

## **Statement of Work**

### **SLAC TrustDer Key-Maker**

#### **Table of Contents**

##### **1. Introduction**

- a. Background and Motivation
- b. Project Goal
- c. Broader Vision
- d. Why this approach ?
- e. Business Advantages
- f. Key Stakeholders
- g. Major Deliverables
- h. High level Duration and Timeline

##### **2. Scope of Work**

- a. What is included ?
- b. What is not included ?
- c. High Level Requirements
- d. Assumptions
- e. Constraints
- f. Risks
- g. Deliverables
- h. Success Criteria

##### **3. Detailed Deliverables**

- a. High Level Milestones
- b. Technical Deliverables
- c. Non-Technical Deliverables
- d. Communication Plan

##### **4. Guidelines**

- a. Project Organization and Individual Roles
- b. Progress Review Process
- c. Change of Scope Procedure
- d. Non-Staffing Costs
- e. Staffing Resources
- f. Documentation Resources

##### **5. Acceptance**

## Revision History

Document Version	Date
1.0	09/13/2022
2.0	09/20/2022
3.0	10/07/2022
4.0	11/04/2022

## Summary

<b>Project Name:</b> TrustDer - Key Maker		
<b>Business Owner(s):</b> SLAC National Accelerator Laboratory		
<b>Project Manager(s):</b> Pramod Illuri		
<b>Date of First Draft:</b> 09/13/2022	<b>Latest Version No.:</b> 4.0	<b>Date Agreement Reached:</b>
		<b>Latest Revision Date:</b> 11/04/2022

## **Introduction**

### **Background and Motivation**

Currently, the method used to store identities of devices is imprinting a secret/identity information in a silicon chip such as an EEPROM or SRAM. These identities are verified using hardware cryptographic operations like digital signatures and encryptions. The disadvantage in this method is that the manufacturing cost of imprinting secrets in these types of silicon is high. Moreover, The hardware required to implement Secure Hash Algorithms for digital signatures is expensive. This method also requires an additional protection mechanism, to prevent invasive attacks, which would consume a lot of power.

### **Project Goal**

The goal of this project is to develop software for an information theoretic approach that allows device identity to be verified by network participants. This approach aims to be decentralized, prevents a single point of failure, and can be as effective as imprinting an identity in silicon.

### **Broader Vision**

Connecting multiple home energy devices for building a smart energy ecosystem is one of the SLAC's broader energy management initiatives. Secure way of identifying new devices entering the network is crucial for keeping the network secure. Although SLAC aims to build the project for this use-case, the core algorithm can be applied to any IOT network that intends to secure its network from untrusted entities.

### **Why this approach ?**

The motivation behind a software-based decentralized verification system is that the identity of devices can be verified while preserving privacy, meaning it does not need an additional protection mechanism. In doing so, the cost and power consumption of the devices are also reduced. An additional advantage of implementing this approach as a set of smart contracts on a blockchain-based network is, the code is shared and run on every single device, making it easier to scale reliably.

**Business Advantages**

1. Decentralized verification system which prevents single point of error
2. Cost advantage by moving to a software-based approach
3. Ability to enable verification system on already installed assets
4. Common technique for verifying devices manufactured from different vendors

**Key Stakeholders**

SLAC National Accelerator Laboratory

- Represented by Mayank Malik

Carnegie Mellon University

- Practicum coordinator - Cynthia Kuo
- Faculty advisor - Hanan Hibshi
- Student Team - Pramod Illuri, Keshava Srinivas, Noora Alfayez, Nithin Ram Gomatam Vasudevan, Prerit Pathak, Vaanya Gupta

**Major Deliverables**

1. Working prototype of the keymaker protocol on the proposed system
2. Open-source GitHub repository of developed code
3. Summary of the project presented on a poster
4. Contribution to a research paper (optional)

**High level Duration and Timeline**

Project duration - 14 weeks (Until Dec 16th, 2022)

Project includes various intermediary milestones, which act as check points (Details given in further sections)

## Scope of Work

### What is included ?

The scope of this project is to implement the keymaker protocol in its entirety on a distributed blockchain network as a smart contract. This is to be done by integrating and testing the entire workflow on 5 Raspberry Pi devices which will act as a proxy for a variety of DER devices installed at Grid Integration Systems and Mobility (GISMo) lab at SLAC. The scope of the keymaker protocol is to provision device identity, compute and distribute identity shards, and perform a social verification/authentication of a device that newly joins an existing network of trusted devices.

