CHALMERS
UNIVERSITY OF TECHNOLOGY

UNIVERSITY OF GOTHENBURG

Investigating Trust Factors in Peer-to-Peer E-commerce: a Design Science Study

Bachelor of Science Thesis in Software Engineering and Management

Sarah Aldelame
Måns Thörnvik

Department of Computer Science and Engineering
UNIVERSITY OF GOTHENBURG
CHALMERS UNIVERSITY OF TECHNOLOGY
Gothenburg, Sweden 2019

CHALMERS
UNIVERSITY OF TECHNOLOGY

UNIVERSITY OF GOTHENBURG

This work investigates inter-user trust factors in the online Peer-to-Peer (P2P) domain
Online Peer-to-Peer services have been gaining traction over years. Services such as AirBnB, Uber, Hygglo (Swedish loaning site) and more have been emerging, all of which require trust between its users to function at all. This work is intended to address the trust issue by creating an overview of the current body of knowledge, confirming the current knowledge with current users of such P2P services, and lastly to evaluate each found trust factor's individual feasibility.

Supervisor: Jennifer Horkoff
Examiner: Richard Berntsson Svensson

University of Gothenburg
Chalmers University of Technology
Department of Computer Science and Engineering
SE-412 96 Göteborg
Sweden
Telephone + 46 (0)31-772 1000

Department of Computer Science and Engineering
UNIVERSITY OF GOTHENBURG
CHALMERS UNIVERSITY OF TECHNOLOGY
Gothenburg, Sweden 2019

Investigating Trust Factors in Peer-to-Peer E-commerce: a Design Science Study

Måns Thörnvik
Software Engineering and Management Programme
University of Gothenburg
Gothenburg, Sweden
gusthomaa@student.gu.se

Sarah Aldelame
Software Engineering and Management Programme
University of Gothenburg
Gothenburg, Sweden
gusaldesa@student.gu.se

***Abstract*—Trust is a vital actor in a healthy relationship between any parties, both on and offline. In E-commerce, specifically Peer-to-Peer (P2P) platforms, the presence of trust factors among peers is what defines the success or failure of the platform. While there is a sizable amount of studies on trust, the E-commerce P2P domain is relatively untouched. In order to find the most significant and relevant trust factors that can improve trust among peers in a P2P platform, this paper will explore the definitions of trust among online P2P users, specifically private individuals who engage with each other to buy or sell services or products. Furthermore, the paper will evaluate its findings, from both literature and current users of online P2P services, to show the feasibility of implementing the found trust factors.**

I. Introduction

The term trust is often considered to be a multi-definition concept in literature [1]. Schoorman, Mayer, and Davis described trust as "the willingness to take risk, and the level of trust is an indication of the amount of risk that one is willing to take" [20]. Wang and Emurian, argue that trust is an abstract concept that is sometimes used interchangeably with relevant concepts like reliability, credibility, and confidence [1]. Lewis and Weigert argue that trust is a multi-faceted concept that incorporates cognitive, emotional, and behavioral dimensions in humans [21]. Gefen studied trust from a multi-dimensional perspective, he claims that the antecedents to trust are the beliefs of integrity, ability, and benevolence [23]. In E-commerce, integrity represents the stated online rules that are to be adhered to by online users, ability represents the quality delivered by an online user depending on their competence in delivering the product or service, and benevolence is the belief that an online user intends to be good to another user irrespective of whether they will involve in a transaction or not [1].

The recent emergence of sharing economy platforms has urged for more research to improve trust among P2P platform users. E-commerce P2P technologies have been utilized in some of the most valuable and economically profitable businesses today. Businesses like the accommodation-sharing platform Airbnb or the transportation network Uber, have largely impacted people and the economy [6]. These P2P platforms let users exchange, buy, or sell services or goods with each other. The site acts as the provider that facilitates the exchange and communication tools [6]. The increasing number of P2P technologies has created many options for online users to communicate and interact with each other. Exposure to the immense amount of information, products, or services creates more complexity for people in terms of trust [6]. The constantly growing digital world of sharing, buying, or selling among peers creates the increasingly anonymous and impersonal society, which causes people to feel that the outcome of an online interaction in terms of exchanging, buying, or selling with other peers is unpredictable and even perceive it untrustworthy at times [6].

In E-commerce, trust is an important and powerful factor which makes it an important topic in the software domain. Trust is widely studied in the context of business to consumer (B2C), since the presence of trust between the site and its users is important for the success of an E-commerce B2C platform [11]. What is less studied is trust among peers in P2P platforms.

In this study, we will take a closer look at P2P platform users and find what important trust factors needs to be present between peers to create a more trustworthy environment. We pay special attention to how we can find and utilize trust factors that can positively affect trust in P2P E-commerce among peers. We aim to provide trust factors that can help an E-commerce P2P platform to strategically implement the right assets i.e. factors to increase their trustworthiness and be proactive against traffic and revenue loss due to trust issues among peers on the site.

We viewed publications to gain insight of the current body of knowledge in the context of E-commerce P2P platforms. We found that researchers like Ba [5], Möhlman & Geissinger [6] have been researching the P2P trust domain. Ba studied how one could use Community Responsibility Systems (CRS) to enhance user trust and mathematically proves that a CRS could improve trust conditions in a P2P E-commerce platform. Möhlman & Geissinger explain the intricacies of P2P transactions, how trust should be viewed in these situations, and give concrete examples of digital cues (user interface elements) that can promote trust [6].

The trust factors we aim to gather focus on different areas in P2P E-commerce, e.g., promoting the reliability of a private individual as a peer on the site, and enhancing the site's design to promote better impressions by its users to gain traction. The

trust factors will be a mix of features that a P2P system could implement, in order to enhance their users' overall ability to trust others peers of the site.

Moreover, the study aims to analyze and provide the feasibility of implementing the found trust factors by online P2P platforms. Exploring the feasibility of the found trust factors will enable the readers to decide on which trust factors could be feasible for their own systems. We will use a feasibility evaluation technique referred to as TELOS (an abbreviation of all included perspectives), which is normally used to evaluate the feasibility of projects [10]. We argue that TELOS could also be employed to address the found trust factors as all five categories of feasibility can be related to the software engineering world and evaluating the feasibility of individual factors: Technical, does the proposed trust factor require significant technical changes and/or domain knowledge? Economic, what costs are connected to implementing the trust factor? Legal, does the trust factor involve personal data, and if so, does General Data Protection Regulation (GDPR) aspects need to be considered? Operational, does the P2P system's protocols support the proposed change? Schedule, does the time to implement the proposed trust factor fit into the software project's general time plan? We intend to prioritize only technical and schedule since currently, we only have access to E-commerce software engineers that are only capable of answering the technical and schedule aspects of TELOS.

II. Related Work

A. P2P and B2C Publications

The following publications are covering a mix between P2P and B2C related trust issues. The authors have set out to find trust factors in E-commerce in general and not only specific to a single business model.

Our study builds upon and extends related work and literature on trust factors in order to find the most important trust factors among private peers in a P2P E-commerce platform. Wang and Emurian carried out research on trust among private individuals in E-commerce. They believe the future of E-commerce is at jeopardy without trust among peers in an E-commerce platform, "The future of E-commerce is tenuous without a general climate of online trust." [1].

The authors in paper [1] provided a detailed description of different concepts of trust from different perspectives. Furthermore, they investigated and concluded online trust inducing elements among peers in E-commerce and concluded their research by proposing a framework of trust-inducing features that mainly focused on user-interface interactions i.e. web interface design. The design features in the framework [1] suggested four main dimensions, graphic design, structure design, content design, and social design. While we gathered the trust factors in our research, we used six of the suggested trust-inducing features proposed in the framework provided by Wang's publication. With regards to web-interface design, simplicity, consistency, and accessibility were seen important to our work and extracted to be a part of our list of factors.

In regards to other areas like social design, we used pictures, privacy policy and terms and conditions, and finally domain name importance from the framework. Wang and Emurian [1] focused on human computer interaction (HCI) when they created their framework, mainly in how to design websites that are perceived as trustworthy by users. Wang et al. argue that the platform design is important as without trust in the platform, it is very difficult to gain any traction [1]. Furthermore, they argue that users need to trust the platform enough to input their personal data to be able to transact with their peers on the site making the platform's interface design vital for enhancing trust [1].

Work in [2] thoroughly reviewed the antecedents of online trust from different aspects. It defines and discusses trust as an individual features, as an expectation, as acceptance of and exposure to vulnerability, and as an institutional phenomenon. This publication discussed both off and online trust from a commercial and non-commercial perspective. Furthermore, the authors suggested features that can help enhance trust online. Firstly, they argued that to be assessed as a trustworthy business, organizations online should improve their reputation, performance and appearance [2]. [2] suggests that appearance corresponds to the design of the website interface, for instance, ease of use from the user's perceptive. Furthermore, they postulate that providing features that encourages social presence in a websites for online transactions could increase users' trust among each other and towards the platform [2]. Moreover, the researchers suggest social presence in the context of being identified with online groups and communities [2].

Another suggested criteria is the perception of trustworthiness. Online users are ready to trust other users with whom trustworthiness has been tested [2]. We formulated the suggested features in [2] to fit some of its content into our list of trust factors. User-interface design, social presence and history of transactions were seen relevant and important to be further investigated in this research, however, the publication [2] did not provide concrete features or a concrete model to follow that can help enhance trust in the P2P platforms or any other platforms. Our work tries to achieve concrete features that can be tested for feasibility and eventually be realized by P2P platforms.

In order to thoroughly understand how trust is built between people, we need to consider how deception occurs between people. In [11], Castelfranchi & Tan argue that people will continue to deceive each other using computers as agents just as they would in real life interactions. Castelfranchi & Tan also explain and argue on the benefits of different types of trust using the help of Lewicki & Bunker [19]. Lewicki & Bunker [19] have identified deterrence based-trust, knowledge based-trust, and identity-based trust as the base typology for all kinds of trust [19]. We reused Lewicki's & Bunker's [19] typology to understand our trust factors on a deeper level.

