Functional Description of the EUU / EAA Tools

29.10.09, last rev 18.3.10

Rudolf Dimper, Dominique Porte, ESRF Grenoble
Olaf Schwarzkopf, HZB Berlin
Derek Feichtinger, Daniel Lauk, Heinz J Weyer, PSI Villigen

1. Introduction

The goal of this specification is to define common IT tools for the users of the European neutron and photon research facilities. These will provide them with new possibilities for easy access to the facilities.

Currently, there are more than 30'000 users performing experiments at the presently about two dozen existing European photon and neutron facilities. In most cases, these facilities are part of national research institutions. They perform research in a broad range of disciplines, like materials sciences, life sciences, physics, chemistry, environmental sciences, and studies in cultural heritage.

The normal sequence for an experiment begins with several scientists forming a collaboration and submitting a research proposal (formal document) to one facility or to several facilities. Each facility has proposal review committees, which at regular intervals select the best proposals and assign to them beamtime. If successful, the users then come to the facility (typically for a few days) and perform their experiment with the results published in standard scientific journals. For handling all the administration issues, each facility runs a user office consisting of several persons with a Web-based User Office (WUO) as the IT backbone. In Europe, these WUOs are based currently on two systems; DUO-type (PSI, HZB, DESY , SOLEIL , FRM II♣, MAX-lab♣) and SMIS-type (ESRF , DIAMOND, ANKA). An essential part of each system is the user database. Currently, there is no connection between the various databases of the different facilities and users have to register individually to each facility with all the administrative overhead this entails.

Two FP7 roadmap projects (ESRFUP, IRUVX) contain initiatives for a common EU-wide service to their users. The two projects joined efforts at an early stage in order to avoid two similar but separate systems, catering for almost the same user community, from being developed. It has been decided to implement a prototype system as a proof of concept for the specifications contained in this document.

The guiding principle is that users enter a common web portal before being directed to the appropriate facility. It has, however, to be taken into account, that the facilities concerned are collaborators but at the same time competitors being, with few exceptions, financed by their national authorities. This political aspect puts significant constraints on the conceptual design of the common portal.

Independent of the details of the implementation, the basis of any common solution is a EU-wide federated user database containing just enough information to be able to define a *user* in a unique way. Any further information is optional and can be kept at the local facilities.

As mentioned before, all European facilities providing beamtime to external users have existing digital user office systems in operation. All WUO realizations have invested considerable effort to cater for the local environment (e.g. security and accommodation aspects). These investments must be preserved, and a pan-European authentication approach has to be designed in such a way that it can be interfaced easily to these local digital user office systems.

♣ development

As will be shown below, the new system will be advantageous to all the different players:

The *users* will have novel opportunities to maintain their user accounts simultaneously at all European facilities. For them, it will be much easier to manage their experiments at these facilities. The basic preparatory steps are being made for future remote access to beamlines and data at any of these facilities.

The *facility staff* will profit from the fact that users can maintain their information themselves and that in this way the information will be more accurate and up to date. In addition, for the first time it will be possible to minimize doublet user registrations –a persistent problem with present WUO systems.

In respect to the whole *community,* the system will foster the 'community identity'. The system will be able to provide active PR – if the user has registered for that. In addition, it will be easy to extend the system to provide information to the science public and public relation sectors.

2. Definition of Services

Scientific users of the European photon and neutron facilities firstly determine the best experimental method or methods to solve their research problem and secondly, which of the possible facilities offer the best possibilities to carry out the experiments. Sometimes, scientific investigations for a single project are pursued with experiments at several facilities. This means that a user cannot be related to a single facility only and that a cross-facility solution is required from the beginning.

2.1. Unified User Umbrella / EuroFEL User Umbrella

The name of the final tool (*U^3, Unified User Umbrella)* should indicate that this is a service for the whole community, with a common approach to common requests at the facilities. It is a pan-European tool, which - by the hybrid central / local character of the solution – will keep existing local solutions as much as possible.
The step would, however, be too large to set up such a tool right from scratch. Therefore, within Work Package 2 of the EuroFEL FP7 Roadmap project a first version is being set up (*EUU, EuroFEL User Umbrella*) for the members of the EuroFEL consortium. As soon as experience is available and as there is interest, feedback will be incorporated and the tool can be expanded to serve the full community.

