LEDGER
ledgerjournal.org

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2016.27

BIX Certificates: Cryptographic Tokens for Anonymous Transactions Based on Certificates Public Ledger: Open Review

Author: Sead Muftic*†

Reviewers: Reviewer A, Reviewer B, Reviewer D

Abstract. The final version of the paper "BIX Certificates: Cryptographic Tokens for Anonymous Transactions Based on Certificates Public Ledger" can be found in Ledger Vol. 1 (2016) 19-37, DOI 10.5915/LEDGER.2016.27. There were four reviewers who responded, three who provided comments. None of the reviewers have requested to waive their anonymity at present, and are thus listed as A, B, and D. After initial review (1A), the author submitted a revised submission. The revised submission was reviewed by Reviewer B (2A), and responded to by the author (2B). After this, the assigned Ledger editor determined, in agreement with Reviewer B, that the author had adequately addressed the reviewer concerns. The assigned Ledger editor then asked the author for minor revisions which were carried out by the author, completing the peer- review process. Author's responses in are in bullet form.

1A. Review, Initial Round

Reviewer A:

The manuscript is concerned with a novel concept, design and implementation of a block-chaining information exchanges (BIX) via a certification infrastructure using certificates similar to X.509 certificates, and a set of appropriate protocols for initiation, generation, distribution, verification, management of the certificates to enable online transactions. In particular, the system provides secure peer-to-peer connectivity with anonymity through the use of a public ledger. It is a very innovative idea.

The paper is very well written, but I am not sure of its layout and presentation, especially with respect to presenting the keywords immediately after the author's name. (I have not checked this as well other things against the Ledger Journal's Author's Guidelines.)

† S. Muftic, Ph.D. (sead.muftic@setecs.com) SETECS Corporation, Washington DC, USA.
*15Dvv5QxpcJ4LDz38GQXkg5aKfMLUGgm7f

In general, the technical content is very good. There is no doubt about it, but I would strongly suggest that the author consider improving the paper with very minor issues to make it really worthy of publication without much effort as follows:

1. BIX as an abbreviation should be defined/expanded at the outset in its first use in the Abstract.

2. Section 2 title should be reworded as: RELATED CONCEPTS AND ASSOCIATE LITERATURE (The author could replace "LITERATURE" with the word "WORKS")

3. At the end of Section 2.1:

   a) To make the story more complete, it would be appropriate to state what the X.509 certificate's extensions are, how they affect or enhance BIX, and what are the foreseeable "probable" BIX certificate's extensions and their purpose.

   b) It would be most convenient for the reader to be informed in a summarizing paragraph (of about 5 to 10 lines) what are the important/key drawbacks of (near) similar existing conventional systems (if any) which the BIX system overcomes.

4. The mention of "new applications" at the end of Section 2.3 should be defined as to what these actually are.

5. Section 3 should be introduced with the Title; ""DESIGN AND IMPLEMENTATION OF BIX SYSTEM" because it is the **core** of the manuscript. Thereafter, current Section 3 through to Section 5 should be given as **Sub-Sections** to be more meaningfully presented to the reader. *(Note that the current Sub-Sections within Sections 3 to 5 will need to be adjusted.)*

6. Given item 5 above, it should be noted, however, that in the current Section, 4 (which will become a Sub-Section), a diagram to visualize the BCI together with the use of the BIX certificates and the supporting protocols should be provided, possible with a "legend" of the sequence of execution of operations so that the (novice/well-versed) reader can get a better *"look & feel"* of the system. (The manuscript will be greatly enhanced by this figure.)

7. Before the Conclusion Section 7, it would be appropriate to add a **new**Section - one A4 page at most - (with a possible Tile such as: "CONTRIBUTION, CHALLENGES AND OPEN ISSUES"), that would significantly add to the value of the manuscript and it could become a major source of reference by policy makers, researchers and practitioners alike by the author addressing the following:

   a) Summarize the novelty of the BIX System forcefully, and the contribution it makes not only to the body of knowledge/literature but also the practical benefits to the service providers and end-users.

   b) Discuss, briefly, the challenges and issues posed by the BIX system.

   c) How anonymity of transactions will be disclosed out of legal and ethical necessity during audit or digital forensic investigations. This is a very important issue when it comes to cyber criminals using anonymity to hide their identities. How will the BIX system handles or support this specific requirement?

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2016.27

Given the above suggestions as minor set of improvements, I have no particular concerns of this paper being published.

Reviewer B:

The idea behind the paper is ingenious. The author wants to construct a new certificate protocol using a blockchain-like mechanism instead of a standard PKI architecture. Although we appreciate the innovation, we see some major issues that need to be addressed in a revision before the paper could be accepted.

Issues:

1. The BIX system relies on an IM system, that is, quoting the paper "the BCI requires as the operational presequisite a broadcast messaging system with instantaneous delivery of messages". For the way the protocol is explained, all users need to be notified any time a user decides to request a BIX Certificate, which would be infeasible if we're thinking of massive broadcast systems.

