Information security in eHealth systems

Marošević, Hristina

UNIVERSITY OF ZAGREB

FACULTY OF ELECTRICAL ENGINEERING AND COMPUTING

Hristina Marošević

Information security in eHealth systems

SPECIALIST THESIS

Zagreb, 2022

UNIVERSITY OF ZAGREB

FACULTY OF ELECTRICAL ENGINEERING AND COMPUTING

Hristina Marošević

Information security in eHealth systems

SPECIALIST THESIS

Supervisor: prof. dr. sc. Boris Vrdoljak

Zagreb, 2022

SVEUČILIŠTE U ZAGREBU

FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

Hristina Marošević

Informacijska sigurnost u sustavima elektroničkog zdravstva

SPECIJALISTIČKI RAD

Mentor: prof. dr. sc. Boris Vrdoljak

Zagreb, 2022.

Committee for Specialist Thesis Evaluation:

1. Associate Professor Miljenko Mikuc, PhD - Chair
2. Professor Boris Vrdoljak, PhD - Mentor
3. Adjunct Assistant Professor Miroslav Končar, Phd, Phillips d.o.o. – Member

Specialist Thesis Defence Committee:

1. Associate Professor Miljenko Mikuc, PhD - Chair
2. Professor Boris Vrdoljak, PhD - Mentor
3. Adjunct Assistant Professor Miroslav Končar, Phd, Phillips d.o.o. – Member

Date of Public Defence: 25 February 2022

Table of Contents

1. Introduction

With the introduction of Internet and expansion of IT (Information Technologies), demand for eHealth (electronic Health) services has raised to the scale that almost every developing country is using eHealth systems.

Furthermore, the need for interoperability of different eHealth systems motivated healthcare professionals and industry to establish the international initiative IHE (Integrating the Healthcare Environment). IHE addresses specific clinical needs using well-known standards thus defines and recommends specifications to provide more secure, effective, coordinated, and synchronized processing, transmission, and usability of medical information in computer systems.

Security in integrated health environments is crucial for keeping patient health and related information safe from unauthorized use. However, there are no security measures that can prevent the potential misuse of protected health information by those who are authorized to gain access to it. These possibilities raise needs of a distributed governance and accountability in integrated and protected eHealth environments. IHE defines specific profiles to address these issues in integrated environments with custom but standardized settings where patient's specific preferences about using their health information is also enabled.

The main goal of this thesis is to give insight in high-level definitions of security related IHE ITI (Information Technology Infrastructure) profiles, and their implementation explained by use cases which meet security requirements i.e., confidentiality, integrity, availability, authenticity, authorization, and non-repudiation by using different standards and norms.

The content of this thesis is structured in four main chapters. In the chapter "Electronic health (eHealth) and IHE (Integrating the Healthcare Enterprise)" terms "eHealth" and "IHE" along with the purpose of these concepts are explained in detail. Security requirements and guidelines for those environments are introduced in chapter "Security

in eHealth and IHE environment". In chapter „Security related IHE ITI (Information Technology Infrastructure) profiles", IHE technical frameworks and more concrete IHE ITI security related profiles are discussed, and implementation examples are given in chapter "Use cases". Summary and proposal for further investigation are given in the last chapter "Conclusion".

2. Electronic health (eHealth) and IHE (Integrating the Healthcare Enterprise)

2.1. Electronic Health (eHealth)

In general, the result of opportunities and challenges created by Internet and accepted by the traditional healthcare information technology industry can be considered as one of directions towards the definition of eHealth. To give a specific definition of eHealth is as hard as it is to define Internet due to its constantly moving and dynamic environment although its use is mostly recognizable. Additional reason which complicates the definition of the term eHealth is that it is not used only by academic institutions, but also by industry leaders, professional bodies, funding organizations, marketing people and individuals, having different perspectives upon it.

So far, some simple and intuitive definitions, often used to describe eHealth are [1]: “The use of Internet technology in the delivery of health care” or “Integration of the Internet into health care”.

One comprehensive definition of eHealth considering more aspects than the field of IT and medicine is given by Gunther Eysenbach [2]: “eHealth is an emerging field in the intersection of medical informatics (discipline at the intersection of information science, computer science and health care [3]), public health and business, referring to health services and information delivered or enhanced through the Internet and related technologies. In a broader sense, the term characterizes not only technical development, but also a state-of-mind, a way of thinking, an attitude, and a commitment for networked, global thinking, to improve health care locally, regionally, and worldwide by using information and communication technology”.

Within this definition, ten more meanings than just “electronic” are proposed for the letter “e” in the term eHealth i.e., “efficiency”, “enhancing quality”, “evidence based”, “empowerment”, “encouragement”, “education”, “enabling”, “extending”, “ethics”, “equity” which are explained as:

- Efficiency i.e., increased efficiency in health care is one of the promises of eHealth, which should decrease the cost. Enhanced communication between health care establishments allowing patient involvement decreases costs by avoiding duplicated and unnecessary diagnostic or therapeutic interventions.
- Enhancing quality of care is provided by comparing different health care providers, allowing consumers to contribute to the process of quality assurance and direct the patients streams to health care providers rated with the best quality.
- Evidence based interventions using scientific evaluation additionally increases the effectiveness and efficiency of eHealth services.
- Empowerment of consumers and patients by enabling patient-centered medicine and evidence-based patient choice served by knowledge bases of medicine and personal electronic records.
- Encouragement of patient-healthcare professional relationships with the intention to improve decision-making in shared manner.
- Education of physicians and consumers. Continuous medical education and training for physicians and health education and preventive information for consumers.
- Enabling communication and information exchange between health care establishments in standardized way.
- Extending the geographical as well as conceptual scope of eHealth giving opportunities to consumers to obtain simple advices and very complex interventions online and from global providers.
- Ethics i.e., newly introduced ethical issues with many challenges and threats considering online professional practice, privacy and equity issues, informed consents, etc.
- Equity is another promise of eHealth, but it is still not clear how fast and if that can be achieved globally. People who do not have money, skills or access to computers cannot benefit from the eHealth services unless it is enabled by political measures.

Some other suggested meanings are: “easy-to-use”, “entertaining”, “exciting” which are not definite and give space to many more definitions to elucidate the scope and interpretation of eHealth.

2.2. IHE (Integrating the Healthcare Enterprise)

IHE is a global, non-profit initiative by healthcare professionals and industry, founded in the US in 1998 and motivated by RSNA (Radiological Society of North America) and HIMSS (Healthcare Information and Management Systems Society). Its vision is to enable seamless and secure access to health information that is usable whenever and wherever needed [4].

IHE is dedicated to improving interoperability in health care informatics and the way computer systems in healthcare, also HIT (Health IT) systems share information. However, it does not attempt to solve any issues involved in exchanging health information. It promotes an unbiased and coordinated use of established standards such as HL7, DICOM, CDA, OASIS, W3C, ISO, IETF, IEEE, etc., and supports their unambiguous usage defined in IHE integration profiles also known as system implementation guides meeting specific clinical needs.

IHE implementation strategy is to offer pragmatic, flexible i.e., not dependent on architecture, and applicable approach of interoperability in different use cases [5]. Thus, IHE implementation framework provides standards-based communication between disparate clinical information systems and otherwise unaffiliated care providers with the main goal to efficiently deliver optimal health care while effectively using EHR (Electronic Health Record).

IHE is organized across a growing number of clinical and operational domains [6]:

- IHE Cardiology (CARD)
- IHE Dental (DENT)
- IHE Devices (DEV)
- IHE Endoscopy (ENDO)
- IHE Eye Care (EYECARE)
- IHE IT Infrastructure (ITI)
- IHE Pathology and Laboratory Medicine (PaLM)
- IHE Patient Care Coordination (PCC)

- IHE Pharmacy (PHARM)
- IHE Quality, Research and Public Health (QRPH)
- IHE Radiation Oncology (RO)
- IHE Radiology (RAD)
- IHE Surgery (SURG)

Each domain publishes its own technical framework in coordination with other IHE domains. IHE technical frameworks specify the technical details of included IHE integration profiles and are used as guides for implementing the concrete IHE functionality. Organization of the technical framework is shown on figure 2.1.

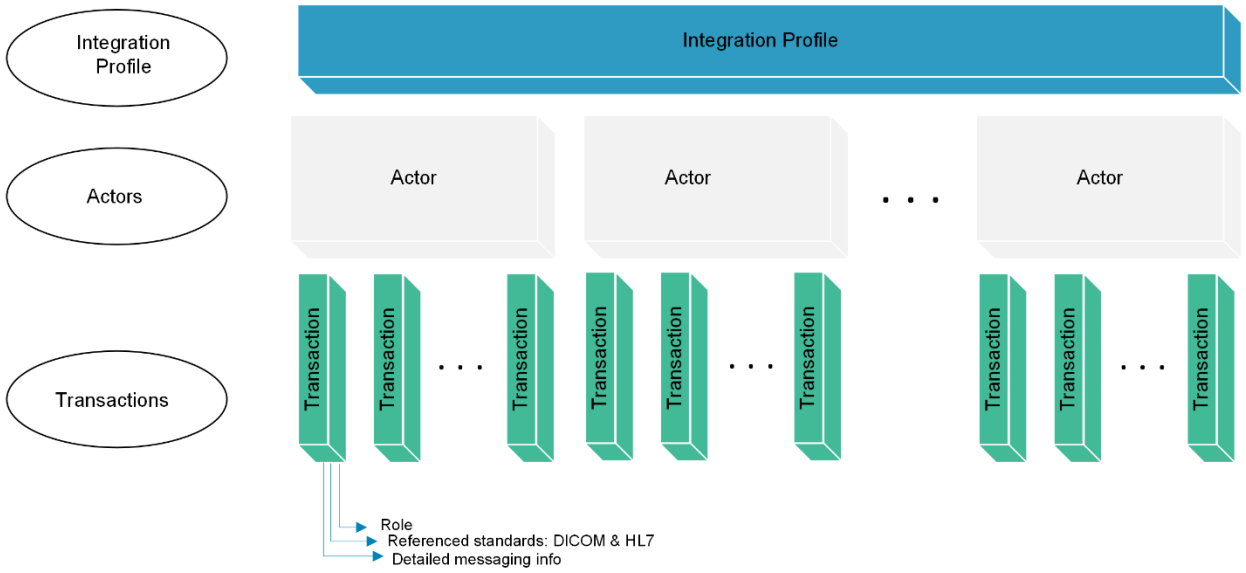

Figure 2.1. Organization of the technical framework [7]

Technical frameworks are published in volumes. Within the first volume specific key concepts i.e., integration profile with the associated actors and transactions are described along with use cases and conformance requirements. Second volume specifies the implementation and definition of transactions within the specific IHE integration profile.

Third volume gives instructions on related document sharing metadata and content profiles while last volume is reserved for national or regional adjustments or extensions.

The number of IHE integration profiles and the content of technical frameworks is not finite and is continuously changing. Initially, each profile is published for public comments and after addressing reviewed comments is republished for trial implementation and used only in the IHE implementation testing process. After criteria for passing the test are successfully met, the profile is published as final text and joined to the specific domain's technical framework.

IHE integration profiles describe workflow use cases, standards, and relationships to achieve transparent interoperability [7]. They describe the communication between systems but do not specify the implementation within systems. In the process of solving a specific integration problem IHE integration profile use actors to describe set of application roles within the system and transactions with their unique identifier containing one or more interactions and set of messages and protocols to describe their communication in a specific scenario.

Implementation of IHE integration profiles can be tested annually on structured vendor-to-vendor testing event, known as Connectathon, supervised by neutral IHE technical project management team. Participants use testing software developed for IHE by contractors, such as GAZELLE as a preparation for this event. During a Connectathon systems exchange information, performing transactions required for the actors used within specific interoperability use cases i.e., integration profiles. As a result, Connectathon gives detailed validation of the vendor's interoperability and compliance with IHE integration profiles. This process is illustrated on Figure 2.2.

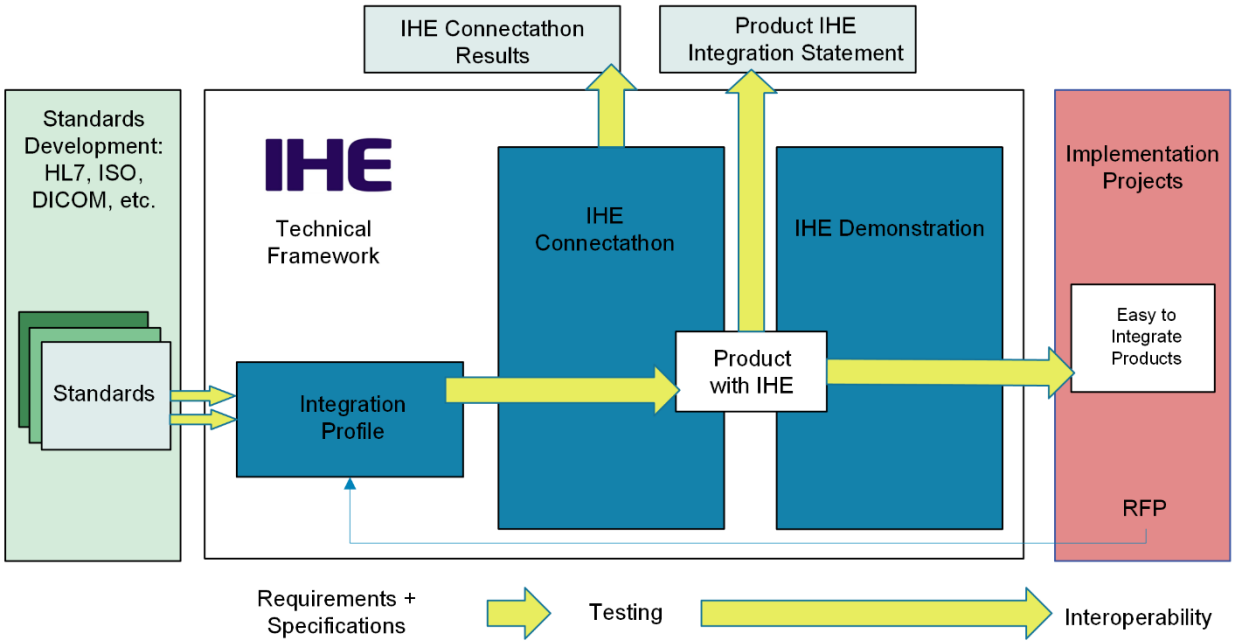

Figure 2.2. IHE process [7]

Projectathon, a testing session is organized for more specific scenarios i.e., business use cases for a specific deployment project using a set of IHE integration profiles. Participants test compliance and interoperability of their systems or solutions against the specification for interoperability of the deployment project, based on IHE integration profiles. Testing criteria is defined by the organization who has the lead of the project which publishes results at the end of this session and forwards them to IHE team.

