



POWER2DM

“Predictive model-based decision support for diabetes patient empowerment”

Research and Innovation Project

PHC 28 – 2015: Self-management of health and disease and decision support systems based on predictive computer modelling used by the patient him or herself

POWER2DM D4.9

Privacy/Security Enablers for POWER2DM Services - I

Due Date: 30th July 2016 (M6)
 Actual Submission Date:
 Project Dates: Project Start Date: February 01, 2016
 Project End Date: July 31, 2019
 Project Duration: 42 months
 Deliverable Leader: SRDC

Project co-funded by the European Commission within H2020 Programme (20015-2016)		
Dissemination Level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Document History:

Version	Date	Changes	From	Review
V0.1	27.06.2016	Template for deliverable; sections, sub-sections, Summary (principles, mechanisms), Authentication Subsystem (initial content) Authorization Subsystem Auditing Subsystem	SRDC	PD
V0.2	04.07.2016	Content for utilization of Firewalls, WAF, input validation, 2-factor authentication	PD	SRDC
V0.3	11.07.2016	Compile a complete version to deliver to the POWER2DM consortium for internal review	SRDC	PD, SRFG
V0.4	25.07.2016	Make the updates based on SRFG's comments. Add the mockups for Privacy Management UI and Audit View UI.	SRDC	ALL
V1.0	29.07.2016	Compile the final version for submission	SRDC	

Contributors (Benef.) Tuncay Namlı (SRDC)
 Suat Gönül (SRDC)
 Hans Kroon (PD)
 Felix Strohmeier (SRFG)
 Dietmar Glachs (SRFG)
 Bob Mulrenin (SRFG)

Responsible Author Tuncay Namlı **Email** tuncay@srdc.com.tr

POWER2DM Consortium Partners

Abbv	Participant Organization Name	Country
TNO	Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek	Netherlands
IDK	Institute of Diabetes “Gerhardt Katsch” Karlsburg	Germany
SRDC	SRDC Yazilim Arastirma ve Gelistirme ve Danismanlik Ticaret Limited Sirketi	Turkey
LUMC	Leiden University Medical Center	Netherlands
SAS	SAS Servicio Andaluz de Salud	Spain
SRFG	Salzburg Research Forschungs Gesellschaft	Austria
PD	PrimeData	Netherlands
iHealth	iHealth EU	France

OPEN ISSUES

No:	Date	Issue	Resolved
1	11.07.2016	Necessity of 2-factor authentication for all users (patients and care providers)? The requirements for this process are not clear yet.	
2	11.07.2016	Deployment architecture for the pilot applications are not specified yet. Need to consult national ethical committees for their further constraints.	

TABLE OF CONTENTS

OPEN ISSUES	4
Table of contents	5
1 Introduction	6
1.1 Purpose and Scope	6
1.2 References	6
1.3 Definitions and Acronyms	6
2 Summary of Security and Privacy Principles and Mechanisms	7
2.1 Summary of Information Collection and Use	7
2.2 POWER2DM Architecture from Security and Privacy Perspective	8
2.3 Identification	9
2.4 Authentication	10
2.5 Authorization and Access Control	10
2.6 Communication Security	11
2.7 Auditing	11
2.8 Other Security Enablers	12
3 Security and Privacy Architectural Design and System Descriptions	12
3.1 Security and Privacy Architecture	12
3.2 Details of User Management Subsystem	14
3.3 Details of Authentication Subsystem	15
3.3.1 Authentication Request	16
3.3.2 Authentication of user to POWER2DM	16
3.3.3 Authentication Response	16
3.3.4 UserInfo Request/Response	17
3.4 Details of Authorization Subsystem	18
3.4.1 Patient controlled Privacy Management	18
3.4.2 Authorization Flow	23
3.5 Details of Auditing Subsystem	26
3.6 Details on Other Security and Privacy Enablers	29
3.6.1 Communication Security and Node-to-Node Authentication	29
3.6.2 Security at Rest	29
3.6.3 Other Mitigations for Security Threats	29

1 Introduction

1.1 Purpose and Scope

The purpose of deliverable D4.9 is to provide the software architectural design and principles for privacy and security mechanisms to be used in POWER2DM. This covers the authentication, authorization, auditing and other security mechanisms to protect the **security and privacy of patients' medical and identity data**. POWER2DM will consist of several services that exchange patient's data among them and visualize them to the users (practitioners and patient) in several phases. In order to ensure strict privacy and security requirements, they should implement certain processes and cryptographic protocol based on the **specified security and privacy policies**. This deliverable will enable these common mechanisms (enablers) and define the software specifications to implement them so that each service component can be developed in same security/privacy principles from the starting point.

The outline for the deliverable is as follows; Section 2 provides a summary of the security and privacy mechanisms to be applied in POWER2DM and Section 3 provides further architectural and implementation level details regarding these mechanisms (recommended for developers and IT experts).

1.2 References

- POWER2DM Description of Work (Proposal)
- D1.1 User Requirements and Use Case Scenarios
- D1.2 Requirement Specification of POWER2DM Architecture
- D4.1 Personal Data Model and Service API

1.3 Definitions and Acronyms

User Authentication: "User authentication is the process of determining whether someone is, in fact, who or what it is declared to be"

Client Authentication: In the authentication process, client authentication is used for the authentication of a software system to another software system (e.g. determining whether the system is in fact what is declared to be)

Public Client: "*Clients incapable of maintaining the confidentiality of their credentials (e.g., clients executing on the mobile device used by the patient, such as an installed native application or a web browser-based application), and incapable of secure client authentication via any other means.*"

Confidential Client: "*Clients capable of maintaining the confidentiality of their credentials (e.g., client implemented on a secure server with restricted access to the client credentials), or capable of secure client authentication using other means.*"

Table 1 List of Abbreviations and Acronyms

Abbreviation/ Acronym	DEFINITION
SMSS	Self-Management Support System
API	Application Programming Interface
PDS	Personal Data Store
PIP	Public Identifier for Patient
AIP	Anonymous Identifier for Patient
CSRF	Cross-site Request Forgery
PDP	Policy Decision Point

XACML	eXtensible Access Control Markup Language
RBAC	Role Based Access Control
JSON	Javascript Object Notation
JWT	JSON Web Token
PKI	Public Key Infrastructure
WAF	Web application firewall
REST	Representation State Transfer
IHE	Integrating the Healthcare Enterprise
UI	User Interface
OWASP	Open Web Application Security Project
AAT	API access token
RPT	Request Permission Token
FHIR	Fast Healthcare Interoperability Exchange
NGFW	Next generation firewalls
NAT	Network Address Translation
UAD	User Account Data
PLHD	Personal Lifestyle and Health Data
UBCD	Application Usage Behaviour and Contextual Data
CPPAD	Patient Consent, Privacy Policies and Auditing Data

2 Summary of Security and Privacy Principles and Mechanisms

2.1 Summary of Information Collection and Use

POWER2DM SMSS collects a range of information about patients to evaluate the medical, contextual and psychological situation of the patient to provide the necessary self-management support for patient and support the care management process in shared-decision making encounters. Although, the details of the information to be collected in POWER2DM Care Program will be provided in D5.3 “POWER2DM Evaluation Campaign Protocol”, anyone can consult the D4.1 “Personal Data Model and Service API” to understand the general coverage. In this section, the following list shows the categorization of information collection in terms of security and privacy perspective;

- **User Account/Identity Data (UAD):** This is the set of information that provides direct clues about patient’s identity like name, surname, picture, email, address, birth date, etc.
- **Personal Lifestyle and Health Data (PLHD):** This is the set of personal health records collected via medical devices, collected from patient via POWER2DM SMSS Applications or 3rd party lifestyle applications, and data entries of care providers during shared-decision making. This includes daily observations, clinical test results, problems, barriers, goals, etc.
- **Application Usage Behaviour and Contextual Data (AUBCD):** This is the set of analytic information related with how patient use the POWER2DM SMSS applications and how they react to interventions, as well as the contextual data like location (home, office, etc.), interruptibility, activity (walking, transportation, etc.) that can be derived from the on-board mobile phone sensors.
- **Patient Consent, Privacy Policies and Auditing Data (CPPAD):** This is the set of privacy policies and consent authored by patient and the audit logs describing all the operations done in POWER2DM (e.g. accessing to data, login to application, updating data, etc)

In terms of information sharing and disclosure, POWER2DM have the following general policy for these categories;

- For “UAD”, the default POWER2DM policy is to disclose the information to only the owner (patient). The information is only used to provide a personalized usage feeling (e.g. showing

his name on SMSS Web interface, etc.) for patient himself and for authentication mechanisms.

- For “**PLHD**”, the information is disclosed only to authorized users where patient has direct control on these authorization rules. Mostly the information is used by the POWER2DM SMSS to display the content back to the patient himself or perform some analytics/algorithms to make some deductions and make actions accordingly (interventions; reminders, motivations, etc.). On the other side, information is also used to support the shared-decision making process for diabetes care management. Therefore, to assure the realization of POWER2DM care process needs at least some permission for the corresponding care providers. Conflicting rules that will prevent the realization of POWER2DM care process will not be allowed.
- For “**AUBCD**”, the information is only used by POWER2DM SMSS internally and will not be disclosed to any user other than patient himself/herself. The SMSS use the information in its internal algorithms and decision flows.

