Project # 643735
www.do-change.eu

The Identity and Permissions Management Framework Design

[Deliverable 4.10 (D61), Revision 1.0]

Key Information from the DoA	
Due Date	30-Nov-2016
Type	Report
Security	Public

Description:

This document presents the identity and permissions framework that is to be employed in the phase 2 Do CHANGE clinical field trials.

Lead Editor: Robert Smith (DOC)	**Internal Reviewer:** Idowu Ayoola (OMNI)

Versioning and contribution history

Version	Date	Author	Partner	Description
0.1	01-Nov 2016	RS	DOC	Initial document skeleton setup.
0.2	21-Nov-2016	RS	DOC	Completed the body of the document ready for review.
0.3	22-Nov-2016	RS	DOC	Updated following preliminary review: • added missing information; • corrected typos.
0.4	23-Nov 2016	MW	TU/e	Reviewer's updates.
0.5	24-Nov 2016	IA	OMNI	Reviewer's updates.
0.6	24-Nov 2016	RS	DOC	Final correction of minor types and formatting issues and added missing details to the "Deliverable context" table.
1.0	25-Nov 2016	AB	SmH	Official release

Statement of originality:

This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

Executive Summary

This document presents the identity and permissions framework to be employed within the Do CHANGE ecosystem. It builds on the relevant models presented in the Do CHANGE architecture document (Ref. [A]), identifying how these are to be used in the distributed ecosystem to facilitate patient controlled access to information.

This document taken in combination with other Do CHANGE design documents defines the ecosystem architecture that will be implemented for use in the 2nd phase of Do CHANGE clinical field trials.

Table of Contents

Abbreviations

HTTP	Hypertext transport protocol
JWT	JSON WebToken

References

Unless otherwise stated, please refer to the latest version of the document specified.

[A] eSMART deliverable D4.9 (D60) Overall Do CHANGE Ecosystem Infrastructure Architecture

[B] RFC 2616 (Hypertext Transfer Protocol -- HTTP/1.1) and associated RFCs that obsolete this version and or updated it as specified at URL - https://tools.ietf.org/html/rfc2616

[C] RFC 6749 (The OAuth 2.0 Authorization Framework) - https://tools.ietf.org/html/rfc6749

[D] RFC 7797 (JSON Web Token (JWT)) - https://tools.ietf.org/html/rfc7519

[E] Section 4.1 of RFC 6749 - https://tools.ietf.org/html/rfc6749#section-4.1

1. About This Document

DoCHANGE aims to develop and provide a health infrastructure for integrated disease management of citizens with high blood pressure, patients with ischemic heart disease or patients with heart failure. In this context, the ecosystem aims to give patients access to a range of personalized health services intended to encourage behaviour change and to allow their behaviour and clinical parameters to be monitored. This is to be based on information collected from patients being shared amongst the health services in a manner that reflects the patient's wishes and aims to optimise their health and well-being. This document presents the design for the identity and permissions management framework to be employed for information exchange within Do CHANGE project ecosystem.

1.1. Deliverable context

Project item	Relationship
Objectives	This document is linked to the following WP4 objectives: To Specify and develop the overall Do CHANGE Ecosystem Architecture, both the services & component infrastructure, the data infostructure and its semantics. • The Data collection, storage, management and communication will take place in a secure patient controlled environment and feedback on transactions will be fed back to the individual. • All incoming data will be semantically tagged such that background knowledge, context and precise meaning are stored with the data and will inform any use of the data and its analytics. To define the end2end trust assurance including pseudonymity and policies. Within 8 months the security, infra- and infostructure is configured and adapted to the specific needs of the Do CHANGE health ecosystem applications and analytics.
Exploitable results	This part of the project is service design. It is anticipated that the services developed from this design would be further developed to commercially exploitable systems.
Work plan	This deliverable is associated with Task 4.2 in Work Package 4.
Milestones	This deliverable is not linked to an overall project milestone but does mark the submission of D4.10 (D61).
Deliverables	This document presents the identity and permissions framework that is to be employed in the phase 2 Do CHANGE field trials.
Risks	By having this document available, the risk of not being able to share patient information in the way intended during within the Do CHANGE phase 2 clinical trials, should be reduced.

