XDI Trust Information
— A Trustability Protocol for Validating Distributed Information

Elizabeth Cano Grégoire Burel

Department of Computer Science,
University of Sheffield,
Sheffield, United Kingdom
{elizabeth,gregoire}@dcs.shef.ac.uk

Abstract

Trust of information has always been a critical issue in large distributed environments. With the rapid and recent development of online communities and social networks, it has been evident that the Web will rely more and more on user-edited information. As a consequence trust in the correctness of data is falling dramatically and no general solution has been proposed in order to consider that specific but fundamental problem.

Trustworthiness on the Internet is usually addressed as a problem of privacy and security(1). So, until now, the solutions to the trust issues are focused on privacy and security. For instance, certificates and the TLS protocol address authentication and data transfer security. The OASIS Consortium addresses information control through the XDI contract links, which are part of the Dataweb architecture (2).

This paper is introducing a method for endorsing content correctness based on social participation and the Dataweb paradigm. The general idea is that by creating special XDI contract links supporting trusty-trustee relationships (XDI Trust Information(XTI) contract links), people will be able to estimate the correctness of information using collective intelligence or give their trust to any data for improving the social perception of its correctness.

In the future, a new generation of web browser would be able to use the power of XTI and the Dataweb architecture in order to give people a critical view of information. For spreading the technology it should be necessary to fully specify XTI and integrate it in XDI and make it an Internet standard. However, this cannot be done at the moment since the first official release of the XDI specifications is expected before April 2009.
Index Terms: Identity federation, Collective intelligence, Trust metric, Content correctness, Dataweb.

1. Introduction

It is becoming increasingly difficult to ignore the fact that trust in online information is still one of the most important issues in today's Internet. Trust is a broad concept that can be approached from different perspectives. Online trust is conventionally related to the level of confidence in the reliability and security of the Internet (1). At the moment, information can be issued using different protocols and formats ensuring a safe and authorized data transfer between two different network endpoints. Although, this can give a sense of trustworthiness, it still does not resolve the other perspective of online trust related to the issues of content validity in collaborative or multi-sourced environments. Certificates do not ensure that information is actually validated or controlled by the certificated entity. Consequently, it is not always possible to regard the provided content as true.

The past decade has seen the rapid development of online communities and social networks, making evident the evolution of the web towards a user-centric Internet. Every time more and more services have to rely on user personal information and on user edited content. Trustworthiness can be questionable in online environments, particularly in online communities such as Wikipedia [1] where encyclopaedic articles can be built up from contributions of undocumented users. Also, in social networks like Facebook [2] the validity of information can be debatable since it is possible for a user to steal or fake other users' profiles in order to access private or restricted information of related users. So far, mashing up information coming from different sources in order to make deductions about a user entity, relies blindly on the accuracy of the sources content. As a consequence, wrong information provided by a faked user can be taken indistinctively, leading to inaccurate deductions about the real user attributes.

Addressing the validity of content against the reliability of the information provider depends tightly on the mechanisms used for attaching a digital identity to such a provider. This has drawn attention to the importance of establishing federated identity management for sheltering the user's private information and for representing the user as a valid entity.

With the introduction of the Extensible Resource Identifier (XRI [3]), the OASIS consortium has helped in alleviating the issues related in expressing unique, persistent and non-reasignable identifiers for online resources [4] (3). Moreover, through the integration of the Dataweb paradigm and the use of XDI contract links the users could have direct control of their data, deciding what can be known about them and who can access their information.

Despite of the important work done on the field of trustworthiness, no solution for addressing trust in content correctness has been proposed. In this paper, a methodology for endorsing content correctness based on social participation is proposed. First a set of trust scenarios approaching different perspectives of trust is described for situating the context of this document. Then, some of the challenges introduced by these scenarios are discussed. A proposal for solving the challenge of addressing

[1] http://en.wikipedia.org/
[2] http://www.facebook.com
[3] http://www.oasis-open.org/committees/xri/
[4] The emergence of OpenID along with the use of XRI offers a management of single digital identities in an open and decentralized way.

the validity of content is described in the forth section. Finally, the proposed model is applied to two different scenarios involving information correctness.

2. Trust Scenarios

There is no commonly agreed definition of the term "trust" that covers all the disciplines and subject areas where it can be applied. In order to contextualize the use of this term, this section provides concrete examples involving four different trust perspectives.