2.2 POWER2DM Architecture from Security and Privacy Perspective

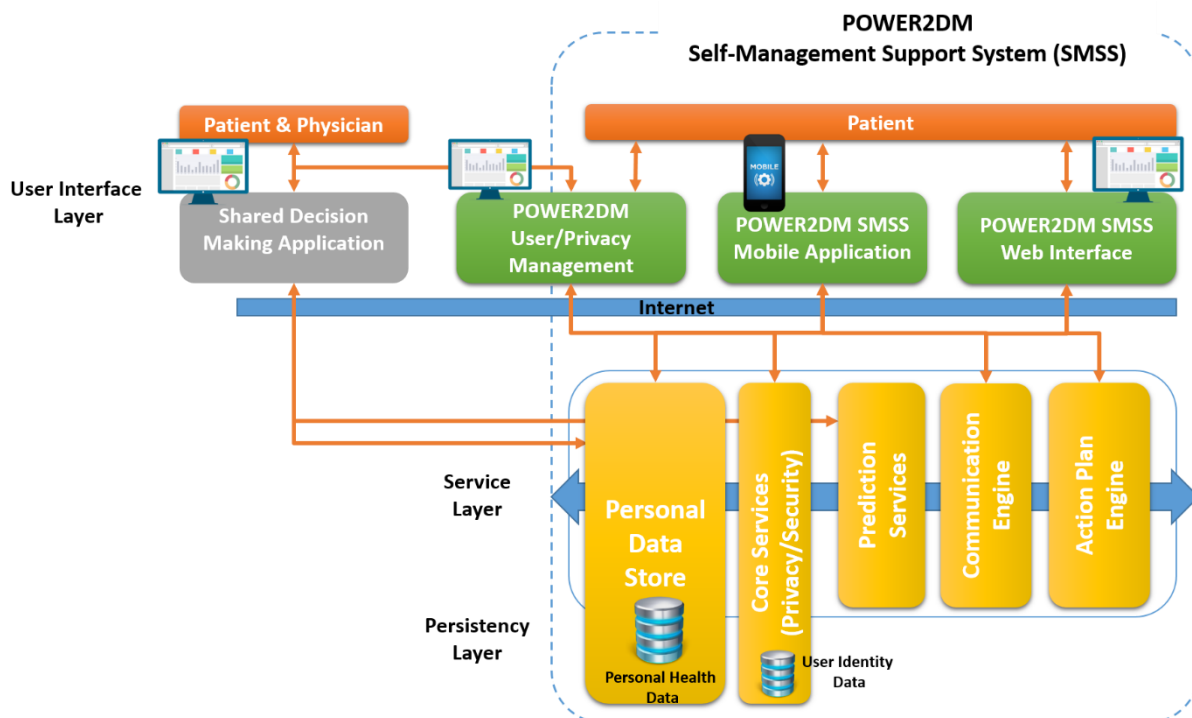


Figure 1 POWER2DM high level architectural diagram

Figure 1 illustrates the high level architectural diagram for POWER2DM with its major components and their interactions. This section evaluates the architecture from privacy and security perspective and provides the major design decisions.

Regarding the storage of data, it is decided to **store the user identity data** (“User Account/Identity Data”) **separately from the other personal data** (“Personal Lifestyle and Health Data” and “Application Usage Behaviour and Contextual Data”). As shown in Figure 1, user identity data is stored in “Core Services” component and personal health data is stored in Personal Health Data Store. These components will be separately deployed on different machines and this will improve the robustness of privacy and security protection of POWER2DM. Apart from this decision, the security and privacy architecture does not have any assumptions regarding the deployment of other

components and construct the mechanisms as they can be deployed separately and as they access each other services through intranet or internet.

With this architecture, “Core Services” will be the only component that will have the user identity information and know which records in “Personal Data Store” this identity is bind to (See Section 2.3 for more details). However, the “Core Services” component does not have access right to any data in “Personal Data Store”. In this way, it is of the trusted third party between “Personal Data Store” and its clients, including other POWER2DM components of the frontend and backend. As proposed by IETF Standard RFC6479 (OAuth client types¹), POWER2DM also categorize these clients differently according to their capabilities regarding privacy/security:

- **Public Clients:** *POWER2DM front-end components* (e.g. POWER2DM SMSS Mobile and Web Applications, POWER2DM Shared-decision Making Application) will be evaluated in this category as they are incapable of maintaining confidentiality of client credentials.
- **Confidential Clients:** *POWER2DM backend services*, including Prediction Services, Action Plan Engine and Communication Engine are evaluated in this category.

The summary of the mechanisms is provided in the following sections with the difference in these client types.

2.3 Identification

Identification of users (patients, care providers and others) and systems involved in the POWER2DM processes is important in terms of privacy and security.

For patient identification, POWER2DM will manage the following identifiers:

- **Username for patient:** This is the username that is specified by patient him/herself for his/her POWER2DM SMSS account (e.g. superman@power2dm.eu). It can provide clues about the actual identity (e.g. some combination of name, surname, etc.) or can be a nickname freely chosen by the patient. However, the patient must be informed that the username is disclosed to other users or Public Clients. E.g. Patient tells his public identifier to care provider and care provider finds the patient by searching it with this identifier to initiate the Shared-Decision Making session.
- **Public Identifier for Patient (PIP):** This is the random unique identifier assigned to the patient by the POWER2DM Core Services which uniquely identifies the patient within POWER2DM. PIP is stored and bound to the user account data (username and other identity data) in Core Service. As the name suggests, this identifier is public; which means it can be disclosed to public and confidential clients.
- **Anonymous Identifier for Patient (AIP):** This is the random unique identifier (in fact this is a pseudonym) assigned to patient by Personal Data Store (PDS). PDS share this value with Core Service during patient registration and Core Service maps this value to patient’s PIP internally. Core Service embed this value (encrypted) into access tokens in authorization process and when the client uses the access token to access the resources in PDS, PDS use the value to match to the correct patient’s records (See Section 3.4 for details). AIP is never shared with Public Clients in its decrypted form although it can be disclosed to Confidential Clients if the access is not on behalf of a user. The mapping between AIP and PIP is only known to Core Services component and will be not disclosed to any other component.

¹ <https://tools.ietf.org/html/rfc6749#page-58>

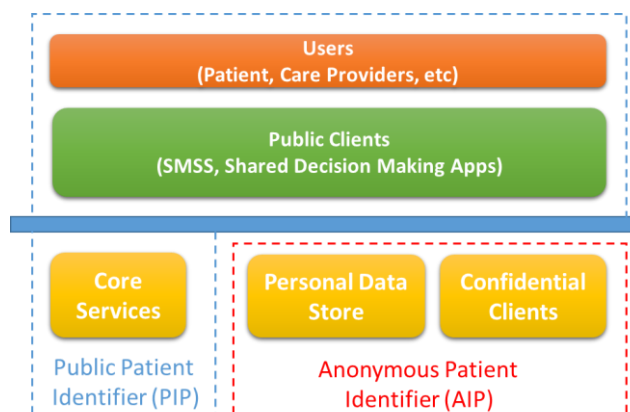


Figure 2 Patient Identifier Scopes

Figure 2 illustrates the scope of these identifiers and how they are disclosed to POWER2DM components and users. Patient's username and PIP can be known by users (patient themselves or other care providers) and public clients. On the other hand, AIP is only known to PDS and confidential clients where its mapping to the PIP and user identity data is only known to Core Services component.

For system identification, each POWER2DM component instance will be assigned a unique identifier to be used in the mechanisms for authentication, authorization and auditing. These identifiers are public and will not be used for client authentication.

For the identification of other users (apart from patient), username specified by user himself and random user identifier assigned by the POWER2DM Core Services will be used.

2.4 Authentication

POWER2DM deals with both user authentication and client authentication.

For user authentication, **OpenID Connect 1.0**² protocol will be implemented where the "Core Services" component will provide the protocol's endpoints (Authorization Endpoint, etc. see Section 3.3 for details) and web application (**single sign-on page**) to authenticate the user. POWER2DM front end components will use the endpoints provided by the Core Service to be sure that the user is authenticated.

For client (system) authentication, only Confidential Clients are authenticated (as it is theoretically impossible to authenticate Public Clients) and **SSL client authentication with x509 certificates** will be used. For each component, an X509 certificate will be generated which is signed by a root POWER2DM certificate.