2.1.1. Proposal Handling

The most obvious interaction of a user with the facility management is in connection with an experiment characterized by the various phases of a proposal.

- It will foster the often-missed 'corporate identity' feeling of the community if a proposer is able to enter one and one-only website for submitting a proposal to any of the facilities. After that, the user can be forwarded to the specific facility of his choice.
- Experiments are typically performed in an iterative way, where the largest part of the experiment stays the same and only one or few parameters are modified or another facility is selected. Here, it would be a big help for a proposer, if he/she could export an old proposal and submit an updated version. A standard style for the scientific part

(selection and sequence of topics) would be of big help. Because of the confidential character of the proposal information, data protection issues are very important.

2.1.2. Future Developments

There are many more user issues as e.g. remote file access (data catalogs and data themselves), and remote access to analysis tools at facilities. These are very important but they are so complex that they can be addressed only in a succeeding step. Nevertheless, the design of the present system has to foresee future extensions as much as possible.

2.2. EAA, European Authentication and Authorization

A prerequisite for the services of EUU is an EU-wide authentication and authorization concept. The context, in which the system will be used, implies several boundary conditions:

2.2.1. Access to User Information

User information will be kept as much as possible, where it is in the present WUO systems, i.e. with the local facilities. Only that part will be centralized which is necessary for unique user identification. It will not be possible for one facility to access information on a user registered at another facility. Storage of personal information is under the control of the user him/herself.

2.2.2. Authentication vs. Authorization

There will be no central storage of authorization information about a user. Facility-related information will remain fully under the control of the respective facility.

2.2.3. Multi-Level Authentication

There is a broad spectrum of usage of the services. For example, a user may want to register for a workshop or a users meeting. For that, no special security control is required and the administrative threshold should be as low as possible. A *soft* Google-type registration with an email handshake is sufficient. On the other hand, if a user is requesting a badge at a facility, which will allow him/her to access a restricted site, the management has to be sure about the identity of a user. This can be solved in such a way, that a user with a valid soft registration shows an official identification document at a facility user office and the user officer marks the successful user in the database (*hard registration*). There are different security requirements at the local facilities for different services, which must be obeyed. For some facilities, it will be sufficient to require a user to perform a once-only hard registration, other facilities may require a hard registration with each visit for specific services.

2.2.4. User Friendliness

The user friendliness of the system will determine its success. E.g., mobility is high among the users and when they move from one affiliation to another one, it will be highly appreciated if they have to enter their new coordinate only at one site.

2.2.5. Facility Friendliness

Operational resources for running user offices at the individual facilities are very much limited and it will be important to delegate account maintenance obligations as much as possible to the users. An issue will be double registrations of users, which the tool must be able to identify and to correct – at least manually.

2.2.6. Compatibility with Existing and Future WUO Authentication Tools

For several reasons, the EAA will have to coexist with the authentication mechanisms of the existing WUO tools. In addition, new WUO systems are under development. Therefore, clear interface definitions have to be developed for the communication between the EAA and these tools.

2.3. EAA Databases

2.3.1. Central and Local User Databases

At present, due to confidentiality issues, a consensus cannot be reached among the participating facilities to centralize all user information. In addition, the new system will have to coexist with the current systems at the local facilities for a long time. The approach, therefore, consist in splitting the user information into a central part, which contains the information necessary for a unique authentication of a user (non-strategic information), and a local part at the respective facility with the rest of the information and the authorization information.

2.3.2. Central Affiliation Database

With very few exceptions, users of the facilities are linked to affiliations. Usually, the affiliation names are complex names without generally accepted definition rules. The only solution is to define the rules (e.g. language, definition depth) within EAA. The user browses within the list of defined affiliations. If the respective entry is not found the user sends a request to the database manager, who then enters the new item. In additional to a real entry, alias definitions can be added.

3. Functional Description and Use Cases

3.1. EAA, European Authentication and Authorization

3.1.1. New User Registration (Soft)

Personal information: The user goes to the EAA website and asks for a new account. He enters the few personal information items requested. These have to be agreed upon by the participating facilities in order to define a minimum number of items for unique identification of the user. The username must be unique. If the user proposes a name already in use, EAA will propose automatically another one. The email address is verified by a standard handshake mechanism.

