



SMARTESB™



SmartESB™ is a drop-in framework that can be easily added to existing client-server or web-based applications to automatically secure all communications and manage authentication from the enterprise servers out to and including the devices on which the client software or web browser is used.

1

Introduction

The Smart Enterprise Service Bus (SmartESB™) is a ready-made solution that can be dropped into existing client-server or web-based applications to automatically secure all communications and manage authentication from the enterprise servers out to and including the devices on which the client software or web browser is used.

It does this by using elegant, light touch proprietary methods that work seamlessly with most web applications and any client using standard HTTP/HTTPS libraries. SmartESB™ provides full data encryption at rest in the devices themselves as well as in transit and across the entire SmartPoints™ technology stack.

2

The Problem

Hospitals and clinics must secure and control information anywhere it may reside. However most off-the-shelf web applications don't offer the degree of security and data privacy that is required.

Managing and configuring data privacy goes far beyond simply enabling HTTPS. Maintaining complex networked applications is error prone and expensive both in real costs and with respect to the amount of time and energy necessary to maintain and monitor them.

Hospitals and clinics increasingly need to manage private information, which needs to be made available on external networks and mobile devices. The lack of inherent information privacy leads to enormous added costs and limits the ability to deliver the features demanded by the end users of the information.

3

The Solution

The Smart Enterprise Service Bus (SmartESB™) provides an elegant and simple solution using a combination of patented and proprietary technology. Multiple deployment options are available to suit any distributed application without requiring any change to the application itself.

Once deployed, SmartESB™ seamlessly provides complete auditability, security and authentication, while protecting and encrypting information at rest, in transit, and during use.

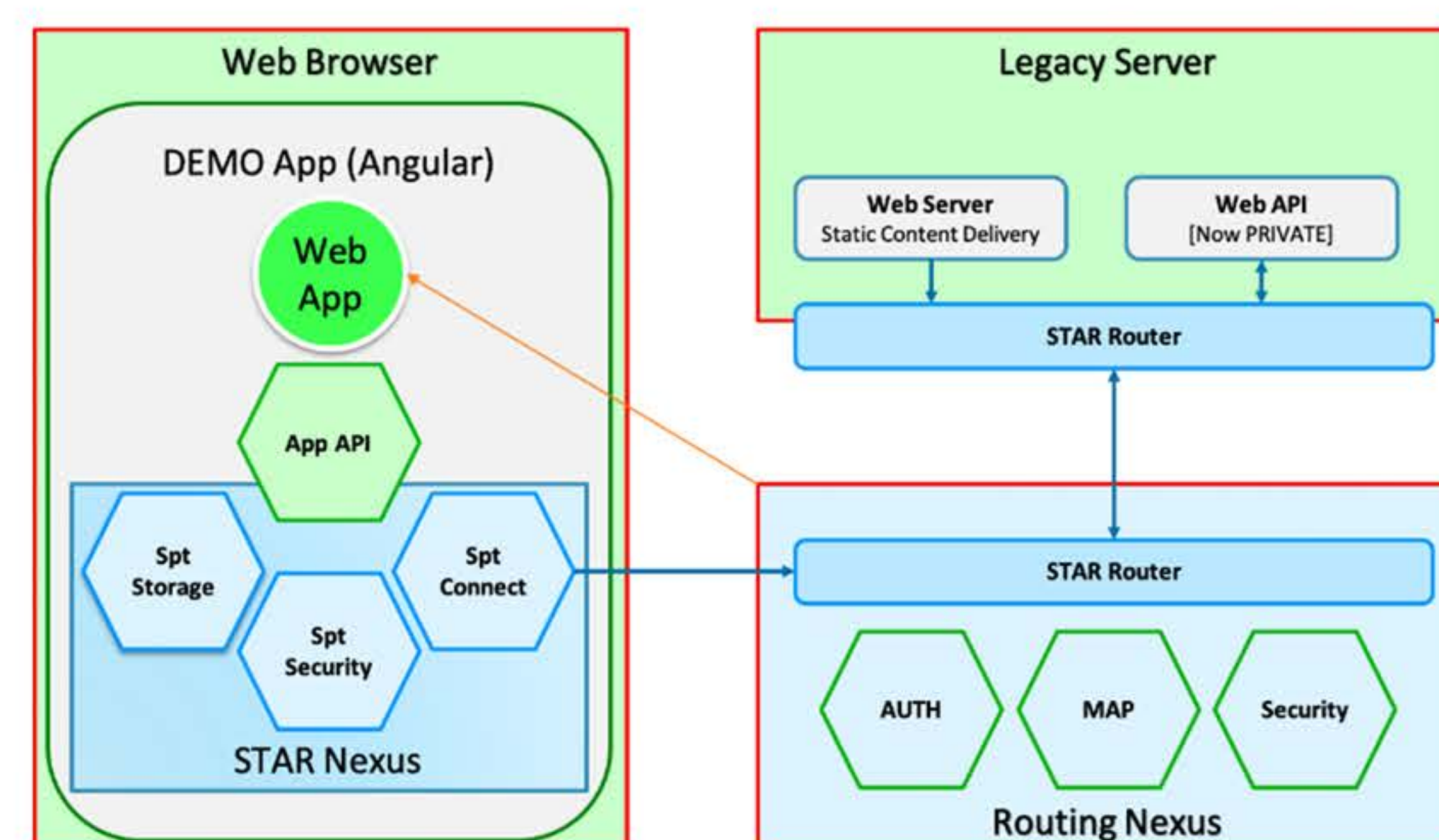


Figure 6 : High Level Architecture. Note that the SmartESB™ Router is the only added component as the "Web app" pulls the libraries from it.