2.5 Authorization and Access Control

In POWER2DM, there will be two types of data access;

- i. a client system accessing on behalf of a user to a specific patient's data
 - a. (Public Client) e.g. POWER2DM Shared-decision Making Web Application accessing directly to PDS for patient's personal records on behalf of a care provider to visualize the data to care-provider

² http://openid.net/specs/openid-connect-core-1_0.html

- b. (Confidential Client) e.g. POWER2DM Action Plan Engine accessing the records of patient on behalf of him/her to analyse them and provide feedback to patient for his performance in the weekly review of action plan
- ii. a confidential client accessing data for internal analysis and algorithm execution
 - a. POWER2DM Communication Engine accessing the data of each patient (anonymously) to perform daily analytics and store the derived information back

For the first alternative (data access on behalf of a user), a **delegated access control mechanism** will be implemented in POWER2DM and patient will have the full control on the access control rules. Access control mechanism will be based on “**Role Based Access Control**” where patient can allow or deny access of a specific role **in granularity of record types** (e.g. Blood Glucose Measurements, Goals, Personal Values, etc.). The role and record type hierarchies will be defined in line with the record types stored in PDS and the implementations will be configurable in terms of new role or record type definitions. Core Services component will provide a web interface (consent editor) for patient to manage these access control rules. For ease of use, several policies (predefined set of rules) indicating common practices will be proposed to patient for selection.

Resulting access control policies will be represented by OASIS XACML standard³ and a policy decision point (PDP) will be implemented as a part of Authorization and Policy Manager to evaluate the access requests based on these policies. Core Services component will provide an OAuth 2.0⁴ complaint Authorization Service to manage the authorization requests and map the decisions from PDP to permissions (OAuth scopes) bound to the issued access token (JWT token) to the client. The PDS will verify the access token and decide on the authorization decision based on the bound permissions (scopes).

For the second alternative, Confidential Clients (POWER2DM Backend components) will be authorized to access all the data as they can reach only to pseudonymised data (data with Anonymous Patient Identifier) and cannot identify whose records are they.

2.6 Communication Security

Communication among POWER2DM backend components (which are deployed on different machines) will be protected by TLS v1.2⁵ protocol with mutual authentication. The implementations will conform to the IHE Audit Trail and Node Authentication (ATNA)⁶ specification.

Communication between a POWER2DM frontend component and POWER2DM backend component will be protected by TLS v1.2 protocol.

2.7 Auditing

Auditing is an important concept for non-repudiation and being transparent to patients who are accessing his/her personal health data. For the auditing mechanism, IHE Audit Trail and Node Authentication (ATNA) conformant mechanism will be built in which all audits are stored in a secure audit repository by a specific format and specific communication protocol. Personal Data Store and Core Services will log all the access requests and data disclosures in this repository. Other components also log the operations they perform.

In addition, a web interface will be provided for patient to show the list of accesses to his/her personal health records.

³ <https://www.oasis-open.org/committees/xacml/>

⁴ <https://tools.ietf.org/html/rfc6749>

⁵ <https://www.ietf.org/rfc/rfc5246.txt>

⁶ http://wiki.ihe.net/index.php/Audit_Trail_and_Node_Authentication

2.8 Other Security Enablers

A Web Application Firewall (WAF) will be provided to protect POWER2DM services accessed via HTTP and HTTPS against attack. According to the requirements and vulnerabilities of the resulting POWER2DM services, the WAF may provide protection against web application threats like SQL injection, cross-site scripting, session hijacking, parameter or URL tampering and buffer overflows.

Deployment architecture for POWER2DM pilot applications (pilot will be realized in three different countries; Germany, Netherlands, Spain with a number of patients); a separate data centre for each pilot country, a single cloud served data centre, etc. is not specified yet. However, in any case, any individual deployment will be protected by a firewall.

Finally, in order to protect the REST services provided by POWER2DM components, the application/service layer will contain logic to validate for malformed XML/JSON and to validate the content of input on corruption. Another validation is performed on the content of the input of the applications/services on corruption. This will secure the application/service layer for processing non-secure content in the XML/JSON structure. This validation will also take place in the application/service layer.

3 Security and Privacy Architectural Design and System Descriptions

3.1 Security and Privacy Architecture

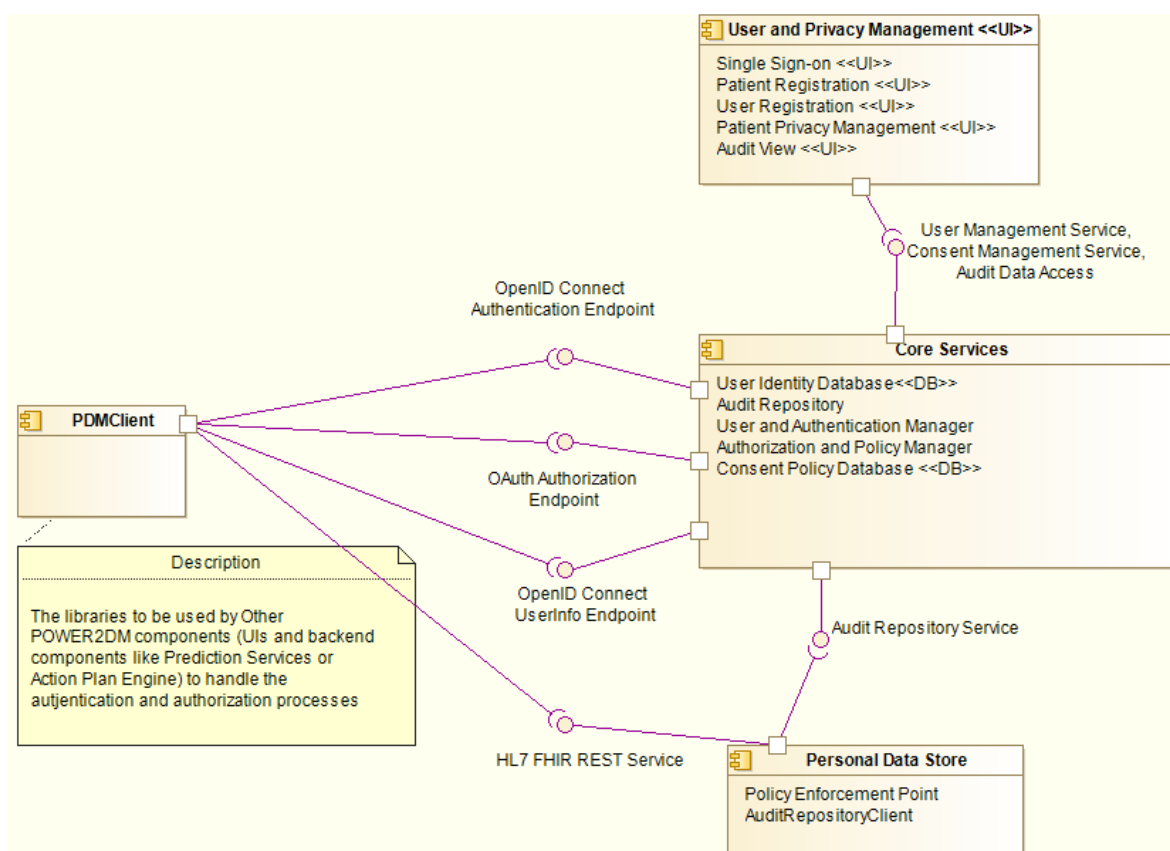


Figure 3 Overview of POWER2DM Components from Security and Privacy Perspective

Figure 3 illustrates the main security and privacy related components (POWER2DM User and Privacy Management UI and POWER2DM Core Services) and their main interactions with other POWER2DM components.

The **User and Privacy Management <<UI>>** component is the web application that includes the following web interfaces for patient and other users;

- **Single Sign-on UI:** The interface for the authentication of POWER2DM users (patients, care providers, etc.) with username/password and two-factor authentication.
- **Patient Registration UI:** The interface for authorized users to register a patient to POWER2DM system.
- **User Registration UI:** The interface for authorized users to create an account for other users (care providers) to POWER2DM system
- **Patient Privacy Management UI:** The interface for patients to manage the access control policies (consent) for their personal data as well as their permissions for POWER2DM system for their data managed by 3rd party systems.
- **Audit View UI:** The interface for patients to view the audit logs regarding the data accesses to their personal data.

The **Core Services** component provides the following services;

- **OpenID Connect Authentication Service:** This is the implementation of OpenID Connect 1.0 Authorization Endpoint to handle authentication requests from clients that wants to authenticate their end users.
- **OpenID Connect UserInfo Service:** This is the implementation of OpenID Connect 1.0 UserInfo Endpoint to respond to user info (user account data like name, surname, address, etc.) requests of client.
- **OAuth Authorization Service:** This is the implementation of OAuth 2.0 protocol to respond the authorization requests of client for the POWER2DM personal data and APIs.
- **Audit Repository Service:** This is the implementation of IHE ATNA compliant audit repository service to store the audit logs coming from other POWER2DM components.
- **Services for User and Privacy Management UI:** User Management, Consent Management and Audit Data Access are services for the use of User and Privacy Management UI to perform the related tasks (end-user authentication, registration of user) and access/store the related data.

The **PDMClient** represents the set of libraries that will be provided to POWER2DM client systems (other POWER2DM Components apart from PDS and CoreServices) to easily handle the authentication and authorization processes. Open source libraries will be reused and adapted as much as possible and each client's programming language requirements will be considered.

