Factors Affecting the Use and Adoption Open-Source Software Development Process among Nigerian Undergraduate Students

Odulaja, G.O.
Tai Solarin University of Education, Ijagun, Ijebu Ode, Nigeria
goddyseyi@yahoo.com

Ogude, U.C.
Dept. Of Computer Science
University of Ibadan, Nigeria
ogudecyril@yahoo.com

Adegbempe, A.I.
Dept of Computer Science
Emmanuel Alayande College of Education, Oyo, Nigeria
dradebempela@yahoo.com

Akinfosade, E.O.
Tai Solarin College of Education, Omu, Ijebu Ode, Nigeria
akinyosad1@yahoo.com

ABSTRACT
Using a questionnaire titled “Factors Affecting the Use and Adoption of Open-Source Software Development Process Among Nigerian Undergraduates” to solicit responses in selected Institutions of Higher learning in Nigeria, we investigated the factors that motivate or prevent students from adopting and using the open-source paradigm for software development. Findings from the analysis of data obtained from the research showed that students are keen about using the open source software platforms as a means of developing software systems. However, there are concerns among students of the implication of collaborative efforts on open source platforms on project completion time, equitable access to internet facilities and metrics for assessing individual contributions to the success of the final product from such development process. We conclude by making recommendations on how open-source platforms can be used among students.

Keywords: Open-source, Undergraduates, Nigeria, proprietary, Software and Paradigm.


1. INTRODUCTION
Apart from the issue of making robust software products generally available with the additional edge of combined productivity, collaboration remains one the most welcomed advantage of the Free Open-Source Software (FOSS) initiative among programmers. However, associated with this merit are intrinsic concerns regarding the determination for a successful completion of software projects within record time and the challenges of working with faceless individuals on such intense project. Another pressing issues among open-source collaborators include knowing who is doing what in an open-source initiative. Since it has proven remarkably successful in circumstances that are extremely challenging for traditional development methods and environments, open source software development has received the attention of many researchers within the software engineering community (Feller & Fitzgerald, 2001).

With almost no face to face communication, and very little use of industry-style project management and coordination, open source developers have built a variety of widely-used, reliable, well-known software systems, e.g. the Apache web server and the Mozilla browser (Mockus et al, 1995).

2. THE NATURE OF OPEN-SOURCE SOFTWARE
Open source software development has been described as "extreme distributed software development" (Mockus et al, 1995). The community around an open source software project is usually located around the globe and interacts primarily through asynchronous textual modes of communication, such as email and discussion boards, that are logged in publicly browsable archives. Although open source software projects can vary considerably in their particulars, they do possess a few typical features.
According to Anupriya et al (2003) every successful open source software project has a community of people involved with the project at various levels. The largest group within the community is usually the user community, which is primarily interested in using the Software. Some users report bugs, but that is more commonly the domain of a smaller group of contributors. Contributors are not only users of the software, but are also interested in the general development of the project. They are likely to download the most recent (possibly unstable) versions of the software, actively report bugs, and submit code, either to fix bugs, provide further enhancements to the software or to contribute patches.

At the centre of the community lies a small select group, sometimes even a single person, of 'core' developers, who not only contribute code, but also guide the project by reviewing contributed code and selecting a subset to be committed to an 'official' release of the software.

### 3. FOSS – THE NIGERIAN EXPERIENCE

Borrowing from the experience of countries such as India and some parts of the Tiger nations who are making giant strides in foreign exchange earnings from exporting programmers, Nigerian universities are making efforts to embrace the open-source initiative. Although, no large scale FOSS project can be pointed at as at the time of writing, feelers from the universities under investigation showed that the enthusiasm for collaborative FOSS projects is on the increase in computer science and information technology departments. Training in LINUX and UNIX has become part of the curriculum and a lot of training centres are being established for LINUX and UNIX certification.

Talking about the open-source adoption across Africa, John (2003) opined that countries in Africa are gradually adopting strategies that promote the use of Linux (an open source software) as an alternative to Windows, and South Africa is leading the charge, with the government's recent approval of an open source software adoption plan. Meanwhile Nigeria, which had been lagging behind other countries on the continent in terms of open-source adoption, also has made some moves to adopt Linux in the public education sector. Cost saving seems to be the main factor that has fueled these developments. Besides saving the South African government several billion rand, which amounts to several hundred million dollars, adopting open source software would boost the local software industry, said Mojailefa Moseki, the chief information officer of South Africa's State Information Technology Agency (SITA), when the proposal was put together earlier this year. SITA is a South African government agency that provides information systems and other related services to participating departments.

