Ready to improve Cybersecurity for health data exchange?

Cybersecurity is now considered a key priority for all entities creating and managing health data. The concerns to remove cyber vulnerabilities apply both within the health delivery organizations such as hospitals, and in the platforms for health information exchange serving the regional, national and cross-border levels.

IHE takes this challenge very seriously and now offers its support for an important next step.

For over 10 years IHE has enabled vendors to address security risks for health data exchange in standard-based ways. In 2018, IHE approved a major incremental in its security specification step (see below for an overview of the three new Options for the ATNA Profile).

2019 is the year where the digital health technology community wants to deliver much stronger Cybersecurity protection than was previously available. Vendors of a wide range of health IT systems and devices products can demonstrate their support for such enhanced Cybersecurity by testing their products in the world's largest health interoperability events – the next IHE Connectathons in the USA (January 2019) and in Europe (April 2019). This also enables users that deploy or use these products to witness the readiness of their technology partners.

What is the next step?

For vendors that are already registered to the IHE-USA Connectathon (Registration is already closed):

- ⇨ It is still possible to add these three Cybersecurity protection ATNA options to your testing goals

For vendors that are planning to register to the IHE-Europe Connectathon (Registration opens December 1st and closes January 10th, 2019):

- ⇨ Include these three Cybersecurity protection ATNA options to your products testing goals

For users and policy makers:

- ⇨ Register to the IHE-USA newsletter (www.iheusa.org)
- ⇨ Attend the IHE-Europe Connectathon Symposium on Tuesday April 9th in Rennes (France) to see the testing in action and register to the IHE-Europe NewsPulse (https://ihe-europe.net/newsletter/subscribe) to hear about the testing results

How does this accelerate the deployment of a stronger Cybersecurity?

Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing any country's security, economy, and public safety and health at risk. Similar to financial and reputational risk, cybersecurity risk affects a company's bottom line or the credibility of a government's institutions. It can drive up costs and impact revenue. It can harm an organization's ability to innovate, to gain and maintain trust of its citizens or customers.

Approaching cybersecurity is mainly undertaken as a set of risk management activities. Organizations may choose to handle risk in different ways[1], including mitigating the risk, transferring the risk, avoiding the risk, or accepting the risk, depending on the potential impact to the delivery of critical services.

Integrating the Healthcare Enterprise (IHE) is focused on facilitating the adoption of standards for the exchange of health information. IHE's objective -- to facilitate interoperability -- does not put it at the center of Cybersecurity Risk Management activities, except on the dimension of protecting health information whilst in transit. This includes:

- Establishing secured communication pathways using cryptographically strong authentication, so that individuals and systems authentication prevents unauthorized access to systems or devices functions
- Encrypting information exchanged between mutually authenticated systems

In summary, there are many facets to address Cybersecurity risks. Support of these three new options in IHE-ATNA covers one of them: Cyber protection of health information exchange.

Is IHE qualified to address this facet of Cybersecurity?

IHE is multi-stakeholder, non-profit organization dedicated to improving standards-based interoperability in healthcare (www.ihe.net and www.ihe-Europe.net). Security and Privacy are core elements included in that mission. Its mission is to identify and profile standards (widely adopted internationally) for effective interoperability in support of user selected use cases.

One such profile, widely used world-wide in eHealth, is the current IHE ATNA (Audit Trail and Node Authentication) Profile:

- It is one of the 27 IHE Profiles formally recognized by the European Commission (http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2015_199_R_0011).
- It is listed in the Interoperability Standards Advisory (ISA) publication issued annually by the US Department of Health and Human Services (http://www.healthit.gov/isa/ISA_Document/Appendix_I)
- It is used in a large number of eHealth Deployment in Europe, the USA, and around the world.
- Health IT applications and devices products from 320 vendors world-wide have been recorded for support of the original ATNA Profile at IHE Connectathons. https://connectathon-results.ihe.net/.

IHE IT Infrastructure domain recently published three new Options to the IHE ATNA (Audit Trail and Node Authentication) Profile, it is now easy for vendors to claim compliance to the IETF most current Cybersecurity best practice (BCP 195 – Support of TLS1.2 and stronger cypher suites, and certificate validation). For details, see below Section called: The three new Cybersecurity Options introduced in ATNA.

With these Options, users and vendors are offered the best balance between flexibility and guaranteed interoperability. This is why testing of these three Cyber protection options at the IHE Connectathons is important:

[1] International Organization for Standardization, *Risk management – Principles and guidelines*, ISO 31000:2009, 2009. http://www.iso.org/iso/home/standards/iso31000.htm

- For vendors to confirm their product readiness and be assessed positively as part of the official IHE Connectathon results.
- For users to assess that interoperability is achieved with the highest level of Cyber protection available in 2019.
- For the public authorities to know that a stronger level of cyber protection for health information exchange is now established for policy making.

More about the three new Options in ATNA Profile for Cybersecurity

The technical details are available in the approved IHE Change Proposal ITI CP-ITI-1145, which introduces three new options:
ftp://ftp.ihe.net/IT_Infrastructure/TF_Maintenance/CPs/3_FinalText/CP-ITI-1145-01-ballot49.doc

1. **BCP195 TLS Secure Transport Connection – All TLS versions**
   This option offers the highest level of protection for the TLS-protected communication channel by adopting the IETF Best Current Practice (BCP195), but include backward compatibility requirements to maintain interoperability with systems that do not support BCP195, by down-grading to TLS Version 1.1 or Version 1.0 and/or cypher suites under specific conditions that are allowed by BCP195. It will maintain interoperability as appropriate with existing ATNA implementations.

2. **BCP195 TLS Secure Transport Connection - TLS 1.2 Floor**
   This second option adds additional requirement to (a) not allow any TLS protocol lower than TLS 1.2 and (b) it makes mandatory some newer cypher suites that are only recommended in BCP195.

Both options are compatible with similar options present in Digital Imaging and Communications in Medicine (DICOM), thus ensuring that DICOM transactions tested in IHE Profiles meet the requirements of DICOM Supplement 204 – TLS Security Profiles.

These above two ATNA options are also being included in the IHE international Conformity Assessment program (ISO/IEC 17025 accredited laboratories) for release in January 2019.

3. **FQDN Validation of Server Certificate.**
   This third option enables the verification that the digital certificates have been issued by a trusted authority to the fully qualified domain name (FQDN) of the server to which the request or submission has been addressed. This allows for the prevention of traffic interception by a malicious attacker (man-in-the-middle attacks). These are significantly more dangerous over the public Internet, since more methods exist. Many of these methods are widely known; this is why RFC 6125 requires server certificate verification for all TLS traffic.

By bringing such a special focus at the IHE-Europe Connectathon, April 8-12, 2019 in Rennes, France the goal is to test a large number of interconnected systems from about 80 vendors in Europe. By moving forward the state of cyber protection in health, IHE is supporting in a practical way one of the goals set by ENISA (www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals), the European Network and Information Security Agency (ENISA).