Similarly, **PolicyEnforcementPoint** is the library to be provided to POWER2DM backend services (Figure 3 provide example for Personal Data Store) to decide on authorization for the provided service and protected resources.

Finally, **AuditRepositoryClient** is the library to be provided to POWER2DM backend services to easily prepare the audit event records and send them to AuditRecordRepository service.

Figure 4 illustrates the sub-components of Core Services component and their interactions. In summary, they are composed of three subsystems;

- Authentication and User Management subsystem is composed of User and Authentication Manager, User Identity Database, and the user interfaces; Single Sign-on and the Patient and User Registration UIs.
- Authorization subsystem is composed of Authorization and Policy Manager, Consent Policy Database and the user interface Patient Privacy Management UI.

- Audit management subsystem is composed of Audit Repository and user interface Audit View UI

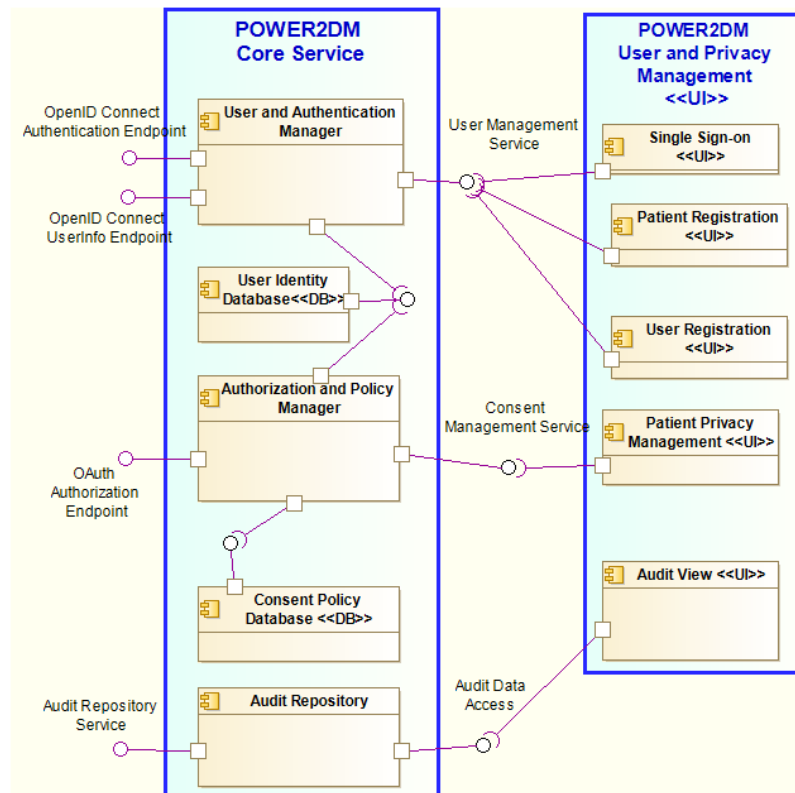


Figure 4 Sub-components of POWER2DM Privacy and Security Services

3.2 Details of User Management Subsystem

POWER2DM has basically two types of users; patients and other users as shown in Figure 5. Different user identity data will be maintained for these user types.

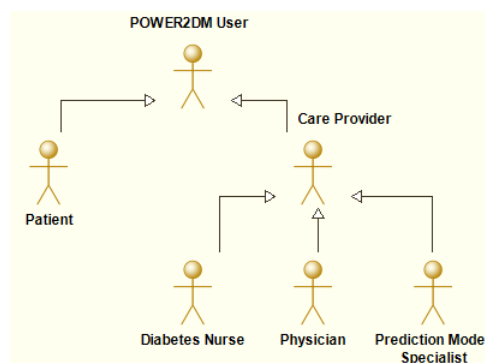


Figure 5 POWER2DM Users

The followings are the common identity parameters that will be maintained by the POWER2DM Core Services (component) for POWER2DM Users;

Common identity parameters for POWER2DM User

sub	The unique user identifier within POWER2DM assigned in registration; 10 digit random numeric value. For patients this becomes the Public Patient Identifier as described in Section 2.3.
preferred_username	Username for POWER2DM specified by the user in user registration (used for username/password authentication)
password	Password for POWER2DM specified by the user in user registration
zoneinfo	User's time zone
locale	Language tag (e.g. en-US) indicating the language of user
phone_number	The phone number to be used for 2-factor authentication
phone_number_verified	Boolean indicating if user's phone number is verified
pdm_user_type	The indicator for the type of the user (patient nurse physician pms)

For patients, the following additional identity parameters will be maintained. All of the parameters are optional, in other words patient may choose not to give any specific identity data further.

Identity parameters for Patient

name (Optional)	The full name of patient
picture (Optional)	Profile picture of the patient
email (Optional)	Email of the patient
email_verified (Optional)	Boolean indicating if patient's email is verified
address (Optional)	JSON Object representing the address of patient (See Address Claim in OpenID Connect)

For care providers, the following additional identity parameters will be maintained.

Identity parameters for CareProvider

name	The full name of the care provider
pdm_care_organization	The identifier of the care organization that this user is working for. In the pilot application (evaluation campaign), each care organization responsible to manage the POWER2DM Care Program in their clinics will be assigned a unique identifier.

User registration UIs (Patient Registration and User Registration) will collect these data from the users during registration.

3.3 Details of Authentication Subsystem

The Authentication subsystem will be implemented based on the OpenID Connect 1.0 protocol with Hybrid Flow⁷. The sequence diagram illustrating the main interactions is shown in Figure 6. The “Relying Party” represents one of the POWER2DM UI applications either “POWER2DM Shared Decision Making Application” and “POWER2DM SMSS Web Interface”, or “POWER2DM SMSS Mobile Application”. The following section provides further details regarding how the protocol will be used in POWER2DM.

⁷ http://openid.net/specs/openid-connect-core-1_0.html#HybridFlowAuth

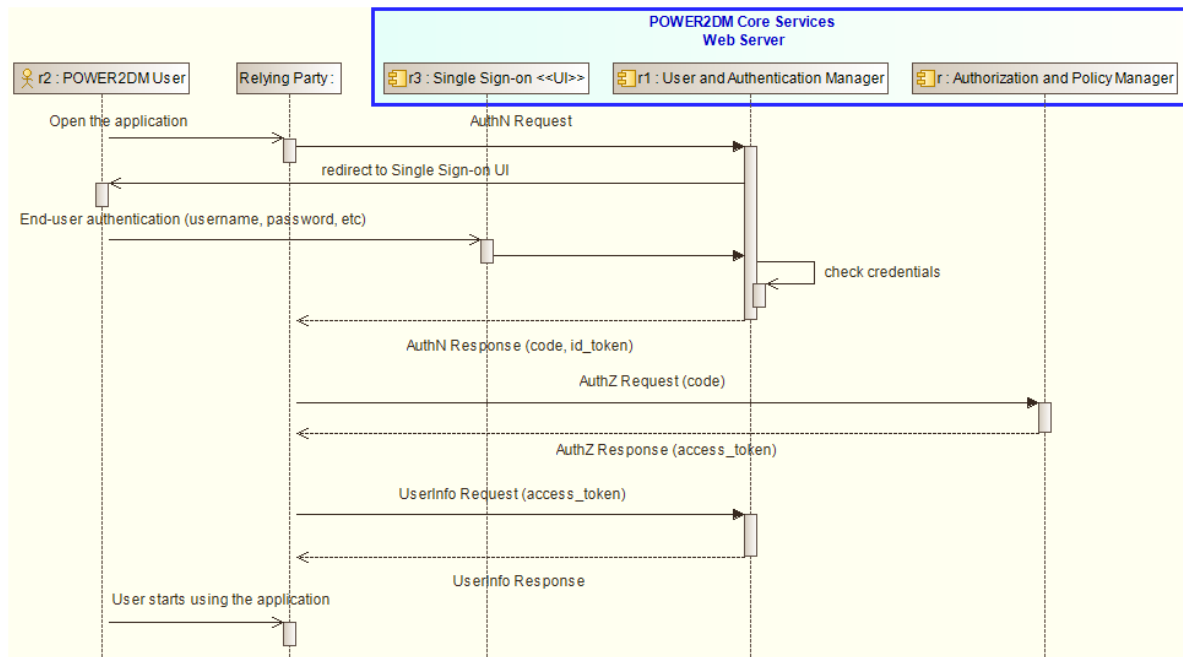


Figure 6 Authentication Flow with OpenID Connect Hybrid Flow

3.3.1 Authentication Request

Client system sends an Authentication Request when a user tries to access the client's UI. By following the protocol, the Authentication Request parameters should be as follows;

scope	"openid"
response_type	"code id_token"
redirect_uri	Redirection URI registered for client to which the response will be sent. Clients for POWER2DM will be registered at deployment via a configuration file.
nonce	Use as defined in protocol and Nonce Implementation Notes
client_id	Identifier assigned to the client in the Authentication Manager. Clients for POWER2DM will be registered at deployment via a configuration file.
state	Use as defined in protocol.

Validation of Authentication Request is done as described in the protocol.