2.1. Trusted authentication and data integrity: The bank scenario

Addressing the authentication of the parties exchanging information can be considered the most simple and at the same time the most important approach to trust. In this type of trust both parties must prove their respective identity in order to complete a transaction. Authentication relies on another trust-based relation that assures that what one party is sending is actually what the other party is receiving. For instance, in the case of online banking, the user must make sure that he is giving his security credentials to the correct entity by checking the bank's certificate and by making sure that the communication channel is encrypted.

2.2. Trust in user identity: The identity thief scenario

A user in a social network like Facebook with a finite number of friends can be the target of an identity thief. A thief could easily copy his profile information and ask to be accepted as a friend of the real user's relationships. In this way the user's friends personal information could be in the hands of a malicious person who could use this information at their expense. How can the friends of the user disambiguate between the real user and an identity thief even though both of them share the same relationships?. How can privacy be guaranteed when sharing user profile information?

2.3. Trust of content in reliable entities environments : The CV validation scenario

When a hiring manager receives a job candidate's CV, a common way of checking the validity of the CV information is to call the referees provided on it. Even though the referee can assert part of the CV's information, he does not have enough knowledge for validating the whole background of the candidate. With the emergence of digital identities, hiring managers tend also to rely on personal information left by the job candidates on the Internet; such as in blogs, social network profiles, etc. Although this information is accountable in some way it does not necessarily imply that the CV information is fully correct and it does not cover all the CV statements. For instance, if a job candidate fakes their profile information in well known professional social networks such as LinkedIn[5], the hiring manager would be relying on fake basis for making critical decisions. How can the manager be sure that the person he is supposed to hire is not a completely faked personality? How can he know that all those bits of information found online are true? How can the job candidate assure that his information will be provided only to the right people, avoiding privacy issues?.

[5] http://www.linkedin.com

2.4. Trust of content in distrusted environments: The blog scenario

When somebody is accessing a page, for instance a blog, he has no formal way of knowing if the written information is right or wrong unless he has a previous knowledge on the domain treated by the article. A way of trusting in the validity of the content is to read other users' comments or relying on the references given by the article (aka. "Common consensus").

3. Challenges

Some of the previous trust scenarios are already covered by existing or already proposed technologies. Nowadays, user authentication and channel encryption for securing safe transport of data have been implemented in many different ways. For example, it can be addressed by using digital signatures for data integrity purposes.

Recently, the user identity field has attracted the attention of the research community. As stated in the introduction, OpenID [6] provides a unique identity to users by incorporating the XRI specification. As a consequence, OpenID offers an answer to the identity ubiquitousness. However, there is still no method for completely addressing the user identity disambiguation.

When addressing the trust of content scenario, difficulties arise. Trust in content relies on the previous scenarios' solutions: authentication, data integrity, and identity uniqueness. For some specific entities, such as a Bank or a governmental agency, it is reasonable to accept the provided content since it is certainly endorsed by the reputation of the certificated entity. However, in general situations, content comes from entities that are not personally known. Moreover, knowing personally an entity does not mean necessarily that his content will be correct (users are likely to commit mistakes on what they write). At the moment there are no technologies at the Internet level addressing these issues. One way of giving an answer to these issues is to take advantage of the collective intelligence provided by a social reviewing system.

This paper is proposing a solution to theses issues based on the Dataweb architecture. A social reviewing system can be implemented by extending the XDI contracts. The collective intelligence extracted from the extended contract can be used in order to provide an estimate of the trustworthiness of a content.

4. Proposal

As stated previously, this proposal is based on the DataWeb architecture which applies the REST architecture principles for standardizing data control in distributed environment . This approach includes a way for globally identifying data and data authorities by using XRI, an XDI-RDF model for representing and linking data, and an XDI service for exchanging it (2).

Because Web links are one-way "strings" between HTML resources, they can be broken when the target resource is moved, since at the moment those resources are not addressed through XRI. Therefore, it is not possible to address any resource ubiquitously. A social content reviewing can be seen as a set of trust relationships between people and content. A trust relationship involves to parties: the first one, the owner of the content who wants to be trusted (trusty), and the second one, the trustee who is the one supporting the correctness of the content. The trust relationship depends on a bidirectional agreement between the parties. As a result, standard web links cannot sup-

[6] http://openid.net

port that type of agreement due to the unidirectional nature of the Web link.