Linked facility: After having entered the personal information, the user is asked for a facility link. After selecting a facility from the list, the user is then forwarded to the

linked facility where further local items can be entered (guesthouse, registration for calls for beamtime etc).

3.1.2. User Registration (Soft) at an Additional Facility

A user may have more than one linked facility. For defining additional linked facilities, the user logs on to the EAA and selects the ***Add Further Linked Facilities*** button.

3.1.3. Hard Registration of a User

Certain functions at a facility require the identity of the user to be verified in person. For that, the user has to go at least once in his life to a user office at a facility and to show to the officer a legal document (ID card). The officer verifies official entries such as name, first name, gender, and birthday and confirms this official act by setting the *hard registration* flag for the respective entry in the user database. In addition, because of possible legal consequences, this is documented in writing and archived at the facility. Once a user has passed hard registration, he/she will be allowed access to safety-critical elements at the facilities. The details are defined by each facility separately. It has also to be agreed upon where the hard-registration flag is stored. In case it is done centrally, facilities could make mutual use of this information.

3.1.4. User Information Maintenance (User, User Office)

The maintenance of his/her personal information (change of affiliation, phone number etc) is performed by the user him/herself by logging on to the EAA portal. In this way, updates are performed only centrally and the system takes care of automatically distributing the modifications to the local databases of the participating facilities. This update option has to be agreed upon actively by the user (once only).

3.1.5. Authorization Aspects

The central database contains no authorization information with the only possible exception of hard-registration information (yes/no and if yes, by which facility). In this way, if a user is marked in the central database as hard-registered by a facility, other facilities can decide if this user is sufficiently trustable and is allowed to access to safety-relevant local facility components.

3.1.6. Authorization within Local WUO

With the exception of the multilevel-registration concept, the security handling is the same as that at the existing WUO's. Security-relevant information (e.g. access to specific areas at a facility, management functions at a facility) for a user is stored at and linked with the corresponding entry in the local user database.

3.1.7. Handshake between EAA and Local WUOs

Shibboleth: There exist various professional authentication systems, that could be used to provide the handshake between the EAA and the local WUOs so that there is no need for developing something from scratch. It has been decided to go ahead with Shibboleth.
Single Sign On (SSO): The cooperation of the umbrella (see below) is performed in such a way that a user logs on at the central site and after few steps is forwarded to the local

facility of his choice. Apart from certain exceptions, as defined by the local facilities, there is no further need for authentication.

Push-only operation: When a user is forwarded from the EUU site to the WUO, he/she carries the necessary certificate for the operations to perform. There is no way for local facilities to interrogate user information from the central database.

Unique username: The system needs an EU-wide unique username. This can in part be ensured during the new-user registration process. Because of the hybrid local/central character, nevertheless, problem cases may occur, which cannot be taken care of completely in an automatic way and resources for a certain amount of manual checking has to be foreseen.

3.2. EUU, EuroFEL User Umbrella

3.2.1. Function of the Umbrella

Once an *EAA (European Authentication and Authorization)* scheme is established, a multitude of services can be offered by the *UUU (Unified User Umbrella)* to the community, ranging from access to experimental and published data stored at remote facilities and proposal handling to PR and science-political issues. The *EUU (EuroFEL User Umbrella)* as the first version concentrates on proposal-related issues.
Proposals consist of two parts, a *general* part, which focuses on the scientific aspects of the proposed experiment and is largely facility-independent and a *local* part, which describes the facility-specific aspects.
For the foreseeable future, there will be a coexistence of UUU and non-UUU proposals and the workflows of UUU and local WUOs have to be designed such that they are able to handle both options. The duty of the EUU is, therefore, to optimize/harmonize the generation of the *general* part and to forward the proposer to the respective local facility for entering the *local* part of the proposal (umbrella concept).

3.2.2. Standard for the General Part

As part of the EUU, a template will be defined, which specifies the various items (e.g. topics, sequence, length) for the *general* part. For the – predominantly – iterative-type experiments this will allow users to prepare a new proposal based on a previous proposal in an efficient way.