At the end of these events, vendor can publish integration statement containing information about IHE integration profiles supported by a specific release of a specific product in case of satisfactory results. This information is stored in the IHE product registry and help vendors to be easily recognized by end-users and other participants in eHealth implementation projects.

Finally, all stakeholders benefit from IHE in some way. For health providers it is the improved workflow of health information, decreased possibilities for errors and reduced implementation costs. Vendors have decreased cost and complexity of interface

installation and management and aligned product interoperability with industry consensus which allows them to focus more on competition regarding functionality. Standardization bodies benefit from the rapid feedback on IHE adjustment and their widespread adoption.

3. Security in eHealth and IHE environment

IHE's main objective is to address specific aspects of healthcare information exchange by integration profiles, solving interoperability problems through implementation of standards, whether the exchange of healthcare information takes place within affiliated or between unaffiliated care providers. Each integration profile solves part of the extensive set of challenges of the healthcare information exchange but does not address policy choice and governance for implementing communities. While there is an existing definition for each integration profile, the definition of service specifications, application, and operating system functionalities and specifications, system design, organizational plans, physical or network controls is community-specific and is not provided by IHE. IHE integration profiles enable security and privacy and are policy sensitive but do not define them. Implementing communities need to define and implement their policies and to conduct appropriate risk analysis and risk management. IHE recognizes that as an important element of the eHealth system implementation and gives some guidance on the policy building activities, supported by security and privacy related IHE integration profiles defined within the IHE ITI domain.

The policy environment consists of many layers of policies, working in an interlocking hierarchy. On the top of that hierarchy are international policies under which are country-specific or region-specific policies. Horizontal policies are applied to specific industries such as the medical professional society. Finally, within the enterprise there are IT policies. Underlying policy landscape for each community participating in the eHealth should be strictly defined before it is built.

Community policies must be harmonized with the policies applied in the local healthcare enterprises connected to the community. Different community policies should exist to define [8]:

- Who has access and to what type of documents in the community
- Who is allowed to publish documents in the community

- Acceptable types of documents that may be published in the community
- User provisioning and de-provisioning within the community and local operation
- Acceptable user authentication methods
- Acceptable third-party access
- Secondary use of the information in the community
- Period within which information should be maintained in the community
- Acceptable network use
- Security and data privacy training and awareness plans
- Acceptable risk levels within the community
- Sanctions that need to be taken for individuals who violate the policies within the community
- Backup and recovery planning
- Availability of the community systems
- Maintenance downtime
- Emergency modes needed in different use cases:
    - Natural catastrophe
    - Utility failure
    - IT infrastructure failure
    - Break-glass use cases i.e., need for privilege elevation due to a patient emergency
    - Overriding a patient specific privacy block due to a real danger for that patient

Security and privacy requirements for eHealth systems implemented by IHE compliant communities are addressed by security related IHE ITI integration profiles. Recommended common set of security and privacy technical IT controls based on the experience of the IHE implementing communities are [8]:

- Audit log controls
- Identification and authentication
- Data access controls

- Secrecy controls
- Data integrity controls
- Non-repudiation controls
- Patient privacy controls
- Availability controls

Relation between these security controls and supporting security related IHE ITI integration profiles is given in table 3.1.

Table 3.1. Relationship between security related IHE ITI profiles and common set of security controls [8]

	Audit Log	Identification /Authentication	Authorization	Secrecy	Integrity	Non-repudiation	Patient Privacy
Audit Trail and Node Authentication	x	x	x	x	x	x	x
Consistent Time	x	.				x	
Enterprise User Authentication		x	.			.	.
Internet User Authorization		x	x			.	.
Cross-Enterprise User Assertion		x	.			.	.
Basic Patient Privacy Consents			.				x
Mobile Care Services Discovery		x	.			.	
Personnel White Pages		x	x			.	
Healthcare Provider Directory		x	.			.	
Document Digital Signature		x			x	x	
Document Encryption			x	x	.		

Columns of the table represent security controls from the common set while rows represent security related IHE ITI profiles. Symbol “x” in the intersection of a security related IHE ITI integration profile and a security control indicates a direct relationship between the specific security control and the profile i.e., application of the specific security control is supported by the profile. Symbol “**.**” in the intersection of a security related IHE ITI integration profile and a security control indicates an indirect relationship between the specific security control and the profile i.e., application of the specific security control is assisted by the profile.

More details about security related IHE ITI integration profiles are given in the next chapter.

4. Security related IHE ITI (Information Technology Infrastructure) profiles

IHE security and privacy model includes security while enabling flexible and safe provision of healthcare by offering security related IHE ITI integration profiles, leveraging security controls in the local eHealth system.

Within the “Security Considerations” section in the technical framework of any IHE integration profile defined are application of security related IHE ITI integration profile, other security requirements, risks that should be mitigated by the recommended security related IHE ITI integration profile and open risks that need to be addressed by system development or system deployment. This section may appear in the first and in the second volume of the technical framework. In the first volume it applies to whole profile, while in the second volume it gives transaction-specific security considerations.

Security related IHE ITI integration profiles are defined within the ITI IHE domain. At the time of writing this thesis, actual list of security related IHE ITI integration profiles include:

- Audit Trail and Node Authentication (ATNA) profile provides basic security through functional access control, defined security audit logging and secure network communication
    - This profile is published as final text
- Consistent time (CT) profile synchronizes clocks between computers within a network with median error less than one second
    - This profile is published as final text
- Enterprise User Authentication (EUA) profile enables single-sign-on within an enterprise
    - This profile is published as final text
- Internet User Authorization (IUA) profile provides user authorization for RESTful interfaces
    - This profile is published for trial implementation and is subject to changes

- Cross-Enterprise User Assertion (XUA) profile provides communication of claims of the authenticated entity across enterprise boundaries i.e., federated identity
    - This profile is published as final text
- Basic Patient Privacy Consents (BPPC) profile provides recording and enforcing patient privacy consents
    - This profile is published as final text
- Advanced Patient Privacy Consents (APPC) profile extends BPPC and provides structural representation of a patient privacy policy
    - This profile is published for trial implementation and is subject to changes
- Secure Retrieve (SeR) profile defines a framework enabling the use of centralized access control in XDS (Cross-Enterprise Document Sharing) environments
    - This profile is published for trial implementation and is subject to changes
- Mobile Care Services Discovery (MCSD) profile provides RESTful interface to discover healthcare organizations, locations, practitioners, and services
    - This profile is published for trial implementation and is subject to changes
- Personnel White Pages (PWP) profile provides access to basic human workforce user directory information
    - This profile is published as final text
- Healthcare Provider Directory (HPD) profile provides management of healthcare provider (individual and organizational) information in a directory structure
    - This profile is published for trial implementation and is subject to changes
- Document Digital Signature (DSG) profile specifies the use of digital signatures for documents shared between organizations
    - This profile is published as final text
- Document Encryption (DE) profile provides a means to encrypt documents independently of transport, healthcare application or healthcare document type
    - This profile is published for trial implementation and is subject to changes

Stable profiles commonly used in document sharing scenarios to help the definition of accountability i.e., audit control and access control models are ATNA, BPPC and XUA.

Different policies may be applied by organizations in an interoperable way using these profiles. Therefore, these profiles enable the use of policies but do not define them.

Primary method of accountability enforcement is audit control. This basic security principle is provided by the security related IHE ITI integration profile ATNA. ATNA requires:

- User authentication and access control
- Security audit logs
- Strong network authentication and communication encryption

All security measures established by meeting these requirements along with the applied policies and procedures (defined within the enterprise/community/organization/local healthcare provider) provide the common set of security controls: audit log, authentication, authorization/access control, secrecy/confidentiality, integrity, non-repudiation, and patient privacy. One system with enforced audit and access controls can be connected to other systems enforcing the common policies which leads to forming a base of the chain of trust through accountability.

In IHE document sharing environments, access control can be defined in different ways and by different sources. First is the definition of functional roles and their privileges which can be overwritten by the patient's requirements about its medical information created, processed, stored, and transmitted within a specific community.

Patient information confidentiality can be further categorized by different levels of confidential information to instruct their proper handling within an eHealth system. Security/privacy classification of clinical document i.e., confidentiality level of the contained information is defined within the confidentialityCode field also known as content sensitivity. This is a security/privacy concept built into almost all healthcare standards such as HL7 CDA, FHIR, etc. and can be combined with the functional roles defined within an eHealth system thus facilitate the definition and usability of access control policies. In such cases RBAC (Role Based Access Control) makes decisions based on the document sharing metadata i.e., sensitivity explained by condifentialityCode. An example of access

control policies in Opt-in healthcare environment (where patient explicitly agrees on sharing clinical documents within the community) is given in table 4.1.

Table 4.1. Example of access control policies in Opt-in scenario [8]

	U	L	M	N	R	V
Administrative Staff		✓	✓			
Dietary Staff			✓			
General Care Provider			✓	✓		
Direct Care Provider			•	•	•	•
Emergency Care Provider				•		
Researcher	•					
Patient or Legal Representative		•	•	•	•	

Rows of the table represent functional roles. Columns of the table represent value of confidentialityCode. Confidentiality levels are defined using HL7 confidentialityCode vocabulary: U – unrestricted, L – low, M – moderate, N – normal, R – restricted, V – very restricted. As discussed so far, sensitivity is self-describing meaning that confidentialityCode is defined within the medical document. Functional roles are defined within a community and can be also conveyed from the requesting community by using integration profiles such as IUA (Internet User Authorization) or XUA (Cross-Enterprise User Assertion) which provide definition of the user and the privacy/security context of the request. Other than confidentialityCode, purposeOfUse can be also carried within the request explaining what the user intends to use the data for which may or may not be permitted by the source system's security policy.

Privacy policies can navigate the results of applied access control rules based on any user context, patient identity or document metadata. Another important concept considered for document sharing, using that functionality is patient privacy consent. Community or

individual requesting medical information can be fully authorized or not authorized at all to receive, collect, use, or disclose it. Some examples of such policies are [8]:

- Explicit Opt-in enabling document sharing (patient gives consent for sharing medical information)
- Explicit Opt-out stopping document sharing (patient does not agree on sharing medical information)
- Implicit Opt-in allowing document sharing
- Explicit Opt-out for sharing medical information outside of local healthcare provider, but allowing emergency i.e., break-the-glass
- Explicit Opt-out for sharing medical information outside of local healthcare provider, not allowing emergency i.e., break-the-glass
- Explicit authorization for specific research project(s)
- Changing consent policy from Opt-in to Opt-out

BPPC profile enables the use of basic patient privacy consent controls considering and applicable to defined policies within a community. APPC profile addresses more complex rules specific to a basic patient privacy consent by offering the ability to include deviations in structured and coded format. Whatever is defined using BPPC and/or APPC, use of IUA or XUA and ATNA is necessary. IAU and XUA are important regarding identity and security/privacy context while ATNA ensures governance on appropriate use of medical information within and between trusted document sharing domains.

ATNA, BPPC and XUA integration profiles are widely used for accountability in IHE environments. Therefore, their technical frameworks will be explained in the next chapters.

4.1. ATNA (Audit Trail and Node Authentication)

Using ATNA profile only cannot offer overall security. This profile does not define cybersecurity requirements which affect the privacy and security governance but assumes it is well established. Implementation of this profile requires support of specifically defined security controls on management, operational and technical level of governance and adequate system security services.

In ATNA profile any local or enterprise-wide healthcare information systems managing, or processing PHI (Protected Health Information) are involved.

ATNA profile specifies foundational privacy and security elements such as:

- Node authentication
- User authentication
- Authorization i.e., access control
- Audit event logging
- Secure communication

Node authentication enables mutual authentication of server and client systems. Mutual authorization of server and client systems is also enabled by ATNA but is not enforced. Local governance policies should decide if access control on machine level is going to be used.

When using ATNA, participating users must be identified and authenticated. These identities are used within the audit event logs to identify users and by required access control (along with other information) to decide which information and system services is the user authorized to gain access to. These identities are not used only for audit, authentication, and authorization, but may be also utilized by some other system security services. Local governance policies should decide which authentication method will be employed. It is not required to be defined by IHE profile such as XUA or EUA. However, these methods can be used. Other non-IHE approaches are also permitted.