Various private organization and government officials across the continent, in countries including Kenya, Uganda, Namibia, and Senegal, are pushing state agencies to consider adopting Linux and open source software. In June Nigeria also got into the act, with three organizations -- SchoolNet Nigeria, the Federal Ministry of Education and the Education Tax fund -- pushing the use of Linux, according to Emmanuel Otokhine, who reports on IT for Punch, one of Nigeria’s large circulating newspapers. (Adaora, 2006).

The three organizations have provided 35 Nigerian high schools with Internet access and other educational technologies built on Linux. Aside from that, they are helping to incorporate the study of Linux in the curriculum of those 35 high schools, Otokhine told the IDG News Service. Like South Africa the government is pursuing Linux because it finds it a cheaper alternative to Windows. The Open Source Networking Group has also been established as a subset of the ngNOG (the nigerian ICT Forum) for cooperation and the exchange of technical information between operators of Internet-connected networks in Nigeria. Its focus is to accelerate capacity building in networking with a focus on Free and Open Source software and technologies whilst ensuring adequate participation of Nigerian Academic Network Operators. Lately, the ngNOG called for Collaborators on VSAT monitoring using Free and Open Source Software.

The ICT forum is interested in monitoring VSAT links of member institutes using free and open source software which will be non invasive and have no impact on the VSAT bandwidth. The information to be extracted from the data includes; the bandwidth utilization of the VSAT link, the various software applications in use and other relevant network traffic characterisation such as the source and destination address, data volume, the protocol used etc.

### 4. CURRENT CHALLENGES IN THE OPEN SOURCE DOMAIN

In a Federal survey on FOSS projects carried out in the US (www.networkworld.com) while findings showed that open source projects were coming into their own, many challenges are afoot. For example, those agencies who have implemented an open source project, the greatest challenges are:

- 34% security issues
- 30% concerns that proprietary applications won’t work/port to open source
- 27% lack of trust of open source vendors
- 25% lack of consistent established standards

For those agencies who have not implemented open source, the greatest challenges are:

- 42% Organization reluctance to change from status quo
- 40% Security
- 28% Lack of consistent standards
- 26% Lack of tech support
- 25% Lack of open source knowledge on site
- 20% Lack of senior management support

For those agencies who have implemented open source, the top benefits have been:

- 30% Ability to access advanced and multi-leveled security capabilities
- 17% Data center consolidation
- 17% Ability to customize applications
- 12% Ability to enable cross-system, cross-agency applications and process sharing
- 9% Cost savings from application and operating system software
5. THE CHALLENGES IN PERSPECTIVE

According to Anupriyal et al (2007), each open source project defines its own community, which is a 'community of interest' or a 'community of practice', in that it brings together people who are interested in the same domain and issues and share similar practices. Today’s undergraduate, constitute tomorrow’s manpower. Therefore, if we are to reap the benefits of the FOSS initiatives in Nigeria in the future, we must as a matter of urgency begin to sow the seeds today. The internet has dissolved virtually all limitations within academic communities, enhancing collaboration and creating the right atmosphere for FOSS projects to breed. The major challenge therefore is to find deal with other psycho-academic tendencies that can serve as delimiters to the evolution of the FOSS paradigm among Nigerian undergraduates include creating a development environments that will support collaboration among developers, dealing with the fears of failure, supporting new and potential contributors, and in bringing users and developers together.

Research Questions

Based on the foregoing, this paper wishes to provide answers to the following research questions that have emanated:

1) What are the levels of acceptance of the FOSS initiative among Nigerian undergraduates?
2) What are the perceptions of these undergraduates about the adoption of this method of software developments?

Research Hypotheses

The following null hypotheses were formulated for the purpose of this research:

Hypothesis I:- There is no perceived significant difference related to project success in their expectation of project completion time.

Hypothesis II:- There is no perceived significant difference related to project success among students resulting from being credibly supervised on Open-Source projects.