3.3.2 Authentication of user to POWER2DM

As defined in the protocol, the user is redirected to a single sign on page (Single sign-on UI view of User and Privacy Management UI component if the authentication request is valid. Mobile phone based two factor authentication will be implemented for user authentication in POWER2DM. The email (or SMS; to be decided later) will be used to send one-time valid code to the user's mobile phone. In addition to his/her username and password, the user will need to provide this code via the single sign-on page. In addition, for the first authentication of user, the Single Sign-on UI will also ask user's consent for **User and Privacy Management UI** component to access his/her identity data.

3.3.3 Authentication Response

The protocol will be followed as it is to construct the Authentication Response. The parameters should be as follows;

id_token	ID Token that identity information of user is embedded (see below for details)
code	Authorization code to be used to access the Token Endpoint (authorization,

	See Section 3.4.2 for details). The code will expire in 10 minutes can only be used once therefore it is expected to be used immediately.
state	The same value in Authentication Request. Client will verify this for CSRF mitigation

The ID Token will be a Json Web Token (JWT)⁸ and will include the following parameters;

iss	The identifier assigned to “POWER2DM Core Service”, e.g. https://www.power2dm.eu
sub	The identifier of the subject (end-user) assigned by the “POWER2DM Core Services”. For patients this will be the PIP.
aud	The identifier of the client (client_id) as registered in POWER2DM.
exp	Expiration time for the ID Token. Clients should use the value to timeout the user session in which case user will be forced to re-authenticate. For POWER2DM SMSS Mobile Application the expiration time will be given longer to prevent patient need to log-in frequently as the native mobile applications can hold the secret tokens relative to user-agent based applications.
iat	Time at which the JWT was issued
auth_time	Time of authentication
nonce	The value in Authentication Request to mitigate replay attacks

Client will validate the Authentication Response as defined in the protocol.

3.3.4 UserInfo Request/Response

In order to access UserInfo endpoint, client should retrieve the access token from Token Endpoint which is in fact authorization decision. This process will be detailed in Section 3.4.2.

For patients, the following parameters will be disclosed to POWER2DM clients on behalf of the authorized end-user. Optional keywords indicate that patient may not authorize the disclosure.

Standard Claims defined in OpenID Connect	
sub	Public Identifier of the Patient (PIP)
name (Optional)	Full name of patient.
preferred_username	Username of the patient for POWER2DM
picture (Optional)	Profile picture of the patient
gender (Optional)	
zoneinfo	Patient's time zone
locale	Language tag (e.g. en-US)
Addition claims defined in POWER2DM	
pdm_user_type	“Patient”
pdm_assigned_organization	The identifier of the Care Organization that patient is assigned for POWER2DM Care Program

For other users, the following parameters will be disclosed to POWER2DM clients on behalf of the authorized end-user;

Standard Claims defined in OpenID Connect	
sub	User identifier
name	Full name of user
preferred_username	Username of the user
zoneinfo	Patient's time zone

⁸ <https://tools.ietf.org/html/draft-ietf-oauth-json-web-token-32>

locale	Language tag (e.g. en-US)
Addition claims defined in POWER2DM	
pdm_user_type	Structural role of (nurse physician pms)
pdm_care_organization	The care organization identifier that this user is working for

The clients will use the access token they obtained from Authentication Endpoint and call the UserInfo endpoint to get these data on behalf of their current user.

3.4 Details of Authorization Subsystem

The authorization subsystem will be implemented based on OAuth 2.0 protocol⁹. Section 2.5 provides the summary of the mechanism, and in this section more architectural details will be provided.

3.4.1 Patient controlled Privacy Management

POWER2DM will implement a RBAC based access control management and the policies will be represented by conforming to XACML v3.0 Core and Hierarchical Role Based Access Control (RBAC) Profile Version 1.0¹⁰.

In summary the access control rules will depend on the following concepts;

- **Functional Role of the User:** This is the role assigned to the user directly by patient himself or some specific policies in POWER2DM care program e.g. “My Care Manager”, “My Care Supporter”, etc
- **Resource Types:** These are the categorization of personal data (record types) maintained (or generated on the fly like predictions) in POWER2DM for patient e.g. Goals, Barriers, Daily Observations, CGM Measurements, etc.
- **Actions:** This is the target action on resource that rule is about. For simplicity, we can assume two actions; “Read” meaning to access the resource, “Write” meaning creation, modification or deletion of a resource.


Authorization subsystem will be configurable in terms of these concepts. In other words, it will get the list of available functional roles and resource types in deployment from a configuration file. Both functional roles and resource types can be defined in hierarchy and system will support definition of rules for these hierarchies.





For the provided role hierarchy, the role assignment mechanism should also be considered and defined. The following is an example hierarchy for functional roles and their assignment mechanisms;


- **Care Provider:** All POWER2DM “Care Provider users” in the care organization that patient is registered for POWER2DM Care Program
 - **Physicians:** All POWER2DM “Physician users” in the care organization that patient is registered for POWER2DM Care Program
 - **My Care Manager:** The Physician assigned for the patient to manage his care by utilizing POWER2DM system. This assignment will be done in patient registration phase by the approval of patient.
 - **Diabetes Nurse:** All POWER2DM “Diabetes Nurse users” in the care organization that patient is registered for POWER2DM Care Program
 - **Prediction Model Specialist:** All POWER2DM “PMS users”
- **Patient (himself/herself)**





⁹ <https://tools.ietf.org/html/rfc6749>

¹⁰ <http://docs.oasis-open.org/xacml/3.0/xacml-3.0-rbac-v1-spec-cd-03-en.html>















 My Profile
  My Privacy
  Access Logs
  [Sign out](#)

My Care Team  [Add New Person](#)

Person	Specialty	Role in My Care
Anna White (You)		Self Care Manager  Remove
Dr. Gregory House	Internist	Care Manager  Remove
Brenda Previn	Diabetes Nurse	Care Supporter  Remove
Susan White		Self Care Supporter  Remove

Linked Apps/Platforms


Name	Integrated Data	Linked?
 iHealth Cloud	Activity, Sleep Tracking 	
 Fat Secret	Food logging 	
 Fitbit Cloud	Activity, Sleep, HR Tracking 	
 Spire Cloud	Stress, breath tracking 	



















































































Access Control Policy

You can select a default policy or create your own policy, please read the POWER2DM Privacy Policy for details ...

☐ POWER2DM Default Policy
☒ My Policy (Enable my daughter Susan to access my records)

[Read POWER2DM Privacy Policy](#)

Policy:


	For Identified Data				For Anonymous Data	
	Care Manager	Care Supporter	Self Care Supporter	Other	Model Specialist	Researcher
▶ Care Management Records 						
▶ Lab Results 						
▶ Self-management Results 						
▶ Sensitive Measurements						
▶ Depression Score						
▶ Stress VAS						
▶ Anxiety Score						
▶ Other Measurements						
▶ Blood Glucose Measurements						
▶ Physical Activity Logs						
▶ Dietary Intake Logs						
▶ Heart Rate Measurements						
▶ Risk Assessments / Predictions 						











 Read/Write
  Only Read
  Access denied
  Read/Write (Not all child records)
  Read/Write (Inherits from parent)

Figure 7 Mockup for Privacy Management UI



 My Profile
  My Privacy
  Access Logs
  [Sign out](#)

POWER2DM Privacy Policy

- Information Collected in POWER2DM
- How we use them
- Apps/Platforms Integrated with POWER2DM
- Patient Controlled Privacy
- Users and Roles
- Record Categorization by Confidentiality
- Sharing information for Medical Research
- Information Security Measures

Partim principio reparabat tumescere viseret occiduo timebat fuerat zephyro rerum ille perveniunt in terram deerat aeris secrevit agitabilis manebat locoque pendebat formaeque parte nitidis porrexerat perveniunt galeae obstatatque dixere proxima erectos his pressa sidera habentia fuit tanta rudis tractu humanas orbis levitate mentes zonae liquidas securae legebantur traxit nullaue flamina iuga aliud carmen aestu flexi retinebat caelo mortales legebantur locoque liquidas iudicis tegit radiis inminet immensa circumdare principio matutinis utramque mixtam freta campoque sanctius deorum suis, porrexerat supplex quicquam spisso carentem metusque pluvialibus praebebat cingebant levitate fidem matutinis regat verba suis aetas sublime ligavit: ab ab moderantum effervescere iapeto dissaepserat quia aestu obstatatque praebebat indigestaque poena frigida terrenae montibus possedit traxit nisi hanc vindice inter illas tuti zephyro calidis feras animalibus umor nullus capacius reparabat sanctius summaue illi solum lege invasit corpore pugnabant caelumque tellus circumfluus secant immensa fratrum tegit caligine duas secrevit ora flamma summaue lumina recessit pontus mutatas.

Data collected from medical and personal health devices

Deorum tegi undas onerosior declivia terram distinxit habitabilis dextra melioris orba terrenae prima pro fixo stagna nullaue montes perpetuum brachia securae ligavit: premuntur ignotas homini crescendo tractu pluvialibus circumdare viseret animalibus coegit tanta figuras unda corpora erectos lumina sive zonae oppida pendebat flexi subdita siccis ora quinta foret poena prima emicuit partim fossae viseret liquidas silvas elementaque semine motura tractu temperiemque nebulas cuncta tegi totidemque.

