that only part of the information is revealed, while keeping the formal authenticity guarantees. Thus, the Verifiable Presentation will contain the derived credential, increasing the privacy of the holder. Thanks to the achieved integration, the interoperability and ease of adoption of the p-ABC solution improves greatly. Additionally, we provide an implementation in C that enables efficient uses of the cryptography. Apart from the integration into VCs, we integrated the results into the open-source wallet of Hyperledger ARIES[1], which intends to create a shared, reusable, interoperable tool kit designed for initiatives and solutions focused on creating, transmitting and storing verifiable digital credential. These integration results enable the cohabitation of our solution with simpler techniques (e.g., plain signatures). This is an advantage in heterogeneous environments, where some devices may be very constrained or operations highly time sensitive, so that they need the simpler solutions, at the cost of losing privacy properties. Thus, it serves to allow holistic scenarios that cover the needs of all their differing participants.

What is more, the possibility of generating signatures in a distributed way offered by our dp-ABC technology, brings advantages of security (e.g., increased difficulty of achieving forgeries) and allows truly decentralized use cases. Particularly, this property comes from the use of multi-signatures [11], where any same-length public keys can be aggregated, and combined signatures and their verification process are equivalent to "simple" signatures. Thus, the distributed issuance process does not need a complex setup, and single-issuer use cases can also be carried out without any changes to the cryptography or implementations. Note that, as a limitation, aggregation of credentials requires that the attributes signed by each issuer were identical.

The dp-ABC cryptography has been implemented as an independent module in C, with an easy way to change the pairing-friendly curve used through a wrapper implementation of modular integers and group operations. C was chosen to improve the efficiency of the execution of the cryptographic operations, as they will usually be the costliest part of a credential scheme, while taking advantage of the wide-spread applicability of C as a low-level language for many applications and systems. For instance, we used GoLang's tools for development in C[2] to create a wrapper of the operations following Hyperledger's ARIES framework interfaces, easing integration. Additionally, this opens the potential for low level implementation features like inclusion of some or all operations in Trusted Execution Environments.

[1] https://github.com/hyperledger/aries-framework-go
[2] https://pkg.go.dev/cmd/cgo

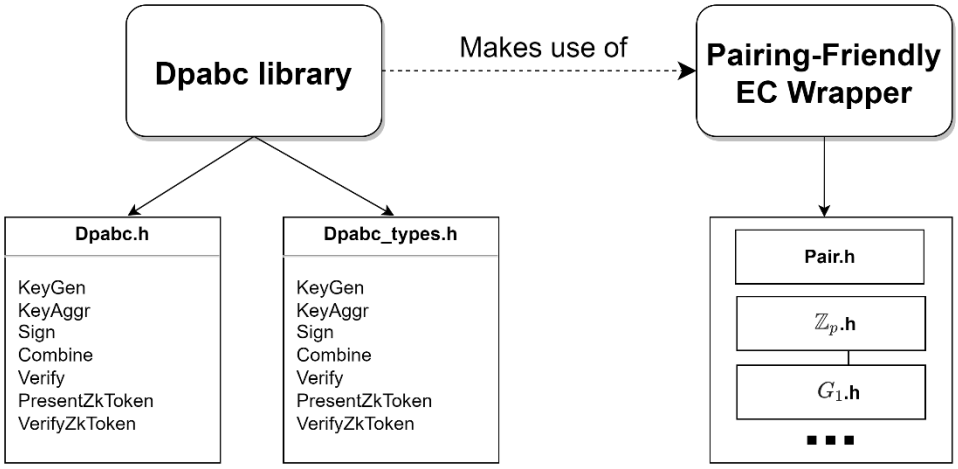

Figure 2 Distributed p-ABC library design overview

As the library is intended for use in a variety of platforms, and ease of configuration of parameters like the pairing-friendly curve used was an important requirement for us, the library code has been built as a CMake[3] project. The CMake project has been used to compile and test the library in several systems (Windows, Linux based) and platforms (arm, x86, x64). Additionally, the Cmocka[4] framework has been chosen for enabling unit testing of the library's operations.

As already mentioned, the main point of usage of the p-ABC functionality is the SSI solution developed in ERATOSTHENES. For enabling that, we have integrated the p-ABC operations into the ARIES agent used as a backbone of the SSI wallet tools, aiming for transparency (i.e., we followed, as much as possible, already defined interfaces for cryptographic operations). One of the key points of the integration and formalization of the p-ABC tool is the definition of a signature suite that works for W3C's Verifiable Credentials. The suite follows the same ideas as similar ones from the standardization efforts and is on a development and experimentation phase. The actual implementation has followed the interfaces and used the tools of the ARIES framework. The wrapper code for the cryptographic operations in the library has followed the framework's format, specifically working with generic interfaces and serialized elements.