ATNA event audit logging provides surveillance function by capturing all detected security events, also system activity and transaction events used to define a baseline of normal operation. Detail level of system activity and transaction events is not specified by ATNA but should be sufficient to define normal operation and at the same time should not reveal PHI. ATNA profile specifies the standard events to be reported i.e., system activities-related events and IHE transactions-related events, and standard schema for encoding the reported events. All detected security events should be also logged. An audit record repository must be defined and implemented to collect and report on the event audit logs. TLS (Transport Layer Security) and UDP (User Datagram Protocol) are suggested as the two communication alternatives for transporting the event reports containing syslog messages from the reporting system to the audit record repository. Besides surveillance, forensic and workflow analysis logs may use ATNA schema and transactions due to the detection of suspicious activities and security events, and tight coordinated system controls, respectively. However, ATNA's event audit logging is not designed with that purpose.

TLS (Transport Layer Security) can provide secure communication allowing mutual authentication, reliable and private communication using encryption. Using this protocol is recommended but not enforced by ATNA. TLS mutual authentication is based on the use of private and public certificates. If it is used, root CAs (Certificate Authority) and trust chains in healthcare enterprises should not be the same as those commonly used in Internet applications satisfying certificate policies designed for financial risk reduction. Root CAs and trust chains in healthcare environments should support system authentication and need to be installed to any ATNA implementation so systems can be recognized within the local governance. While some other methods other than those specified by ATNA may be also used, TLS should exist within the implementations due to interoperability reasons. It should be implemented and available to be configured. Implementations should allow configuration of different protocols, algorithms, and other settings. Encryption may also not be used if some other way of communication protection is decided by the local governance policies.

ATNA actors and transactions are illustrated on figure 4.1.

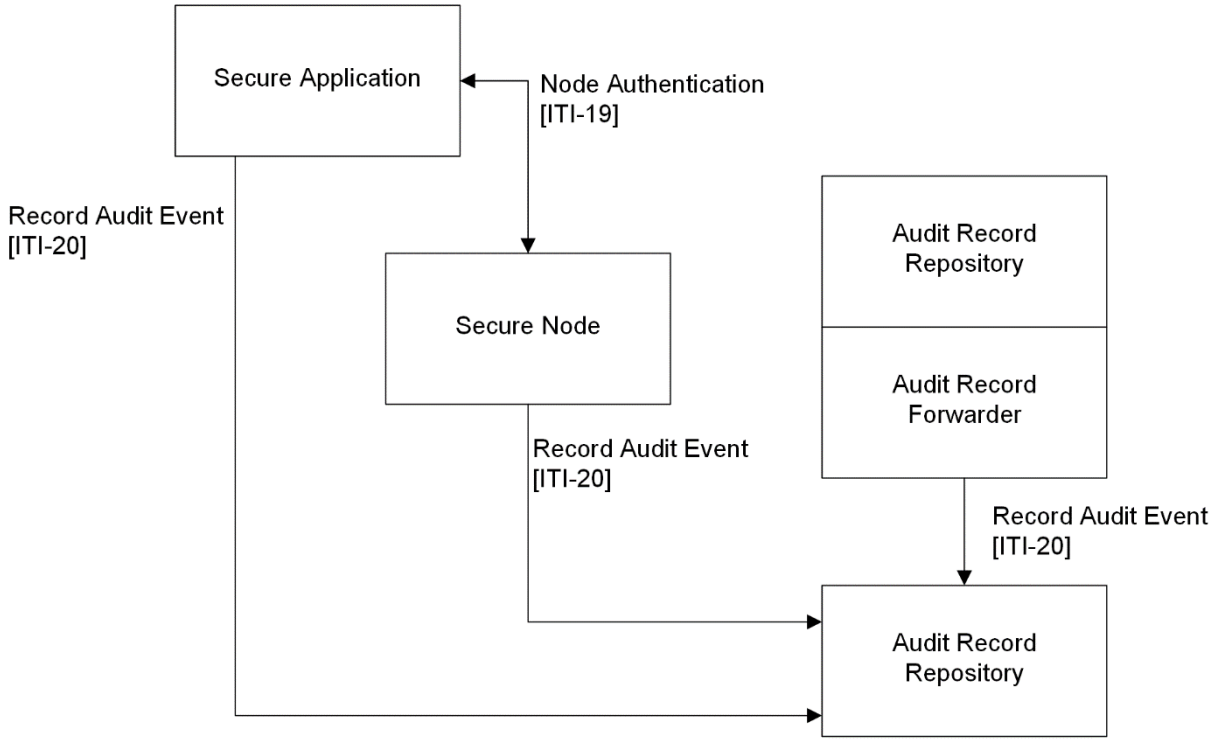

Figure 4.1. ATNA actors and transactions [9]

All requirements set by ATNA profile apply for all included actors from the figure 4.1. This means that secure application, secure node, audit record repository should offer authentication, access control, event audit logging and other security and privacy services.

Actor secure node represents a system providing security and privacy services for the whole stack from the hardware to the user interface and to the external communications. It should ensure that authentication, secure communication, security audit recording and security policy enforcement is performed for each aspect of that system by applied contractual controls. System architecture is not specified by ATNA and non-IHE components may be part of it and process PHI. In any scenario comprehensive risk

assessment should be conducted. Some security and privacy controls may not be applied in cases where risk analysis find their application as not necessary but documented list of those exceptions must exist. ATNA requirements for the secure node actor are:

- Using Authenticate Node [ITI-19] transaction for network connections to and from the secure node. This transaction protects private information from being exposed.
- Providing sufficient authentication methods decided on the base of the conducted risk assessment as a precondition for accessing the secure node. Only authorized users should access the secure node.
- Detecting and reporting event audit logs for activity-related and transaction-related events for the secure node as it is specified by Record Audit Event [ITI-20] transaction.

While secure node is responsible for the whole hardware and software stack, secure application should cover only IHE actors with which it is grouped, and functionality of the software and services secure application is providing. Security and privacy services such as authentication, secure communications, security audit recording and security policy enforcement should be provided only for those elements. Other components like operating systems, databases, and other parts of the environment out of the scope of the secure application are out of its control. ATNA requirements for the secure applications are very similar to those for the secure node:

- Using Authenticate Node [ITI-19] transaction for network connections to and from the secure application. This transaction protects private information from being exposed.
- Providing sufficient authentication methods as a precondition for accessing the secure application. Only authorized users should access the secure application.
- Detecting and reporting event audit logs for activity-related and transaction-related events for the secure application as it is specified by Record Audit Event [ITI-20] transaction.

Audit record repository's function is to receive and store event audit reports. ATNA profile does not specify the capacity of this repository as it may vary per deployment. Besides the capacity, capabilities for analysis and reporting are also not specified but are expected. Regarding repository implementation, it may be part of a federated network of repositories. ATNA requirements for the audit record repository are:

- Supporting at least one of the audit transport mechanisms (ATX) specified by [ITI-20]
- Capability of receiving at least one of the message formats specified by IHE (repository may or may not accept non-IHE messages due to backwards compatibility or other reasons)
- Providing local security and privacy services and user access control

This actor should be grouped with secure node or secure application.

Actor audit record forwarder should be grouped with audit record repository. Its function is to filter and forward selected messages received by the audit record repository to other (one or more) audit record repositories. ATNA requirements for this actor are:

- Grouping with secure node or secure application
- Grouping with audit record repository
- Filtering and forwarding selected messages as they arrive. Filtering and forwarding are specified by [ITI-20] and syslog RFC5424
- Availability of configuring forward settings for messages intended for destination audit record repository

To summarize the relationships between actors and transactions in ATNA specified by ATNA profile, given is list of actors and transactions related to each one of them in table 4.2.

Table 4.2. ATNA actors and transactions

Actor	Transaction	Optionality
Audit Record Repository	Record Audit Event [ITI-20]	R
Audit Record Forwarder	Record Audit Event [ITI-20]	R
Secure Node	Authenticate Node [ITI-19] Record Audit Event [ITI-20]	R R
Secure Application	Authenticate Node [ITI-19] Record Audit Event [ITI-20]	R R

For each actor in the first column, given is a list of transactions within the second column of the table along with its optionality in the third column. Optionality may be labeled “R” meaning required or “O” meaning optional support of the transaction is required by the specific ATNA compliant actor.

Support of a transaction specified by ATNA is achievable through actor options. ATNA specifies few options for each actor, depending on the transaction. Some of the options were mentioned while defining ATNA actors and concepts.
In the table 4.3. given is a current list of actors’ options which are protocol alternatives for [ITI-19] and [ITI-20] transactions. First column of the table represents an actor while second column contains the specific actor’s options. ATX and STX abbreviations in the second column are used to indicate audit transport and security transport protocol, respectively.

Table 4.3. ATNA actors' options

Actor	Options
Audit Record Repository	♦ ATX: TLS Syslog ♦ ATX: UDP Syslog
Audit Record Forwarder	♦ ATX: TLS Syslog ♦ ATX: UDP Syslog
Secure Node	♦ Radiology Audit Trail (for actors from IHE radiology domain profiles) ♦ FQDN validation of server certificate (RFC6125; DNS-ID should be contained within the subjectAltName field of the X.509 certificate) ♦ STX: no secure transport ♦ STX: TLS 1.2. Floor using BCP195 (highest level of cyber protection for TLS per IETF Best Current Practice) ♦ STX: S/MIME ♦ STX: WS-Security ♦ ATX: TLS Syslog ♦ ATX: UDP Syslog
Secure Application	♦ Radiology Audit Trail (for actors from IHE radiology domain profiles) ♦ FQDN validation of server certificate (RFC6125; DNS-ID should be contained within the subjectAltName field of the X.509 certificate) ♦ STX: no secure transport ♦ STX: TLS 1.2. Floor using BCP195 (highest level of cyber protection for TLS per IETF Best Current Practice) ♦ STX: S/MIME ♦ STX: WS-Security ♦ ATX: TLS Syslog ♦ ATX: UDP Syslog

In table 4.4. given are required groupings for ATNA actors. When grouping, ATNA actors should implement all required transactions within this profile in addition to all transactions required for the grouped actors. The same rule should be applied regarding the required content modules. In this case there are no content modules to bind to.

Table 4.4. Required ATNA actor groupings

ATNA actor	Profile / Actor to be grouped with
Audit Record Repository	Consistent Time / Time Client ATNA / Secure Node or Secure Application
Audit Record Forwarder	Consistent Time / Time Client ATNA / Secure Node or Secure Application ATNA / Audit Record Repository
Secure Node	Consistent Time / Time Client
Secure Application	Consistent Time / Time Client

In table 4.4. first column contains ATNA actors and required grouping actors from other profiles are given in the second column along with the profile they origin from. Requirements for groupings are defined within the ATNA profile and outside of it including actors from Consistent Time (CT) IHE integration profile [10].

When actors from other IHE profiles need to be grouped with ATNA actors such as secure node or secure application, all requirements specified by ATNA profile apply to all actors within the implementation.

4.1.1. ATNA transactions

Transactions included in ATNA profile are:

- Authenticate Node [ITI-19]
- Record Audit Event [ITI-20]

To explain the need for these transactions it is sufficient to understand the scope of the transaction together with roles included and integration diagrams illustrating the message flow.

4.1.1.1. Authenticate Node [ITI-19]

This transaction is used by ATNA secure node and secure application actors.

The scope of this transaction comprises of mutual secure node authentication and user authentication on the local secure node. Communication between the local secure node and remote secure node is preceded by identifying and authenticating local secure node to the remote secure node and vice versa after which any other secure transaction may be performed between them. Authentication of the user who requests access to a secure node does not require participation of a remote secure node and is a local operation. These interactions are shown on the figure 4.2.

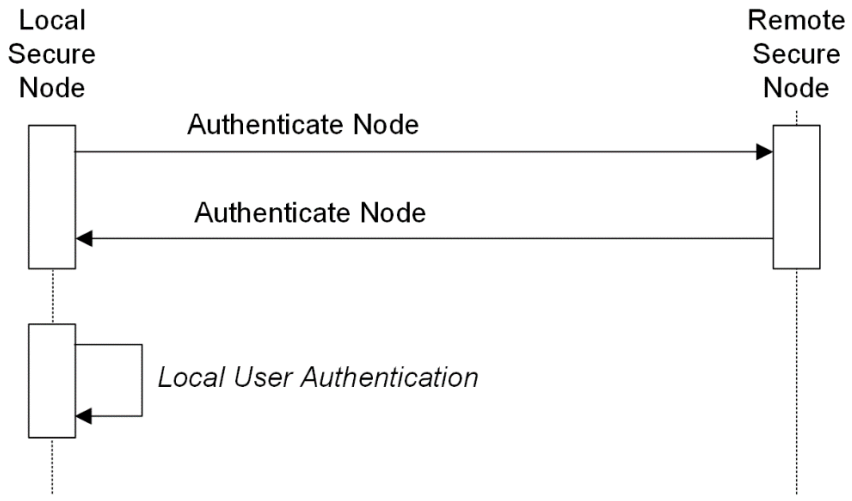

Figure 4.2. [ITI-19] interaction diagram [11]

The two use case roles defined within this transaction are used in the interaction diagram. These are:

- Secure node
- User

Role secure node is defined by activities of establishing secure connection between two nodes in a network, authenticating a user and authorizing a user to access the data and/or applications on the secure node.

Role user is defined by the user activity of attempting access to the data and/or applications within the secure node.

Standards referenced by this ATNA transaction, message formats, semantics and other details are given in the second volume of the technical framework [11].

4.1.1.2. Record Audit Event [ITI-20]

This transaction is used by all ATNA actors.

The scope of this transaction consists of reporting auditable events to an audit report repository. Interactions between ATNA actors within the scope of [ITI-20] transaction is shown on figure 4.3.