2. The most serious issue relates to security. According to the proposed protocol, the last user (X) who obtained a certificate will act as Issuer for the next user requesting a certificate (Y). However, if X refuses to perform his signing, then the certificate chain is broken and it seems that there is no way for Y (or anyone else!) to obtain a valid certificate.

A way to overcome this would be with a certificate revocation, which is however not foreseen in the present paper. Actually we find it difficult since the aim of this paper is to avoid trust in a third party and only a TTP could have the authority to revoke a certificate.

3. It is not clear the contribution to the BIX idea contained in this paper compared to that in [Muftic, 2015a]. This must be made crystal clear otherwise it is difficult to judge the novelty contained in this submission.

4. Finally, a new user will need to obtain the entire BCL (Bix Certificate Ledger) before trusting any certificate. In practice this would be extremely cumbersome and it is not clear who can be trusted on this. Moreover, any user will need to store the entire blockchain locally.

Reviewer D:

The paper is extremely interesting and certainly innovative. It is made clear by the authors that the “contribution” is:

a) The absence of a third party

b) Pure peer-to-peer transactions without needing a service provider that can profile your actions.

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2016.27

Some minor issues that I found not very clear and thus they could be justified further are:

a) The authors claim that the concept of "community" is that anonymous users have agreed to participate in specific applications. OK !! However someone could ask: Why should I trust this community and accept to participate ? How can I find some assurance for the operation of this community?

Also, taking into account that joining the community is easy, how can I identify and reject malicious users ?

Finally, what are the risks if the community becomes VERY large (mainly in terms of performance) ?

b) Regarding the BIX certificates. There are two things that are not very clear. How are the 10-digit BIX identifiers generated by the IM? When generated they form a "convenient reference - identification" to the individual. If I have understood it correctly, when two registered users communicate, under some application context, they exchange their certificates which are validated and thus each one knows who is the other through the BIX ID? However they remain "anonymous" is terms of all the remaining users since no one can monitor the use of their certificates ???? If this is correct, then the anonymity is based on the fact that a malicious user cannot monitor the use of each certificate ?

Finally, in what way each user generates its pair (private-public) of keys ?

2A. Review, Second Round

Reviewer B:

Paragraph 3.1

- What does "double-signature" mean? I suppose that he should say "a pair of signatures". What exactly is "counter-signing"?

- Next Subject description: BCI should be BCL

- This is an important point.

It is not clear WHO is supposed to sign in the field Next Subject signature. He says "the issuer", but it is not clear if is the issuer of the current certificate or the next certificate. Furthermore, in Paragraph 3.3 he says something different.

Paragraph 3.2

- Why does he speak about "a BCL"? It seems that there could exist multiple BCL's.

Paragraph 3.3

- How is it possible to renew a certificate?

- What happens if the issuer does not accomplish his task? In other words, how can we enforce the owner of the last certificate to issue a new one? if no enforcement is foreseen, how can the system go on and select another potential issuer?

- BIX BCL is redundant since BIX is already part of BCL (BIX CERTIFICATES LEDGER)

- The backward CrossSignature is not sufficient to avoid that an issuer cheats, unless the system enforces that he cannot modify his certificate once it's completed.

- How does a new user receive the existing BCL?

Paragraph 4.4 is not convincing

2B. Author's Response to Second Round

Reviewer B:

Paragraph 3.1

- What does "double-signature" mean? I suppose that he should say "a pair of signatures". What exactly is "counter-signing"?

- The term "double signature" has been replaced with the suggested text "a pair of signatures"

- Next Subject description: BCI should be BCL

- Corrected

- This is an important point.

It is not clear WHO is supposed to sign in the field Next Subject signature. He says "the issuer", but it is not clear if is the issuer of the current certificate or the next certificate. Furthermore, in Paragraph 3.3 he says something different.

- Clarified

Paragraph 3.2

- Why does he speak about "a BCL"? It seems that there could exist multiple BCL's.

- The text "the BCL" has been replaced with the text "an instance of the BCL" throughout the paper.

Paragraph 3.3

- How is it possible to renew a certificate?

- New protocol has been introduced as section 3.3.5

- What happens if the issuer does not accomplish his task? In other words, how can we enforce the owner of the last certificate to issue a new one? if no enforcement is foreseen, how can the system go on and select another potential issuer?

- The issue has been resolved with the solution described in the new section 4.5

- BIX BCL is redundant since BIX is already part of BCL (BIX CERTIFICATES LEDGER)

- Redundancy has been eliminated throughout the text.

- The backward CrossSignature is not sufficient to avoid that an issuer cheats, unless the system enforces that he cannot modify his certificate once it's completed.

- The system does guarantee, by the protocol and structure of mutual signatures, that a user can not modify his/her certificate after it has been issued.

- How does a new user receive the existing BCL?

- This has been clearly described in section 3.3.4

Paragraph 4.4 is not convincing

- The section has been completely re-written by introducing new procedure to accomplish the same goal.

Ledger is published by the University Library System of the University of Pittsburgh as part of its D-Scribe Digital Publishing Program and is cosponsored by the University of Pittsburgh Press.

ISSN 2379-5980 (online)
associated article DOI
10.5915/LEDGER.2016.27