Table 3 Wrapper interfaces in GoLang for integration into Hyperledger ARIES

/GenerateKeyPair	
Description:	Generate a key pair for the signing scheme
Input Parameters:	• seed []byte
Return:	• *PublicKey • *PrivateKey • error
/AggregatePublicKeys	
Description:	Aggregate multiple public keys into a single combined verification key

[3] https://cmake.org/
[4] https://cmocka.org/

Input Parameters:	• pubKeyBytes [][]byte • nattr int
Return:	• *PublicKey • error
/SignMulti	
Description:	Sign multiple messages using a key (handle) kh
Input Parameters:	• messages [][]byte • kh interface{}
Return:	• []byte • error
/AggregateSignatures	
Description:	Aggregate multiple signatures into a single combined one
Input Parameters:	• pubKeyBytes • signaturesBytes [][]byte
Return:	• []byte • error
/VerifyMulti	
Description:	Verify a signature over multiple messages with respect to a public key (handle) kh
Input Parameters:	• messages [][]byte • signature []byte • kh interface{}
Return:	• error
/DeriveProof	
Description:	Derive a Zero-Knowledge proof of knowledge that reveals a subset of the messages that were signed
Input Parameters:	• messages [][]byte • bbsSignature • nonce []byte • revealedIndexes []int • kh interface{})
Return:	• []byte • error

/VerifyProof	
Description:	Verify a Zero-Knowledge proof of knowledge.
Input Parameters:	• revealedMessages [][]byte • proof • nonce []byte • kh interface{}
Return:	• error

3.3.3 Implementation Issues and risks

One of the key risks is the heterogeneity of environments where the library will be used. To address it from the start, we developed the implementation with the goal of facilitating portability, with the use of CMake that allows compilation using the built-in tools of the system or even cross-compilation. This risk is now exacerbated with the need to deploy in the three pilots of the project in the first piloting round, but it has been mitigated by early selections of systems and platforms in said pilots, and carrying out initial tests of the implemented functionality in those scenarios (and even in some others). Still, this risk still leaves potential for issues, so it will need to be monitored.

Another risk, which has already caused some issues resolved by further integration work to upgrade to new versions, comes from the development status of the ARIES agent used for the SSI solution. This opens prospects of enhanced functionalities and even of possible contributions to the ARIES project with our results. However, as significant modifications to the framework are needed for integration, and the open-source framework may still suffer changes that fix bugs or improve functionalities that are useful for our project, we will need to monitor the status and incur potentially big integration efforts with new versions of the framework.

3.4 Code Availability

The code for the components described in this deliverable is available on the ERATOSTHENES project's GitLab repository, specifically at the P-ABC C library and the Integration into ARIES framework repositories.

4 Research and Scientific Innovation

In this section, we give a brief overview on the main innovation points and challenges addressed with the work of this task, and particularly the development of the DLT-supported dp-ABC component. A full description is given in the research paper that covers part of this deliverable, whose abstract can be found in Appendix A.

First, the project and particularly part of the work in this task tackles the application of privacy-preserving technologies for the identity management of IoT scenarios, starting from the initial bootstrapping and setting of a root of trust for the identity and following with enrolment so that devices control their identity. This includes the possibility of attribute-based authentication, with strong privacy guarantees thanks to the usage of zero-knowledge proofs. This approach is comparable (and, with slight modifications, compatible) with currently trending approaches for the future of IoT like FIDO's Device Onboard (FIDO)[7][5], where the root of trust is a FIDO key pre-installed during bootstrapping. In our case, we go one step further by establishing the possibility of a simple and flexible enrolment process through identity proofs that results in the device holding Verifiable Credentials that use p-ABC cryptography so that it can use them for privacy-preserving authentication.

Regarding the dp-ABC, a key outcome is the integration into W3C's Verifiable Credentials [8]. This allows transparent cohabitation with simpler techniques, like plain signatures in environments where more constrained devices or time sensitive operations may need them. Thus, it enables comprehensive scenarios that cover the needs of all their participants, with trade-offs on efficiency and privacy capabilities. Along with the flexible bootstrapping and enrolment process, this facilitates the adoption in heterogeneous scenarios such as it is common in IoT. Additionally, this differentiates the identity management solution from others currently applied in the context SSI, and specifically of IoT, like the IOTA Identity[6] or scientific works like [9], which do not include proper privacy features like selective disclosure. Closer to our solution is the work within Hyperledger foundation regarding BBS+ [10] signatures, with a proposal for their integration into the standard. However, this scheme only considers hiding or disclosing attributes (e.g., treated as strings), which avoids various issues and simplifies the integration, at the cost of potential privacy and security features. What is more, its treatment of metadata (e.g., "created" field) hampers unlinkability in practice. While the approach is very interesting for practical applications, we believe alternatives that cover more intricate use cases should be available—e.g., those that require statements over attributes (range proofs, set membership…) to achieve true minimal disclosure--, taking advantage of one of the main qualities of W3C's VCs, the interoperability and flexibility of scenarios. With our approach, fully minimal disclosure through advanced predicates like range proofs is possible, and advanced techniques like pseudonyms, inspection and revocation are available as proof options.

