# 1 Work Plan

## 1.1 Project title/goal

"Investigating the feasibility of generating near-collisions for pEp TrustWords and its affect on security"

**Points:**
Use-case for TrustWords:

- Users are often deterred by difficulty in key authentication (e.g. PGP web-of-trust).

### 1.1.1 RFC drafts

`draft-marques-pep-handshake-02`
*"Short Trustword Mapping (S-TWM) requires a number of Trustwords that MUST retain **at least 64 bits** of entropy. Thus, S-TWM results into at least **four Trustwords** to be compared by the user."*

Showing that 4 words is too low in certain cases could be very useful?

`draft-birk-pep-trustwords-00`
In another draft document it also states:

*"It is for further study, what minimal number of words (or entropy) should be required."*

This shows there is some sort of research gap.

## 1.2 Literature review

**Usability and Security of Out-Of-Band Channels in Secure Device Pairing Protocols**
Paper shows the usability of current schemes. The can be useful to show the need for trustwords and how they would fit in. Maybe even that the security needs improving for word based auth schemes?

**Can Unicorns Help Users Compare Crypto Key Fingerprints?**
Another paper talking about the usability of user authentication schemes.

**An Empirical Study of Textual Key-Fingerprint Representations**
Another study on the usability of methods of comparing key-fingerprints. This one highlights on the high usability of words.

## 1.3 Formulation specific research questions

What is the purpose of this project and how could it be useful?

### 1.4 Methods for creating similarities in words

Visual:

- Levenshtein

Auditory:

- Soundex
- Metaphone (successor to Soundex)

Combined:

- Metaphone + Levenshtein

### 1.5 Experimentation

What do we want to look at?