Hypothesis III:- There is no perceived significant difference related to project success based on access to internet facilities

Hypothesis IV:- There is no perceived significant difference related to project success based on the measurement of member contribution to the open-source software development process.

The survey method employed in this project is the use of questionnaire which solicits information from respondents.

Population

The population consists of 250 students stratified into 3 groups viz: diploma students, degree undergraduate and other certificate undergraduate students from five institutions in South Western Nigeria. 223 Questionnaires were returned out of which 200 were selected that satisfy the stratification for research purposes.

Sampling Technique

The sampling technique used in this research work is the stratified sampling method in combination with simple random sampling. The simple random sampling technique is a method employed in selecting a sample of considerate size from a given population of data used in the survey, we find the estimate from the population in simple random sampling, sample size got from the given population is one in which every response has the same probability of being chosen.

Research Instruments

The research instrument titled “Perceptions of the Proprietary and Open-Source Software Development Process Among Nigerian Undergraduates” on a three point Lickert Scale, was self-constructed and administered to evaluate the respondent’s perceptions. The research instrument was partly administered by the researchers and partly distributed to respondents through the Internet.

DATA PRESENTATION AND ANALYSIS

**Table 1: General Awareness of FOSS**

<table>
<thead>
<tr>
<th>RESPONSES</th>
<th>High Awareness</th>
<th>Aware</th>
<th>Not Aware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diploma Students</td>
<td>40</td>
<td>34</td>
<td>30</td>
</tr>
<tr>
<td>Degree Undergraduate Students</td>
<td>89</td>
<td>61</td>
<td>65</td>
</tr>
<tr>
<td>Others</td>
<td>36</td>
<td>20</td>
<td>25</td>
</tr>
<tr>
<td>Total</td>
<td>165</td>
<td>115</td>
<td>120</td>
</tr>
<tr>
<td>Average</td>
<td>82</td>
<td>58</td>
<td>60</td>
</tr>
</tbody>
</table>

**Table 2: General Acceptability of FOSS**

<table>
<thead>
<tr>
<th>RESPONSES</th>
<th>Highly Acceptable</th>
<th>Acceptable</th>
<th>Not Acceptable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diploma Students</td>
<td>20</td>
<td>42</td>
<td>30</td>
</tr>
<tr>
<td>Degree Undergraduate Students</td>
<td>99</td>
<td>73</td>
<td>65</td>
</tr>
<tr>
<td>Others</td>
<td>48</td>
<td>35</td>
<td>25</td>
</tr>
<tr>
<td>Total</td>
<td>168</td>
<td>150</td>
<td>110</td>
</tr>
<tr>
<td>Average</td>
<td>53.10</td>
<td>50</td>
<td>36.67</td>
</tr>
</tbody>
</table>
Table 3: Decision Based on Chi Square Analysis

<table>
<thead>
<tr>
<th>SNO</th>
<th>Hypothesis (HL)</th>
<th>Computed 'x' Value</th>
<th>Table Value at 3 df</th>
<th>Comparison</th>
<th>Decision at .05 level of Sig.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Hypothesis H1: There is no perceived significant difference related to project success in their expectation of project completion time.</td>
<td>6.635</td>
<td>9.21</td>
<td>$\chi^2 &lt; \chi^2_{0.05}$</td>
<td>Accept Null Hypothesis</td>
</tr>
<tr>
<td>2</td>
<td>Hypothesis H2: There is no perceived significant difference related to project success among students resulting from being credibly supervised on Open-Source projects.</td>
<td>5.59</td>
<td>9.21</td>
<td>$\chi^2 &gt; \chi^2_{0.05}$</td>
<td>Reject Null Hypothesis</td>
</tr>
<tr>
<td>3</td>
<td>Hypothesis H3: There is no perceived significant difference related to project success based on access to internet facilities.</td>
<td>15.26</td>
<td>9.21</td>
<td>$\chi^2 &gt; \chi^2_{0.05}$</td>
<td>Reject Null Hypothesis</td>
</tr>
<tr>
<td>4</td>
<td>Hypothesis H4: There is no perceived significant difference related to project success based on the measurement of number contributions to the open-source software development process.</td>
<td>3.11</td>
<td>9.21</td>
<td>$\chi^2 &gt; \chi^2_{0.05}$</td>
<td>Reject Null Hypothesis</td>
</tr>
</tbody>
</table>

6. FINDINGS

From Table 1 the computed average revealed a generally high awareness of the FOSS initiative among Nigerian undergraduates. Table II also showed a generally high acceptance of the FOSS initiative. Chi square analysis of research data at 0.05 level of significance revealed that there is no perceived significant difference among students in being credibly supervised on Open-Source projects. However, there is perceived significant difference in their perception of project completion time, access to internet facilities and measuring member contribution to the open-source software development process.