### What is not included ?

The scope of the project does not include the following:

1. Real world testing of protocol
2. Incident response when an imposter device is detected
3. Scalability is out of scope in the context of this prototype

## High Level Requirements

### Functional Requirements

1. The system should provision device identity using specified identity protocol.
2. The system should compute and distribute identity shares to nodes on the network.
3. The system should successfully verify the identity of a device entering the network.
4. The Social Verification of a device identity should be implemented using the keymaker protocol involving Shamir secret sharing and symmetric encryption. The verification should abide by the following constraints:
  - a. Only  $k$  shards are required to perform the verification of the secret key.  $k < n$  where  $n$  is the total number of shards distributed
  - b. Any shard must not be a subset of the key
  - c. All shards combined must not reveal the key
5. The verification should utilize authenticated encryption along with the Shamir secret sharing (SSS) in order to retrieve the device key in an event of key loss.
6. The proof of concept should be deployed on a network of 5 raspberry pi devices or a virtual network of 5 containers.

### Non-Functional Requirements

Note : Since the project is an early proof of concept for a research idea, NFRs doesn't have much relevance at this stage of the project. However, highlighting a few key ones to be kept in mind.

1. The social verification algorithm must respond with consensus in few seconds and must be under a minute
2. The proof of concept (POC) design should be scalable to a large network of devices in the blockchain. However, this is out of scope to be demonstrated in the context of this POC
3. The performance of the verification system must be as effective as imprinting device credentials in silicon

### **Assumptions**

1. The team will be able to identify a suitable layer 1 blockchain network after evaluating the potential options available
2. The blockchain network should be reliable and not susceptible to attacks. The smart contract should be executed securely in all devices. The potential security issues of the block chain network is out of scope in executing the current project.
3. The network devices already present in the context of the demo are assumed to be trusted.

### **Constraints**

#### Technical Constraints

1. Choice of blockchain - Limited time to validate different blockchains to select the one that suits the requirements of the project
2. Choice of programming language - Dependency on the choice of blockchain used, availability of packages, and developer support
3. Mode of final demonstration - Dependency on hardware constraints to be explored in future. Decisions will be made based on the outcomes.

#### Business Constraints

- None

**Risks**

Lack of real world domain expertise on blockchain technology that could impact the deliverable expectations

- Mitigation plan: Learning plan and sessions from mentors to fasten the process

Not being able to demonstrate the working prototype using hardware devices

- Mitigation plan: Exploring exact hardware requirements and also exploring to demonstrate using EC2 instances

**Deliverables**

1. Proof of concept of the keymaker protocol that runs reliably, on either a network of virtual nodes on the cloud or a network of 5 raspberry pi devices
2. Code for the keymaker protocol
3. Project poster
4. Final project report

**Success Criteria**

1. Working prototype of the key-maker protocol installed on Raspberry Pi devices connected in a block-chain network
2. The system should be able to successfully verify the identity of a device through participation from network members. Similarly, deny the untrusted device.
3. Meeting both technical and non-technical deliverables (Agreed upon the list shown below)

## Detailed Deliverables

### High Level Milestones

Item #	Description	Milestone #	Tentative Timeline
1	Exploring the problem space Technology exposure and handson Reference architecture System diagram	1	<b>Target date:</b> <b>10/07/2022</b>
2	Key-maker protocol local implementation - Identify provisioning - Sharding Identify verification	2	<b>Target date :</b> <b>11/04/2022</b>  Extended deadline: 11/11/2022
3	Setting up blockchain on AWS (Hyperledger Fabric)	2	
4	Integration - API setup - Shard distribution - Chain code	2	
5	Decentralizing key-maker protocol	3	<b>Target date :</b> <b>11/30/2022</b>  Extended deadline: 12/09/2022
6	On-Prem Hyperledger Fabric	3	
7	Raspberry Pi Integration	3	
8	Working prototype of the key-maker protocol and poster	4	<b>Target date :</b> <b>12/09/2022</b>  Extended deadline: 12/16/2022