2. Framework Design

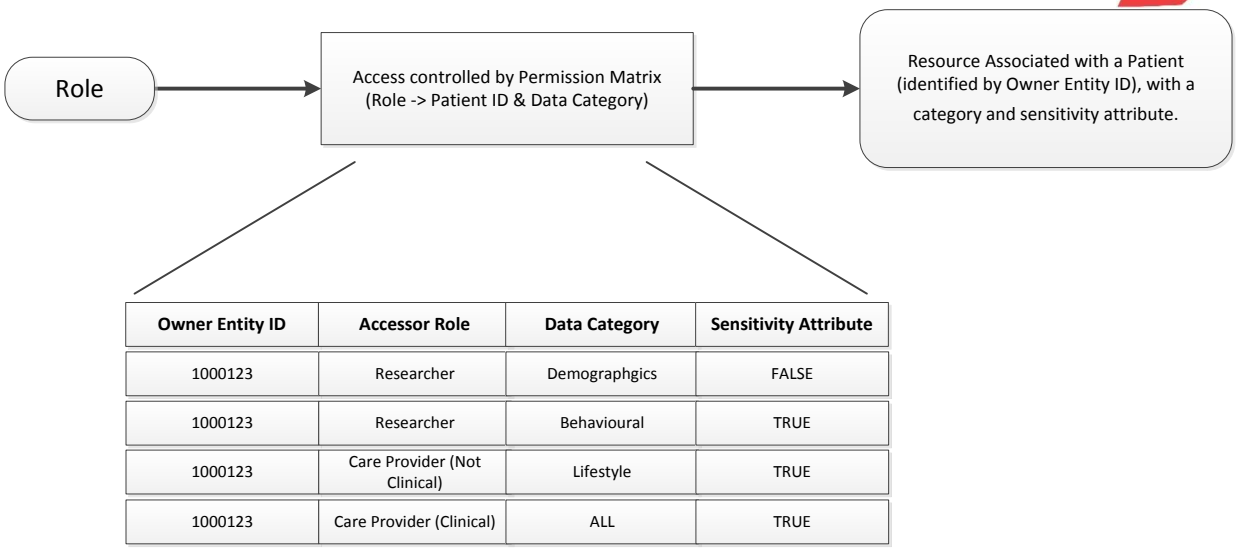
2.1. Distributed Guardian Approach

In Section 4.2 of the Do CHANGE architecture document (Ref. [A]), the concept of a Data Controller is introduced as an entity that has responsibility for determining how personal data (held on behalf of say a patient) is processed. Within the context of the Do CHANGE architecture, the Data Controller is associated with the service provider that is the primary host for the personal data in question, that is, each service acts as a guardian for the personal data that is hosts. Hence, a key aspect of the identity and permissions framework used within DO CHANGE is a distributed guardian approach, where the service that is associated with the data controller role (the guardian of the data) determines access to that date both within the scope of its isolated operation and operation within the Do CHANGE ecosystem.

2.2. Permissions Representation

To provide coordination between each service within the Do CHANGE ecosystem, conceptionally[1], each shall support the common trust and permissions model specified in Section 4.5 of the Do CHANGE architecture document (Ref. [A]). In this context, the user shall be able to exhibit different levels of granularity in terms of controlling access to their information. At a highest level, they may wish only to control access by role (see Section 4.5.1 of Ref. [A]). To facilitate such access control, each service shall effectively maintain for each patient, details of the access permitted by role for different categories of information; this is summarised in Figure 1. In this example, a Researcher may access non-sensitive demographics (e.g. age, gender, social group, ethnicity, general location) and all behavioural data, a non-clinical carer may only access lifestyle data, while a clinical care provider may access all data.

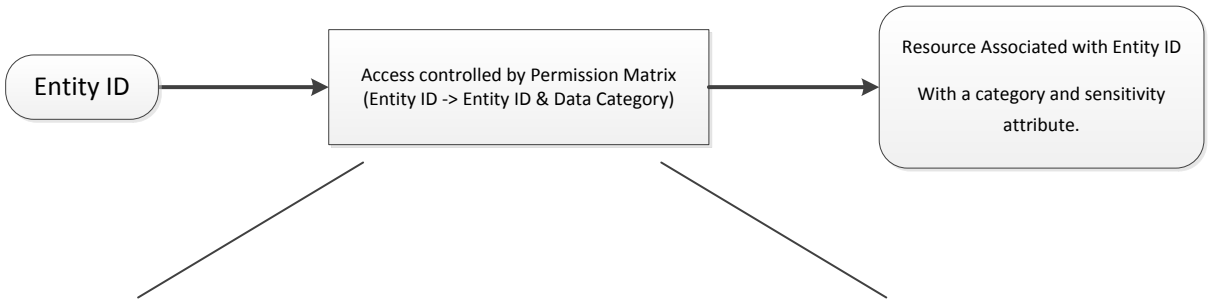
[1] The way that a service supports the common trust and permissions model is an implementation decision. At one extreme, a service dealing with a wide range of data and stakeholder types may implement it fully. In another extreme, a service dealing with a narrow range of data types and stakeholders / relationships between stakeholders may effectively implement it because of these constraints. The key thing is that they effectively implement the model and support communication of its associated data categories, roles and data access types on external interfaces.