3.2.3. Proposal Submission

A user registered at the EUU is allowed to submit a proposal for an experiment at any of the participating facilities. For that, he/she logs on at the EUU and selects from a menu the facility of choice. He/she enters the *general* part and after that the *local* part of the proposal. After that, the standard proposal handling at the facility continues. The proposal is stored within the local WUO with read access only to the proposers and the management of the local facility.

3.2.4. Proposal Export

Proposal information is confidential. Access is allowed only to the proposer and the co-proposers specified in the document and to the management of the respective facility. Proposers have the right to access their own proposal, e.g. as basis for submitting a follow-on proposal. EUU in handshake with the local WUOs will provide the corresponding export mechanism.

3.2.5. Proposal resubmission

Quite often users resubmit a modified version of a proposal to the original or another facility. For that, they can access the old proposal, modify it and submit it to the facility. Two options are possible, which have still to be decided upon:

(a) *Manual:* the user logs on the facility where the proposal is stored and generates a copy. Then, if the proposal is to be submitted to another facility, he/she logs on that facility, which because of SSO does not need any identification. After

performing the modifications based on the copy generated, the proposal is submitted.

(b) *EUU*-supported: the user logs on the ‘old’ facility, fetches the ‘old’ proposal and selects the ‘new’ facility. After that, the EUU transfers the user to the new facility and submission proceeds as usual.

In any case, a user can access an ‘old’ proposal only if he/she is author or co-author.

3.2.6. Coaching for novice users

Increasingly, users are coming to the facilities with no or very low experience in working in such an environment. For that, a coaching service is offered, which should help them to pass the first threshold barriers. This will require experienced coaches, which will have to be ‘protected’ against excessive load. These coaches are appointed in the first phase by EuroFEL, later by a more general community body (e.g. common ELISA/NMI3). They work on a peer basis, like referees.

A user enters the respective page of the EUU website. A list of FAQ is provided, which may already solve some of the issues. In case of further need the user can fill a LoI (Letter of Intent). For that, he/she is provided a template with specific questions concerning e.g. science field, sample information, detection technique. The Umbrella Manager directs this LoI to one of the coaches and the coach comments on the LoI, in general electronically. Personal contact to the applicant is up to the decision of the coach.