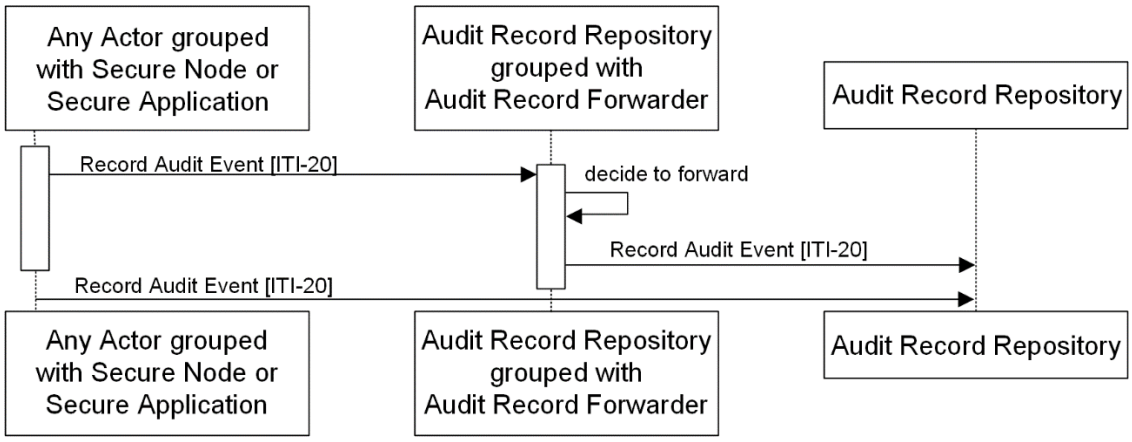

Figure 4.3. [ITI-20] interaction diagram [12]

The three actor roles defined within this transaction are used in the interaction diagram. These are:

- Role of any actor or any other application grouped with Secure Node or Secure Application
- Role of Audit Record Repository
- Role of Audit Record Forwarder

Role of any actor or any other application grouped with the secure node or secure application is to create and send audit record to the audit record repository.

Role of audit record repository is to receive and store the audit event report from the audit report creator.

Role of audit record forwarder actor is to forward the filtered audit report to audit record repository actor(s).

Audit report creator can be either any other application grouped with the secure node or secure application, or audit report forwarder actor. On the figure 4.3. illustrated are both scenarios.

Standards referenced by this ATNA transaction, message formats, semantics and other details are given in the second volume of the technical framework [12].

4.2. BPPC (Basic Patient Privacy Consents)

This profile provides the possibility for recording and enforcing patient privacy policy consents within a patient privacy policy domain e.g., an XDS (Cross-Enterprise Document Sharing) affinity domain. An XDS affinity domain is formed by a group of healthcare enterprises sharing the same infrastructure and working together according to a common set of policies. Both, healthcare providers and patients have benefits using this mechanism. Healthcare providers are able to develop privacy policies and implement them with different access control rules within the system. Patients have insight of the implemented policies to patients and are allowed to selectively control access to their healthcare information.

The BPPC integration profile can be used by all systems publishing and using clinical documents through IHE profiles, such as XDS [13], XDR (Cross-Enterprise Document Reliable Interchange) [14], XDM (Cross-Enterprise Document Media Interchange) [15] or XCA (Cross-Community Access) [16].

When BPPC profile is not implemented with XDS it is required that single policy is created and agreed per XDS affinity domain. This policy is distributed to all systems involved in the XDS affinity domain which enforce the policy by the implemented supporting access controls. BPPC integration profile requires an overall privacy policy of the XDS domain as a set of many patient privacy policies and provides a mechanism for defining a basic code vocabulary to identify those policies.

Patient privacy policies defined within the privacy policy domain may be individually used or be combined. Each of the patient privacy policies should contain a legal text, necessary for human interaction and should be given an identifier or OID (Object Identifier) which will be used in the computer logic. Patient privacy policy's OID should uniquely identify the specific policy, and the legal text contained by it should describe it. Within the legal text it should be precisely defined what is the acceptable use and re-disclosure uses of the policy, which functional roles may access which document, based on the level of sensitivity of the contained data and under which condition, etc. Some guidelines for writing the policies are given by IHE, but definition possibilities and content are not

specified [17]. Finally, when a patient agrees on the application of a specific policy to its healthcare information, a patient privacy policy acknowledgement should be generated. Patient privacy policy's OID should be referenced by the patient privacy policy acknowledgement document generated for the specific patient consent.

Diagram with actors and transactions specified by BPPC profile is given on figure 4.4.

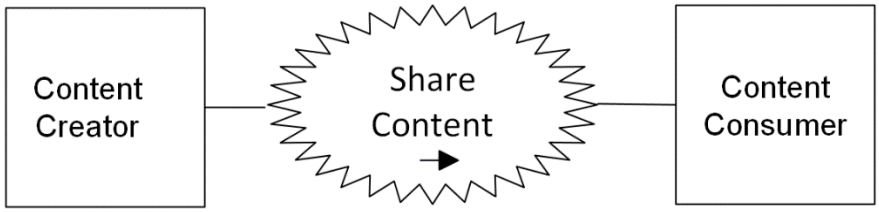

Figure 4.4. BPPC actors and transactions [18]

Two actors defined within this profile are content creator and content consumer. Content creator creates the BPPC content which should be received and used by the content consumer. Depending on the IHE integration profile combined with BPPC profile, content creator can be grouped with document source actor of the XDS or XDR profile, or XDM's portable media creator actor. The same way, content consumer actor from BPPC profile can be grouped with document consumer actor of XDS or XDR profile, content consumer actor of XDS-SD (XDS Scanned Document) profile (in cases when patient acknowledges a specific patient privacy policy by non-electronic signature which is stored as a scanned document) or with portable media importer actor of the XDM profile.

BPPC transaction depends on the IHE integration profile working together with BPPC profile. This means that all transactions between grouped actors should be implemented, respectively to the integration profile combined with BPPC. On the figure 4.4. all possible transactions are illustrated as "share content". BPPC as a content profile specifies only the encoding of the BPPC document so it can be transmitted using XDS, XDR or XDM transactions [19]. Currently, required specification of clinical documents in these scenarios

is HL7 CDA R2. Options for each actor to support any of possible transactions carrying the BPPC document is given in table 4.5.

Table 4.5. BPPC actors' options

Actors	Option
Content Creator	Basic Patient Privacy Acknowledgement Basic Patient Privacy Acknowledgement with scanned document
Content Consumer	Basic Patient Privacy Acknowledgement View

In the table 4.5. BPPC actors are given within the first column. In the second column are specified required options for the respective actor in column "Actors". Basic patient privacy acknowledgment is also some clinical document and options specified for content creator define the information that should be possible to be added by this actor:

- Effective time of the acknowledgement
- OID/OIDs of acknowledged patient privacy policy/policies
- Text description of the patient privacy policy
- Scanned document with signature of the patient

All this information should be readable and displayed by the content consumer actor.

Example of HL7 CDA R2 patient privacy policy acknowledgement document is given bellow:

```
<ClinicalDocument xmlns='urn:hl7-org:v3'>
  <typeId extension="POCD_HD000040"
  root="2.16.840.1.113883.1.3"/>
  <templateId root='1.3.6.1.4.1.19376.1.5.3.1.1.1'/>
  <templateId root='1.3.6.1.4.1.19376.1.5.3.1.1.7'/>
  <id root=' ' extension=' '/>
```

```
  <code code='57016-8' displayName='PATIENT PRIVACY
ACKNOWLEDGEMENT' codeSystem='2.16.840.1.113883.6.1'
codeSystemName='LOINC'/>
  <title>This is a patient consent</title>
  <effectiveTime value='20211111012005'/>
  <confidentialityCode code='N' displayName='Normal'
    codeSystem='2.16.840.1.113883.5.25'
codeSystemName='Confidentiality' />
  <languageCode code='en-US'/>
     :
  <component><structuredBody>

  </structuredBody></component>
</ClinicalDocument>
```

LOINC code for these documents is 57016-8 with description “Privacy Policy Acknowledgement Document” and the code system is 2.16.840.1.113883.6.1. OID 1.3.6.1.4.1.19376.1.5.3.1.1.1 is template ID for IHE medical document and OID 1.3.6.1.4.1.19376.1.5.3.1.1.7 is template for IHE ITI BPPC document with no scanned part.

Within an HL7 CDA R2 clinical document header all patient consents with same effective time, given by that document should be identified. The template ID for service event recording a patient privacy policy acknowledgement is defined by IHE OID 1.3.6.1.4.1.19376.1.5.3.1.2.6. An example is given bellow:

```
<documentationOf typeCode='DOC'>
  <serviceEvent classCode='ACT' moodCode='EVN'>
    <templateId root='1.3.6.1.4.1.19376.1.5.3.1.2.6'/>
    <id root='1.2.3.4.5.6.7.8.9'/>
```

```
    <code code=1.1.1.1.1.1.1' displayName='Sample consent'
codeSystem=1.1.1.1.1.1.10' codeSystemName='Sample XDS affinity
domain'/>
    <effectiveTime>
      <low value='20211116'/>
    </effectiveTime>
  </serviceEvent>
</documentationOf>
```

In this example service event with ID 1.2.3.4.5.6.7.8.9 records an acknowledgement to “Sample consent” patient privacy policy with OID 1.1.1.1.1.1.1 from the patient privacy policy domain code system 1.1.1.1.1.1.10 described as “Sample XDS Affinity Domain”.

4.3. XUA (Cross-Enterprise User Assertion)

This profile provides options for transferring user identities between different healthcare enterprises and specifies how these assertions should be referenced by event audit logging. The focus of requirements of this profile is identity federation which is agnostic to the type of user directory used. Different healthcare providers may use different approaches to user authentication i.e., some of them may have unique authentication methods applied to identities kept in their own user directory, while others may have only a user directory used by third party, authenticating the identities. Some of them may use already defined IHE profiles like PWP for handling identities, while others may have non-IHE directories. In addition to that, user directories may be centralized or federated. These are some examples although there are many possibilities for establishing and maintaining user directories for which many different authentication and authorization mechanisms may be used, depending on the healthcare needs and preferences. Technologies, procedures, and role models implemented within a specific healthcare enterprise may be unique. However, an agreed policy level of the processing rules between different healthcare enterprises may support the proper use of XUA integration profile. User assertion is valuable and must be protected. Moreover, in all possible scenarios of user assertion security audit logging is very important to keep track of identities recorded.

IHE XUA integration profile does not define:

- How is a principal (user, application, system, etc.) authenticated within a specific healthcare enterprise
- How is a principal (user, application, system, etc.) authorized within a specific healthcare enterprise
- If a user assertion is further used by the receiving healthcare enterprise i.e., authenticated, or authorized and how
- If a user assertion is further ignored by the receiving healthcare enterprise

That way, IHE does not limit implementations and configurations using XUA profile. Nonetheless, misuse of the information transferred using this profile which is very

sensitive can result as high risk. It is recommended that a specific risk assessment is conducted by the individual enterprises to mitigate risks not addressed by this profile.

IHE XUA integration profiles specifies:

- How should some options regarding identity, authorization, or purpose of use be transmitted between different healthcare enterprises within WSS (Web-Services Security) header with SAML (Security Assertion Markup Language) 2.0 token
- How should a user assertion be referenced in event audit logging when using ATNA profile
- Grouping actors from IHE EUA profile which handles user assertions within a specific healthcare enterprise
- Grouping actors from IHE XDS profile enabling document sharing between different healthcare enterprises

Systems involved in XUA profile implementation may be:

- Any application using web-services transactions
- Any service using web-services transactions

In such scenarios, profiles from non-healthcare standard like Web-Services Security, SAML 2.0 Token and other defined by W3C or OASIS may be used for identity federation.

Actors and transactions required for implementing XUA integration profile are given in table 4.6.:

Table 4.6. XUA actors and transactions

Actor	Transaction	Optionality
X-Service User	Provide X-Assertion [ITI-40]	R
X-Service Provider	Provde X-Assertion [ITI-40]	R

In the first column of the table 4.6. are given XUA actors directly involved. In the second column given are transactions respective to the actors from the first column. In this case there is only one required transaction which is the same for each actor. “R” within the third column implies that transaction [ITI-40] is required for XUA actors.

Diagram showing the interaction between the actors and transactions directly involved in XUA integration profile is given on figure 4.5.

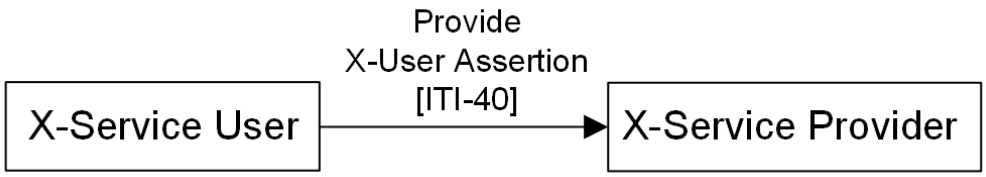

Figure 4.5. XUA directly involved actors and transactions

On the figure 4.5. are shown actors and transactions directly involved in XUA profile:

- Actor X-Service User
- Actor X-Service Provider
- Transaction Provide X-User Assertion [ITI-40]

These actors and transactions are combined with other actors specified as ancillary actors involved in the user assertion process and grouped actors using possible XUA actors’ functionalities. There are also interactions between and to the ancillary actors, fulfilling the diagram of XUA actors and transactions, shown on figure 4.6.