Owner Entity ID	Accessor Role	Data Category	Sensitivity Attribute
1000123	Researcher	Demographgics	FALSE
1000123	Researcher	Behavioural	TRUE
1000123	Care Provider (Not Clinical)	Lifestyle	TRUE
1000123	Care Provider (Clinical)	ALL	TRUE

Figure 1 Role based permission matrix

To facilitate finer grained access control, conceptionally[2], each service may optionally and in accordance with its scope support an entity based permissions matrix as indicated in Figure 2, where in accordance Section 4.4 of the architecture document (Ref. [A])), an entity may be an individual person, an organisation or a service. Hence, this controls that access that specific entities in the Organisational Structure Model are permitted to have to a patient's resources.



Owner Entity ID	Accessor Entity ID	Data Category	Sensitivity Attribute
1000123	a@b.c	Demographgics	FALSE
1000123	a@b.c	Clinical	TRUE
1000123	a@b.c	Lifestyle	TRUE
1000123	1000392	ALL	TRUE

Figure 2 Entity based permission matrix

2.3. Distributed Resource Access Management

To facilitate the control of access by one entity to resources that are associated with another entity, it is necessary to have a mechanism for managing the identity of the entities. In general, each service may have its own, localised identity provider functionality to manage professional users and patients. To allow coordination between services, support for federated identity management is required.

[2] See footnote 1 for an explanation of the phrase "conceptionally" in this context.

Hence, within the Do CHANGE ecosystem, multiple identity providers may be present. For service-to-service interactions, hypertext transport protocol (http – see Ref. [B]) communications based on OAth2 (Ref. [C]) are to be employed. For this purpose, identity providers federated within the Do CHANGE ecosystem shall authorise access to resources associated with one entity by another entity using JSON Web Token (JWT – see Ref. [D]). In its simplest form this will control the access that one service has to the functionality provided by another service, with this achieved as follows:

a) The provider service and consumer service are registered with the federated Resource Access Manager.

b) Through the federated Resource Access Manager, the provider grants the consumer access to an API associated with specific functionality. This results in the issue of JWT access tokens to the consumer. These tokens consist of a primary, time-limited token for access and second token for refreshing access once the first expires.

c) When the consumer wishes to access the resource made available by the provider, the consumer employs the access token to allow its authorisation to access a resource via an API to be verified, with the http interactions with the provider's API conveying the tokens. If required, the consumer refreshes its primary tokens.

The entities may be specified by plain text or pseudonymised identifiers as explained in Section 4.4 of the Do CHANGE architecture document (Ref. [A]).

Regarding the access tokens (JWT), the payload shall include the following claims:

iss – the identity of the issuer, which should be the plain text identity of the identity provider.

aud: – the identity of the entity associated with the resource being accessed, which may be plain text or pseudonymised.

sub – the identity of the resource being accessed, which may be plain text or pseudonymised.

exp – the expiry date of the token.

Scopes – list of data categories, with for each whether access to sensitive information is granted and the access type, each specified in the following format:

Category#S#access-type

Where:

category is a Do CHANGE data category as specified in Section 4.5.2 of the Do CHANGE architecture document (Ref. [A]);

S is present if access to sensitive data of that category is permitted, otherwise no character is present.

access-type is a Do CHANGE data access type as specified in Section 4.5.3 of the Do CHANGE architecture document (Ref. [A]).

Some example are as follows:

Demographics#S#View – permission to view demographic data including sensitive items.

Clinical##View – permission to view non-sensitive clinical items.

ALL##Full – permission for full access to all data non-sensitive data.

ALL#S#Full – permission for full access to all data including sensitive data.

As indicated in Figure 3, the federated Resource Access Manager, which manages the issue of tokens may be implemented by the service provider or may be a common provider shared between services. The latter is intended to be used where the level of control required is limited to service and / or organisational entries, while the former is envisaged for control down to the level of individual care professional and patients.