The dataweb architecture provide bidirectional links or "pipes" between XDI resources (2). This type of links are called XDI links. An XDI link is not enough for representing a trusty-trustee relationship. This relationship requires the establishment of a hierarchy for defining the role of each party. It also requires data control management for addressing other security issues such as party authentication.

XDI contract links allows fine-grained control over the data by providing a way of stating a set of constraints on each bit of data contained in an XDI document (for instance: authenticating parties, assigning access control list, replicating information of documents, etc.). Because of that, XDI contract links are particularly suitable for representing a trusty-trustee relationship. Accordingly, the XDI contract link will be used for implementing the trusty-trustee relationship which will be referred to as XDI Trust Information (XTI) contract link.

For ensuring that an XDI document's content is likely to be correct, a facility for establishing trust between two resources is allowed by establishing an XTI contract link. When a trustee establishes an XTI contract link between himself and a document it means that the trustee is ensuring that given his knowledge that content is for him "true" or "correct".

Basically it is not possible to have a blindly trust in what a trustee is relying on, unless it is a certificated or trusted authority. Having more trust links in a given content makes it more likely to be correct. This is a collective perception of correctness.

Since the XTI contract links can be signed between two XRI addressable resources, it is also possible for a user to use his own content as an XRI resource for signing other content. When a user is signing another document with his own document this can be considered as a reverse or back reference to another similar idea. By doing that, the user is indirectly supporting the idea of the trusty through the reliability of his own document.

When a document is new and it doesn't have yet any trustee party it is not necessarily true that the document is incorrect. In this case it could be possible to get an estimation of the content's correctness. The method proposed is based on the idea that it is always possible to get from the service provider a sample list of documents from the content's owner. Since each document of this list can contain XTI contract links, an estimation of the correctness of the owner's contents can be derived. This estimation can be used for guessing the correctness of the current content. This estimation could be based on already existing trust metrics applied for instance in P2P environments (4), or mobile agent environments (5) This metric could be provided by a standard web service.

In the Dataweb approach the operations between resources are done through the XDI protocol. This protocol is embedded in an XDI service. For using the XTI contract it will be necessary to add support for handling this new type of relationship enabling procedures for resolving the trusty-trustee relationships and the sample list of document containing XTI contract links. This service will be referred as the XTI service.

4.1. XDI contract vs XTI contract

This control feature in dataweb links is what enables the creation of dataweb safe links through XDI contract links. Since dataweb links can provide active identification and data interchange control, XDI contracts can be as flexible and extensible as real-life contract. XDI contracts intends to mediate: authentication, authorization, access control, usage control, distribution and forwarding control, and synchronization. All these mediations are related to the control of security in the communication and sharing perspectives. None of them covers the perspective of addressing validity of correctness by being trusted by a third party. Here is where the XTI contract can add this new perspective to the XDI contract link model.

In the case of an XDI contract link, when a user wants to add sharing constraints to one of his existing XDI document, he will have to create an XDI contract link ,and another XDI document, stating the terms under which the data may be shared. Finally he would have to publish the Dataweb address of that contract link. In this way the final document could be addressed only through the link contract.

In the case of an XTI contract link, a user wants to add reliability to his existing XDI document. This document may or may not have a contract link stating the terms under which it can be shared. For adding reliability to his document, the user will have to create an XTI contract link between his documents statements and a trustee that can in some way validate that the document statement is reliable.

4.2. XDI service vs XTI service

XTI services as XDI services are based on the REST[7] paradigm. The XDI protocol defines the following operations: $get, $add, $mod, $del(6). These operations are the foundation for adding permissions in XDI link contracts. For instance, for requesting an XDI document in html format, the operation would be like: `$get$a$mime$text$html`.

In the same way the XTI trusting operations would be carried out through these four operations. For instance, the $get operation could be used for requesting a list of trustees of a resource.

The XTI extension to the XDI model would act like a contract link but with a different purpose. It would enable the role of a "trusty"(meriting trust) and a "trustee" parties. It would also enable an XDI service provider the facilities presented in the Table 1.

Table 1: The XTI procedures

XDI REST Operation	**XTI Procedure**	**XTI Procedure Result**
$get	Trustee	The XRIs of the trustees or a list of XRIs linking to other documents
$get	Trust	If the trustee trusts in the resource
$add	Trust	Signs an XTI contract link
$del	Trust	Revokes an established XTI contract link

[7] http://www.ics.uci.edu/~fielding/pubs/dissertation/top.htm

5. Applying the XTI model

The use cases presented in the second section can be used in order to understand this proposal.

