## Two-Sentence Overview

The goal is to protect Personally Identifiable Information (PII) or Protected Health Information (PHI) that are utilized in digital health software tools or approved Digital Square global goods. StrongKey’s appliances, deployed in an on-premise or managed service mode, run an open source software stack that protects PII and PHI by with strong authentication and data encryption. StrongKey has 18-years of related cyber-experience delivering such capabilities to organizations on six continents.

## Executive Summary

* The overarching goal is to protect Personally Identifiable Information (PII) or Protected Health Information (PHI) that are utilized in digital health software tools or approved Digital Square global goods. Protecting this type of information is critical to Digital Square being able to realize the value of its investment in digital health software tools or global goods that utilize PII or critical information.
* A typical investment for an on-premise deployment would be around $100,000 for an infrastructure that provides fault tolerance and high-availability, with about $25,000 annual support costs. Professional Services integration costs (for framework or specific global goods integration) would range from $25,000 to $50,000.
* StrongKey provides strong authentication and data protection using an open source software stack deployed on hardware appliances that can house either a Trusted Platform Module (TPM) or a Hardware Security Module (HSM). The hardware (TPM or HSM) is chosen to protect the security keys required for the cryptographic techniques required to achieve the overall goal.
* StrongKey has developed and delivered the reference server for the FIDO2 protocol which is an authentication protocol adopted by 250 key Fortune companies, including Microsoft, Google, and Apple, to name but a few. The FIDO2 server provides strong authentication, while sensitive data such as Personally Identifiable Information (PII) or Protected Health Information (PHI) can be secured through the use of simple web service (SOAP or REST) API calls. For the non-technical this makes cryptography easily implementable to developers, and takes away the headache of understanding the nuances of cryptography.
* One thing to note is the type of tools and goods that Digital Square is investing in is open to ransomware attacks by aggressive bad actors. StrongKey is able to mitigate such attacks with the use of the appliances described here.

## Consortium Team

Rather than partnering with any one particular organization, StrongKey would like to make itself available to assist any organization participating in Digital Square projects. Part of becoming shelf-ready is to ensure that data security and authentication of users is not just an afterthought, but rather a feature tightly integrated with the application and implemented by digital security experts. It is our hope that other E0 applicants may see our offering here and recognize synergy with their project.

Examples may be:

* + *For the concept* ***Improving the Resiliency, Privacy, and Interoperability of the Open Smart Register Platform (OpenSRP) t****hey mention Work Package 2: Add Personally Identifiable Information masking across all OpenSRP APIs*
	+ An example of an Approved Global Goods project may be **OpenELIS**. We would be able to protect the PII data to the highest level of security standards.
	+ There seem to be many other opportunities for the use of the StrongKey technology as part of the OpenHIE initiatives/community.

## Project Description

**Objectives**: StrongKey stands ready to help Notice E0 Phase1 Shelf-readiness applicants either via product or simply via conversations on application and data security. The StrongKey appliance presents simple web services (either REST or SOAP) for applications to implement strong authentication or data protection. These systems have been designed to make cryptography easy for the developer. The technical approach or anticipated activities would be a very straightforward software integration to the Digital Path software tools or global goods. In terms of software development projects this is an order of magnitude easier than attempting to develop security capabilities from scratch.

**Deliverables & Schedule**: We anticipate that a fully integrated system could be achieved within 90-days. integrated software APIs. We have answers to many issues related to connectivity, that we can describe in greater details.

In order to protect PII or other critical data, many cryptography techniques can be used which could include some, all or others such as:

* Use a FIPS 140-2 Level-2 Trusted Platform Module (TPM2) as a standard cryptographic hardware module for key-management, or a FIPS 140-2 Level-3 Hardware Security Module (HSM) as an optional module in the appliance;
* Issue millions of X.509 digital certificates to humans, devices, applications, etc.;
* Manage hundreds of millions of symmetric keys for encryption, Hashed Message Authentication Code (HMAC) operations;
* Encrypt and Tokenize sensitive information, such as:

◦ Personally identifiable information (PII) for General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) compliance;

◦ Personal health information (PHI) for Health Insurance Portability and Accountability Act (HIPAA) compliance;

◦ Personal financial information (PFI) for Payment Card Industry Data Security Standard (PCI-DSS) compliance, etc.;

* Encrypt files of any-type and any-size while ensuring only authorized entities may decrypt content;
* Enable the storage of encrypted files on seven (7) different public cloud storage services while protecting cryptographic keys within the appliance;
* Enable digital signatures of files to preserve the integrity of content;