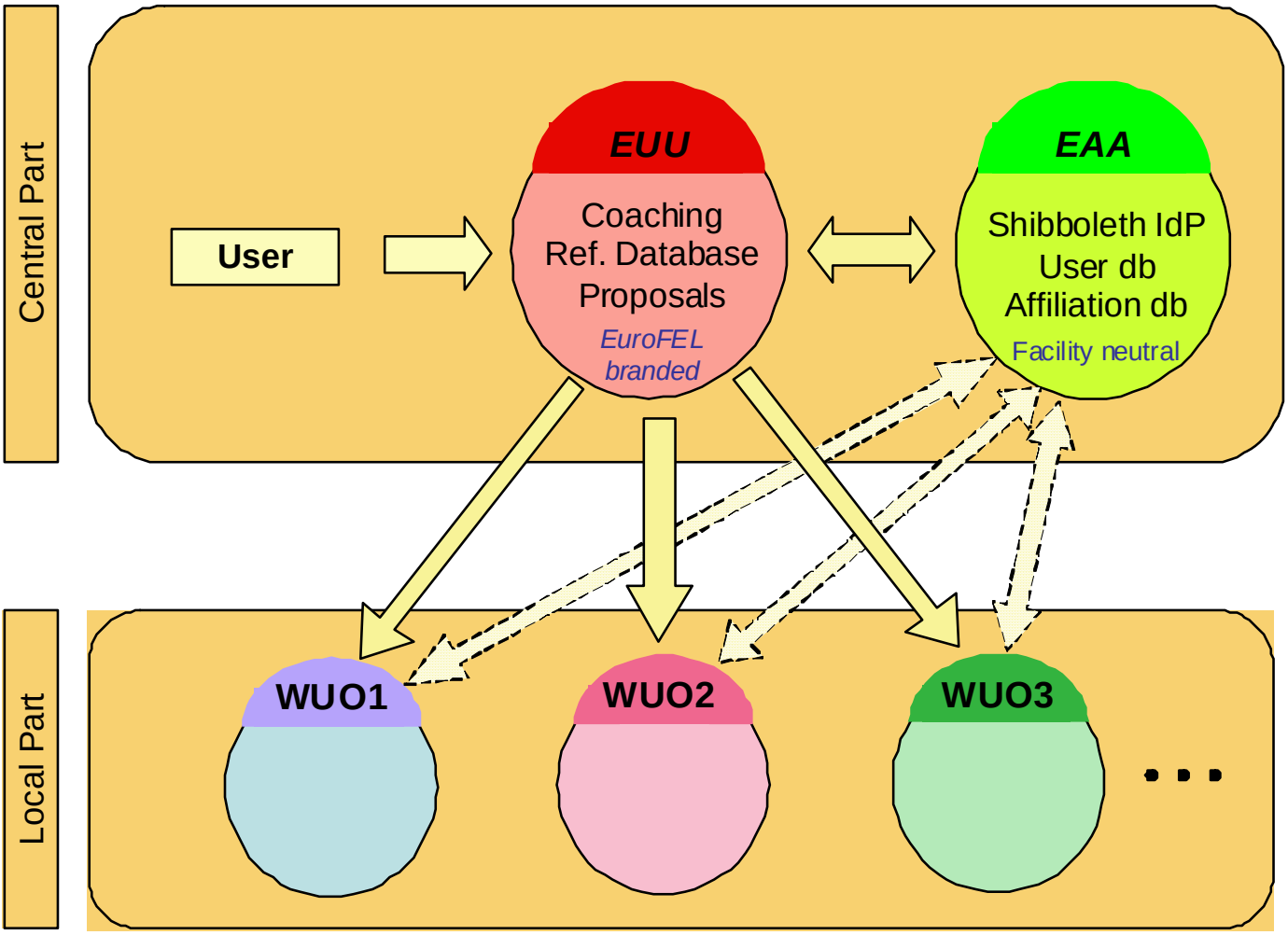
There may be a second iteration, e.g. with a formal check of a proposal by the user. In any case, however, the full responsibility for the final proposal is with the user.

3.2.7. Referee database

A list of referees will be entered in the EUU database. This list will be operated by the Umbrella Manager and visible to the co-referees, the management at the local facilities and during the EUU prototype phase the EuroFEL management, later to a more general community body (e.g. common ELISA/NMI3). Data included are name, affiliation (link to user DB), email and phone info, fields of expertise and list of facilities, where he/she is referee. The personal information is under the control of the referee. In part, local WUOs already have such lists. The goal is to synchronize this information via the EUU.

3.2.8. Access to Services at a Local WUO

In the first version, central user services will concentrate on proposal-related issues. For further services, users are forwarded to the local facility WUO’s.


Central Part
User
EUU
Coaching
Ref. Database
Proposals
EuroFEL
branded
EAA
Shibboleth IdP
User db
Affiliation db
Facility neutral
Local Part
WUO1
WUO2
WUO3

4. Specification Summary

4.1. EAA, European Authentication and Authorization

1. Central for service, federated for info
2. Only non-strategic info is stored centrally, strategic info is stored at the local WUOs
3. Info update by the user
4. Parallel EAA and WUO operation
5. Push only
6. Multi-level authentication (soft, hard)
7. Update of non-strategic info by user, strategic by local User Office
8. Unique user name, affiliation-independent

4.2. EUU, EuroFEL User Umbrella

1. Web based, central portal
2. Submission to local WUO, export option
3. Resubmission possibility
4. Parallel EUU and WUO operation
5. Harmonized scientific part (template)

4.3. Coaching

1. Support for novice users
2. Well-defined procedure, limited number (2) of iterations
3. No direct communication user to coach

4.4. Referee table

1. Central list of referees
2. Information to participating facilities only
3. Read access for participating facilities only

5. Road map

(As no personnel are hired yet the deadlines are provisional and may have to be revisited as soon as the personnel situation is fixed)