7. CONCLUDING REMARKS

Given the current enthusiasm and impetus for the FOSS initiative in Nigeria, one can predict that the benefits of this approach to software development will payoff in our nation in the very nearest future. Although there seem to be diverse set of challenges, better integration and presentation of information from the various tools in open source projects may address some of the limitations of open source software development. Furthermore, increased visibility of the social network within a project community and improved possibilities for social interaction between members of the community would ease a new developer’s initiation into the culture and the community of a project. The various agencies at the cutting edge of the open source initiatives in Nigeria and Africa at large must as a matter of urgency create more awareness about their activities specifically among Nigerian undergraduates and other allied institutions.

REFERENCES

A Proposed Cryptography-Based Identity Management Scheme for Enhancing Enterprise Information Systems Security

Adebimpe, L.A
Dept of Computer Science
Emmanuel Alayande College of Education, Oyo, Nigeria
drdeibimpela@yahoo.com

Longe, O.B (PhD)
Fulbright Fellow
International Centre for Information Technology & Development
Southern University System
Baton Rouge, Louisiana, USA.
longeolumide@fulbrightmail.org

Abstract.
Enterprises are faced with the challenges of managing users’ identity across multiple systems and applications. User identity usually includes personal information such as names, contact information, and demographic data; legal information which is the information about legal relationship between the enterprise and the user; and login credentials to managed systems for identification and authentication such as login ID and password, PKI certificate, tokens, biometrics, and so on. As a result of these challenges, enterprises contend with problems of data inconsistency, repetition of access to multiple systems, security exposure, unreliability of data, complexity in systems usage, and difficulty in managing large data. These problems are compounded as enterprises deploy more IT infrastructures (systems and applications) and have more users (employees, customers, partners, contractors, vendors, and so on). Our research is aimed at addressing these challenges by building on existing identity management technologies through the creation of a hybrid technology using Identity Management and Cryptographic techniques. We present the research direction in this paper.

Keywords: Enterprises, Identity Management, Identity Management Technology, Cryptography


1. INTRODUCTION

Identity management is the collection of business process and technology used to manage data on IT systems and applications about users. Managed data includes user objects, identity attributes, security entitlements and authentication factors.[1] The area of identity management also covers anonymising techniques and user profile storage.[2] Identity management is a source of worry for enterprises. Modern enterprises run a complex combination of IT infrastructure, which includes: Network operating systems; Application servers running web servers, databases and similar software; Mainframe and midrange servers; E-mail and other collaboration software; User directories publishing lists of users and other network objects; Human resources, payroll and contractor management systems; Customer relationship management (CRM) and enterprise resource planning (ERP) applications; and Electronic commerce applications.

Several kinds of users access these systems including Employees, Contractors, Partners, Vendors, and Customers. Every system and application tracks its own users, how they sign in and their privileges. Therefore, identity data such as Personal information, Legal information, and Login credentials to managed systems should be effectively managed by these systems. The diversity of these systems, each with their own security management user interface, administrators and change request processes creates complexity. This complexity impacts the IT operation, e.g. the same human user must be managed by different IT staff on different parts of the infrastructure. The complexity also impacts users, e.g. it can take a long time to make required changes and users are forced to memorize multiple login IDs, passwords and application sign-on processes. This complexity leads to high IT cost, lower user productivity and security exposures.
The remaining part of the paper is organized as follows. In the next section we review related work. This is followed by a section on research methodology. Next is the analysis of research data. We present the discussion of findings and conclude in the last section.

