Interfacing IHE® profiles with Smart Storage Controllers for patient privacy in healthcare settings

Abstract

In the age of big data analytics, the medical realm seems a particularly demanding subject area to conquer. Digitized healthcare processes are expected to speed up or automate administrative and documentation-related tasks, make crucial medical information readily available when needed, and establish the foundation for data analysis systems that lay claim to revolutionize the modus operandi of clinical research. With all signs pointing toward digitization, ensuring patient privacy is a core issue to all of these objectives. Not unlike the GDPR, handling patient privacy consent requires adaptability to different scenarios, multi-level privacy clearances, and tying access to defined purposes or periods of time.

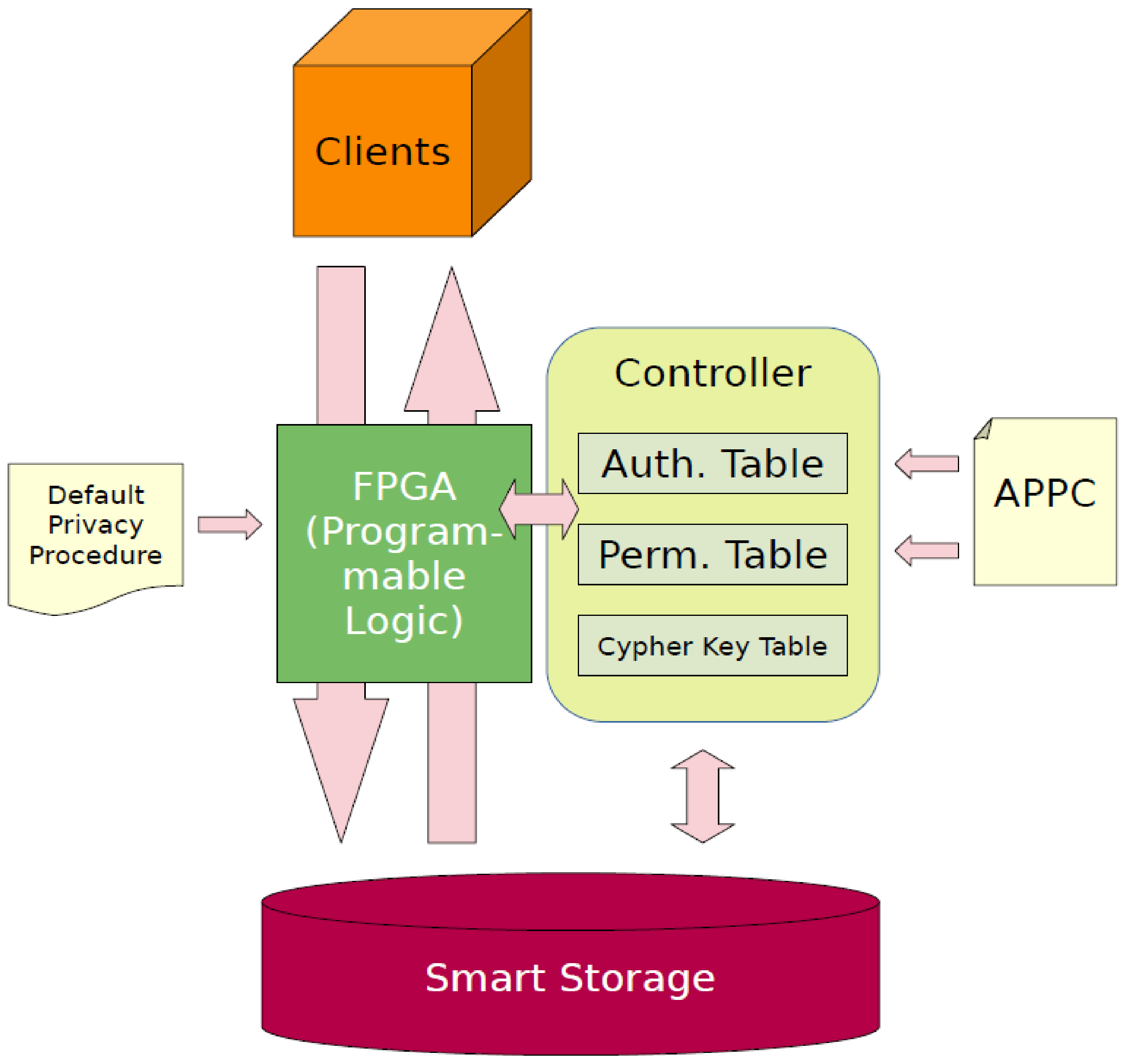
Against this backdrop, Integrating the Healthcare Enterprise® (IHE) profiles such as the Advanced Patient Privacy Consent could complement the concepts presented in Prof. Zsolt István's lecture when implemented in a healthcare setting. While default privacy practice might be introduced on a hardware level, IHE profiles could serve as consumable input to the Controller component. This research proposal explores the opportunities, challenges, and implications of interfacing digitized patient privacy consent forms in Smart Storage systems.

Problem

Secure and reliable management of privacy concerns is of utmost importance when handling clinical data. Fail-safe means of storage and access control of medical information are required to comply with patients' rightful demand for more control and agency in their treatment and prevent unauthorized disclosure of medical documentation to outside parties. As of today, the lack of a reliable and scalable infrastructure concept that meets these requirements hinders digitizing healthcare environments and processes.

Goal

Although there is no shortage of experience in how specific privacy consent situations are to be implemented, a sustainable solution to the problem should be adaptable to the plurality of healthcare settings and consent situations that would arise from opting out from routine data privacy handling. Viable approaches to the problem would allow for updating a patient's privacy consent information, e.g., to facilitate access clearance for large-scale data analysis and research purposes, while meeting the highest security standards to impede access with malicious intent.



Solution

IHE's Advanced Patient Privacy Protocol (APPC) allows digitally storing structured patient privacy consent information. By making IHE's APPC profile consumable to the Controller, Authentication and Permission tables are updated with the consent information held within. In implicit consent or opt-out scenarios, the implied standard procedure is represented as programmable logic on a Field Programmable Gate Array (FPGA) device in the Smart Storage's hardware.

In explicit consent or opt-in scenarios, the most commonly used handling of information serves as default and is processed through FPGA devices.

Any exceptions to the hardwired default privacy procedure are managed by the Controller component, which will take APPC-informed decisions. With APPC, an internationally recognized healthcare communication standard of privacy consent would be incorporated into Smart Storage solutions. This interface facilitates the development of infrastructure ready to take on the plethora of clinical data that will soon be generated in digitized healthcare environments and paves the way for meeting the objectives described above.

Daniel Jühling
Master Student
Digital Health

IHE INTERNATIONAL | Integrating the Healthcare Enterprise

HPI Hasso Plattner Institut

Lecture Series on Database Research