Topic	Title	Deadline	Description	
1.	**Management**			
1.1	Spec document	12.02.10	Specification document ready	
1.2	Select Friendly WUO's (FWUOs)	1.03.10	Select WUO sites which collaborate in testing the new products (ESRF, HZB, MAX-lab…)	
2.	**EAA, Authentication**			
2.1	Protocol, Interface	15.03.10	Select basic protocol (e.g. Shibboleth, OpenID)	
2.2	Database	15.03.10	Select database type (Oracle, MySQL)	
2.3	Specification	1.04.10	Detailed specification	
2.4	Interface to WUO's	15.04.10	Definition of interface bw. Central and WUOs	
2.5	Central spec.	1.05.10	Specification of central part	
2.6	Central code	1.06.10	Coding of central part	
2.7	WUO spec	1.07.10	Specification of WUO part, incl.EAA-WUO parallel concept	
2.8	WUO code	15.07.10	Coding of WUO part	
2.9	Tests	15.08.10	Test of EAA with EAA and WUOs	
2.20	EuroFEL intranet with EAA	15.09.10	Specification and test of EuroFEL intranet as non-WUO application (optional). This depends in part on the progress of the EuroFEL website.	
3	**EUU, User Umbrella**			
	Specification		Detailed specification	
3.1	Interface EUU to Portal EAA	1.10.10	Definition	
3.2	Interface EUU to WUO's	1.10.10	Definition	
3.3	Soft registration			
3.3.1	Portal	1.11.10	Coding of portal part	
3.3.2	Communication to WUO	15.11.10	Communication part	

	WUO	15.12.10	Coding of WUO part	
	Export	15.01.11	Export function	
	Field tests with FWUOs	31.01.11	Field test with all functions	
4.	**Coaching**			
	Procedure	31.2.10	Define procedure	
4.1	Coding	15.3.10		
4.2	Set up structure	15.4.10		
	Field test	15.5.10		
5.	**Referee database**			
	Detailed specification	1.7.10		
5.1	Programming	15.8.10		
5.2	Set up structure	1.9.10		
	Field test	1.10.10		
6.	**Final Complete Prototype**			
6.1	Tests	15.02.11		
6.2	Publication	1.04.11		

6. Glossary

1	Authentication	Who am I; the goal of the EUU is to identify a person uniquely Europe-wide.
2	Authorization	Which roles (i.e. rights) do I have (e.g. facility access, computer resources), what is my function.
3	Central Affiliation Database	The proposed database, which contains the address information (e.g. postal address) in a standardized format.
4	Coaching	Structured support of novice facility users by peer coaches, managed by the EUU / UUU.
5	EAA	*European Authentication and Authorization*, service, which uniquely identifies a user within the European Neutron and Photon user community. *Authentication* is via a central portal (Umbrella), *authorization* is performed by the local WUOs. In order to minimize the administration overhead *authentication* is realized as *multi-level authentication*.
6	ESRFUP	*ESRF upgrade program*, one of the projects of the FP7 roadmap program.
7	EUU	*EuroFEL User Umbrella*, prototype for the UUU for the members of the EuroFEL consortium; project within WP2 of the IRUVX-PP EU Roadmap program.
8	IRUVX-PP	*EuroFEL Consortium Preparatory Phase*, one of the projects of the FP7 roadmap program.
9	Multi-Level Authentication	In order to minimize the administration overhead for users and management, *authentication* is realized as *multi-level authentication*. *Soft authentication* is sufficient for services like registration for news, conference services, *hard registration* e.g. for access to facility sites, beamline components. The details for a specific site are defined by the local management.
10	Soft Authentication	Standard forum-type identification, e.g. via email handshake.
11	Hard Authentication	In-person identification of a user, e.g. via a legal document at a local user office.
12	Push-Only Operation	The EAA system will be set up in such a way, that the central portal, triggered by a user, can push information to a local WUO. Pulling of central information by a local WUO is not allowed.
13	Shibboleth	Federated open-software authentication system, basis of the handshake between the central portal and the local WUOs.
14	Single Sign On	A user, who has once been authenticated by logging on at the central portal, has access to the services he/she is authorized to without need for additional authentications.

15	UUU, Triple-U	*Unified User Umbrella*, final tool for EU-wide services for the neutron and photon community, including common portal for proposal handling, coaching, authentication services.
16	WUO	*Web-based User Office*, the application that supports a local user office in managing user-related issues (e.g. proposal handling, on-site user issues).