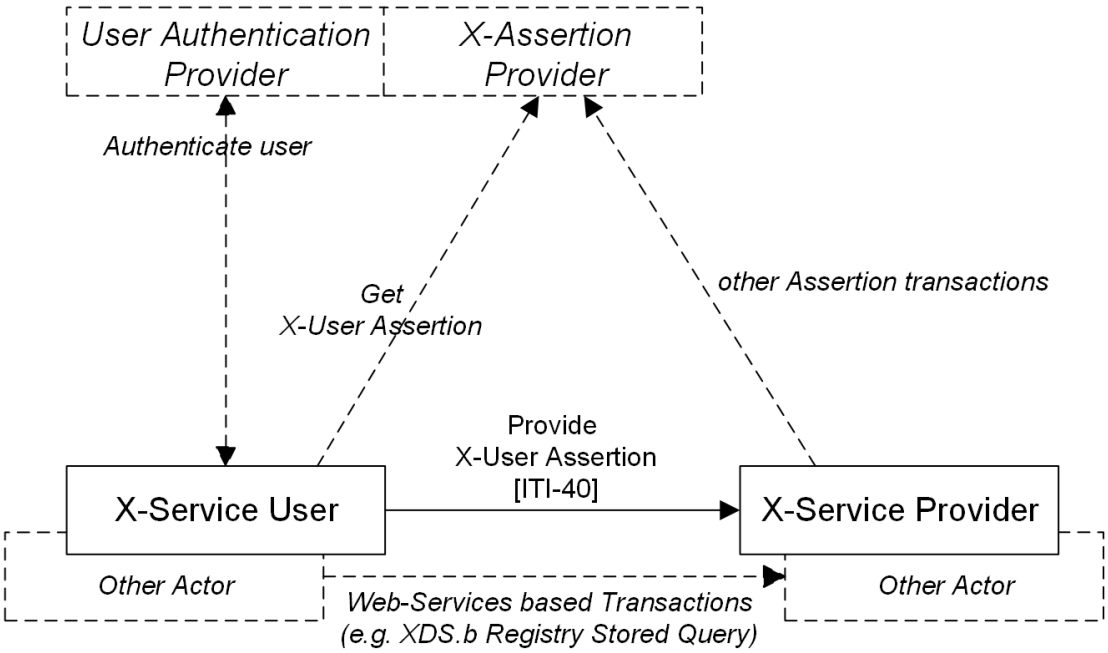

Figure 4.6. XUA actors and transactions [20]

Ancillary actors within the XUA profile shown on figure 4.6. are:

- Ancillary actor User Authentication Provider
- Ancillary actor X-Assertion Provider

Interactions with ancillary actors considered by XUA profile, shown with dashed lines on the figure 4.6. are:

- Authenticate User between directly involved X-Service User XUA actor and ancillary XUA actor User Authentication Provider
- Get X-User Assertion between directly involved X-Service User XUA actor and ancillary XUA actor X-Assertion Provider
- Other Assertion transactions between directly involved X-Service Provider XUA actor and ancillary XUA actor User Assertion Provider

Technologies and system configuration of the ancillary actors and associated transactions may vary regarding internal services and identity management infrastructures. However,

these actors are important for the implementation of XUA profile due to their indirect participation in the XUA process.

On the figure 4.6. actors from other IHE profiles that can be grouped with XUA actors are shown with dashed boxes and described as “Other Actor”. Any IHE actor that uses web-services transactions can be grouped with the appropriate XUA actors. These actors should communicate through web-based transactions as a prerequisite for using options XUA actors may provide. For example, XDS document consumer actor can be grouped with XUA X-Service User, XDS document registry or XDS document provider can be grouped with XUA X-Service Provider when XDS profile interoperates with XUA profile. Another example is grouping XUA with IHE EUA, IHE PWP and SAML identity provider. The communication flow in similar case to this example is given on figure 4.7.

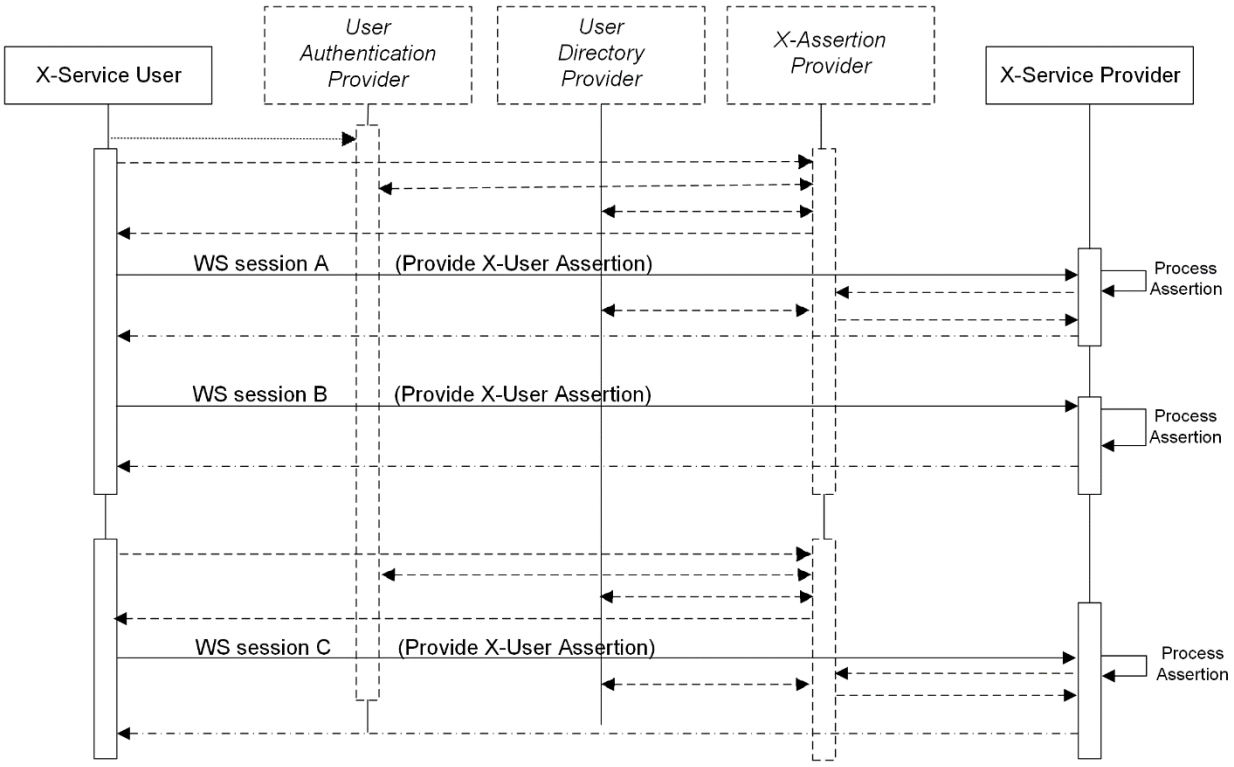

Figure 4.7. XUA example process flow [20]

On the figure 4.7. IHE profile or other non-IHE solutions for user authentication provider, user directory provider and X-Assertion provider are not specified. All these components can be different per enterprise but should be interoperable when using web-based transactions and implement XUA profile. The dashed lines on the picture represent any standard-based transaction while the bold solid line is XUA transaction. Web-services sessions A and B use one XUA transaction while web-services session C is using another XUA transaction, needed in case of asserting different user identity than the one used by A and B sessions or when the timeout of the first X-user assertion has passed. Other reasons for using a different XUA transaction are also possible.

Besides suggested groupings, there are required groupings specified by XUA for its actors. These are given in table 4.7.

Table 4.7. Required XUA actors' groupings

XUA actor	**Profile / Actor to be grouped with**
X-Service User	CT / Time client ATNA / Secure Node or Secure Application
X-Service Provider	CT / Time client ATNA / Secure Node or Secure Application

In the table 4.7. XUA actors are given within the first column and actors which grouping is required along with originating IHE profiles are given for each actor, respectively. In the case of XUA profile both actors should be grouped with the time client actor of CT profile [10] and secure node or secure application actor from ATNA profile. CT profile is very important for synchronizing the time between the system elements for which ATNA plays very important role regarding node authentication, secure communication, and event audit logging. In other words, X-User Assertion is valuable and must be protected against confidentiality and integrity risks. This can be achieved by grouping XUA actors with ATNA actors due to requirements specified by ATNA and applying to all grouped actors.

Within this profile three options can be applied to its actors. By implementing these options XUA actors support the XUA transaction [ITI-40]. List of XUA actors and applicable options are given in table 4.8.

Table 4.8. XUA actors' options

Actor	Option
X-Service User	Subject-Role Authz-Consent PurposeOfUse
X-Service Provider	Subject-Role Authz-Consent PurposeOfUse

In the first column of the table 4.8. XUA actors are given and in the second column list of respective options is given.

All options given for each actor offer different type of authorization information to be transmitted which may or may not be interpreted properly on the destination point. This depends on the implementations of policies and access controls and their application by both enterprises. XUA profile only provides the possibility to transfer user related information and gives some interoperability directions.

Subject-Role option may help in access decision making on the X-Service Provider side if RBAC model used at the X-Service User and RBAC model used at the X-Service Provider are analog or consistent. This means that the role value set should be understood by both actors equally. This may be a problem due to the allowed loose coupling between the identity management and access control point. XUA addresses this problem by suggesting use of standardized role codes found in healthcare such as SNOMED-CT, ISO 21298, or ASTM E1986.

Authz-Consent option leverages the BPPC model. For example, a newly published patient privacy policy document may be included in the user assertion. It may be used in cases when requester of transaction has some consent or authorization evidence. The evidence

may be required for the transaction by some legal regulation or is needed as part of the access control model.

PurposeOfUse option enables inclusion of the intended purpose of use of the data. Consistent value-sets are very important for proper use of this information. Standardized approaches are recommended such as ISO 14265 and XSPA. Examples requiring this option are providing a patient privacy policy consent but disallowing using the data for which a consent is given in research purposes. Another specific purpose of use is break-glass or emergency mode access. Finally, purpose of use is essential for reporting of accounting of disclosures and breach notifications thus important to event audit logging.

4.3.1. XUA transactions

There is one required transaction by XUA profile:

- Provide X-User Assertion [ITI-40]

To explain the need for this transaction it is sufficient to understand the scope of the transaction together with roles included and integration diagrams illustrating the message flow. This will be discussed in the next chapter.

4.3.1.1. Provide X-User Assertion [ITI-40]

Within this transaction defined are two use case roles [21]:

- Role of the XUA actor X-Service user: user of a transaction requesting a cross-enterprise user assertion
- Role of the XUA actor X-Service provider: service provider on a transaction requiring cross-enterprise user assertion

The scope of this transaction includes a third-party issuer of the claimed identity assertion described as X-Assertion provider, communicated by X-Service user and X-Service provider XUA actor, also interacting with each other through [ITI-40] transaction.

Message interaction within the scope of the transaction [ITI-40] is given on figure 4.8.

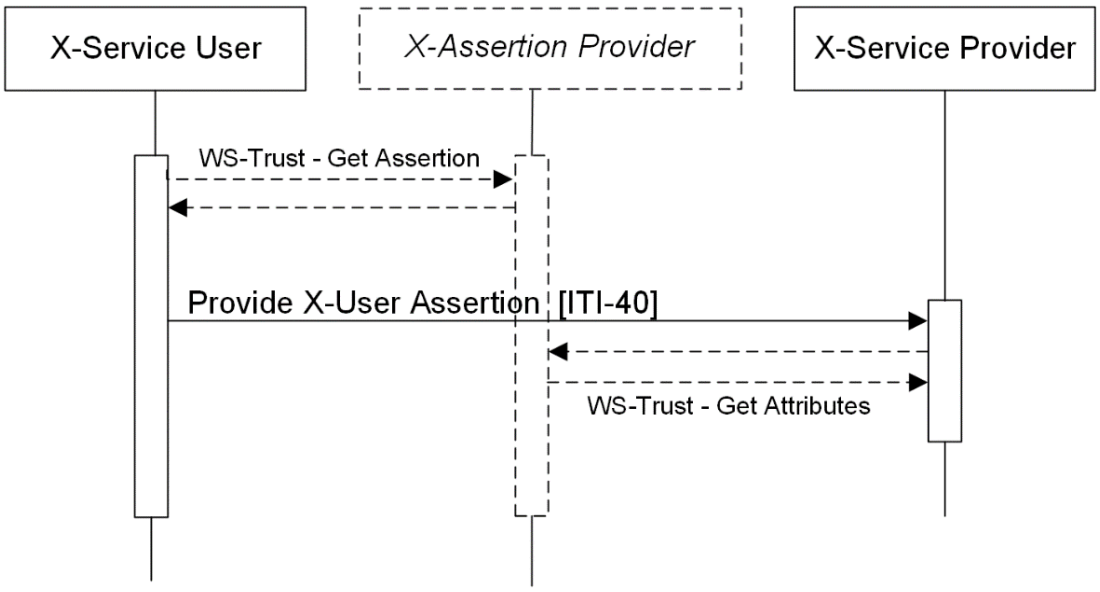

Figure 4.8. [ITI-40] interaction diagram [21]

X-Assertion provider is contacted by the X-Service user to get the user assertion about the user requesting a service. WS-Trust, SAML 2.0 protocol may be used as a standard communication. Assertion is provided by the X-Assertion provider and transmitted to X-Service provider through [ITI-40] transaction. X-Service provider actor receives the user assertion which can be used for authentication validation and access controls. In cases X-Service provider need information about the user not included in the user assertion it communicates with X-Assertion provider to get the missing attributes.