In order for us to comprehend trust on a deeper level, we also reviewed and used work in [13], definitions and principles of trust online and offline. This publication thoroughly reviewed trust, covering both on and offline aspects.

The publication suggested trust definitions components and principles. The authors of [13] argue that the definition of trust and its principles provide a strong starting point and help create the basis to build trust. We used [13] to help strengthen and clarify the existence of one of our trust factors regarding authentication methods and its role in establishing online trust among private individuals.

B. P2P publications

The following related work examines trust factors among peers in a P2P E-commerce platform settings.

P2P trust can be enhanced with a Community Responsibility System (CRS) according to [5]. Ba [5] concludes and proves that the CRS concept can improve trust among peers in E-commerce using game theory. We have extended the work in her publication by deriving features from the CRS that can be implemented by P2P platform engineers.

Furthermore, Ba [5] defines and explains different types of trust and the life cycle of its development to achieve the highest levels of trust. Information-based trust comes from information available. Calculation-based trust comes from weighing the value gained from a successful transaction versus that of an unsuccessful one, also taking into account value gain versus loss in the case a user is considering cheating another user in a transaction. Transference-based trust comes from trusting in another entity, and that trust spills over and is transferred to another, for instance through certification or word-of-mouth referrals.

Möhlmann & Geissinger [6] wrote a publication on trust in the Sharing Economy. We found [6] in particular to be very related to our work. The authors discuss digital cues and their ability to build both interpersonal and institutional trust in the context of sharing economy in P2P E-commerce platforms. Furthermore, the authors argue that the more cues a sharing platform provides, the more trust is produced. The recorded digitally displayed trust cues were mainly: peer reputation, digitized social capital, provision of information, escrow service, insurance cover, and certification and external validations.

The work in [6] provides sources of platform-mediated peer trust. However, the publication did not present empirical evidence in the form of asking the users themselves to suggest the digital ques in the study, we therefore argue that our study will extend the recorded digital cues and prove their validity and viability by asking P2P platform users whether these trust factors will enhance their inter-user trust or not.

Xiong & Liu [12] developed a dynamic P2P reputation-based trust supporting framework. The framework includes an adaptive trust model to quantify trust among peers based on a transaction feedback system. We will use the reputation-based trust framework to help us build our factors with consideration to reputation systems as an integral actor among peers in an online system.

The model in [12] introduces five parameters and a trust metric that combines them all. The parameters to evaluating trustworthiness of peers are: (i) feedback a peer obtains from other peers. (ii) the feedback scope, total number of transactions a peer has with other peers. (iii) the credibility factor for the feedback source. (iv) the transaction context factor for discriminating mission-critical transactions from less or non-critical ones. And (v) the community context factor to address community related characteristics and vulnerabilities.

[12] further presents a formula to prove and show how to calculate the credibility of peer reviews, they also extend their paper with guidelines and architectural design for how their model can be implemented by P2P platforms and which shortcomings of implementing it can occur. We will use their reputation-based trust model to expand our list of trust factors and build upon their trust model.

We do see the relation between [12] and our work. However, our list of factors is more comprehensive in the way that it captures trust inducing features from all perspectives and not solely reputation-based systems.

Motta et al. studied the factors that determines from whom people would seek recommendation from in general [14]. The study concluded factors that influence the choice of source people make and their perceived trust [14]. The factors found were expertise, experience, impartiality, affinity and track record. We believe the results [14] found are of significance to our list of factors since we consider increasing the perception of trustworthiness between peers when an interaction prior to a transaction occurs important.

C. B2C publications

B2C is an abbreviation of Business-to-Consumer, and the following related work examines trust factors between a business and a consumer.

Publication [3], examines three trust building mechanisms: third-party certifications, reputation, and return policies. The study only focuses on customer to business relationships in E-commerce. We have used some content from this publication (see section V), however, the publication did not present concrete requirements for how to build E-commerce trust even in the customer to business settings.

[17] studies and tests the effects on perceived trust of online information and subsequent attitudes of different online trust cues. Perceived strong vs. weak social relationships, and positive vs. negatives online messages. This publication provided insights on trustworthiness perceptions online, however, it is not focused on P2P. [17] analyzes and discusses the perception of trustworthiness from a general point of view.

Pan & Chiou [17] included in their study a reputation system's effect on users in both the *credence*- and *experience* goods categories. Credence goods are goods whose quality cannot be verified by users even after consumption, examples of credence goods are health foods. Experience goods are goods whose quality can be verified after consumption, but not before. Examples of experience goods are in general services, where one would not know the quality of a service until it has been purchased and one can see the result of the conducted work.

For the purpose of this study, we decided not to put any additional emphasis on the findings of [17] in relation to a reputation systems effect when dealing with different types of goods. We concluded that it is possible for online P2P websites to trade just about anything, meaning both experience and credence goods are likely involved. However, we found that evaluating reputation systems separately, for credence and experience goods, would not be appropriate as this study aims to find a solution that should fit *any* P2P system.

In order for new as well as existing E-commerce P2P technologies to increase or maintain their user base, their users need to form some level of trust towards each other in the platform [6]. By looking at the present related work on trust in P2P platforms, we notice that a few publication have indeed gathered significant trust factors to help peers develop and maintain certain levels of trust among each other. However, we will further investigate the affects of the gathered trust factors in this study by asking peers of P2P platforms. We believe it is important to test the factors' validity and value by asking the people who will be affected by them.

III. Methodology

This study produced an artifact, namely trust factors that can be implemented by online P2P technologies to improve inter-user trust, as well as a feasibility evaluation for each factor. We used the design science research method (DSR) to carry out our research. DSR is generally used to develop new technologies and solve problems [7]. The aim was to develop our artifact in one iteration that would consist of three phases. Each of the phases strives to answer one or some of the research questions asked in this study in an effort to produce the results we aimed for and the artifact we promised to deliver.

In the first phase, we obtained trust factors from previous literature in an effort to answer RQ1. In the second phase, we updated, eliminated, prioritized, and improved the list of trust factors from RQ1 by surveying users of P2P platforms to help answer RQ2. Lastly in the third and final phase, we carried out a feasibility study for the found factors to answer RQ3. The research questions were the following;

A. Research questions

1) What are the trust factors that need to be present in an E-commerce P2P platform in order to increase inter-user peer trust that have appeared in previous literature?
    1) What are the most frequently mentioned P2P-related trust factors derived from RQ1, according to the literature used to answer RQ1?
2) What are the most and least important P2P-related trust factors derived from RQ1, according to E-commerce P2P platform users?
    1) Are there any other trust factors according to users of P2P platforms, besides those derived from RQ1?
3) How feasible is it to implement the trust factors derived from RQ1 in an E-commerce P2P platform according to E-commerce software engineers?

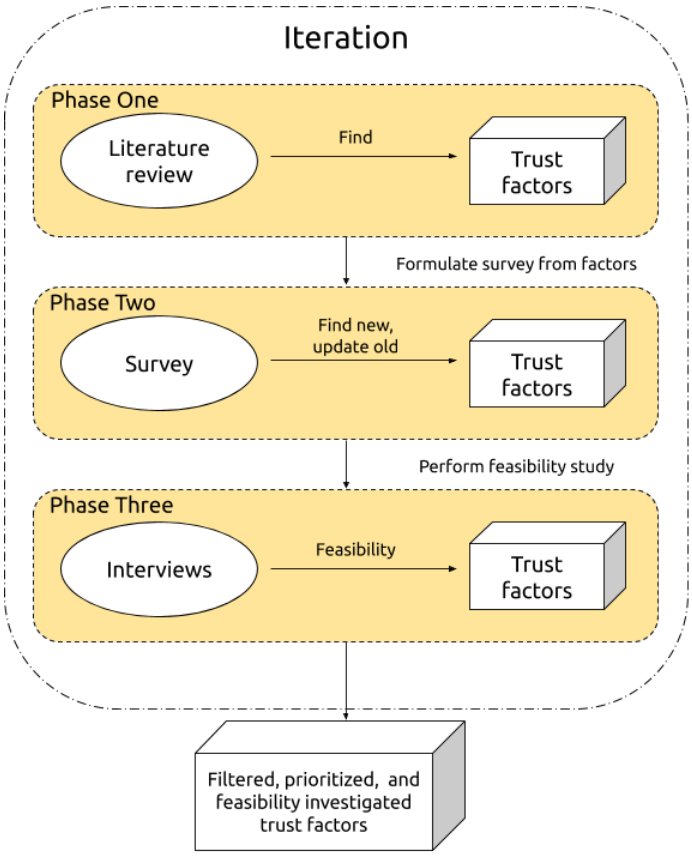

Figure 1. The figure above illustrates the three phases within one iteration, the transitions among them and the artifacts produced by each phase

B. Phase I

For the first phase, a literature review was conducted in order for the study to obtain its baseline trust factors and answer RQ1. It is important to consult existing literature in the problem domain to get a complete grasp of what is already known [8], avoiding re-inventing the wheel. Aside from seeking out trust factors, the study's literature review sought to find what trust means in the online P2P domain; where it should be addressed, when (in time) it is critical, and how it could be maintained.

When selecting literature for phase I, we searched for papers on the internet that contained one or more of the following relevant keywords: Online, trust, requirements, P2P, E-commerce, Peer to Peer. Furthermore, publications were checked for quality and validly through looking at the number of citations they had. We did not choose a threshold to dismiss or include papers, however, the higher the citations were, the more quality the paper had for us to use in this study.

The results from the literature review were used to create the first version of the study's artifact, three tables showing each of the found trust factors. The tables were divided based on the type of trust that the found factors attempts to address. For this study, we have chosen the definition for *information*, *calculation*, and *transference*-based trust as a way to differentiate between the found factors, see section II-B for

an overview of each trust category. At this point of the study, the factors were ordered in terms of mention frequency in the literature, with the most mentioned trust factors on top in order to answer RQ1.1.