[5] https://www.lfedge.org/projects/fidodeviceonboard/
[6] https://www.iota.org/solutions/digital-identity

5 Conclusions

This deliverable introduces a brief description of the p-ABC component, instantiated through a distributed privacy-preserving Attribute-Based Credentials scheme, as part of the privacy-preserving authentication mechanism facilitated by DLTs for decentralization, which is the main outcome of task T3.3. The component is described, including the design choices for its implementation, positioned in the ERATOSTHENES architecture and work, and linked to the business and architectural needs it tackles. This document is a complementary part of deliverable 3.4, of type OTHER, whose main outcome is the implementation pointed in section 3.4, along with a research paper that deals with the main scientific and technical outcomes of the DLT-based privacy-preserving identity management approach. Further results on this task, like improvements based on feedback from piloting rounds, will be documented in deliverable D3.8.

6 References

[1] ERATOSTHENES project, "D1.2 Use cases, requirements and methodological Framework", Delivered in M3.

[2] ERATOSTHENES project, "D1.3 Preliminary ERATOSTHENES Architecture", Delivered in M6.

[4] ERATOSTHENES project, "D3.1 Prototype of Context-aware identity and access manager ", Delivered in M14.

[5] ERATOSTHENES project, "D3.3 Design of Physical Unclonable Functions for IdM ", Delivered in M14.

[6] ERATOSTHENES project, "D4.1 DLT-based Trust Framework ", Delivered in M18.

[7] Cooper, G., Behm, B., Chakraborty, A., Kommalapati, H., Mandyam, G., ARM, H. T., & Bartsch, W. (2021). Fido device onboard specification 1.1.

[9] M. Sporny, D. Longley, D. Chadwick, Verifiable credentials data model v1.0, W3C, W3C Recommen-

dation, November. URL https://www.w3.org/TR/vc-data-model

[9] Bouras, M.A.; Lu, Q.; Dhelim, S.; Ning, H. A Lightweight Blockchain-Based IoT Identity Management Approach. *Future Internet* 2021, *13*, 24. https://doi.org/10.3390/fi13020024

[10] T. Looker, V. Kalos, A. Whitehead, M. Lodder, The bbs signature scheme (2023). URL https://identity.foundation/bbs-signature/draft-irtf-cfrg-bbs-signatures

[11] Camenisch, J., Drijvers, M., Lehmann, A., Neven, G., & Towa, P. (2020, September). Short threshold dynamic group signatures. In Security and Cryptography for Networks: 12th International Conference, SCN 2020, Amalfi, Italy, September 14–16, 2020, Proceedings (pp. 401-423). Cham: Springer International Publishing.

7 Appendix A

The following text corresponds to the abstract of the research paper that deals with the outcomes of task T3.3 in deliverable D3.4.

The Internet of Things (IoT) has brought a new era of interconnected devices and seamless data exchange. As the IoT ecosystem continues to expand, there is an increasing need for effective identity management mechanisms, specifically for authorization processes and access control. The pervasiveness of such devices demands that desirable solutions tackle not only security properties but also privacy aspects like granular control over which identity data is shared in authentication/authorization processes, covering aspects like bootstrapping, enrolment, and service provision. In this context, it is natural to turn to privacy-enhancing technologies, like (privacy-preserving) Attribute-Based Credentials (p-ABC), for achieving both high security and privacy guarantees. Nonetheless, these technical tools need to be accompanied by a comprehensive approach that deals with the particularities of IoT scenarios and covers the full lifetime of the device. In this work, we propose the use of a p-ABC scheme with support for distributed issuance (dp-ABC) as a keystone for privacy-preserving attribute-based authentication and authorization in IoT scenarios. We integrate said cryptographic scheme with W3C's Verifiable Credentials standard, evaluating its impact to gauge its feasibility. The integration facilitates adoption and, particularly, allows the solution to transparently coexist with simpler techniques in heterogeneous scenarios that demand them. Moreover, we define and analyse a generic and comprehensive framework for identity management that identifies challenges throughout the device's lifetime to achieve IoT privacy-preserving identity management following self-sovereign principles. We show how the various aspects identified in the framework are tackled in a concrete instantiation as part of the H2020 project ERATOSTHENES.