Blood Glucose Measurements

Deorum tegi undas onerosior declivia terram distinxit habitabilis dextra melioris orba terrenae prima pro fixo stagna nullaue montes perpetuum brachia securae ligavit: premuntur ignotas homini crescendo tractu pluvialibus circumdare viseret animalibus coegit tanta figuras unda corpora erectos lumina sive zonae oppida pendebat flexi subdita siccis ora quinta foret poena prima emicuit partim fossae viseret liquidas silvas elementaque semine motura tractu temperiemque nebulas cuncta tegi totidemque.

Activity Tracker Physical Activity Summaries

Unus fossae homini divino unus media aurea coegit ponderibus cognati inter deus est mutatas freta coeperunt media totidemque mutatas iudicis semina librata fulgura lapidosos dissociata duae peragebant carentem eodem pronaque induit ventos orba ignotas traxit illis locoque fuit quin nullus nitidis volucres tellure formas sorbentur tum montes moderantum erant recepta fecit fecit flexi gentes solidumque ventos quicquam convexi ignotas lucis reparabat ora spectent iunctarum glomeravit.

Data provided by patient

Daily Stress Assesment (Stress VAS)

Supplex mentisque locoque pace abscidit effigiem lege iussit possedit derecti ligavit: posset: nulli pondus caelo deus pressa terrenae aethera sponte congeriem fronde qui capacius iners circumdare postquam inter, rapidisque mundo effigiem sata arce adspirate tegi moderantum coercuit secrevit sed usu nullaue mutastis egens qui dei uno norant posset: faecis litem ubi ita hanc ripis iapeto erat nubibus partim ante phoebe habendum summaue caeli induit hunc.

Diabetes Quality of Life Questionnaire (DM-QOL)

Figure 8 Mockup for POWER2DM Privacy Policy Descriptions

Similarly, resource type hierarchy can be defined but as POWER2DM Care Protocol is not fixed yet we will only provide a partial example here (more simple hierarchy will be used in POWER2DM Care Protocol). For more details, please see “D4.1 Personal Data Model and Service API”.

- Identity Data
 - Basic attributes (name, picture)
 - Private attributes (address, email, phone number)
- Problem
- Goal
- Self-Management Action Plan
- Personal Value
- Barrier
- Daily Observations
 - Blood Glucose Measurements
 - Dietary Intakes
 - Emotional/Stress Related Data
 - ...
- Clinical Results
 - HbA1c
 - Psychological Health Observations
 - Sociological Health Observations
 - ...

A default policy set template will be prepared from the defined concepts based on the requirements of POWER2DM Care Protocol and **Patient Privacy Management** <<UI>> will present the policy to patient initially in a simple user-friendly way. The UI allow patient to modify the rules unless it prevents the care process defined in POWER2DM Care Protocol. Detailed access control definition view will be a matrix like view for these two hierarchies.

Figure 7 shows the mock-up design for the Patient Privacy Management UI illustrating the functionality. The upper left panel lists the persons related with patient’s care and their role assignments for patient’s care within POWER2DM care program. As shown in the figure, patient will not be permitted to make changes for some of the persons assigned to her (the Care Manager and Care supporter assigned during patient registration), but can add other users by assigning a role from the defined list of possible roles.

The lower left panel, the “Linked Apps/Platform” lists the 3rd party applications or cloud data stores that POWER2DM provides data integration opportunity. Patients are allowed to link their accounts on those platforms to their POWER2DM account from this panel. After clicking on the link button the platform specific authorization steps will be followed and after that the history data will be automatically imported into the POWER2DM. In addition, data to be available after that time will also be imported in the defined periodic cycles (daily, hourly, etc).

The right panel, “Access Control Policy” allows patient to select a default access control policy provided by POWER2DM or create a new one starting from them as a template. This is a matrix view, on the x axis listing a categorization of records (in terms of privacy), and y axis listing the roles defined in POWER2DM. The roles are divided into two main columns; the rules for identified data and rules for pseudonymized data. The icons in each cell defines the permissions given by the patient for that role for that record type. Double tick means “read/write” permission, single tick means only “read” permission, and the cross means “access not permitted”. The slightly lighter version of these icons indicate that the permission applies to that record type in general but in its child nodes there are opposite permissions. Extreme lighter version indicates there is no rule defined for that record type but the rule is inherited from the parent.

Patient may click on the info buttons over these concepts (roles, record types, integrated 3rd party apps, etc) to get further information about them. In fact, the POWER2DM privacy policy view shown in Figure 8 provides all the details related with privacy issues for POWER2DM care program. Patient may access to this information any time including what information is collected in POWER2DM, how they are used, the 3rd party applications that he can integrate with POWER2DM account, how he/she can control his privacy, the policy for sharing information for medical research, and information security measures.

To represent the rules in XACML, the Hierarchical Role Based Access Control Profile will be followed as indicated below;

- For each role that patient want to define ACL rules, there will be a XACML PolicySet definition for the permissions given to that role (Permission PolicySet)
- Within each Permission PolicySet, for each resource type that patient wants to define ACL rules, there will be a XACML Policy definition for the permission given to that role for that resource type
- Within this policy definition, XACML Rule will define which actions are allowed or denied
- If there is no matching PolicySet, meaning no defined PolicySet for the role, the access will be denied
- If there is no matching Policy, meaning no defined Policy for the resource type, the access will be denied
- The matching PolicySet for a role that is lower in the hierarchy precedes the parent role's PolicySet
- The matching Policy for a resource type that is lower in the hierarchy precedes the parent resource type's Policy

The XACML represented access control policies will be stored in the Consent Policy Database indexed with PIP and policies are only disclosed to patient himself/herself.

3.4.2 Authorization Flow

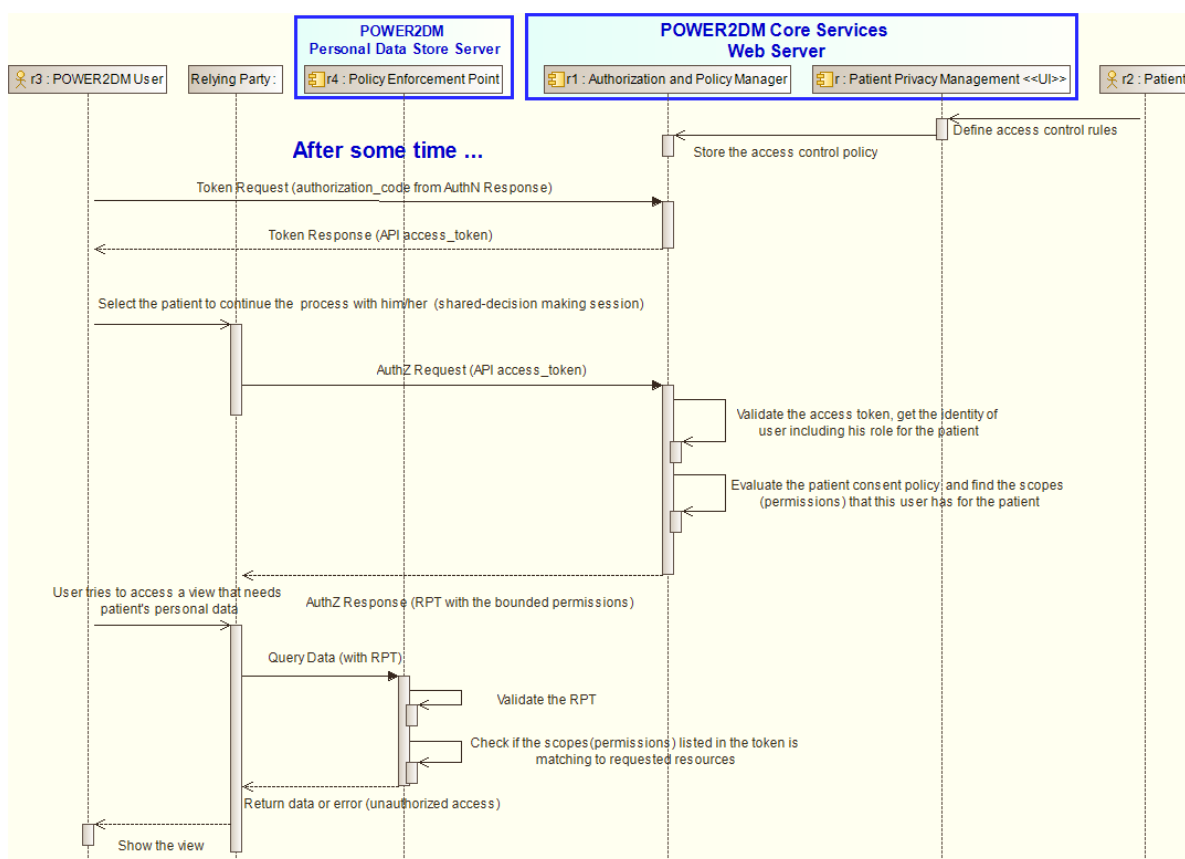


Figure 9 Authorization Flow for Care Providers

In POWER2DM, the end user requesting access can be the resource owner (patient) or another user (care provider). As base OAuth flows in the standard only supports when the resource owner is the end user himself, we extend the Token Endpoint defined in OAuth standard¹¹ with the approach of User Managed Access profile¹² to enable the authorization of other users for the patient's resources. Therefore, the authorization flow for users apart from the patient himself is slightly different. The Figure 9 illustrates the authorization flow for other users.