C. Phase II

The trust factors found during the literature review phase I, were consulted when constructing a survey for online P2P service users in an effort to answer RQ2, asking them about the applicability, and relevance of each found factor from literature.

Conducting the initial literature review helped us include appropriate questions in the survey for phase II, as the factors found in literature already had established academic relevance, as opposed to manufacturing survey questions based on author experience. Some of the trust inducing factors found in phase I, were not be presented in the survey, and hence were not assigned priority during this phase. The factors that were not presented in the survey were: simplicity, consistency, and accessibility. We excluded them from the survey since we felt it would be difficult to visualize non-functional requirements in text and have respondents comprehend the text attempting to explain them. Additionally, a design being good or bad is a subjective matter and is up to the eye of the beholder. We felt it more in line with this study to exclude evaluating different designs.

The goal of phase II was to eliminate, gather new, update old, and prioritize trust factors by surveying users of current online P2P platforms. We started the second phase by conducting a pilot study to help formulate neutral type questions and avoid biased questions when preparing the final survey questionnaire. We invited two software engineering bachelor students that were not involved in making this study, as well as our thesis supervisor, to help in assessing the created questionnaire. We then distributed the survey after concluding the pilot study. For further information about the survey, visit this link: Survey, or see table VIII to see all questions included in the questionnaire.

The pilot study consisted of the two authors that were involved in conducting this study and two software engineering students that are not involved in this study. The software students were selected for their knowledge in English and E-commerce in general, and were acquaintances of the study's authors. The process started with showing the students the questionnaire and asking them for different qualities that are missing or needs updating in the questionnaire. The qualities were, readability, text comprehension, grammar errors, biased insights, order of the questions, sectioning & grouping, and finally the length of the questionnaire.

The sampling method used for the survey was convenience sampling. However, we also selected to only survey current P2P platform users. We have chosen convenience sampling as the time available for this study was too short to allow for more sophisticated sampling methods. We did, however, ensure that the survey respondents were only online P2P platform users by asking a control question in the survey to help eliminate any other respondents. The sample was selected from the authors social circle, and the target sample size was set to thirty data points. We used e-mail and direct private messaging as our distribution method for all selected participants.

The final survey data was analyzed using descriptive analysis for the quantitative data. We chose to also include one open question in the survey in order to answer RQ2.1. For the open questions results, we set a threshold of 3 times for the factor to be repeated across respondents in order for a trust factor discovered through the open survey question to be included into the list of trust factors. For instance, if a new trust factor was stated by equal to or more than 3 respondents, we would then add it to out list of trust factors subjected to a feasibility analysis in the next phase. The response data gotten from the open survey question was subjected to the same coding scheme as described in the end of section III-D, but of course focusing on RQ2.1 instead of RQ3.

The survey results were used to: 1. Remove trust factors that are not perceived as important and 2. Order the trust factors from highest to lowest scoring according to the survey participants. In order to decide which trust factors to remove and how to prioritize the remaining ones, we use a score threshold, all trust factors scoring below said threshold would then be removed from the resulting table(s). The score for each trust factor was calculated based on the median score of each survey question. We decided to use median scores since the data collected from the survey is ordinal, and the score threshold was set to 3.5. The threshold was set to 3.5 since a median score of 3 or below represents that most respondents were either negative or neutral towards the proposed trust factor. A trust factor with a median score of 3.5 represented that at least half of the responses were positive.

Priority was assigned depending on the median score of the trust factor. If the median score was equal to that of another trust factor, then the number of positive responses were compared. Positive responses meaning a response stating that it would be either "Likely" *or* "Very likely" that a proposed trust factor would have a positive impact on the survey respondent's trust towards other peers of an online P2P platform. If the number of positive responses also matched, then the number of answers in the "Very likely" category determined which will be assigned the highest priority of the two. If all comparisons matched, the trust factors were simply assigned the same priority.

Lastly, the survey results were presented in a stacked bar-chart diagram and in text for the qualitative findings.

D. Phase III

During the third and final phase of this study, we conducted face-to-face interviews with E-commerce software engineers. Interviews are an effective way of getting qualitative data [9], which was desirable for the purpose of the final phase of this study, where we aimed to obtain personal feedback on the feasibility of implementing each factor. Through these interviews, we intended to evaluate the feasibility of the refined list of factors from RQ2. The feasibility of each factor was

approached from two different perspectives, technical and schedule, following the feasibility study technique TELOS [10], (see section I).

Our target population for the interviews was E-commerce software engineers that were, or had been, working on E-commerce platforms, including both user interface (UI) and back-end development.

Sampling was done by firstly creating a list of the authors acquaintances that work within the IT industry (and are working or have been working on online platforms). Secondly, asking the interviewees prior to performing the interviews if they have sufficient experience in all of TELOS's areas, and if not, we would only focus on some areas in TELOS. This resulted in tailoring the TELOS technique in order to fit our interviewees experience. We narrowed TELOS down to only the Technical and Schedule aspects to be exploited for each of the trust factors. And finally, request each acquaintance to participate in the study. By that, a mix of convenience and purposive sampling is used. Convenience since the companies selected are based on that the authors have acquaintances working there, and purposive as only online E-commerce platform software engineers with both UI and back-end experience were selected. We aimed to have a sample size of five engineers.

We aimed for a higher-level overview of the found trust factors' feasibility, without concrete implementation or testing on a particular P2P system. The interviews with the E-commerce P2P system engineers were semi-structured. In semi-structured interviews, the interviewers introduce the topic area as well as areas to focus on along with asking a set of questions [9]. We started off the interviews with a brief introduction of our research topic and the desired outcome. Next, we presented the factors and asked the interviewee a set of questions, see table VIII-B, in order to conduct an analysis of feasibility in relation to similar online systems that they have worked with.

All the interviews had their audio recorded, depending on if consent to record was given by the interviewees. No personal information was gathered during the interviews, in order to protect the privacy of the interviewees and prevent them from being able to be identified through the recorded material.

For analyzing the final interview material we employed thematic coding. Thematic coding is a way of "identifying, analyzing, and reporting patterns (themes) within data" [16]. In order to code the recorded material, we started by transcribing the recordings into text. Then, we divided the transcribed material into two parts, each author taking one of the two. After each author has been assigned part of the material, we employed the following coding process:

1) While keeping RQ3 in mind, read through the entire transcript and write down initial ideas or themes.
2) Read the entire transcript again, very carefully, and code relevant passages, words, sentences, or paragraphs.
3) Compare the extracted codes between authors and align them.
4) Again separately, go through the created codes and create categories for those that are similar.
5) Combine and compare the categorized codes between authors and align the groupings, eliminate codes that are repeated or deemed irrelevant (in relation to RQ3).
6) Label the categories.
7) Determine connections between codes and categories.

By employing the above coding process, we hoped to find common themes in the qualitative material.

The output from the analysis of the gathered interview data was the final artifact of this study: comprehensive, prioritized, and feasibility investigated P2P trust factors.

IV. Threats to validity

A. Internal Validity

During phase I, our biggest challenge was selecting literature. Whether the chosen literature for this study was relevant enough in terms of the found trust factors, specifically in the E-commerce P2P domain, was a threat to our final results. In order to mitigate the issue with the literature relevance, we researched exhaustively on each publication before we selected it, we have read how many times each paper was cited by others in order to determine the paper's quality and relevance in the E-commerce domain. Furthermore, we were searching for papers containing relevant keywords. In our study we used the following keywords: Online, trust, requirements, P2P, E-commerce, Peer to Peer.

During phase II, we carried out a survey, the few threats that can occur to the results are whether the survey questions actually measure what the study claims, and whether these questions are clear enough to the respondents. If some questions have the slightest vagueness, respondents can select anything, just to move on from the question. In order to mitigate these threats, we have conducted a pilot study where the survey questions were subject to analysis by peers that are not involved in carrying out this study. By having others evaluate the survey questions' effectiveness, we have reduced the impact of author bias on the questions asked.

When we analyzed the results from the survey, the score for each trust factor was calculated based on the median score of each survey question. We decided to use median scores since the data collected from the survey was ordinal, and the score threshold was set to 3.5. The threshold was set to 3.5 since a median score of 3 or below represents that most respondents were either negative or neutral towards the proposed trust factor, and a trust factor with a median score of 3.5 had at least half positive responses.

Another internal threat is finding the trust factors that are actually important and whether other researchers could find these factors as well, if they were to repeat this study along with its material. We believe that it is rather subjective to carry out qualitative coding as a method to analyze the gathered data. We aimed to reduce this threat by constantly being aware of it, and keeping in mind to be objective throughout the process of selecting the trust factors.

Table I
INFORMATION-BASED TRUST

#	Trust factor	Explanation	Referenced research
1	Reputation systems	Facilitating the rating and reviewing of peers, by other peers. The reviews and ratings are visible to all other peers in the system	[3], [5], [6], [11], [12], [14], [17]
1.1	*Rater credibility*	A certain situation may lead to that a user's review (or rating) should be assigned a lesser, or greater, weight. Affecting factors could be community (friends, coworkers, or total strangers) and transaction contexts (small, medium, or large transactions)	*[12], [17]*
2	Complete digital profiles	A full description of the user at hand, relevant to the platform's business context, is provided	[1], [2], [5], [6], [14]
3	Strong authentication	A means of confirming that a person is who they claim to be, and to prevent cheat-and-leave situations, where user accounts can be re-created at a low cost for the cheater	[5], [6], [13]
4	Picture upload	Enabling users to present themselves not only in words but also by showing an image	[1], [2], [6]
5	Simplicity in the UI's design	Guiding the users through the service with simple, easy to understand (and learn) controls, as well as displaying important information clearly	[1], [2]
6	Consistency in the UI's design	Each page is similar enough to the previous, as not to force the user's into a new learning phase just for moving to another page	[1], [2]
7	Accessibility in the UI's design	The entire service is designed in such a way that all users feel welcome and well taken care of including those with different needs	[1], [2]
8	Public transaction history	Enable users to browse through past interactions of other site members and assess their abilities and other users past experiences	[2], [5]
9	Privacy policy and terms and conditions	Making it clear to users how their data is treated and what rules the platform applies	[1]
10	Domain name	Keeping the domain name in line with the company name, avoiding names that could be harder for users to connect with the site they are visiting	[1]

B. External Validity

The final threat is the generalizability of the final artifact. The convenience sampling method can cause a threat to generalizing the findings of this study. Can we generalize the results on to the world, having the survey carried out only in Sweden? Is it enough with 5 software engineers to exploit the technical and schedule aspects of each of the trust factors? In order to attempt to mitigate these issues, we performed the literature review first to get sufficient insight on the current body of knowledge on trust factors in P2P platforms globally. We selected publications that are written by authors from many parts of the world, making the results not only applicable to Sweden but globally as well. As for the population selection in the survey, we added a question in the survey to exclude any users of online platforms that are not P2P users. We also selected software engineers that are experienced in E-commerce platforms.