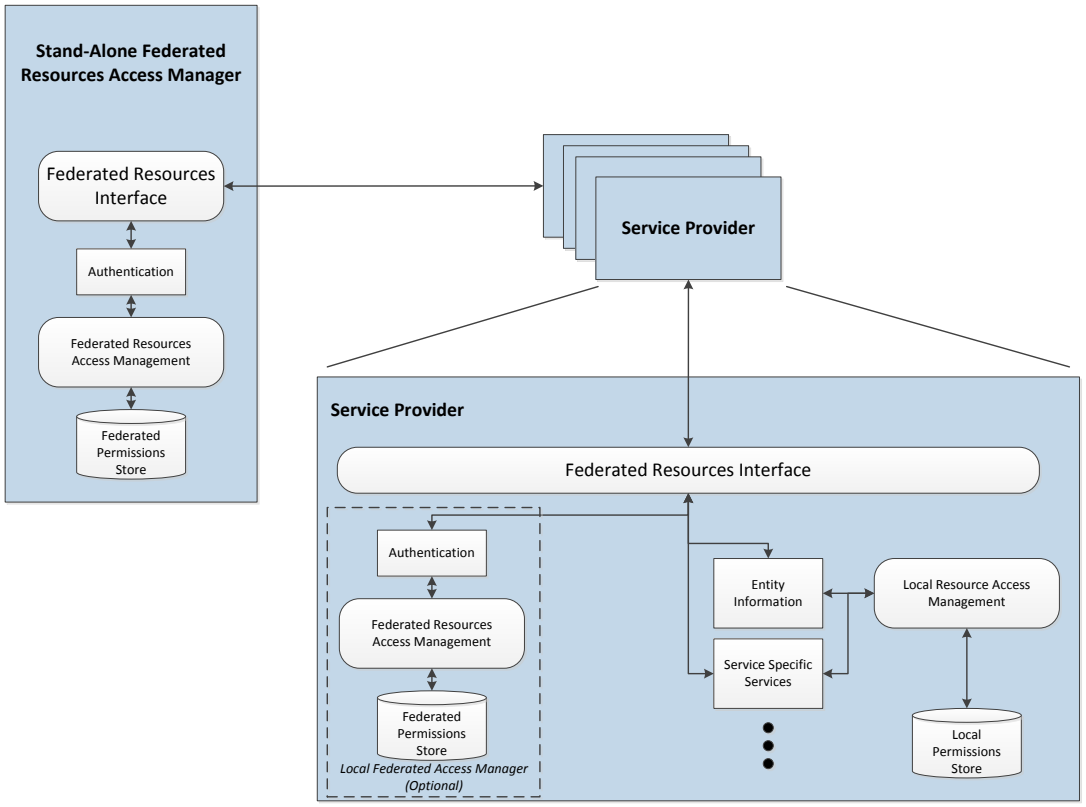


Figure 3 Service-to-service access

2.4. Facilitating Access Control by the Patient

To allow the patient to have control over the access made to their information, the federated Resource Access Managers described in Section 2.3 shall provided a web -browser based mechanism to enabled management by the patient. To facilitate this, the Autherisation Grant Code technique specified in Section 4.1 of RFC 6749 shall be employed (see Ref. [E]). For this purpose, the consumer shall direct new or updated autherisation requests to the Resource Access Manager during an appropriate patient interaction with the consumer's patient portal. The patient will be required to authenticate and then approve the access requested, afterwhich they will be redirected back to the consumer's patient portal.

In some cases it may not appropriate or practical for the patient to use such an interface to manage access to their information. This may be because they do not feel competent to use such and interface, or do not have the physical or mental capability to do so. In such situations, this action will be carried out by a competent and trusted advocate such as a partner, other family member or a trusted carer provider. Hence, the Resource Access Manager shall support the concept of a entity that is an advocate for a patient and therfore is able to manage access to information on the patient's behalf.

Furhermore, a paper-based consent mechanism may be employed in which the service provider or care provider transcribes the patient's data privacy requirements as summarised on a paper form, to the service via the care provider's web interface.

3. Conclusion / Future Work

The design for the identity and permissions framework presented in this document is one of several key elements of the overall Do CHANGE ecosystem. The next stage is to implement this and to combine it with the other key elements to form a working prototype for the Do CHANGE ecosystem to be used in the phase 2 field trials. This working prototype should then be tested and evaluated, making any necessary refinements before commencing the phase 2 field trials.