5.1. The CV scenario using XTI

Let's illustrate this proposal in the context of a hiring manager. Say a hiring manager wants to verify the CV's information provided by a job candidate "Alice". Alice has stored her CV in one of her DataWeb pages and it can be addressed by her XDI service provider as: `xri://=alice/+cv`. In order for this information to be reliable, Alice would have to validate it against the direct source of the information establishing an "XTI contract link" through her XDI service provider. For instance, if she was a graduate from the University of Sheffield, she would have to validate her bachelor's information against the University's records.

Having established an "XTI contract link" to her CV, Alice can make public the addresss of her XDI contract link containing among other information related with the accessibility of the CV document, information related to the XTI link contract.

According to Figure 1:

1. The hiring manager accesses Alice's CV in an HTML format. Meanwhile the hiring manager's browser asks for the XDI view of the document.
2. From that XDI document the hiring manager's browser asks for the trustee list from that CV in order to check its validity.
3. With this information, the hiring manager's browser addresses the trustees asking them if the information is correct.
4. Finally the University confirms that the information is correct. The browser show in some way to the manager that the information has been verified and is correct.

5.2. The blog scenario using XTI

When an XDI document does not have an XTI contract associated with it, it is possible to derive an overall estimation of the reliability of the owner by taking a sample of other contents containing "XTI contract links". Let's explain this in the context of figure 2:

1. A user "Alice" is reading the "article A" from "Bob"'s blog. She wants to know the reliability of article A.
2. Since the article A doesn't have XTI contract links supporting it, Bob's XDI service provider returns a random sample list of Bob's documents containing XTI contract links
3. Alice will have to ask how reliable are the Bob's documents contained in the list. This is done by asking the list of trustees for each of them.
4. Having the trustees, Alice can control that such XTI contracts are valid by addressing the trustees. If the trustees of that document are other documents, the trustees of those documents can be checked recursively as well.
5. The trustee can reply with a yes or no answer.
6. By doing the steps 4 and 5 with each of the documents, Alice could have an estimate of the trust level of Bob by applying a metric.

6. Conclusions

The XTI model provides a solution to the content validation problem. The model relies on the collective intelligence provided by a social graph representing trusty-trustee relationships. This proposal depends on the Dataweb architecture. It is based on the bidirectional feature of the Dataweb links through the use of XDI contract links.

In the future, XTI-enabled web browsers supporting the Dataweb approach, would be able to perform content validation using a social reviewing system. The new generation of browsers would also integrate trusting facilities for helping users to be full or partial validators of document's contents. In order to spread this technology, the XDI model would need to be accepted as an official standard by the majority of the main actors of the web such as W3C.

This paper is concentrated on human reading documents, however this proposal is generic enough for being applied to the semantic web. This would ensure that the statements used for inferring knowledge are correct.

Most of this work is based on the OASIS proposal of the XDI contract, however the first official specification of the XDI contract link will be available in April 2009. In any case this idea should be applicable with some minor modifications to the final specification.

7. References

[1] A. S. W. H. Dutton, "Trust in the internet: The social dynamics of an experience technology," *Oxford Research Report*, no. 3, pp. 2–42, Oct 2003. [Online]. Available: http://www.worldinternetproject.net/publishedarchive/RR3.pdf

[2] S. G. Reed D., "The Dataweb: An introduction to XDI," http://www.oasis-open.org/committees/download.php/6434/wd-xdi-intro-white-paper-2004-04-12.pdf, 2008. [Online]. Available: http://www.oasis-open.org/committees/download.php/6434/wd-xdi-intro-white-paper-2004-04-12.pdf

[3] "XRI and XDI explained," http://www.xdi.org/xri-and-xdi-explained.html, 2006. [Online]. Available: http://www.xdi.org/xri-and-xdi-explained.html

[4] D. Donato, M. Paniccia, M. Selis, C. Castillo, G. Cortese, and S. Leonardi, "New metrics for reputation management in p2p networks," Banff, Alberta, Canada, Tech. Rep., May 2007. [Online]. Available: http://dx.doi.org/doi.acm.org/10.1145/1244408.1244421

[5] M. Klopotek and M. Wolski, "Simple reputation metrics for mobile agent in open environments," 2006, pp. 253–261.