V. RESULTS

A. Phase I: Literature Review

In order to answer RQ1, we present trust factors found from the literature review, presented in tables II, III, and I. Each trust factor is grouped by which category of trust it belongs to, either calculation-, information-, or transference-based trust as stated in section III.

To answer RQ1.1, each found trust factor is presented together with the research that argued for them, and the tables are ordered based on how many mentioning papers they each had, with the highest number of mentions on top.

Some trust factors have sub-factors, these are italicized below and always listed directly below the factor that they belong to, regardless of their respective number of mentions. We listed these factors as sub-factors because of the context they were found in. For instance, *cheating behavior punishment* has the sub-factor *legal contract* due to [11] arguing for legal contracts to be part of realizing the cheating behavior punishment trust factor.

Table II
CALCULATION-BASED TRUST

#	Trust factor	Explanation	Referenced research
1	Cheating behavior punishment	Users that cheat other users need to be detected and punished for malicious actions	[5], [6], [11]
1.1	*Legal contract*	A signed agreement of what is expected of two parties entering into a transaction, including repercussions if one fails to follow the agreement	*[11]*
2	Escrow service	Payment is held by the platform facilitating a transaction and is released only once the agreement between the transacting parties has been fulfilled	[3], [6]
3	Insurance policy	A safety net in case of unexpected outcomes	[3], [6]
4	Return policy	Being able to return goods if they do not meet the expected quality	[3]
5	Internal site activity advertising	Displaying key activity parameters publicly, for instance the number of active users during the past week, day, or hour	[11]

Table III
TRANSFERENCE-BASED TRUST

#	Trust factor	Explanation	Referenced research
1	Community memberships	Showing what community each user belongs to. Friends, family, coworkers, similar interests etc.	[2], [3], [5], [6]
2	Third party certification by trusted third parties	Third parties can be used for various site functions, such as payment service providers or to ensure the truthfulness of statements made by a user, by having a third party vouch for their statements	[1], [3], [5], [6]

As clearly indicated by the factors of the information-based trust type (see table I), Reputation systems were by far the most mentioned trust factor with 7 out of 11 papers referring to it. The second most mentioned was the complete digital profiles with 5 papers mentioning it, and in third place came community memberships, and third party certification by trusted third parties.

B. Phase II: Survey

The questionnaire sent out to online P2P platform users had a goal number of responses set to 30, the actual number of respondents was 40. The first question of the survey was a demographic question, intended to eliminate respondents that had never used a P2P system, four respondents here stated that they had not previously used any online P2P platform. After eliminating those respondents that said that they had never before used a P2P system, we ended up with 36 responses to the online survey, each with a completion rate of 100%. To clarify, the four respondents that had never before used any P2P system were not allowed to proceed with the rest of the survey, and no responses were recorded from them. The survey results are shown in figure 2. Raw survey response data can be found in the appendix, table IX.

As the number of respondents of the online questionnaire was satisfactory, the results were used for further prioritization of the trust factor tables presented in the previous phase's section, thus addressing RQ2. The survey results were used to: 1. Remove trust factors that were not perceived as important and 2. Order trust factors from highest to lowest score. After filtering out all trust factors that scored below the median threshold mentioned in section III, a total of 10 of the surveyed trust factors were kept. The five trust factors that got eliminated from further investigation were: Internal site advertising, complete digital profiles, profile pictures, privacy policy and terms and conditions, and domain names. See the resulting table IV. To set the prioritization shown in table IV, we employed the prioritization calculation described in section III. Simplicity, consistency, and accessibility have not been assigned priority, as these factors were not part of the survey (see section III).

A *domain name's* impact on trust was voted to be the least likely to have any effect on trust, also scoring the highest in terms of most "Very unlikely" responses. Domain names had a total of 30 responses that were either neutral or negative, 17 of which were negative and 7 of those were in the "Very unlikely" category. By that, domain names far surpassed the second-to-

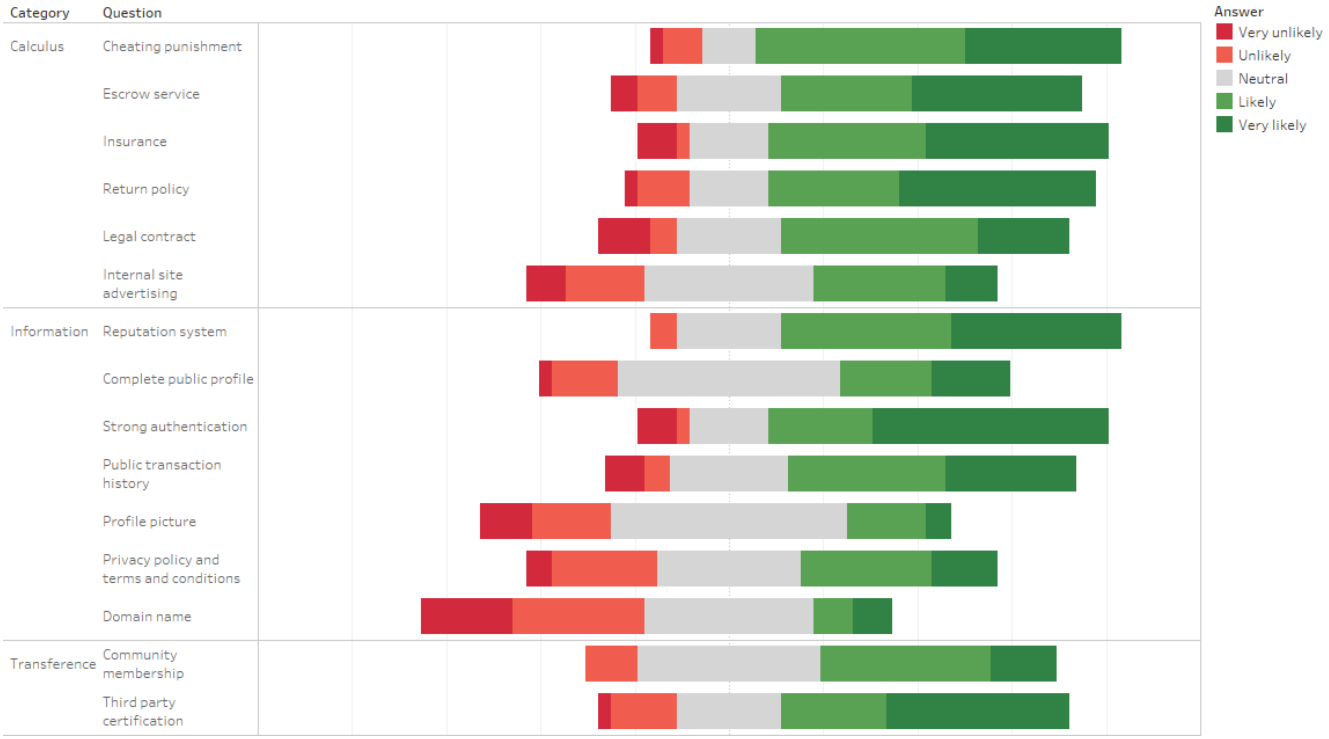

Figure 2. Stacked bar-chart showing the results of the P2P platform user survey on if various trust factors would have an effect on trust

Table IV
PRIORITIZED TRUST FACTORS

Priority	Category	Trust factor
1	Information-based	Strong authentication
2	Calculation-based	Cheating behavior punishment
3	Calculation-based	Insurance policies
4	Information-based	Reputation systems
4	Information-based	Rater credibility
5	Calculation-based	Return policies
6	Calculation-based	Escrow services
7	Transference-based	Third party certifications
8	Information-based	Public transaction histories
9	Calculation-based	Legal contracts
10	Transference-based	Community memberships
-	Information-based	Simplicity
-	Information-based	Consistency
-	Information-based	Accessibility

last trust factors (*profile pictures* and *privacy policy and terms and conditions*) which only had 10 negative responses.

Two factors stood out as the highest scoring ones based on most highest scores (most scores in the "Very likely" category), and most positive scores (most scores of both "Likely" and "Very likely"). The highest scoring trust factor based on the number of responses in the "Very likely" category was *Strong Authentication* with 18 respondents stating that Strong Authentication is very likely to increase their trust in other members of an online P2P platform.

The trust factor that scored the highest based on the number of responses in both the "Likely" and "Very likely" categories was *Cheating Behavior Punishment*. 28 respondents stated that it was either likely *or* very likely that there existing a punishment for cheating members would increase their trust in other members of an online P2P platform.

Some other trust factors that scored high were: Insurance policies, reputation systems, and return policies. Looking at the number of positive responses (meaning responses of either "Likely" or "Very likely), these three factors scored 26, 26, and 25 respectively.

A few survey respondents also chose to leave feedback in the last question, which allowed for free-text answers, addressing RQ2.1. A total of 8 respondents left some form of feedback, all results are shown in table V.

The free-text survey question did not result in any additional trust factor getting added into the refined list of trust factors. Neither mentioned trust inducing factor gotten from the free-text survey question was brought forth enough times to be included, in accordance to the inclusion threshold we had set (see section III-C). Due to the low number of responses, no coding was carried out for the free-text answers as it was quite apparent that no respondents had provided a similar statement even twice.