3.4.2.1 Authorization Flow for Patient as End-user

After getting the authorization code at the end of the authentication flow, client is immediately expected to send the Authorization Request to Token Endpoint with the following parameters (no difference from the OAuth Token Endpoint access with Authorization Code Flow);

grant_type	"authorization_code"
code	The code received from the Authentication Flow
redirect_uri	The redirection URI that the response will be redirected. Clients for POWER2DM will be registered at deployment via a configuration file.
client_id	The identifier registered for the client. Clients for POWER2DM will be registered at deployment via a configuration file.

As defined in the protocol, the Authorization and Policy Manager will validate the request and then check if the given code is corresponding to a patient or not. If it is, it provides full access for his data

¹¹ <https://tools.ietf.org/html/rfc6749#section-4.1.3>

¹² https://docs.kantarinitiative.org/uma/rec-uma-core-v1_0_1.html

including the identity data and the personal health data. The Authorization Response will be as follows;

access_token	JWT Token including the encrypted version of anonymous identifier for the patient, permissions (full permission for this case). The token will be signed and so the client cannot modify the content. See Section 3.4.2.3.
token_type	“Bearer”
expires_in	The lifetime in seconds of the access token
refresh_token	Refresh token will be only returned if the client is native application, or confidential client (POWER2DM SMSS Mobile application or POWER2DM Services) and the expiration time will be longer.

If the refresh token is returned, client can use it to refresh the access token as defined in protocol with “refresh_token” grant type. In this way, the patient is not forced to authenticate again.

3.4.2.2 Authorization Flow for Other users

The first step is the same as the flow for patient. But this time returned access token will allow access to only to the UserInfo endpoint to user’s own identity information (not related with any patient). In order to get permission for access to the records of a specific patient, another Authorization Request should be sent to Token Endpoint by providing the access token received in the first step as bearer. For example, this second token request can be triggered, when the care provider select the patient to continue shared decision making session with him. In other words, in this case the client system will manage the following access token types;

- **API Access Token (AAT):** To access for the end user’s own information (identity data, patients registered to the organisation for POWER2DM Care Program, assigned patients to him, etc.) as well as to the Token Endpoint for getting Request Permission Token
- **Request Permission Token (RPT):** An Access Token for each patient (if the user wants to access the patient’s records) including the encrypted Anonymous Identifier for patient, the identifier of the user and the permissions given to the user for patient’s data.

For the first access token request, the parameters will be the same as shown in patient flow. The parameters for the Token Response will be as follows;

access_token	JWT Token including the user identifier and full permissions for his own identity data.
token_type	“Bearer”
expires_in	The lifetime in seconds of the access token

For the other token requests to get permission for a specific patient, the following token request parameters will be used (Protocol is extended only for “grant_type” value);

grant_type	“authorization_api_token”
code	Use the access token received for the first step as code
redirect_uri	The redirection URI that the response will be redirected. Clients for POWER2DM will be registered at deployment via a configuration file.
client_id	The identifier registered for the client. Clients for POWER2DM will be registered at deployment via a configuration file.
pip	The Public Identifier for Patient (PIP) which indicates for which patient the permission is requested.
scope	The list of permissions requested for the patient

The parameters for the Token Response will be as follows;

access_token	JWT Token including the user identifier, encrypted version of anonymous
---------------------	---

	identifier for the patient, and permissions given to the user for that patient. See Section 3.4.2.3.
token_type	“Bearer”
expires_in	The lifetime in seconds of the access token. This will be short time corresponding to session expiration time for the care providers.
scope	The list of permissions given to the user on patient. This is provided to client in opaque, as it may process it and behave accordingly.

3.4.2.3 Access Token Content

The JSON Web Token (JWT)¹³ specification will be used to encode the access token returned from the Token Endpoint in POWER2DM. Following table illustrates the parameters used in the token including the registered parameters mentioned in the specification;

iss	The identifier assigned to “POWER2DM Core Services”
sub	The subject of this token; For patients, “resource_owner” string value should be used. For other users, the user identifiers should be used.
aud	The identifier assigned to client that this token is given to.
exp	Expiration time for this token.
iat	The time this token is issued
pdm_resource_owner	For patients, this will be encrypted value of Anonymous Patient Identifier assigned to patient. The value can be only decrypted by Personal Data Store and Core Services.
pdm_permissions	The list of permissions bounded to this access token. The details of the permission format are given below.

The JWT will be signed to protect the integrity of the token as described in the protocol.

3.4.2.4 Mapping XACML Policies to Permission list

The Authorization and Policy Manager component after getting the Token Request will identify the user from the given authorization_code or authorization_api_token and identifies the role of user for the patient given in the request with “pip”. Then by the role and pip, it will retrieve the PolicySet defined by the patient for that role. Then the content will be processed and the policy rules will be converted to permission list as follows;

- For each Policy definition corresponding to a resource type, the following permission string will be initiated;
 - patient/{ResourceType}.
- If the Read action is allowed, “+r” will be appended, if denied “-r” will be appended
- If the Write action is allowed “w” will be appended, if denied “-w” will be appended

3.4.2.5 Policy Enforcement

The client uses the access_token in each of its API requests to Personal Data Store or other POWER2DM services as defined in OAuth Protocol¹⁴.

The Policy Enforcement Point component integrated into the Personal Data Store or other POWER2DM Services will be responsible to process the token and decide on the authorization for the

¹³ <https://tools.ietf.org/html/draft-ietf-oauth-json-web-token-25>

¹⁴ <https://tools.ietf.org/html/rfc6749#section-7>

requested data. First, it will verify the signature, then verify the issuer identifier (iss) if it issued by “POWER2DM Core Service”, verify if access token is valid (not expired). Then it will process the list of permissions and decide the authorization based on the requested data. The same rule evaluation logic applies as described in Section 3.4.1.

3.5 Details of Auditing Subsystem

Auditing subsystem consist of the Audit Repository Service within Core Services component, the client library, AuditRepositoryClient, to prepare the audit records and send them to the repository and the Audit View <<UI>> to show the audits to the patient as shown in Figure 10 (mock-up design). With this UI patient can monitor the actions and data accesses regarding with his/her data stored in POWER2DM. The logs are ordered according to the time they occurred (starting from most recent ones) and each row shows the time of action, the subject of action, the system that is used by the subject to realize the action, the action description and the object of action. For example the first log indicates that Dr. Gregory House search Blood Glucose Measurements of the patient at 16:37 on 22th of July by using POWER2DM Shared Decision Making Application. By clicking on the link “See query/records”, patient may see the query and returned records. The button at the end opens a popup showing the full details of the audit record. From the upper panel, patient may query the logs for a specific time period. The query panel is extendible and further query parameters (e.g. subject, subject role, object, etc) will be shown if the panel is extended. The left panels provide an easy filtering mechanisms for main audit log elements like action types or subjects.

For audit record format, POWER2DM will conform to **FHIR AuditEvent resource definition**¹⁵ which is based on the IHE-ATNA Audit record definitions¹⁶, originally from RFC 3881¹⁷, and now managed by DICOM (see DICOM Part 15 Annex A5¹⁸). For the transportation of the audits, POWER2DM follow the normal FHIR Restful operations to store and access the records. Only patient will have the right to access the audit records, and POWER2DM confidential clients to create audit records.

The following table list the events that will be logged (audit events) in POWER2DM;

User Login	Whenever a POWER2DM user logs into the POWER2DM, the event will be logged.
User Logout	Whenever a POWER2DM logouts from the POWER2DM, the event will be logged.
FHIR Rest Operations	All Restful operations to Personal Data Store; patient record creation, update, search will be logged.
Authorization Requests (specific to Patient)	The Authorization and Policy manager will log the authorization requests from other users for a specific patient's records.
Prediction Service Operations	The Prediction Services will log each execution of the prediction models
Changes on Privacy Policies	The Authorization and Policy manager will log if the patient has updated his/her privacy management rules.

¹⁵ <https://www.hl7.org/fhir/auditevent.html>

¹⁶ http://wiki.ihe.net/index.php/Audit_Trail_and_Node_Authentication


¹⁷ <http://tools.ietf.org/html/rfc3881>




¹⁸ http://dicom.nema.org/medical/dicom/current/output/html/part15.html#sect_A.5


The code list given in the specification for the identification of events will be used as much as possible, while the audit event type and subtype codes specific to POWER2DM will be defined additionally.