4

The Design

The SmartESB™ is designed to be simple to setup and manage. The SmartESB™ is deployed using the same techniques that all IT departments are familiar with. Virtual Machine, Docker Images, and appliances are available along with zero touch cloud hosting options.

A SmartESB™ Service acts as a proxy for the application(s) being secured. No change to the application itself is required. A simple configuration update is all that is required to allow clients connecting to the application to be automatically secured with the SmartESB™.

5

Current Versions

SmartPoints™ Medical has multiple working versions of the SmartESB™ currently deployed to secure web applications. Currently the SmartESB™ is delivered as a Virtual Machine that comes pre-configured to suit the deployment environment.

Web based applications built with Angular and React are supported natively. Other client environments are also available.

SmartESB™ currently supports integrated authentication for LDAP and Active Directory.

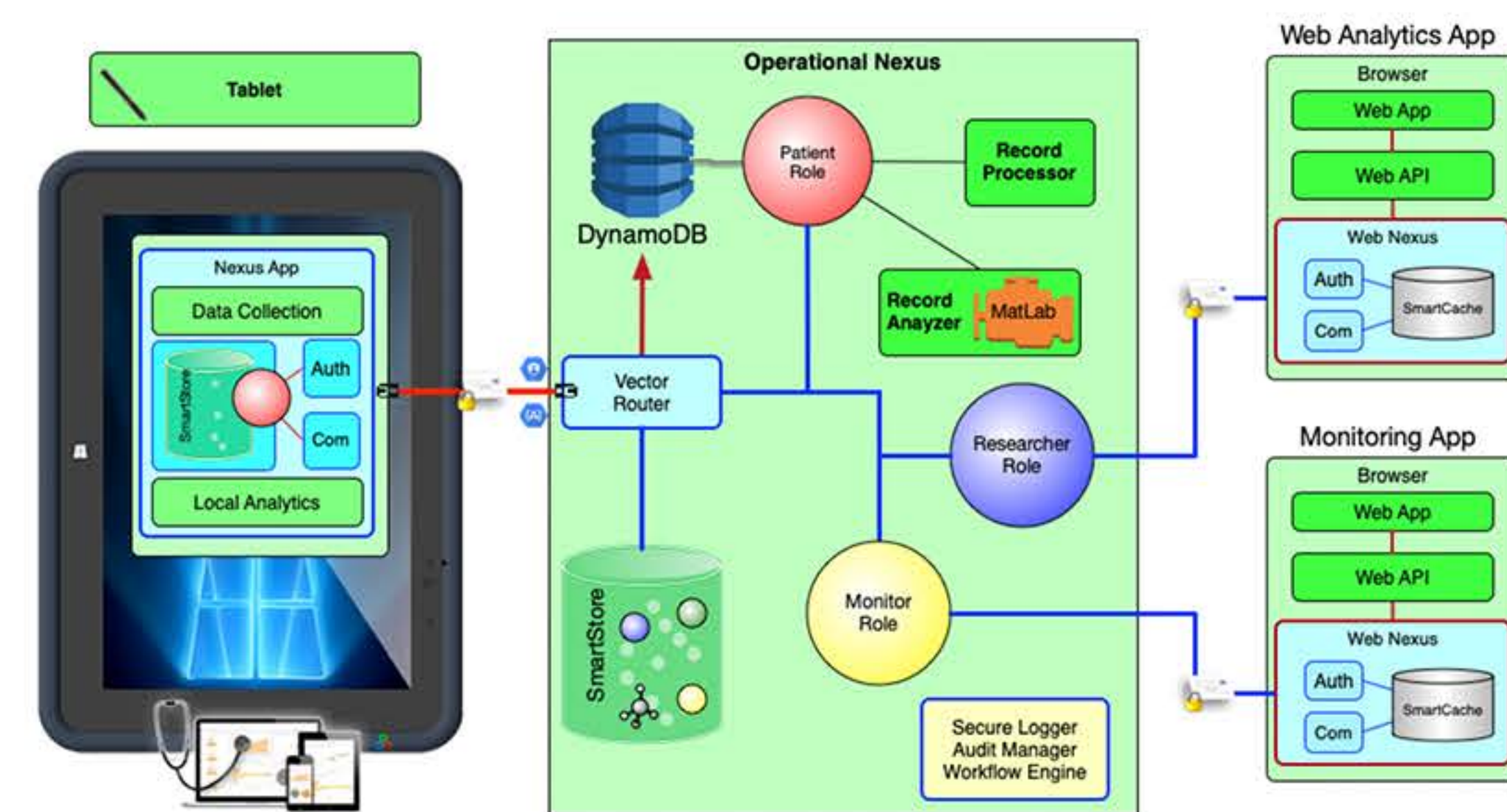


Figure 7 : Example Solution.

6

Future Versions

SmartPoints™ Medical constantly strives to seek out industry expertise to improve features, functions and designs. We work collaboratively with our clients and partners to gather input to develop and deliver best in class solutions. We are currently exploring native support for deployment in mobile devices, expanded audit features, and additional single sign-on capabilities.

6

Requirements for SmartESB™

- Any web-based application that works in modern browsers.
- Any distributed application that uses standard communication libraries.
- The server component of SmartESB™ is available as a physical or virtual appliance. It can also be installed in any existing host running Windows or Linux.

Business Benefits

- Reduced operational costs.
- Significantly increased security via SmartPoints™ Hyper-Secure technology.
- Increased regulatory compliance
- Increased visibility.
- Provides OEM “phone home” capabilities required by most OEMs.
- Eliminates the need for multiple, managed VPNs.
- Eliminates the need for sophisticated network access control lists (ACLs).
- Full enterprise control and visibility.
- Does not require retesting of existing applications.
- Plug and Play configuration.
- Powerful post-installation configuration available.