Table V
ANSWERS FROM FREE-TEXT SURVEY QUESTION

#	Answer
1	Some indication of "closeness", if somebody else I trust (eg. a friend) made a transaction with person X, and my friend was satisfied with the transaction, I would be more likely to trust person X, because I trust my friend's judgment.
2	no
3	The design of the website and how well it works
4	Easy to be able to get in touch with the E-commerce platform to get help in case something goes wrong with the transaction.
5	Nope
6	NO
7	If I know they are licensed and they could loose their licence if they did not adhere to E-commerse laws and or regulations.
8	As long as there is a strong method of authentication and some kind of legal bind on transaction that it mediated by the site, it is not as important for me that the seller has a lot of public info

C. Phase III: Interviews

During the third and final phase, three interviews were held with software engineers. We were unable to obtain five interviewees as planned in section III.

An overview of the feasibility analysis provided by the interviewees responses can be found in table VI.

For the purpose of this results section the names of the interview participants have been changed to protect their identity. The interviewees will be referred to as Jake, Paul, and Janet throughout this section. Jake had four and a half years of experience working with software development and was at the time working as a full-stack software engineer. Paul had almost two years of experience working as a software engineer in various positions, at the time working with product integration for a large public sector project. Janet had over five years experience with software development across a multitude of projects and was working as a senior, full-stack, software engineer at the time of the interviews taking place.

The end result of the interviewees view of the proposed trust factors technical complexity and scheduling implications can be found in table VI.

Strong authentication: Due to differences in personal experience, strong authentication was seen in different ways between interviewees. Jake argued that strong authentication methods would be a huge undertaking, something that would have to co-exist alongside the entire life-span of the product. Janet and Paul, on the other hand, both stated that a 3P solution would be the way forward. Janet also stated that since authentication is an area of functionality without much complexity connected to it, it would be very simple to realize in a product.

Jake argued for keeping authentication as a core part of the full life-span of any product, meaning an indefinite amount of time would need to be spent on maintaining a strong authentication method. Janet and Paul, on the other hand, both stated that it would be quite easy and hence take a short amount of time.

Cheating behavior punishment: Both Jake, Paul, and Janet were in agreement that cheating behavior punishment could be extremely difficult to realize in a P2P system. Their reasoning was grounded in that it is difficult for a system to determine whether cheating has occurred. Paul stated that the "hardest part would be first and foremost to how you define that someone has cheated another person".

Punishment, on the other hand, was perceived to be quite straight forward from a technical perspective. Punishments on digital platforms were seen as well defined, Janet stated that "punishment on an online platform would typically entail something like banning the user from trading or downgrading their account in some way". Due to the business logic being seen as easy to define, most of the interviewees' efforts was put on trying to define fraud or cheating detection.

Difficulties in breaking down the cheating behavior punishment trust factor resulted in that an estimation of time could not be derived. It was however stated by both Jake and Janet that the difficulty in realizing this factor comes from the complexity of the business logic. Simple business logic would mean that the realization would also be simple, meaning that it would, in this case, not require a very long development cycle.

Insurance policies: All three interviewees were fairly in agreement when it came to the technical complexity of providing an insurance policy. There was some uncertainty among the interviewees, but it was mostly boiling down to that they felt it depended on how much responsibility the P2P system would take when it came to insurance claims.

Interviewees agreed that displaying that some form of insurance is provided requires no more than "some kind of checkbox where you consent that you're being provided insurance". When it came to claiming the insurance in case something has happened is where opinions started to diverge. However, the P2P system simply providing a way of acknowledging that the user has knowledge that they are being provided insurance as well as a way for them, through the P2P platform, to notify the insuring party of a claim would not be technically difficult, and would not require a lot of time

Reputation systems: The interviewees had very little input on reputation systems, not because they did not know what to answer but because of the simplicity of the feature. Janet stated that "a reputation system is a CRUD system, the complexity is proportional to the number of data points you're handling", and that a CRUD (create, read, update, delete) system handling an integer and a piece of text is on the easy side of the implementation spectrum. In short, reputation systems were seen as both technically simple and to require only a short development cycle.

Credibility of reputation systems: Something that was not seen as straight forward at all was a way of technically assessing the credibility of a rater or reviewer in a reputation system. Credibility was, together with cheating behavior punishment, considered to be the most technically complex trust factors to

Table VI
FEASIBILITY INVESTIGATED TRUST FACTORS

Priority	Category	Trust factor	Technical	Schedule
1	Information-based	Strong authentication	• Simple to use a 3rd party solution • May prove difficult to develop in-house	• Constant concern if in-house • Short time to implement 3rd party solution
2	Calculation-based	Cheating behavior punishment	• Difficult to define business logic for fraud detection • Easy to define business logic for user punishments • Easy business logic available for fraud detection, but at the cost of efficiency of detecting fraud/cheating	• Easy business logic would yield a short development cycle • Good fraud/cheating detection difficult and hence costly
3	Calculation-based	Insurance policies	• Simple to implement, depending on the degree to which a P2P system is involved in insurance claims. Showing an insurance disclaimer and providing a way for a claiming party to contact the insuring party is technically simple • Could be technically challenging if the P2P site facilitates communication between the insured and the insuring	• Short time to deliver since small technical increment • Could take longer if P2P site facilitates communication
4	Information-based	Reputation systems	• Simple and well standardized	• Short time to deliver
4	Information-based	Rater credibility	• Difficult to define business logic • Could be made simple (averaging ratings), but at the cost of reliability of the credibility calculation • As difficult to implement as the defined business logic • Performance may be impacted if credibility score is based on parameters that are subjected to change, since credibility would then need to be recalibrated as often as the parameters are updated	• Depending on technical solution chosen, either very long or very short • Averaging ratings would take very little time
5	Calculation-based	Return policies	• Technically challenging if integrated into site to control flow of returns through the software • Technically simple if providing a disclaimer stating that a return policy is enforced	• Depending on technical solution chosen, either integrating the flow of returning goods through the software or only displaying a disclaimer, it would either take fairly long or a very short amount of time
6	Calculation-based	Escrow services	• Simple business logic • Depends on 3rd party payment solution, difficult to assess due to inexperience in payment software by interviewed software engineers. However, considering the business logic is simple, the integration work should not be complex	• Integrating with a 3rd party payment solution to allow for putting payments into escrow was thought to take only a short amount of time
7	Transference-based	Third party certifications	• Depends on what is being integrated with, integration work will be as complex as the third party software's API	• Depends on what is being integrated with, integration work will be as complex as the third party software's API

Priority	Category	Trust factor	Technical	Schedule
8	Information-based	Public transaction histories	• Retrieving and displaying information about transactions is technically simple • Complexity could arise if a lot of data transformation is wanted	• Short time to deliver • Could take some additional time to ensure that personal identifiable information is not exposed in an unlawful manner
9	Calculation-based	Legal contracts	• Simple and well defined business logic • 3rd party solutions existing for personally identifiable authentication, which is necessary for signing contracts	• Simple business logic as well as pre-existing solutions to prove the identity of the signing parties means it would take a short time to deliver
10	Transference-based	Community memberships	• Interviewees in disagreement on the complexity of realizing this trust factor, but in agreement that it would require significant effort due to the number of functions needed to support communities • Most interviewees argued the functions necessary are simple in nature, but that there are many of them, meaning complexity could arise if there are a lot of functions that have interdependencies • Argued to be the single largest feature to implement if realizing this trust factor	• Long time to deliver, this trust factor was less seen as an individual feature, but more of a project
-	Information-based	Simplicity, Accessibility, & Consistency	• Impossible to assign a technical complexity due to these trust factors relating to design goals rather than engineering problems. What simplicity means cannot be universally applied to any system, since it depends on the user base, the type of application etc. • Accessibility could be addressed by investigating generic accessibility guidelines, for instance those provided in the WCAG (Web Content Accessibility Guidelines)	• Not possible to evaluate, depends on the system which needs to have its user interface simplified, its size, and its user base

realize. Since the business logic, how to calculate credibility, is so difficult to define, all interviewees agreed that the supporting algorithm for calculating credibility would be the largest technical challenge. However, provided that there is a well defined business logic prior to starting implementation, it would not necessarily be a very large challenge to implement, provided there is a blueprint.

Paul emphasized the performance implications of implementing such a credibility system. He stated that depending on the parameters of the credibility algorithm ”every time someone rates someone, it would have to re-calibrate”. Paul meant that it would be difficult to manage a system that bases the credibility of a rater on a dynamic parameter, as one would have to take care not to overload the P2P platform servers due to rater credibility re-calibrations occurring too frequently.

Janet and Jake alike argued that an algorithm is only as complex as you make it. This means that credibility could be made very easy, or very hard, depending on the level of ambition. Jake stated that ”just to take the average of every opinion given to that person I mean would it really be accurate” when discussing simpler, but perhaps more inaccurate, approaches.

Neither interviewee was able to give a solid time estimation due to the vast number of potential solutions. From averaging each rating since the beginning of time, to basing the credibility on dynamic, ever-changing, parameters. Jake proposed that rater credibility should be kept alive as a feature developed incrementally over a long period of time, since it may be near impossible to define what credibility means right away and in order to find an optimal solution by trial and error.

Return policies: Return policies gained similar responses to that of insurance policies. The interviewees indicated that the technical complexity depends on how returns are expected to be handled in the system. If the P2P system shall support the return procedure, in terms of tracking what transactions have been performed and then ensuring payment is returned to the correct person, it may be quite complex according to Jake.

However, if the P2P system shall only display a disclaimer, agreed to by both transacting parties, and then let each person handle the return claim outside the system, then it would "be quite straight forwards in all aspects I would say", according to all interviewees.

Paul suggested that facilitating returning goods and money as part of the P2P site would not be a very complicated feature, but that it would require some integration work with the payment service provider. However, Paul was not able to estimate the time needed for such a feature.