Some examples for messages containing XUA actors' options explained in the previous chapter i.e., SAML assertions will be given. Details about asserting other user information specified by IHE are given in the second volume of its technical framework [21].

SAML attribute fragment containing subject-role option is given bellow:

```
<saml:Attribute Name="urn:oasis:names:tc:xacml:2.0:subject:role">
<saml:AttributeValue>
  <Role xmlns="urn:hl7-org:v3" xsi:type="CE" code=" 398130009"
```

```
    codeSystem="2.16.840.1.113883.6.96"
    codeSystemName="SNOMED_CT" displayName="Medical student"/>
</saml:AttributeValue>
</saml:Attribute>
```

When this option is used by the X-Service user it should be encoded into the <Attribute> element. The “Name” attribute of the <Attribute> element should be set to urn:oasis:names:tc:xacml:2.0:subject:role. The value of the <AttributeValue> element is a child element <Role>. The namespace of this element is urn:hl7-org:v3 (HL7 v3) and its content is defined by the “CE” data type of the HL7 v3 specification. “code” attribute of the <Role> element should contain the code from the identified value-set for the role as which the X-Service user actor is presenting. In this example the role is “Medical Student” with code 398130009. Finally, “codeSystem” and “codeSystemName” attributes of the <Role> element should contain the OID and the name of the coding system from which the role code is taken from, respectively. In this example it is SNOMED_CT with OID 2.16.840.1.113883.6.96. Only these parts of the CE (coded with equivalents) should be used.

When authz-consent option is used to send a policy identifier actor X-Service user should include the ID of the patient privacy policy acknowledgement document or ID of the patient privacy policy for a previously published policy.

SAML attribute fragment containing authz-consent option carrying a reference to patient privacy policy acknowledgement is given bellow:

```
<saml2:Attribute FriendlyName="Patient Privacy Policy
Acknowledgement Document" Name="urn:ihe:iti:bppc:2007:docid"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
    <saml2:AttributeValue
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:type="xs:anyURI">urn:oid:9.9.9.abc</saml2:AttributeValue>
</saml2:Attribute>
```

Patient privacy policy acknowledgement document ID on the example above is encoded as a SAML attribute in the IHE ITI namespace urn:ihe:iti:bppc:2007:docid as it is specified by this profile. The name format should be urn:oasis:names:tc:SAML:2.0:attrname-format:uri. The ID of the patient privacy policy acknowledgement document should use xs:anyURI data type. For this example, this ID is 9.9.9.abc

SAML attribute fragment containing authz-consent option carrying a reference to patient privacy policy is given bellow:

```
<saml2:Attribute FriendlyName="Patient Privacy Policy Identifier"
Name="urn:ihe:iti:xua:2012:acp"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
      <saml2:AttributeValue
      xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-
      instance" xsi:type="xs:anyURI">urn:oid:9.9.9.xxx</saml2:Att
      ributeValue>
</saml2:Attribute>
```

Patient privacy policy ID on the example above is encoded as a SAML attribute in the IHE ITI namespace urn:ihe:iti:xua:2012:acp as it is specified by this profile. The name format should be urn:oasis:names:tc:SAML:2.0:attrname-format:uri. The ID of the patient privacy policy should use xs:anyURI data type. For this example, this ID is 9.9.9.xxx

SAML attribute fragment containing PurposeOfUse option is given bellow:

```
<saml:Attribute
Name="urn:oasis:names:tc:xspa:1.0:subject:purposeofuse">
          <saml:AttributeValue>
             <PurposeOfUse xmlns="urn:hl7-org:v3" xsi:type="CE"
             code="12" codeSystem="1.0.14265.1"
             codeSystemName="ISO 14265 Classification of Purposes
```

```
                for processing personal health information"
                displayName="Law Enforcement"/>
            </saml:AttributeValue>
</saml:Attribute>
```

When this option is used the value of the “Name” attribute within the PurposeOfUse <Attribute> element should be urn:oasis:names:tc:xspa:1.0:subject:purposeofuse. The value of the <AttributeValue> element is a child element <PurposeOfUse>. The namespace of this element is urn:hl7-org:v3 (HL7 v3) and its content is defined by the “CE” data type of the HL7 v3 specification. “code” attribute of the <PurposeOfUse>. “code” attribute of the <PurposeOfUse> element should contain the code from the identified value-set for the appropriate purpose of use described within the “displayName” attribute of the <PurposeOfUse> element. In this example the purpose of use is “Law Enforcement” with code 12. Finally, “codeSystem” and “codeSystemName” attributes of the <PurposeOfUse> element should contain the OID and the name of the coding system from which the purpose of use code is taken, respectively. In this example it is ISO 14265 Classification of Purposes for processing personal health information with OID 1.0.14265.1. Only these parts of the CE (coded with equivalents) should be used.

5. Use cases

Possible and specific use cases of ATNA, BPPC and XUA security related IHE ITI integration profiles will be explained within this chapter with the main objective to give a general insight in their implementation. These use cases are proposed by IHE and based on vendor's experience and thus are globally applicable. In addition, given are examples for an existing project regarding the implementation of these profiles. This project is deploying central health information system for the Republic of Kazakhstan and covers implementation and maintenance of the national integration platform. If a specific profile is not implemented yet and thus there are no specific use cases within the mentioned project, prerequisites and settings allowing their implementation in the future along with proposal for use cases are explained. All use cases described by next three chapters are globally accepted and do not define the mechanisms, policies and technologies supporting it.

For implementation and use of ATNA profile, required security controls implemented by this project were defined based on the client preferences and adjusted to specified ATNA options. For authentication, user directory containing user identities for patients and professionals is used. Authorization is defined using some LDAP attributes for both types of directories i.e., patient's and professional's user directory and access controls are defined and performed by another component communicating through secure connections with the LDAP directory. That component is known as authorization manager. Its function is to make decisions related to the requests for authentication and authorization from the API (Application Programming Interface) gateway component. Those decisions depend on information stored within the user directories and rules about the access control defined on the authorization manager component. Secure communication between system components is established using TLS protocol and GOST certificates. For recording and transmitting audit events syslog messages and UDP are used.

For implementing and using BPPC profile policies defined by this project can be used and adjusted to most common use cases described in the chapter 5.2. Clinical document used

for this project is HL7 CDA R2 and can be considered as a prerequisite allowing the use of BPPC. Policy details are part of the project's documentation.

Finally, for implementation and use of XUA profile details about the user directories can be used as a motivation for possible use cases. Enabled single sign-on with SAML 2.0 tokens within this platform can be considered as a prerequisite allowing the use of XUA. More details about that are given in chapter 5.3.

5.1. ATNA

Audit Trail and Node Authentication IHE ITI integration profiles provide three security measures:

- User authentication
- Node authentication
- Event audit records i.e., logging

By implementing these security measures satisfied are following security requirements:

- Secrecy
- Integrity
- Authentication
- Authorization
- Non-repudiation
- Audit log
- Patient privacy

How and when the security measures provided by ATNA can be used to satisfy these security requirements will be explained by three typical process flows in next three chapters. Process flows will cover attempts for gaining access to the protected health information by authorized user through authorized node, unauthorized node, and unauthorized user in each chapter, respectively. This profile is used for implementation and deployment of eHealth system for the Republic of Kazakhstan. At this time this project is not fully implemented and IHE compliant. Technical details cannot be given due to the protected project documentation.

5.1.1. Normal process flow

On figure 5.1. the process flow of an authorized access of PHI is illustrated. Three system components are grouped with ATNA secure node actor. These are image display system component, image manager and image archive system component and audit record repository which is also an ATNA actor. A user who tries to gain access to images stored

by image archive and handled by image manager is authenticating locally on the image display system component, which later communicates with the rest of the infrastructure involved in the process flow and in case of successful authentication of the user and nodes retrieves the required results to the image display system component.

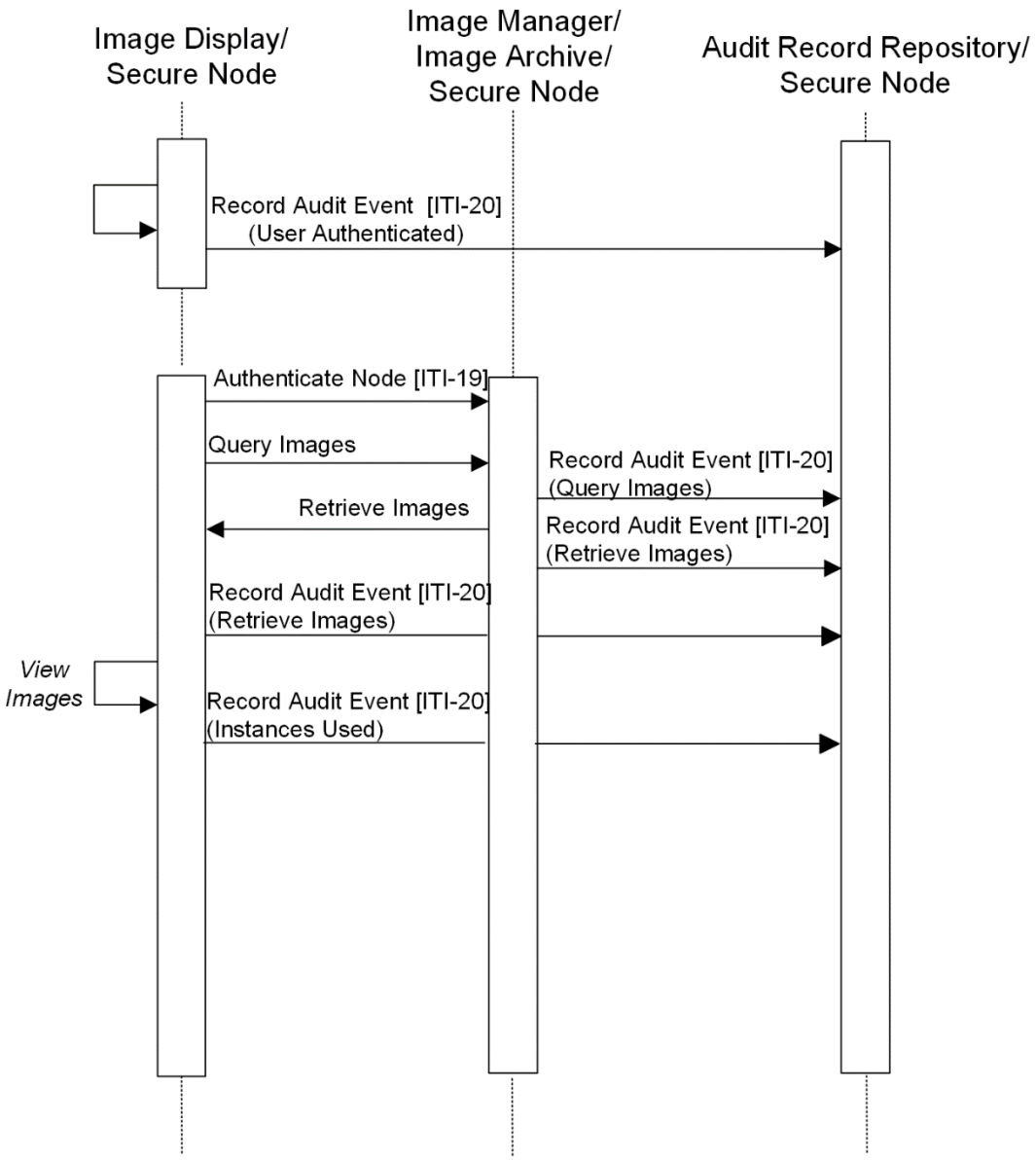

Figure 5.1. Authorized access to PHI

First, user is successfully authenticated on the secure node grouped with the image display system component for which is used specific mechanism defined by the image display system component. This action is logged to the audit record repository by the secure node grouped with the image display system component using ATNA [ITI-20] record audit event transaction. After the successful user authentication, secure node grouped with the image display system component and secure node grouped with the image manager and archive system component are mutually authenticating to satisfy the prerequisite for further transactions. Mutual authentication is achieved by exchanging messages specified by ATNA [ITI-19] authenticate node transaction. This authentication is not logged as it is not specified as a trigger event for audit logging by ATNA. At this point secure communication between the mutually authenticated nodes is established. After the successful authentication of the secure nodes, image display system component queries image manager and archive system component for images. This event is activity-related and is logged to the audit record repository by the secure node grouped with image manager and archive system component using ATNA [ITI-20] record audit event transaction. Respectively to that, image manager and archive system component responds to image display system component by retrieving queried images. Receipt of the requested images is an activity-related event and is logged to the audit record repository by the secure node grouped with the image display system component using ATNA [ITI-20] record audit event transaction, which is later displaying those images as user requested. Viewing images is also an activity-related event and is logged to the audit record repository by the secure node grouped with the image display system component using ATNA [ITI-20] record audit event transaction.

5.1.2. Process flow for unauthorized node

Process flow for a scenario of an attempt for gaining access to PHI by unauthorized node is illustrated on figure 5.2. Two system components are grouped with the ATNA secure node actor while the requesting node is recognized as a malicious node due to its untrusted certificate. System components grouped with ATNA secure node are lab automation manager and audit record repository which is also an ATNA actor. The unauthorized node is not registered within the trusted domain but is trying to gain access to images from the lab automation manager system component. In case of a successful node authentication the lab automation manager system component should retrieve the requested images.

