Research and Proof of Concept of Selected ISKE Highest Level Integrity Requirements

Deivis Treier, supervisor PhD Raimundas Matulevičius

University of Tartu, Faculty of Science and Technology, Institute of Computer Science, MSc Cyber Security

Introduction

In Estonian state IT systems and registries application of IT Baseline Security System (ISKE) is mandatory. Some data carries highest ISKE integrity sub class "T3" where three crucial sections apply. In those sections number of security requirements are elicited. During research we developed Proof of Concept solution to show how to implement selected requirement and achive higher data protection. We propose solution as template for third party developers and state institutions IT departments as reference system to use in production systems. We hope public discussion about problem domain helps to enchange data security in state and private sector.

Research Challenges

- The lack of public and systematic approach to the subject domain
- The lack of understanding about selected security requirements
- The lack of publicly available reference implementations
- The lack of understanding the data tampering detection process

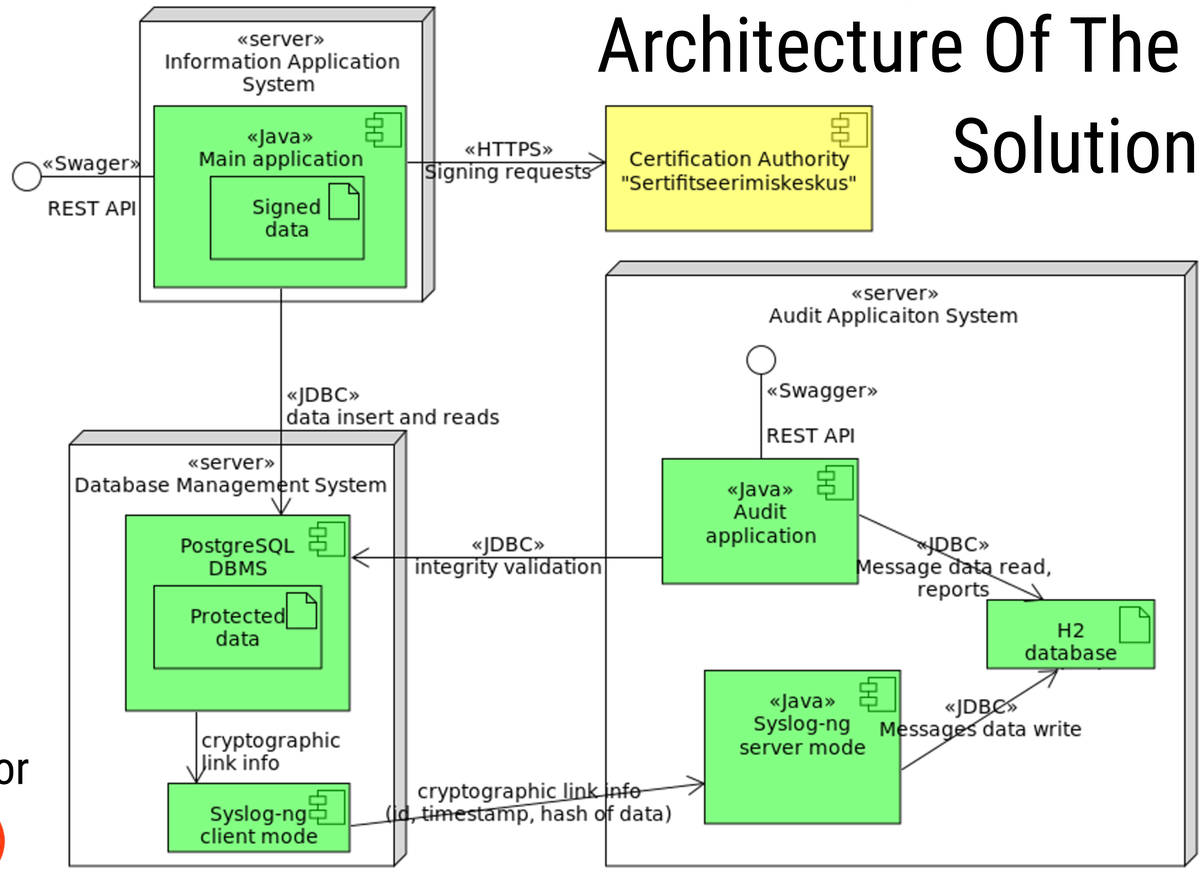
Core Features Of The Solution

- Data is inserted and accessed via REST API
- Data is handled in JSON format
- Data is digitally signed using standardised format
- Digital signature has legal effect outside database
- Digital signature ensures integrity of data
- Data is stored in open source relational database
- Database records are cryptographically linked using hash link
- Hash link meta info is deposited internally
- Database hash link correctness can be regularly validated
- Database tampering detection should be maintained by department of security

Working Principles Of The Solution

Data is stored and accessed via REST API of Information Application System (IAS). In IAS data is digitally signed using format what complies with EU eIDAS regulation. Data is stored in Database Management System (DBMS). All main data records are chronologically linked with previous records forming cronologically ordered hash link. Meta info of hash link is deposited using syslog and Syslog-ng to Audit Application System (AAS) and stored in separate database. When database tampering detection process executed by AAS, hash link meta info is sent to DBMS and table hash link is recalculated. Calculation result is compared with meta info stored in AAS. It is highly recommended to deploy and maintain AAS under separate administrative right than DBMS.

Architecture Of The Solution



https://github.com/DeltaTango/thesis

June 2017

TARTU ÜLIKOOL 1632 arvutiteaduse instituut

IT Akadeemia toetab Skype™

Sponsor SK ID SOLUTIONS