Escrow services: Some interviewees had more experience with integrating with payment systems than others. Janet stated clearly that supporting an escrow service would be "possibly the simplest of all, because you are pushing the implementation to your payment service provider". Other interviewees, with less experience, were not as certain. However, both Jake and Paul agreed that the idea behind escrow services, that money is held until one party agrees to its release, is simple and that a system wanting to support such functionality would not have to spend so much time in getting it realized in a system.

Most interviewee responses depended on that the third party payment service provider would support such functionality, and that it would be a matter of integrating with them, in which case it would be simple and take a short time to realize.

Third party certifications: Third party certifications raised a lot of uncertainty with the interviewees, they stated that since it depends on what is being integrated with, it is very hard to assess this trust factor. Janet only gave one directive, which was that if the integration is as simple as authentication, being the same number of possible actions, then integrating with the 3rd party *should* be equally simple.

Public transaction histories: Displaying public transaction histories for a site member should, according to interviewees, not be technically complex. "I mean, you would just have to do a look-up in some storage and then just compile that to some kind of data that you send out to a UI", according to Jake. Janet argued that complexity *may* arise, depending on what type of data transformation is wanted, and that "the complexity is in how you process that data". However, if data surrounding a transaction can simply be gotten and then displayed, without any extensive transformation, it should be very straight forward to implement.

The simplicity of realizing the trust factor led to a short time estimation, with the only uncertainty that one would need to ensure that the data to be displayed does not compromise the personal integrity of users. Paul stated that the only hurdle which could prolong the development process would be evaluating which personal identifiable information needs to be hidden or obfuscated.

Legal Contracts: With well defined and generally known business logic surrounding the process of signing documents, interviewees agreed that implementing a legal contract to sign would be a straight-forward task. Depending on the interviewees previous experience we got some different approaches to achieve that goal.

Paul suggested a file-upload solution of digital signatures, while Janet and Jake opted for a third party solution that would provide personally identifiable authentication. Both solutions had in common that interviewees described and argued for their respective solutions with solid confidence. All interviewees also stated that the end solution would be just that, simple, adding that the time to realize such a solution would be short.

Community memberships: All interviewees agreed that implementing communities into a P2P platform would be one of the largest increments derived from trust factors found in this study. Communities involve so many sub-features, such as creating the community, adding members, providing a member area, allowing members to communicate, etc. that interviewees saw it as a large undertaking to realize in a system.

Not all interviewees agreed on its complexity, though. Janet stated that "this is probably the most complex" when asked what she thought about communities technical complexity. Paul, on the other hand, stated that "it should be a straight forward feature", still saying that it would take a long time to implement, but that its features and functions should not be difficult to define business logic for. While they were all in agreement that the trust factor's realization as such would be a very large feature, there were disagreements on the matter of its technical complexity.

Simplicity, Consistency, Accessibility: For the three design trust factors, simplicity, consistency, and accessibility, all interviewees were in agreement. Designing something simple, consistent, and accessible is not something that you could put into a backlog, complete, and then never have to worry about again. Janet stated that "simplicity is not really a software requirement. It's a design goal", referring to simplicity as a non-functional requirement. Jake argued that design "it's probably that work that has to be done continuously, it never stops you could say". He went on to state that the design of user interfaces is something so subjective that what works for one person, may be totally wrong for another.

Interviewees agreed that both simplicity, consistency, and accessibility could not be planned for, but should rather be ever-present goals of the product. Janet argued that what is simple and consistent for one application, could not be applied to another, because what simple means is not universally applicable. However, she also stated that out of these three design factors, accessibility is perhaps the most tangible, and that there are well defined accessibility guidelines such as the WCAG (Web Content Accessibility Guidelines) which could be addressed if one wants to make accessibility improvements.

Due to the nature of these design trust factors, neither interviewee could provide a time estimation, but rather suggested that a continuous improvement model be adopted. Employing a design centric approach to feature development, and making sure to ask users for feedback in order to make good design decisions.

VI. Discussion

This discussion section is divided per trust factor, including the most interesting and surprising finds, as well as highlighting what we, the authors, see as the most important findings. The trust factors discussed here are both ones that lasted through the selection process in Phase II (see section III for more information about the selection process and the score threshold), but also ones that were removed from inclusion in the feasibility study of Phase III. We have included some of the removed trust factors as we felt it peculiar in some cases that they were not seen as important by the surveyed P2P platform users. The discussion section ends with a discussion of what P2P specific trust factors have been found and a summarizing subsection intended to highlight the differences between literature and what was found in the survey.

Strong authentication

Surprisingly few papers state that some form of *strong authentication* is wanted for some trust factors to function properly. By strong authentication, we refer to a way of absolutely verifying a person is who they say they are and proving Peter Steiner's famous quote "On the internet, nobody known you're a dog", wrong. In the online P2P context, strong authentication is important in order to avoid a badly rated person changing their identity and starting over [5]. A virtual identity can be confirmed through strong authentication and establishing an identity allows for reviewing and rating that set identity, thereby enabling trust to be built [13].

The contrast was clear between the literature review and survey results. The surveyed P2P users indicated that strong authentication was in fact the most liked trust factor, while in literature we found it mentioned but not very frequently. One reason for this could of course be that the the need for a strong authentication method is closely connected to P2P systems. In fact, 2 out of the 3 referenced papers where strong authentication was found were specifically aimed at P2P systems. B2C E-commerce systems generally do not require a way of confirming a consumers identity, since goods are shipped upon payment, and the B2C system thereby is not required to verify the buyers identity. While having received money, they can safely ship whatever good was purchased without risking any loss.

Reputation systems

Reputation systems were by far the most mentioned trust inducing factor from literature. Two papers, however, took other aspects into account when covering reputation systems. Xiong & Liu [12], Pan & Chiou [17] both suggest that a reputation system on its own may not be enough to instill the wanted level of trust in a service's users. A user is, for instance, more likely to place their trust in negative reviews than they are in positive ones, since positive reviews can be self-serving [17]. This may be due to that reputation systems can be vulnerable to manipulation, if it is enough for any reviewing party only to provide their email address to leave a review. Email addresses are *not* identities [5], and can easily be created without any cost for the creating party.

In order to battle the credibility of online reviews, the authors of both [12] and [17] argue that *rater credibility* needs to be taken into account. Rater credibility refers to how likely it is that a review reflects that of an actual experience. Xiong and Liu [12] present a way of calculating the weight a particular review should be assigned, based on the number of transactions and the transaction and community context, ensuring that the most relevant reviews are assigned the highest weight in a system. The transaction context is important since "A peer can develop a good reputation by being honest for numerous small transactions and then tried to make a profit by cheating for large transactions" [12]. The community context can be used to find whether the reviewing party is closely related to the reviewed and thus is more likely to provide positive feedback.

The survey showed that reputation systems are also popular among P2P service users, scoring among the highest of all surveyed trust factors. Reputation systems today are a common sighting in P2P systems (take Uber for instance) which indicates that users of such sites are used to placing their trust in the information that the reputation system provides them. The common use of reputation systems we feel further emphasizes the need for reviews and rating to also be credible, in order to battle self-serving reviews. Evaluation credibility, however, was deemed during the interviews to be one of the most technically complex tasks out of all trust factors that were presented.

Complete digital profiles

On the web, the web sites are the "faces" towards the online consumers [1]. In an online P2P context, the sites need to facilitate ways for allowing each person to advertise themselves. Much of the reviewed research argued that *complete digital profiles* were vital for the businesses, regardless of if the company dealt in goods, services, or facilitated P2P interactions [1] [2] [5] [6] [14]. Something that was left out was the actual definition of what a complete digital profile is, most likely due to the vast differences between different business areas. Only three of the reviewed papers mentioned pictures as elements that could increase perceived trustworthiness [1], [2], [6].

In Möhlmann & Geissinger's study on trust in the sharing economy [6], they reported on the results from a car sharing service that had measured trust levels of their users. The results showed that the level of trust towards users with no affiliation to the surveyed was at 88%, family at 94%, and friends at 92% [6], based then on that these random people had *complete digital profiles*. The results showed that the level of trust gotten from a complete digital profile could come close to that of someone as close as a family member or friend, far surpassing that of neighbors and coworkers (42% and 58% respectively).

The survey showed that online P2P platform users were neutral at best towards *complete digital profiles* and *profile pictures*. Looking at the scoring of these two factors, they

both had a dominating presence of neutral votes, 18 and 17 respectively, which was the two highest number of neutral votes among all surveyed factors. We found this to be quite surprising, as much of the literature on online P2P systems argued very strongly for the presence of exposed personal information to allow for trust to be build among P2P platform users.

One view into why the surveyed gave the responses that they did, and which possibly could explain why some chose to score *complete digital profiles* the way they did was a response to the last, open question. The respondent stated that "As long as there is a strong method of authentication and some kind of legal bind on transaction that it mediated by the site, it is not as important for me that the seller has a lot of public info". The respondents answer indicates that some trust inducing factors are not necessarily better if combined, if a P2P system uses a strong authentication method, the perhaps that is enough to prove that the transacting partner is a trustworthy individual.

We also want to note the possibility of a different scoring outcome from the survey if the questions would have been re-arranged. As it was sent out for this study, the survey respondents were asked about both strong authentication and legal contracts as trust inducing factors *before* complete public profiles. It is possible that if they would have been asked about public profiles first, that the outcome would have been different.

Internal site activity advertising

A find in literature, that scored below the set survey scoring threshold (see section III), was that of *internal site advertising* [11]. Castelfranchi & Tan [11] argue that many times, trust comes from perceived reliability, and that "perceived reliability is more important than objective reliability". Castelfranchi & Tan state that while technologies such as security protocols, strict authentication, and cryptography surely are important, one should not forget about social and psychological aspects and that technology alone cannot solve the trust problem [11].

In order to increase perceived reliability, one could attempt at enabling herd behavior, in particular for already established sites where the user base is established. For example, by displaying a site's currently active users, one could increase perceived reliability since "an important way to induce trust is to show that everybody shares the same trusting view" [11].