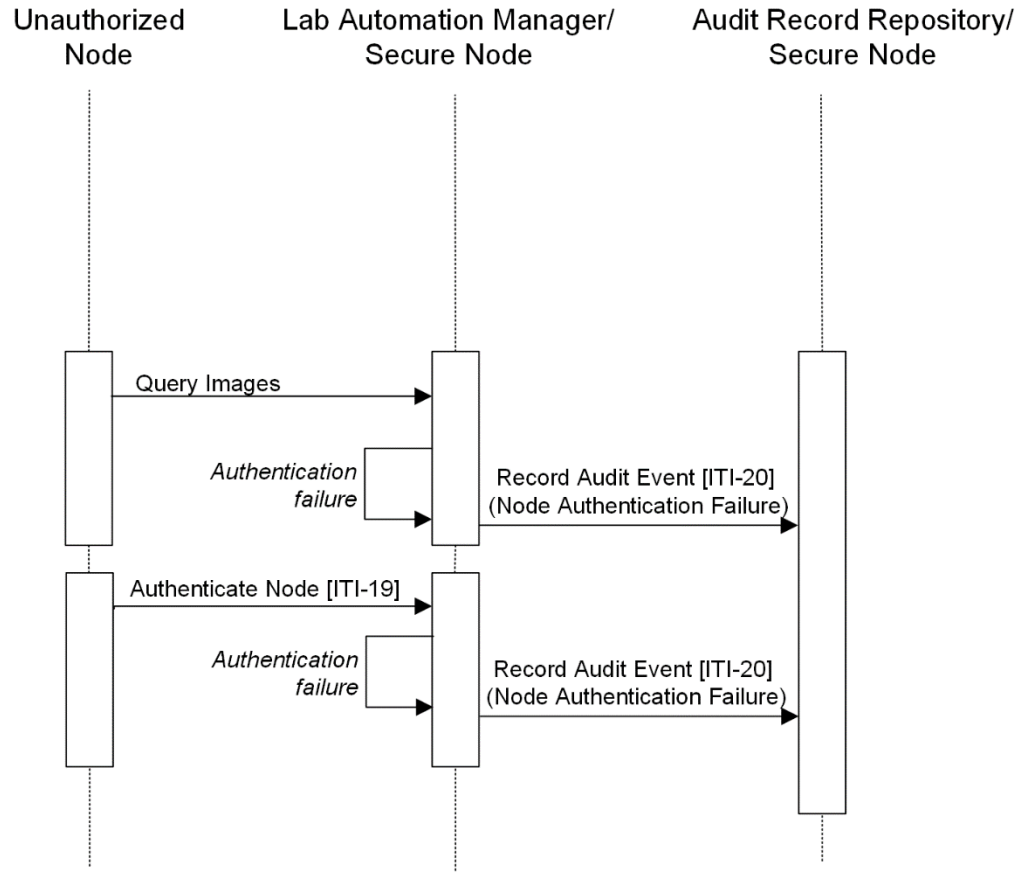

Figure 5.2. Unauthorized node attempting to access PHI

Within the first transaction, the unauthorized node is querying the lab automation manager system component for images which fails because no authentication has taken place. Event of a failed node authentication is specified as a trigger event by ATNA and is logged by the secure node grouped with the lab automation manager system component to the audit record repository using ATNA [ITI-20] record audit event transaction. After this event, the unauthorized node and secure node grouped with the lab automation manager system component are mutually authenticating using ATNA [ITI-19] authenticate node transaction. Certificate presented by the unauthorized node is not trusted by the secure node grouped with the lab automation manager system component and thus authentication fails for the malicious node. This event is logged by the secure node grouped with the lab automation manager system component to the audit record repository using ATNA [ITI-20] record audit event transaction after which no communication is enabled between the malicious node and the secure node grouped with lab automation manager system component.

5.1.3. Process flow for unauthorized user

Process flow for a scenario of an attempt for gaining access to PHI by unauthorized user is illustrated on figure 5.3. Two system components are grouped with the ATNA secure node actor. These are ECG display system component and audit record repository which is also an ATNA actor. An unauthorized user is initiating the communication by authenticating locally on the ECG display system component. If this authentication was successful, the communication would continue, and ECG display system component would retrieve the requested resources to the successfully authenticated user.

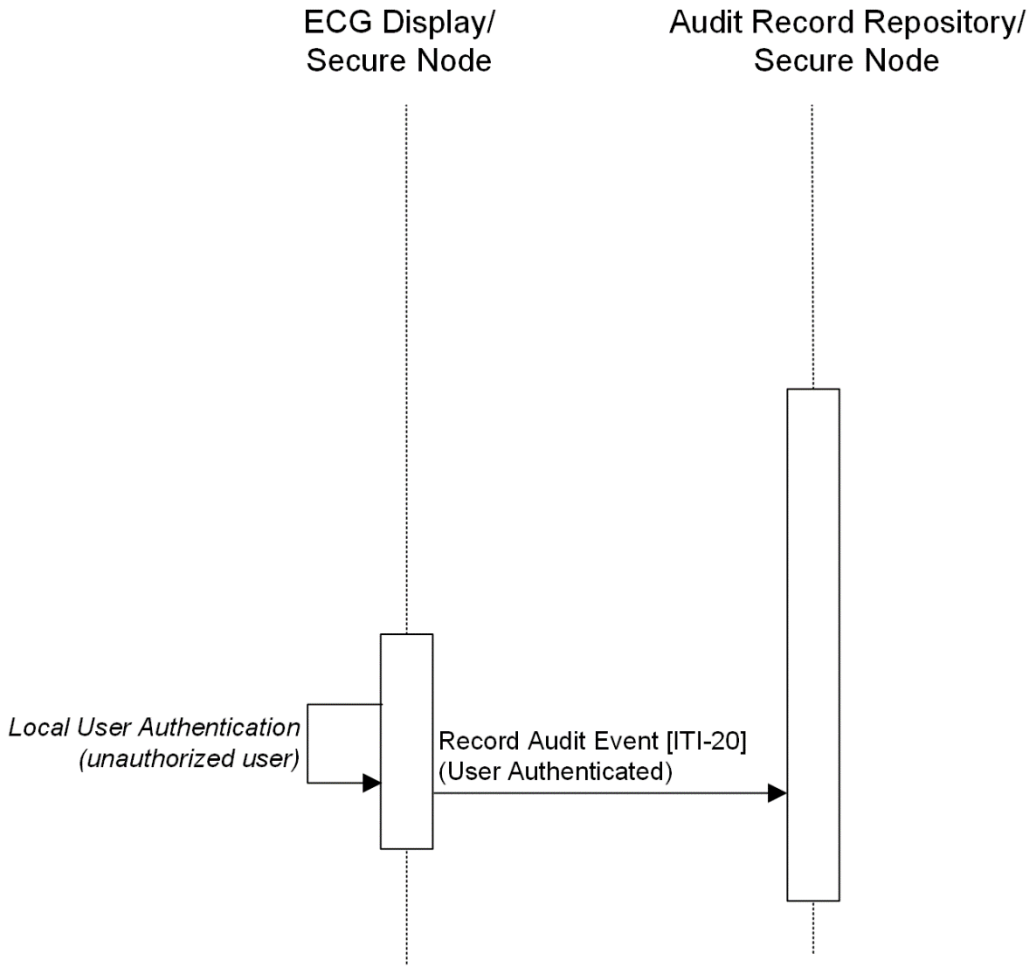

Figure 5.3. Unauthorized user attempting to access PHI

An unauthorized user is initiating an authentication process on the secure node grouped with the ECG display system component. For authentication used is specific mechanism defined by the ECG display system component and this use case does not depend on it. The username and credentials presented to the secure node grouped with the ECG system component are not verified as valid and user access is rejected due to failed authentication. User failed authentication is specified as a trigger event and is logged to the audit record repository by the secure node grouped with the ECG system component using ATNA [ITI-20] record audit event transaction. The communication between the ECG display system component and unauthorized user is stopped at this point.

5.2. BPPC

Environments supported by this profile are those with implied and explicit consent on patient privacy policies. Acknowledgement of a patient privacy policy is not required within an implied environment, while the explicit patient privacy policy environment may include many structures of consents for the clinical document sharing which are recognized as use cases for this profile.

Two main structures of sharing clinical documents, also BPPC use cases are opt-in and opt-out. Opt-in is more common structure which requires a patient's consent before its medical information is shared. Policies on which a patient should agree need to be defined by the clinical document sharing domain explaining which document are available to whom and under which conditions. The definition of such policies is not specified by IHE as it was previously mentioned. Whatever is defined within the clinical sharing domain's policies, there should be one overriding policy indicating that patient's medical information may not be shared until the patient has explicitly agreed on sharing its medical information within that clinical document sharing domain. Opt-out structure of sharing clinical documents presumes implicit patient's consent of sharing its medical information when its choses to get care within the specific healthcare. Like the opt-in structure, opt-out clinical document sharing domain should have clear policies defining the actual behavior within it. Opt-out structures offers that a patient may not participate in its medical information sharing which also indicates that the patient's clinical documents should not be used within the specific healthcare.

The project on implementing and deploying eHealth in the Republic of Kazakhstan includes the use of XDS which is a prerequisite for using the IHE BPPC profile. BPPC profile is currently not implemented and used although policies that may be used for opt-in use case of clinical document sharing exist. However, before implementing the BPPC profile some specific scenarios that may be part of the opt-in BPPC use case should be correctly addressed and planned for its optimization i.e.:

- BPPC satisfies two security requirements which are authorization (indirectly satisfied) and patient privacy (directly satisfied) by supporting the appropriate

security controls. Additionally, non-repudiation of the patient privacy policy consent may be enabled by using digital signature for the patient privacy policy acknowledgement document. This security requirement should be satisfied for both types of patient privacy policy acknowledgement documents, those which include wet signature using scanned document within the XDS domain and those which do not use wet signatures i.e., use XDS domain without XDS-SD actors as consumers. IHE also specifies a profile for digitally signing clinical documents within XDS domains. That is DSG IHE ITI profile [22] and may be considered for enabling this option.

- Sensitivity of the clinical documents specified by HL7 is defined within the confidentialityCode. This code in combination with functional roles enables access controls defined within the XDS domain's policies. Usually, confidentialityCode is used to define the sensitivity of the clinical document to which a patient privacy policy is attached, but also it may be used to classify the sensitivity of the patient privacy policy acknowledgement document. Thus, there may also be policies defining the appropriate use, creation, disclosure, and other handling of the patient privacy policy consent documents and not just those regarding the contained information within the clinical document. For example, in cases when a terminally ill patient chooses not to share specific prognosis with its family members, existence of that consent may indirectly inform them of a negative prognosis. Because of that, appropriate confidentialityCode should be assigned to the patient privacy policy acknowledgment document possibly describing it by a high sensitivity level. This may present a live threatening situation when access to these documents is not defined properly and is a reason for defining more detailed and well-organized policies, also handling the risks of accidental or malicious disclosure of private information. Including XDR and XDM in the clinical document sharing domain may also be considered as these profiles provide an option for reviewing the clear content. However, attached patient privacy policy consents should be also available informing sites using the medical information they

apply to about the patient’s preferences over it. Existing implementation of the ATNA profile should help in assuring the PHI is properly accessed and used.

- Handling emergency cases should be also defined due to the lack of a possibility for a patient privacy policy acknowledgement at that moment if opt-in structure of clinical document sharing is planned to be used. These cases are also known as break-glass.

5.3. XUA

XUA profile is enabling interoperability for different and complex environments using different technologies, procedures, role-base access control models, etc. with the respect to policies defined within an XDS affinity domain. This may be useful in different cases for example when clinical documents should be shared between smaller healthcare providers and large-scale hospitals.

Some proposed use cases for XUA integration profile by IHE are [20]:

- Single assigning authority domain within a country and common service handling all authentication requests. This scenario supports centralized user directories that may not be related to the healthcare providers but used by them.
- User identities managed separately by cooperating hospitals and clinics. This scenario supports distributed user directories.
- User identities provided by custom identity provider based on patient's preferences (e.g., Internet Service Provider, email provider). This scenario supports non-healthcare specific user directories.
- Using smart cards and radio frequency identification for building access and strong authentication of user identities stored within a user directory. This scenario supports claims about the method used to authenticate the user (e.g., strong authentication methods such as smart cards).
- Rural setting environments having a dozen of users within one clinic. This scenario supports small scale systems (e.g., user at a kiosk, system using simple passwords).
- Recording audit trail for an outpatient clinic where is conducted some test, for example. This scenario supports the service provider to get a user identity for audit log purposes.
- Automated retrieval of patient's document synchronized with visits' schedule, preparing the doctor in advance of a specific visit. This scenario

supports user identification as the system for tasks that are not initiated by a human user.

From all these use cases which is not a final and fully defined set of possibilities at this time it can be concluded that XUA supports centralized and distributed user directories equally. Besides that, XUA can offer user assertion regarding the use identity only or also its roles/privileges which may be used with it to enable or improve the function of a typical eHealth service or to provide audit control.

Use case supporting centralized user directory may be used within the project for implementing and deploying eHealth system for the Republic of Kazakhstan. Regarding user directories for this eHealth system two separated user directories are used. One for healthcare professionals, and another one for patients dimensioned to contain 18 million users. Both user directories are replicated and offer high availability. Data contained within the user directories is meant to be used for authenticating users. Authorization is implemented through different access managing solutions and access gateways.

6. Conclusion

Nowadays, use of eHealth is widely recognized in developing countries. eHealth is improving the health care locally, regionally, and worldwide by using information and communication technology. IHE, the initiative by healthcare professionals and industry to improve the way computer systems in healthcare share information expands the limits set by eHealth systems by guiding and specifying standardized interoperability in the healthcare informatics. In other words, IHE continues where eHealth “stops”. IHE does not define the health information exchange within different eHealth systems and does not specify any policies. However, it expects well defined governance and accountability, regular risk assessments and is policy sensitive.