[6] S. M. Reed D., "The XDI RDF model," http://wiki.oasis-open.org/xdi/XdiRdfModel, 2008. [Online]. Available: http://wiki.oasis-open.org/xdi/XdiRdfModel

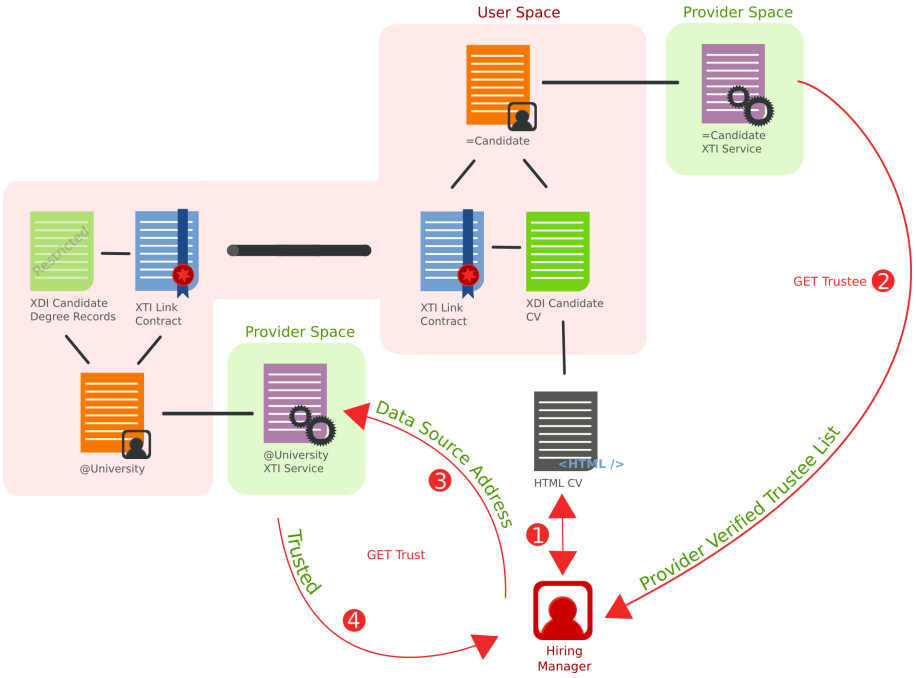

Figure 1: XTI Service applied to the Hiring Manager use case

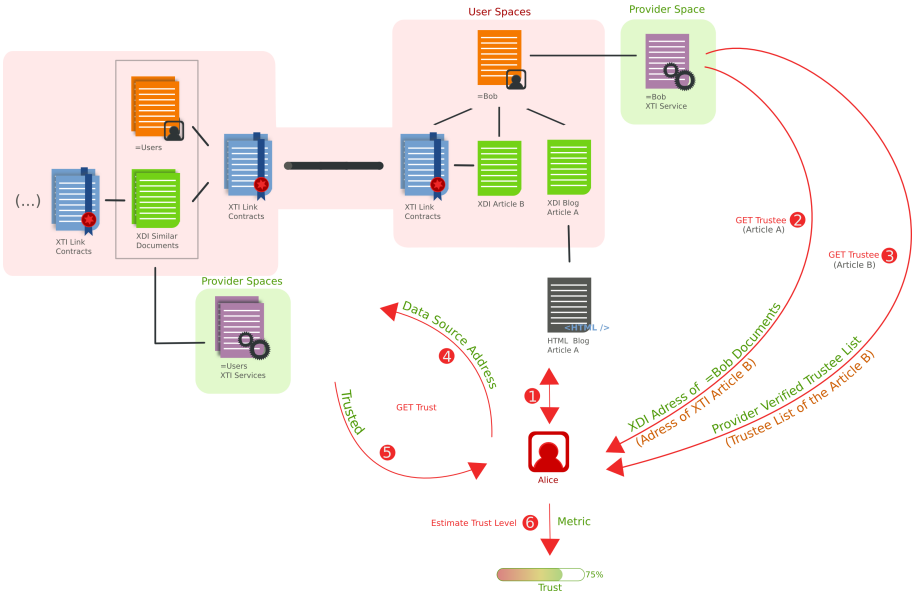

Figure 2: Estimating the reliability of a content