While the surveyed P2P users did not see this as a trust inducing factor, we argue that perhaps P2P service users were not the right demographic for testing Castelfranchi & Tan's [11] idea. Trust factors such as this one we think could be perceived as unnecessary by P2P service users, as they may feel it does not directly influence their decision on who to transact with. What we mean is that since internal site advertising does not directly convey if a transaction partner in front of them is trustworthy or not, they may feel it does not help them trust another user.

In all fairness, internal site advertising is not a trust factor meant to increase trust at the moment of selecting a transaction partner. Displaying the current number of active users is most likely not going to help a P2P user choose between 2 candidates. We argue that internal site advertising really comes into effect *prior* to searching for a transaction partner, when evaluating if the P2P service as a whole can be trusted.

Cheating behavior punishment

Arguably the most complex of all trust factors covered in this study (side-by-side with rater credibility) was cheating behavior punishment. Cheating behavior punishment was brought forth in three [5], [6], [11] out of the eleven reviewed papers, and was thus not very common in literature.

Though the exact nature of the punishment is mostly not mentioned, one paper suggests that monetary penalties could be used [5]. However, Ba [5] also states that even though a site could issue fines, the cheating party could simply opt not to pay it, unless the grounds of the fine has a legal basis.

Punishing users who cheat is not enough on its own, especially if they are able to easily change their identities. We argue that strong authentication is in fact vital to the success of punishing those who cheat. Although [5], [6], [13] bring forth both strong authentication and sanctioning bad behaviors as trust inducing factors, they do not in their papers directly make the connection between the two.

There are other problems as well that need to be addressed when looking at this trust factor. All interviewees collectively agreed that *defining* what constitutes cheating behavior is very difficult to define. As stated by one interviewee, one could implement a simple push-button reporting system to report that cheating has occurred, that would not be the complicated part. Beyond that, *proving* that the reported has in fact cheated the other party is the hard part. A solution that could detect this sort of cheating behavior lacks a clear definition in literature, probably as one would have to basically have to construct a lie detector.

Still, both the literature mentioning sanctioning fraudulent behavior and the surveyed P2P users are in agreement, punishing those who commit fraud is very desirable. Cheating behavior punishment attained the highest score in the survey in the most positive scores category (most scores in either the "Likely" or "Very likely" categories), indicating that it is something that users do care a great deal about.

Simplicity, Consistency, and Accessibility

Both papers [1], [2] argued for site usability as a trust-inducing factor. Wang & Emurian [1] argue that since the websites are the storefronts of online businesses "applying trust-inducing features to the web sites of online merchants is the most effective method of enhancing online trust, given the current state of knowledge".

Wang & Emurian present a framework for how to improve a website's interface with the goal of enhancing user trust, whose elements had largely been derived from work in the Human Computer Interaction (HCI) field. [1] state that being able to navigate a website easily has often been mentioned as one of the most important aspects to improve online trust [2], and that ease-of-use relates to two characteristics "simplicity

and consistency" [1]. Simplicity concerns how easily a website can be understood by its beholder, while consistency concerns how different pages of a website look alike. Consistency is important as to not force a user to have to enter a learning stage with every new navigation [1].

While one could argue for not including design elements in this study at all, we still felt compelled to keep these aspects, especially after reading much of [2]. Although Simplicity, Consistency, and Accessibility are general design non-functional requirements, we could not deny their impact on user trust.

We also received one response to the open survey question stating "The design of the website and how well it works" was an important aspect for them when deciding where to place their trust. Now, one response out of 36 does not constitute any kind of consensus. However, considering that very few survey respondents chose to write a free-text answer, we argue that it does provide some additional proof that design is an important consideration when evaluating trust-inducing aspects of an online P2P platform.

P2P specific trust factors

Three trust factors stood out to be more P2P-related than others: strong authentication, cheating behavior punishment, and community memberships.

Strong authentication has traditionally, as mentioned above, not been considered vital for B2C transactions, simply because of how goods are exchanged on B2C web sites. The consumer providing payment and only then getting a good shipped to them practically eliminates the need for them to state their identity, it would be an unnecessary step for the B2C vendor.

For P2P platforms, however, private individuals need a way of presenting themselves as trustworthy, often. B2C vendors build their brand, but once that brand is established, trusting them from a consumer point of view becomes almost autonomous. For two parties about to initiate a P2P transaction it is very different. Each of the individuals are likely to never have met before, not online nor offline, meaning baseline trust needs to be established. The nature of P2P transactions, that there is always a different person to transact with, makes an online P2P service require vastly different ways of establishing trust from that of B2C platforms. For starters, strong authentication allows for each transacting party to at least confirm that they are a real person.

Cheating behavior punishment also stood out as a clear P2P-related trust factor from the perspective that the triadic association comes into play. One is the claiming party, two is the accused cheater, and three is the P2P platform. Normally, in a B2C context, if a consumer has been cheated they would either complain to the company who sold them a product or service or report the company to the authorities.

Community memberships are also seen as more related to P2P contexts than other trust factors simply because a "normal" B2C context generally does not require a user (or customer) to show their personal affiliations as it simply would not benefit the B2C vendor. In a P2P context, however, it can be seen as valuable information. Quite a few sources argued that community memberships could enforce trust between users of an online platform [2], [3], [5], [6], most of which were P2P-related publications.

Beyond strong authentication, cheating behavior punishment, and community memberships, no more trust factors could be related more than the others to the P2P context. It was expected to have some overlap between trust inducing elements from B2C, general online trust, and P2P, but perhaps not in the extent shown throughout this study. We, the authors, argue that our results show that more work is needed in the online P2P domain to discover new ways of effectively establishing trust between peers.

Summary

In order to highlight the findings of this study in a way that shows a complete overview of both literature support, P2P service user support, and feasibility we present these findings in table VII.

The score shown for the column "P2P user score" is the total score achieved by each surveyed trust factor. The score was calculated by assigning weight to each of the response options, on a scale of one to five, one being "Very unlikely" and five "Very likely".

The feasibility displayed in table VII is greatly simplified from that in table VI. Here, we only show a simple overview, and if there was conflict in the feasibility evaluation, for instance some interviewees stating high technical complexity and others low, VII will display "High/Low". "High/Low" feasibility may also come from a trust factor having two or more different levels of realization.

High feasibility in this table's context shall be seen as the trust factor being very feasible to realize, and low feasibility as it being difficult to realize the trust factor in a P2P system.

From our results, we hope that online P2P services may consult this study and use the trust factors stated here in order to improve trust between peers of their respective platforms. This study should serve as a guideline for P2P services and allow for them to select trust inducing factors for realization, knowing that each trust factor's relevance has been established together with real P2P service users. P2P services should also easily be able to know if a chosen factor can fit into their general time plan, by reviewing the feasibility evaluation presented by this study.

VII. Future work

Something we feel needs more investigation is connections between trust factors, what type of effects could be observed if they were to applied together (or apart). Some small indications were observed in the survey that could suggest that for example strong authentication and complete digital profiles could be trust factors that when applied together have very little effect, in which case one should avoid applying them together.

Observing combination effects would greatly benefit the research community and industry alike. For instance, a company

Table VII
CROSS-PHASE FINDINGS SUMMARY

Trust factor	P2P user score	Median score	Literature support	Technical	Schedule
Strong authentication	145	4.5	[5], [6], [13]	High/Low	High/Low
Cheating behavior punishment	143	4	[5], [6], [11]	High/Low	High/Low
Insurance policies	141	4	[3], [6]	High/Medium	High/Medium
Reputation systems	145	4	[3], [5], [6], [11], [12], [14], [17]	High	High
Rater/reviewer credibility	145	4	[12], [17]	High/Low	High/Low
Return policies	142	4	[3]	High/Medium	High/Medium
Escrow services	137	4	[3], [6]	High	High
Third party certifications	137	4	[1], [3], [5], [6]	-	-
Public transaction histories	132	4	[2], [5]	High	High
Legal contracts	127	4	[11]	High	High
Community memberships	127	3.5	[2], [3], [5], [6]	Medium/Low	Low
Simplicity, Consistency, Accessibility	-	-	[1], [2]	-	-
Privacy policy and TOS	116	3	[1]	-	-
Internal site advertising	114	3	[11]	-	-
Complete digital profiles	120	3	[1], [2], [5], [6], [14]	-	-
Profile pictures	104	3	[1], [2], [6]	-	-
Domain names	93	3	[1]	-	-

wanting to, as quickly as possible, improve trust between users of their P2P service, should avoid implementing two trust factors that in the end would have the same effect if only one were to be chosen, hence saving time.

Another aspect that needs to be considered when looking at future work of this study, is to cover the remaining aspects of TELOS. As the interviewees were all software engineers, some aspects of TELOS were simply not feasible to include as part of the interviews. In any case, Economic, Legal, and Operational aspects should be investigated for the trust factors found throughout this study as part of future work, by also including project managers, lawyers, and other roles into the set of interviewees.

Lastly, the work presented by this study should be expanded in order to collect more trust factors useful to P2P systems and evaluate their respective feasibility. As mentioned in the discussion section, few found trust factors could be connected to P2P systems more than other types for E-commerce platforms (B2C, for instance). We, the authors, feel this is a strong indication that more work is needed in the area of discovering new (as well as outlining old) ways of improving inter-user trust in an online P2P platform. For this study, the survey was limited to Swedish citizens and only collected 36 responses. By conducting a larger study together with P2P service users one could potentially find additional trust factors relevant to P2P systems.

VIII. CONCLUSION

There seems to be a dissonance between what literature suggests for P2P systems and what the actual users want out of a system in order to build trust between peers. What users find important is not necessarily that which literature suggests most frequently, meaning it could need more research conducted for it.

When investigating the topic of online trust in literature, most of what we found was either general or for the B2C context. Papers covering the P2P context were generally newer, suggesting that the topic has gotten more popular over the years, which would be consistent with a number of popular sharing economy platforms that have emerged during the last decade. Considering the ratio between B2C and P2P online trust papers, P2P still has a lot of catching up to do. It proved difficult to find P2P exclusive trust factors, perhaps because much of today's research is either on general online trust or B2C.