This thesis gives an insight of most common security requirements in eHealth systems and standardized implementation of appropriate security controls in IHE environments. Possibilities for supporting different security controls are specified by IHE within the ITI (IT Infrastructure) domain. Main objectives, specifications and use cases of ATNA (Audit Log Trail and Node Authentication), BPPC (Basic Patient Privacy Content) and XUA (Cross-Enterprise User Assertion) security related integration profiles defined within the IHE ITI technical framework are explained in more detail. These profiles support security controls for identification, authentication, authorization, confidentiality, integrity, non-repudiation, patient privacy and audit which is described by use cases proposed by IHE. More specifically, for each security related profile given is an example of current implementation and existing possibilities for supporting it in the future within an existing project for implementation and deployment of eHealth system for the Republic of Kazakhstan.

Future research may include scenarios where mobile access is allowed as valid and verified approach to offered services by implemented eHealth systems in integrated environments. This should include deeper investigation on HL7 FHIR specification and the extending possibilities of fully published or trial implementations of IHE ITI profiles.

References

[1] H. Oh, A. Jadad, C. Rizo, M. Enkin, J. Powell and C. Pagliari, "What Is eHealth (3): A Systematic Review of Published Definitions", *Journal of Medical Internet Research*, vol. 7, no. 1, 2005. Available: 10.2196/jmir.7.1.e1 [Accessed 4 November 2021].

[2] G. Eysenbach, "What is e-health?", *Journal of Medical Internet Research*, vol. 3, no. 2, p. e20, 2001. Available: 10.2196/jmir.3.2.e20 [Accessed 4 November 2021].

[3] "Health informatics - Wikipedia", *En.wikipedia.org*, 2021. [Online]. Available: https://en.wikipedia.org/wiki/Health_informatics. [Accessed: 08- Nov- 2021].

[4] "About IHE - IHE International", *IHE International*, 2021. [Online]. Available: https://www.ihe.net/about_ihe/. [Accessed: 09- Nov- 2021].

[5] M. Končar, "IHE profili", Fakultet elektrotehnike i računarstva, Zagreb.

[6] "IHE Wiki", *Wiki.ihe.net*, 2021. [Online]. Available: https://wiki.ihe.net/. [Accessed: 04- Nov- 2021].

[7] S. Mendelson, D., 2016. IHE Essentials:The Path to Secure and Transparent Interoperability. In: *eHealth week*

[8] IHE international, 2021. *IHE IT Infrastructure White Paper Revision 2.1 - Published*. ITI Technical Committee.

[9] IHE international, 2021. *IHE IT Infrastructure (ITI) Technical Framework, Volume 1 Revision 18.0 – Final Text*. Section 9.

[10] IHE international, 2021. *IHE IT Infrastructure (ITI) Technical Framework, Volume 1 Revision 18.0 – Final Text*. Section 7.

[11] IHE international, 2021. *IHE IT Infrastructure (ITI) Technical Framework, Volume 2 Revision 18.0 – Final Text*. Section 3.19.

[12] IHE international, 2021. *IHE IT Infrastructure (ITI) Technical Framework, Volume 2 Revision 18.0 – Final Text*. Section 3.20.

[13] IHE international, 2021. *IHE IT Infrastructure (ITI) Technical Framework, Volume 1 Revision 18.0 – Final Text*. Section 10.

[14] IHE international, 2021. *IHE IT Infrastructure (ITI) Technical Framework, Volume 1 Revision 18.0 – Final Text*. Section 15.

[15] IHE international, 2021. *IHE IT Infrastructure (ITI) Technical Framework, Volume 1 Revision 18.0 – Final Text*. Section 16.

[16] IHE international, 2021. *IHE IT Infrastructure (ITI) Technical Framework, Volume 1 Revision 18.0 – Final Text*. Section 18.

[17] IHE international, 2021. *IHE IT Infrastructure (ITI) Technical Framework, Volume 1 Revision 18.0 – Final Text*. Appendix P: Privacy Access Policies (Informative)

[18] IHE international, 2021. *IHE IT Infrastructure (ITI) Technical Framework, Volume 1 Revision 18.0 – Final Text*. Section 19.

[19] IHE international, 2021. *IHE IT Infrastructure (ITI) Technical Framework, Volume 3 Revision 18.0 – Final Text*. Section 5.1.

[20] [18] IHE international, 2021. *IHE IT Infrastructure (ITI) Technical Framework, Volume 1 Revision 18.0 – Final Text*. Section 13.

[21] [18] IHE international, 2021. *IHE IT Infrastructure (ITI) Technical Framework, Volume 2 Revision 18.0 – Final Text*. Section 3.40.

[22] [18] IHE international, 2021. *IHE IT Infrastructure (ITI) Technical Framework, Volume 1 Revision 18.0 – Final Text*. Section 37.

Abbreviations

API	Application Programming Interface
APPC	Advanced Patient Privacy Consents
ASTM	American Society for Testing and Materials
ATNA	Audit Trail and Node Authentication
BPPC	Basic Patient Privacy Consents
CARD	Cardiology
CDA	Clinical Document Architecture
CE	Coded with Equivalents
CT	Consistent Time
DE	Document Encryption
DENT	Dental
DEV	Devices
DICOM	Digital Imaging and Communications in Medicine
DSG	Document Digital Signature
eHealth	electronic Health
EHR	Electronic Health Record
ENDO	Endoscopy
EUA	Enterprise User Assertion
FHIR	Fast Healthcare Interoperability Resources
GOST	GOsudarstvennyy STandart
HIMSS	Healthcare Information and Management Systems Society
HIT	Health Information Technology
HL7	Health Level 7
HPD	Healthcare Provider Directory
ID	Identifier
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IHE	Integrating the Healthcare Enterprise

ISO	International Organization for Standardization
IT	Information Technology
ITI	Information Technology Infrastructure
LOINC	Logical Observation Identifiers Names and Codes
MCSD	Mobile Care Services Discovery
OASIS	Organization for the Advancement of Structured Information Standards
OID	Object Identifier
PaLM	Pathology and Laboratory Medicine
PCC	Patient Care Coordination
PHARM	Pharmacy
PHI	Protected Health Information
PWP	Personnel White Pages
QRPH	Quality, Research and Public Health
RAD	Radiology
RBAC	Role Based Access Control
RO	Radiation Oncology
RSNA	Radiological Society of North America
SAML	Security Assertion Markup Language
SeR	Secure Retrieve
SNOMED_CT	Systematized Nomenclature of Medicine-Clinical Terms
SURG	Surgery
W3C	the Word Wide Web Consortium
WSS	Web Services Security
XCA	Cross-Community Access
XDM	Cross-Enterprise Document Media Interchange
XDR	Cross-Enterprise Document Reliable Interchange
XDS	Cross-Enterprise Document Sharing
XSPA	Cross-Enterprise Security and Privacy Authorization
XUA	Cross-Enterprise User Assertion

Key words

eHealth, medical informatics, health informatics, healthcare informatics, health care informatics, clinical informatics, IHE, IHE ITI, security, XUA, ATNA, BPPC

Ključne riječi

eZdravstvo, medicinska informatika, zdravstvena informatika, IHE, IHE ITI, sigurnost, XUA, ATNA, BPPC

Abstract

eHealth is an emerging field with the main objective to improve the healthcare locally, regionally, and worldwide using ICT (*Information and Communication Technologies*). As types and number of different eHealth systems is continuously growing, especially in developing countries, their integration and interoperability present even greater challenge on a day-to-day basis. This is addressed by the global initiative to improve the interoperability in healthcare informatics and the way computer systems in healthcare share information, IHE (*Integrating the Healthcare Enterprise*). Its vision is not only to provide seamless access to health information, but also secure. Security in eHealth, especially in integrated eHealth environments is very important i.e., eHealth is on the list of the top three sensitive industries regarding information created, processed, stored, and transmitted. Moreover, unauthorized access to health information or its misuse can present a different level of risk which in the worst-case scenario may be a patient's life. The main goal of this thesis is to give insight in high-level definitions within the IHE ITI (*Information Technology Infrastructure*) technical framework, more specifically to explain the purpose and implementation of ATNA, BPPC and XUA security related profiles and to propose use cases. These profiles support different security controls for identification, authentication, authorization, confidentiality, integrity, non-repudiation, patient privacy and audit logging for standardized environments, not dependent on the eHealth system's architecture, specific process and mechanisms used but demanding existence of interoperable policies and regular risk assessment.

Sažetak

Područje eZdravstva je u postojanom razvoju, a glavni cilj mu je poboljšanje zdravstvene skrbi na lokalnom, regionalnom i globalnom nivou koristeći informacijske i komunikacijske tehnologije (engl. *Information and Communication Technologies*, ICT). Budući da broj različitih sustava eZdravstva kontinuirano raste, posebno u zemljama u razvoju, njihova integracija i interoperabilnost predstavlja još veći izazov iz dana u dan. Globalna inicijativa za poboljšanje interoperabilnosti u informatici u zdravstvu (*Integrating the Healthcare Enterprise*, IHE) nastoji poboljšati način na koji računalni sustavi u zdravstvu dijele informacije. Njegova vizija nije samo osigurati besprijekoran pristup zdravstvenim informacijama, već i sigurnost pristupa. Sigurnost u eZdravstvu, posebno u integriranim eZdravstvenim okruženjima je vrlo važna, odnosno eZdravstvo je na popisu tri najosjetljivije industrije prema informacijama koje se stvaraju, obrađuju, pohranjuju i prenose. Štoviše, neovlašteni pristup zdravstvenim informacijama ili njihova zlouporaba predstavljaju različite razine rizika, a u najgorem slučaju to može biti i ugrožavanje života pacijenta. Glavni cilj ovog rada je dati uvid u definicije visoke razine unutar tehničkog okvira IHE ITI (*Information Technology Infrastructure*), odnosno objasniti svrhu i implementaciju ATNA, BPPC i XUA sigurnosnih integracijskih profila te predložiti studije slučajeva. Ovi profili podržavaju različite sigurnosne kontrole za identifikaciju, autentifikaciju, autorizaciju, povjerljivost, integritet, nepovredivost, privatnost pacijenata i evidenciju promjena za standardizirana okruženja, te su neovisni o arhitekturi sustava eZdravstva, specifičnim procesima ili korištenim mehanizmima, ali zahtijevaju postojanje interoperabilnih politika i redovitih procjena rizika.

Biography

Hristina Marošević was born in Skopje, Macedonia on 13th of April 1992. She was studying telecommunications from 2010 to 2014 at the Faculty of Electric Engineering and Information Technologies as four-year undergraduate student in Skopje, Macedonia. After finishing undergraduate study, she gained experience in different fields involving information and communication technology and signal processing in Macedonia. One year later, in 2015 she enrolled in graduate studies in the field of telecommunication and informatics, offered as two-years studies by the Faculty of Electrical Engineering and Computing in Zagreb. While studying in Zagreb, she gained more specific experience within the core segment of internet and telecommunication provider ISKON d.d. and core eHealth sector within Ericsson Nikola Tesla d.d. in Zagreb. After finishing graduate studies at the Faculty of Electrical Engineering and Computing in Zagreb in 2017, she decided to direct her career in the information security field in Ericsson Nikola Tesla and is hired as software developer in the security and system administration team. This team is involved in planning, development, implementation, and maintenance of eHealth projects in different countries (Croatia, Republic of Kazakhstan, Belarus, etc.) but also in local activities in DevOps and DevSecOps enabling virtual environments, infrastructure services and continuous improvement of technologies involved. Motivated by various requirements specific for each country or client and in need of a comprehensive insight in security, which is not dependent on industry and regions, she enrolled in specialist study in the field of information security in 2018 by the Faculty of Electrical Engineering and Computing in Zagreb.

Životopis

Hristina Marošević rođena je u Skopju 13. travnja 1992. Studirala je telekomunikacije od 2010 do 2014. godine na Fakultetu Elektrotehnike i Informacijskih Tehnologija u Skopju, Nakon završetka studija stekla je mnoge vještine u različitim poljima koja obuhvaćaju informacijske i komunikacijske tehnologije te procesiranje signala. Godinu nakon, upisala je diplomski studij na Fakultetu Elektrotehnike i Računarstva u Zagrebu. Tijekom studija u Zagrebu stekla je specifičnije iskustvo unutar jezgrenog segmenta u ISKONu d.d., tvrtka koja nudi internet i telekomunikacijske usluge te unutar jezgrenog eZdravstvenog sektora u Ericssonu Nikole Tesle d.d. Nakon završetka studija 2017. godine odlučila je usmjeriti svoju karijeru k informacijskoj sigurnosti te se zaposlila u Ericssonu Nikole Tesle kao član tima odgovoran za sigurnosnu i sistemsku administraciju. Ovaj tim radi na planiranju, razvijanju implementacije i održavanja eZdravstvenih projekta u različitim zemljama (Hrvatska, Kazahstan, Bjelorusije, itd.), osim toga i u lokalnom *DevOps* i *DevSecOps* okruženju omogućavajući virtualne okoline, infrastrukturne servise i kontinuirano poboljšanje postojećih tehnologija korištenih unutar sektora. Motivirana sa strane različitih zahtjeva postavljenih sa strane različitih zemalja i klijenata i u potrebi za sveobuhvatnim uvidom u sigurnost, koji je neovisan o specifičnoj industriji i regijama, upisala je specijalistički studij u području informacijske sigurnosti na Fakultetu Elektrotehnike i Računarstva u Zagrebu, 2018 godine.