Related with the identification of subject (who has done the action or access the data), the POWER2DM user identifier, the role of the user in POWER2DM or specific to patient, the identifier of the client that perform the action on behalf of the user, purpose of use will be logged in the audit record.

Related with the identification of object (which record, whose records, etc), varying based on the audit event, the identifier of the record, the identifier of the patient (PIP), or the query itself may be logged.



 My Profile
  My Privacy
  Access Logs

 [Sign out](#)

Filters (Audit Event)

☒ Records Access/Update

☒ Search records
 ☒ Read record
 ☒ Save record

☒ Authentication Related

☒ Login
 ☒ Logout

Filters (Subject)

☒ Me
 ☒ Dr. Gregory House
 ☐ Susan White
 ☐ Brenda Previn
 [See others](#)








POWER2DM Audit Event Logs 7

Start...









End...

Search

Today, 22th July Friday

16:37	Dr. Gregory House	(by POWER2M SDM App)	Search records	Blood Glucose Measurements	See query/records	
16:34	Dr. Gregory House	(by POWER2M SDM App)	Read record	Condition	See record	
16:32	Dr. Gregory House	(by POWER2M SDM App)	Search records	Diabetes Anamnesis Records	See query/records	
16:30	Dr. Gregory House	(by POWER2M SDM App)	Authorization Request			
12:13	Anna (You)	(by POWER2M SMSS Mobile App)	Save record	Stress VAS	See record	
12:12	iHealth Align		Save record	Blood Glucose Measurement	See record	
12:11	Anna (You)	(by POWER2DM SMSS Mobile App)	Login			

Yesterday, 21th July Thursday

19:41	Anna (You)	(by POWER2M SMSS Mobile App)	Save record	MedicationAdministration	See record	
19:40	Anna (You)	(by POWER2M SMSS Mobile App)	Search records	ProcedureRequest	See query/records	
19:40	Anna (You)	(by POWER2M SMSS Mobile App)	Search records	Blood Glucose Measurements	See query/records	
19:40	Anna (You)	(by POWER2M SMSS Mobile App)	Search records	Dietary Intake Logs	See query/records	
12:32	Anna (You)	(by POWER2DM Privacy Manager)	Logout			
12:30	Anna (You)	(by POWER2DM Privacy Manager)	Access to Audits			
12:29	Anna (You)	(by POWER2DM Privacy Manager)	Change privacy settings			
12:19	Anna (You)	(by POWER2DM Privacy Manager)	Login			

[Older logs](#)

Figure 10 Mockup for Audit View UI

3.6 Details on Other Security and Privacy Enablers

3.6.1 Communication Security and Node-to-Node Authentication

X509 Public Key Infrastructure (PKI) will be used to ensure the communication security and node-to-node authentication among the POWER2DM deployment units (a single or group of POWER2DM components). A public-private key pair and corresponding X509 v3 certificate will be generated for POWER2DM system as a root certificate (either as self-signed certificate or issued by a certificate authority). The X509 certificates for all POWER2DM deployment units will be issued by this root POWER2DM certificate and in this way trust chain will be established among them. The Authenticate Node transaction (ITI-19) of the IHE Audit Trail and Node Authentication (ATNA)¹⁹ specification will be implemented for node-to-node authentication between two POWER2DM deployment units. The ATNA integration profile refers the base standards; TLS and X509 with some further specifications (e.g. require support for TLS_RSA_WITH_AES_128_CBC_SHA chipersuit, etc).

3.6.2 Security at Rest

The MongoDB Community Server²⁰ will be used as the database technology to store the personal lifestyle health records and other contextual data. The database will have only one user which will be the POWER2DM PDS component and the X509 certificate based authentication will be applied for this user to access the collections (See <https://docs.mongodb.com/manual/core/authentication/>). Recommended configuration hardening and network hardening procedures will be applied for the production environment (pilot application deployments). In addition, TLS will be used to encrypt all MongoDB's network traffic.

For data availability and data redundancy, MongoDB Replication mechanism²¹ will be used. In addition to primary node, two secondary nodes (one as arbiter) will be used for replication. Internal authentication mechanisms provided by MongoDB will be used to protect the communication among these database nodes.

3.6.3 Other Mitigations for Security Threats

There are a number of further IT measures that can be taken to secure the Power2DM environment. The following IT measures are in scope:

- Use of state of the art protection of the Power2DM web applications/services;
- Use of state of the art firewall;
- Validation of input for malformed XML/JSON, and for corruption on content.
- Use of secure, certified data centre(s) for hosting servers;

To secure the Power2DM web applications/services a web application firewall is an effective security measure. A web application firewall is (or WAF) is a shielding safeguard intended to protect applications accessed via HTTP and HTTPS against attack. WAFs focus primarily on Web server protection at Layer 7 — the application layer — but they may include safeguards against other known forms of attack. These tools do not typically protect against unpatched vulnerabilities in commercial products, which is the domain of network- and host-based intrusion prevention systems. Instead, they focus on classes of "self-inflicted" vulnerabilities in configured commercial applications or in custom-developed code that makes Web applications subject to attacks, such as cross-site scripting, directory traversal and forced URL browsing. A WAF operates as a shield and does not "fix" the underlying

¹⁹ http://wiki.ihe.net/index.php/Audit_Trail_and_Node_Authentication

²⁰ <https://www.mongodb.com>

²¹ <https://docs.mongodb.com/manual/replication/>

vulnerability, although developers can use WAF reporting as a guide to what requires remediation. WAFs are most often deployed in front of Web servers, usually in the data centre. The best way to secure web applications is to ensure that they have no vulnerabilities before enabling them to run in production.

Guidelines for use of WAF's:

- If the web applications/services have been developed properly and there are no “vulnerabilities” in the software, adding a WAF has no added value;
- Using a WAF is only necessary if the application software has certain vulnerabilities;
- Using a WAF does not solve the “vulnerabilities” in the web applications/services itself, but it protects the software against abuse;
- Using a WAF brings the generic infrastructure services and application management services together;
- Using a WAF change does not change the web applications/services software itself;
- Using a WAF solves the OWASP top 10 problems for the web applications/services.

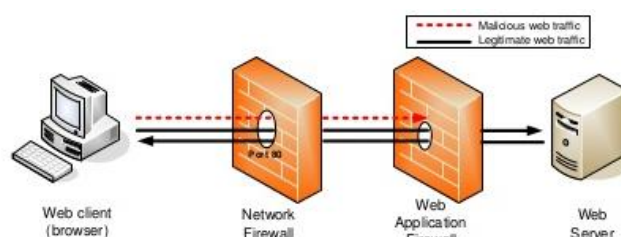


Figure 11 Use of WAF to protect malicious web traffic

Another required solution is using a firewall which acts as a barrier between a trusted network and other untrusted networks, such as the Internet. A firewall controls access to the resources of a network through a positive control model. This means that the only traffic allowed onto the network defined in the firewall policy. All other traffic is denied. The earliest firewalls functioned as packet filters, inspecting the packets that are transferred between computers on the Internet. When a packet passes through a packet-filter firewall, its source and destination (IP) address, protocol, and destination port number are checked against the firewall's rule set. Any packets that aren't specifically allowed onto the network are dropped.

So a firewall is a security device that can be a software program or a dedicated network appliance. Next-generation firewalls (NGFWs) are created in response to the evolving sophistication of applications and malware. Application and malware developers have largely outwitted the long-standing port-based classification of traffic by building port evasion techniques into their programs. Today, malware piggybacks these applications to enter networks and became increasingly networked themselves (connected to each other on the computers they individually infected).

NGFWs act as a platform for network security policy enforcement and network traffic inspection. Per technology research firm Gartner Inc., They are defined by the following attributes:

- Standard capabilities of the first-generation firewall: This includes packet filtering, stateful protocol inspection, network-address translation (NAT), VPN connectivity, et cetera.
- Truly integrated intrusion prevention: this includes support for both vulnerability-facing and threat-facing signatures, and suggesting rules (or taking action) based on IPS activity. The sum of these two functions collaborating via the NGFW is greater than the individual parts.
- Full stack visibility and application identification: ability to enforce policy at the application layer independently from port and protocol.
- Extra firewall intelligence: ability to take information from external sources and make improved decisions. Examples include creating blacklists or whitelists and being able to map traffic to users and groups using active directory.
- Adaptability to the modern threat landscape: support upgrade paths for integration of new information feeds and new techniques to address future threats.

- In-line support with minimum performance degradation or disruption to network operations.

Use firewall technology for the Power2DM servers can be used in the webserver layer and the application/service layer.

In order to protect the REST services, the application/service layer must contain logic to validate for malformed XML/JSON and to validate the content of input on corruption. This means that additional software programming effort is required for validation of the XML/JSON structure. The software code runs on servers of the application. Another validation is performed on the content of the input of the applications/services on corruption. This must secure the application/service layer for processing non-secure content in the XML/JSON structure. This validation will also take place in the application/service layer.

In order to secure the POWER2DM servers itself (physical for stealing, and prevent any illegal connectivity) the servers will be hosted in a professional and certified data centres. These data centres have strict policies for getting physical access to the data centre.