2. RELATED WORKS

Identity management (ID management) is a broad administrative area that deals with identifying individuals in a system (such as a country, a network, or an enterprise) and controlling their access to resources within that system by associating user rights and restrictions with the established identity. [3] Identity management describes the management of individual identities, their authentication, authorization, and privileges/permissions within or across system and enterprise boundaries with the goal of increasing security and productivity while decreasing cost, downtime, and repetitive tasks. [4] Identity management refers to the process of employing emerging technologies to manage information about the identity of users and control access to company resources. [5]

It is a term related to how humans are authenticated (identified) and authorized across computer networks. It covers issues such as how users are given an identity, the protection of that identity, and the technologies supporting that protection (e.g., network protocols, digital certificates, passwords, etc.). [4] The driver licensing system is a simple example of identity management: drivers are identified by their license numbers and user specifications (such as "can not drive after dark") are linked to the identifying number. In an IT network, identity management software is used to automate administrative tasks, such as resetting user passwords.

Enabling users to reset their own passwords can save significant money and resources, since a large percentage of help desk calls are password-related. Password synchronization (p-synch) enables a user to access resources across systems with a single password; a more advanced version called single sign-on enables synchronization across applications as well as systems. In an enterprise setting, identity management is used to increase security and productivity, while decreasing cost and redundant effort. Standards such as Extensible Name Service (XNS) are being developed to enable identity management both within the enterprise and beyond. [3]

The goal of identity management is to improve productivity and security while lowering costs associated with managing users and their identities, attributes, and credentials. [5] A key component of security plans is well-managed access to services that protect online resources and user privacy while enabling ease of use. Centralizing the management of user identity and related information not only reduces the staff required to manage appropriate access and monitoring, but also allows better service through automatic granting (or revoking) of services based on institutional roles. [6] Identity management system acts as the backbone for access control and security, and if it were to be compromised then the security of the entire company would also be compromised.

Therefore, it must encrypt stored confidential information such as social security numbers and passwords. It must also encrypt confidential information during transmission between components of the identity management infrastructure, which includes the network transmissions during synchronization, replication, and authentication. [5]

Respondents to 2003 EDUCAUSE survey ranked security and identity management as critical issues not only because of their strategic importance but also because of the high staff requirements in both the management and technical areas. [6] As contained in computerweekly site [7], Identity and access management (IAM) helps to make sure that IT users are who they say they are, and to ensure that authorisation policies are upheld. A growing range of tools are available, from two-factor authentication, to security tokens and biometrics. We analyse the trends to help you choose the identify and access management products that are right for your needs. Though the technology brings convenience, it also creates a dilemma. For instance Lapses in information security are a result of inefficiencies in current identity management processes. Due to the difficulty in managing user identities, the IT staff usually does not have enough time to correctly manage identities.

For example, users can be granted too much access because it is the easy thing to do. Because the IT staff does not have time to interpret how security policies affect each user, users can be granted access rights in violation of company security policies. Because the priority of the IT staff normally lies with new and existing, terminated users can easily be ignored. Consequently, departing employees find that they can still access company resources through their old accounts, other orphaned accounts, or undocumented access points. [5].
Significant challenges exist for an identity management.[5] Taylor, Lips and Organ (as cited in Wikipedia)[4] provided a glimpse into the issues in identity management, these include privacy issues or risk related to the stealing of identity (identity theft). Christopher Staitie [2] wrote a thesis on “Portable Secure Identity Management”. This paper focused on developing an identity maintenance and distribution system, and the storage of profile data on a centrally accessible, yet distributed system. [2] Also, Jason Crampton Hoon, Wei Lim Kenneth, and G. Paterson [8], in their paper titled “What Can Identity-Based Cryptography Offer to Web Services?”, focused on applying identity-based cryptography (IBC) to web services.

The key idea is to generate and use public keys based on publicly available information which can be used to uniquely identify users. [8]. Birgit Pfitzmann and Michael Waidner [9] published a paper titled “Federated Identity-Management Protocols—Where User Authentication Protocols May Go”, and this paper suggested and discussed Federated identity management as providing a simple user management in an increasingly dynamic world. The paper also discussed the functionalities of Federated identity management protocols. [9] A World Wide Web Consortium position paper, Requirements for a Global Identity Management Service, cited on unified communications site[3] maintains that establishing global identity management is crucial for the development of the Web and Web services. The W3C position paper stipulates, among other things, that such a system that must be universally portable and interoperable; that it must support unlimited identity-related attributes; that it must provide adequate mechanisms for privacy and accountability; and that it must be overseen by an independent governing authority.