ACKNOWLEDGEMENT

This study was contributed to equally by Sarah Aldelame and Måns Thörnvik. We also want to acknowledge our thesis supervisor, Jennifer Horkoff, for her review and support efforts.

REFERENCES

[1] Wang, Ye Diana, and Henry H. Emurian. "An overview of online trust: Concepts, elements, and implications." Computers in human behavior 21.1 (2005): 105-125.

[2] Beldad, Ardion, Menno De Jong, and Michaël Steehouder. "How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust." Computers in human behavior 26.5 (2010): 857-869.

[3] Chang, Man Kit, Waiman Cheung, and Mincong Tang. "Building trust online: Interactions among trust building mechanisms." Information & Management 50.7 (2013): 439-445.

[4] Linaker, Johan, et al. "Guidelines for Conducting Surveys in Software Engineering v. 1.1." (2015).

[5] Sulin Ba. "Establishing online trust through a community responsibility system". University of Southern California, 2001.

[6] Mareike Möhlmann, Andrea Geissinger. "Trust in the Sharing Economy: Platform-Mediated Peer Trust". Warwick Business School & Örebro University School of Business & Ratio Institue, July 2018.

[7] John Venable, Jan Pries-Heje, Richard Baskerville, "FEDS: a Framework for Evaluating n Design Science Research", School of Information Systems, Curtin University, Perth, Western Australia, Australia; 2 Roskilde University, Roskilde, Denmark; 3 Georgia State University, Atlanta, Georgia, USA. October 2012.

[8] Hart, Chris. Doing a literature review: Releasing the research imagination. Sage, 2018.

[9] qual-methods-in-emp, Carolyn B. "Qualitative methods in empirical studies of software engineering." IEEE Transactions on software engineering 25.4 (1999): 557-572.

[10] Taylor, Julie. "In praise of the feasibility study." (2007).

[11] Cristiano Castelfranchi, Yao-Hua Tan. "The role of trust and deception in virtual societies.", International Journal of Electronic Commerce 6.3 (2002): 55-70.

[12] Li Xiong, Ling Liu. "PeerTrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities". Emory University, Georgia Institute of Technology. IEEE Transactions on knowledge and Data Engineering. August 2004.

[13] Aljazzaf, Zainab M., Mark Perry, and Miriam AM Capretz. "Online trust: Definition and principles." 2010 Fifth International Multiconference on Computing in the Global Information Technology. IEEE, 2010.

[14] Heath, Thomas, Enrico Motta, and Marian Petre. "Person to person trust factors in word of mouth recommendation." (2006).

[15] Tanja Rolandsson. "A Study on Software Requirements Specifications", Lund University, School of Economic and Management, 2010.

[16] Cruzes, Daniela S., and Tore Dyba. "Recommended steps for thematic synthesis in software engineering." 2011 International Symposium on Empirical Software Engineering and Measurement. IEEE, 2011.

[17] Pan, Lee-Yun, and Jyh-Shen Chiou. "How much can you trust online information? Cues for perceived trustworthiness of consumer-generated online information." Journal of Interactive Marketing 25.2 (2011): 67-74.

[18] Shankar, Venkatesh, Glen L. Urban, and Fareena Sultan. "Online trust: a stakeholder perspective, concepts, implications, and future directions." The Journal of strategic information systems 11.3-4 (2002): 325-344.

[19] Lewicki, Roy J., and Barbara B. Bunker. "Developing and maintaining trust in work relationships." Trust in organizations: Frontiers of theory and research 114 (1996): 139.

[20] Mayer, Roger C., James H. Davis, and F. David Schoorman. "An integrative model of organizational trust." Academy of management review 20.3 (1995): 709-734.

[21] Lewis, J. David, and Andrew Weigert. "Trust as a social reality." Social forces 63.4 (1985): 967-985.

[22] Belanger, France, Janine S. Hiller, and Wanda J. Smith. "Trustworthiness in electronic commerce: the role of privacy, security, and site attributes." The journal of strategic Information Systems 11.3-4 (2002): 245-270.

[23] Gefen, David. "Reflections on the dimensions of trust and trustworthiness among online consumers." ACM SIGMIS Database: the DATABASE for Advances in Information Systems 33.3 (2002): 38-53.

APPENDIX

A. Survey

1) Questionnaire: Below is the questionnaire used to collect results for iteration two. The first question marked 'D' was a control question, ensuring that results were only gathered from those respondents that had experience using an online P2P site. The demographic question required a simple 'Yes' or 'No' answer. Questions one through sixteen were likert-scale and required answering on a scale of one through five, where one was 'Very unlikely' and five was 'Very likely'. The last question was open and let respondents write a long free-text.

Each numbered question, except for question sixteen, had the prelude "How likely is it for you to trust a private person online and enter into a transaction with them on an E-commerce platform if..."

Table VIII
QUESTIONNAIRE ON TRUST FACTORS FOR ONLINE P2P-PLATFORM USERS

#	Question
D	Have you ever used an online service where you entered into a transaction with a private individual you did not know and placed trust in them? e.g. Blocket, Amazon, ebay, Tradera.
1	The platform you are using punishes members that cheat other members in a transaction in some form?
2	Whenever you pay for a product or service you wish to purchase from a member in the platform, the platform will hold your money deposit until you release it yourself and are happy to conclude the transaction?
3	The platform provides some policy of insurance where you can get compensated for your losses if needed?
4	The platform provides some return policy?
5	The platform provides a legally binding contract to sign by all member of the site that are entering into a transaction?
6	The platform provides clear information and notifications on how many people are actively using the platform and are transacting with each other?
7	The member's public profile showed ratings, reviews as well as the credibility of the ratings in some form?
8	The member's public profile was complete and not missing any information?
9	The site provided a strong authentication methods such as BankId?
10	The member's public profile showed a history of their transactions?
11	The member's public profile showed a picture of them?
12	The site provided Privacy Policy and Terms and Conditions that clearly stated the rules for,carrying out a transaction among individuals on the site?
13	The site's domain name was different from the legal entity or company running it?,for example, www.google.com the service, has the company Dorthy K. company name running it. The domain name differing from the company name that runs it, can sometimes be suspicious for some people since there is no visible correlation between the service and the provider.
14	Members of the site were a part of a community that has ratings and reviews by other communities on the site?
15	Members of the site were certified by third party trusted partners that helps perceive these members as more trustworthy? Ex, A member signs that they have X licence to do a certain service and then sign using the third party "BankId" to verify their statement.
16	Can you think of further factors that would increase your trust in others in E-commerce platforms when transacting with private individuals?

2) Survey results: Below is the raw survey data.

Table IX
RAW SURVEY RESPONSE DATA

	Question numbers														
Response	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
1	5	2	4	4	5	2	5	5	4	5	2	2	5	4	5
2	2	4	1	2	3	2	4	2	5	3	3	2	1	3	2
3	3	4	5	4	4	1	4	3	5	5	2	1	3	3	4
4	4	5	4	3	3	2	4	2	3	4	2	2	1	2	2
5	4	3	5	5	3	4	5	2	5	5	5	3	2	4	2
6	5	5	5	5	5	5	5	5	5	3	3	3	2	3	5
7	4	5	5	5	4	5	5	5	5	5	4	4	3	4	5
8	4	5	5	2	3	3	4	4	4	4	3	3	1	3	4
9	3	4	5	5	4	3	3	2	4	3	4	4	3	3	4
10	4	4	3	3	2	2	3	3	3	3	3	2	2	2	2
11	5	5	5	5	5	4	4	4	5	4	3	4	3	4	5
12	4	5	3	3	4	3	4	3	5	4	2	3	3	4	5
13	3	3	3	5	3	3	3	3	5	3	3	3	3	3	3
14	5	5	5	5	3	4	2	3	5	4	3	3	3	4	4
15	4	5	5	5	5	3	4	5	5	5	1	4	1	2	5
16	4	4	4	4	4	4	4	4	4	4	4	4	4	3	3
17	5	2	3	2	1	4	3	3	1	1	3	3	3	4	3
18	5	1	4	3	1	3	4	3	3	1	1	2	4	5	4
19	5	3	5	5	5	3	5	3	3	4	3	3	2	5	5
20	5	5	5	5	4	3	5	4	5	5	4	4	2	4	5
21	5	5	5	5	5	5	5	5	5	5	3	5	3	5	5
22	3	5	1	1	1	1	5	1	5	5	1	3	5	3	3
23	4	2	4	4	4	4	2	3	4	3	3	2	1	2	2
24	4	3	4	5	4	4	4	4	5	4	3	5	2	3	5
25	2	4	3	4	2	2	3	2	3	3	2	3	2	3	3
26	4	4	2	2	4	3	3	3	5	3	3	3	3	3	4
27	5	5	5	5	4	4	5	4	5	4	3	4	4	4	5
28	2	3	3	4	3	4	5	3	1	2	3	4	3	3	3
29	4	4	4	4	4	3	4	3	4	3	4	5	3	4	4
30	4	4	4	4	4	2	5	3	4	5	2	2	2	5	5
31	1	1	1	4	1	3	3	3	1	1	3	2	2	3	3
32	5	3	4	5	4	4	5	4	5	2	3	4	2	4	5
33	4	4	4	3	4	1	4	3	2	4	1	5	1	4	1
34	4	3	4	3	3	3	4	3	3	4	3	4	3	4	4
35	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
36	4	3	4	4	4	3	3	3	4	4	4	1	1	3	3

B. Interview Questions

Table X
THE QUESTIONS THAT WERE ASKED DURING THE INTERVIEWS

#	Question
1	What is the complexity of implementing trust factor X from a technical point of view?.
2	What is the approximate duration for implementing trust factor X into a P2P platform?.
3	Are there any implications that we did not think of for a P2P platform to implement the found trust factors in this study?.