**Technical Deliverables**

Item #	Description	Target Milestone
1	Reference architecture diagram	1
2	System diagram	1
3	Key maker protocol	2
4	Blockchain smart contracts	2
5	API integrations	2
6	Decentralized cloud application running on virtual nodes, as a prototype	3
7	MVP implementation of keymaker protocol that runs on 5 raspberry pi devices	3
8	Repository containing the keymaker protocol's code	4

**Non-Technical Deliverables**

Item #	Description	Timeline
1	Problem definition document	Project initial research phase
2	Weekly status reports	Continuous (Every Friday/Weekend)
3	Communication Plan	Project planning phase
4	Risk analysis	Project planning phase
5	Project Milestones	Project planning phase

6	Task management dashboard	Continuous
7	Consolidated project report	End of the project

### Communication Plan

#	Purosose	Frequency	Target Stakeholders
1	Project status report	Weekly	Sponsor (Mayank Malik), Faculty advisor (Hanan Hibshi)
2	Team meeting	Weekly	Sponsor, Faculty advisor, and Student team
3	Meeting with faculty advisor	Weekly	Faculty advisor, and Student team
4	Technical documentation	-	Sponsor, Faculty advisor, carnegie mellon university
5	Project management documents	-	Sponsor, Faculty advisor, carnegie mellon university

### Tools and Infrastructure

Project library: **Google drive** to store everything about the project - documentation, reports, and resources

Task management: **Trello**

Code management : **Git**

Infrastructure : **Amazon web services (AWS), Hyperledger Fabric**

Communication : **Slack, Gmail**

## Guidelines

### Project Organization and Individual Roles

The project has the following organization structure:

- Sponsor - Mayank Malik
- Technical Team : Design and Development
  - Nithin Ram Gomatam Vasudevan , Noora Alfayez , Keshava Srinivas , Prerit Pathak , Vaanya Gupta
- Project Manager - Pramod Illuri
- Faculty advisor - Hanan Hibshi

### Progress Review Process

1. Internal team stand-ups
2. Weekly meetings
3. Weekly status reports
4. Task management board (Trello)

### Change of Scope Procedure

1. Any change in scope requires a collaborative discussion with all the stakeholders for acceptance
2. Since timeline is a strict constraint for this project, the project plan is also likely to change accordingly

### Non-Staffing Costs

1. Raspberry Pi devices (5) - Facilitated by SLAC
2. Cost of AWS - Facilitated by SLAC and CMU
3. To begin with, all the tools will be on a free tier. Future upgrades will incur a small subscription expense.

### Staffing Resources



1. Technical resources x 5 - Contributing 24 hours a week
2. Project Manager x 1 - Contributing 12 hours a week

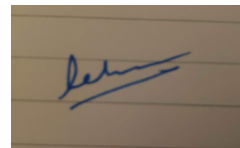


### Documentation Resources

1. Project Documentation Library : [TrustDer - Project Library](#)
2. Risk Register : [Risk Register](#)
3. Meeting Minutes : [Meetings](#)
4. Weekly Status Reports : [TrustDer-StatusReport-weekly](#)
5. Task management board : <https://trello.com/b/bX3axdmB/trustder>

### Acceptance of SOW

The following stakeholders hereby accept the statement of work agreed between the concerned.

Name	Role	Signature
Mayank Malik	Sponsor (SLAC - National Accelerator Laboratory)	Mayank Malik
Hanan Hibshi	Faculty Advisor (Carnegie Mellon University)	Hanan Hibshi
Nithin Ram Gomatam Vasudevan	Student - Technical Team (Carnegie Mellon University)	
Noora Alfayez	Student - Technical Team (Carnegie Mellon University)	

Keshav Srinivas	Student - Technical Team (Carnegie Mellon University)	
Prerit Pathak	Student - Technical Team (Carnegie Mellon University)	
Vaanya Gupta	Student - Technical Team (Carnegie Mellon University)	
Pramod Illuri	Student - Project Manager (Carnegie Mellon University)	