3. STATEMENT OF THE PROBLEM

The major challenges faced by enterprises are managing user identities and entitlements across multiple systems and applications. These challenges are evident because enterprises run a complex collection of IT infrastructures such as Application Servers, Network Operating Systems, Mainframe and midrange servers, email software, user directories, human resources and payroll management systems, e-commerce applications, and so on. In addition, many kinds of users access these systems whose identity data must be effectively tracked and managed. Therefore problems may arise as a result of managing user identities and entitlements across these multiple systems and applications.

Such problems are high IT cost, data inconsistency, usability problem (because users access multiple systems, they may be presented with multiple login IDs, multiple passwords and multiple sign-on screens), low user productivity, redundant administration, and security exposures.

4. RESEARCH JUSTIFICATION

In order to eradicate these challenges of effectively managing of identity data across multiple systems, Enterprise Identity management technologies simplify the administration of this distributed, overlapping and sometimes contradictory data about users. In other words, as enterprises deploy an ever wider array of IT infrastructure, managing that infrastructure and in particular managing users, their identity profiles and their security privileges on those systems becomes easy with Enterprise Identity management. Thus, this research work aims to resolve the challenge of managing that infrastructure and in particular managing users, their identity profiles and their security privileges on those systems and applications by developing network directories (which are network services that manage information about users, the enterprise and IT assets such as servers and peripherals) using Lightweight Directory Access Protocol (LDAP) and Federation (which enables applications in different domains to share information about users).

In order to further enhance the security of users’ identity data, such data are converted into ciphertext (through encryption) during storage and then decrypted by authenticated and authorized users during retrieval using a key. Therefore, the successful completion of this research work will elicit a hybrid identity management technology called LFC (LDAP, Federation, and Cryptography) that will provide a secure, consistent, efficient, usable, reliable, and scalable identity management framework for enterprises to eradicate the challenges of managing user identities and entitlements across multiple systems and applications, as well as ensuring trusted information sharing mechanism among enterprises.

5. RESEARCH DIRECTION

The objectives of this research project are:

1. To develop a network directory to manage information about users, the enterprise and IT assets using lightweight directory access protocol (LDAP).
2. To apply cryptography in securing identity data during storage and retrieval.
3. To develop an authentication and authorization model that will allow applications in different domains (different
enterprises) to access and share identity data (information about users). In this model, an application in one enterprise will be authenticated only once and then granted access to information owned by several enterprises.

6. METHODOLOGY

In implementing the network directory, Lightweight Directory Access Protocol (LDAP), which is an identity management technology, will be used. LDAP also has an associated schema which can be used to build a data structure for the directory. Blowfish encryption algorithm will be used in encrypting and decrypting identity data. To construct authentication and authorization model, Federation will be used. Federation is an identity management technology that makes identities portable across domains so that they can be efficiently shared with and leveraged by trusted partners. It provides the mechanism whereby an enterprise can accept that external users have already been authenticated by a trusted partner and can grant them access — without having to be responsible for managing all their identity information. Within this framework, users enjoy seamless, secure access to partners’ services via a single sign-on (SSO) to multiple applications.

7. SCOPE

This research work focuses on integrating Lightweight Directory Access Protocol (LDAP) and Federation encryption management technologies with Cryptography to create a hybrid technology that will provide a high-level security of identity data and highly effective management of users’ identity data across multiple systems and applications within an enterprise, and also to ensure reliable sharing of users’ information among enterprises.

8. EXPECTED RESULTS

A lot of research work has been carried out in the area of enterprise identity management by developing network directories using LDAP, as well as using Federation to automate the process of sharing identity information across traditional organizational boundaries. Many research projects had been executed in the area of Identity-based cryptography. This research work is expected to contribute to knowledge by combining LDAP, Federation, and Cryptography (LFC) such that cryptography will be applied to encrypt identity information that is sent to the network directory through LDAP, as well as linking several enterprises together for the purpose of sharing identity information through Federation, while pulling data from the network directory. Thus, LDAP and Federation will be made to operate synchronously to provide a high-level identity management framework.

REFERENCES


d?doi=10.1.1.122.8297&rep=rep1&type=pdf

d?doi=10.1.1.4.4874&rep=rep1&type=pdf

ty/wp_id_federation_secure_collab.pdf