# Protocol Overview

## Random Read

```
https://www.uwyo.edu/
```

Every communication from/to the “card” using NFC and the NDEF protocol is using a URL.

Players: Card, Phone, Blockchain (C, P, B)

Card has Private Key PK, and Public Key PP.
Card has Secret for generating OTP.
Card has Nonce NC.

Phone has install and setup the Validation software App.

# Validation Protocol

- Phone validates to Blockchain (SRP6a) This takes 3 requests to Blockchain. At the end both the phone P and the blockchain B share a secret key that has never been transmitted ove rthe wire. After this point all communication from Phone P to Blockchain B is done with AES-256 bit communication and can be uniquely identified.
- Establishes a key-exchange based encrypted communication
- Gets a “signature”, S and a “message”, M and a ephemeral public key, E, and web-of-trust signature W. (Curve25519 derived from Ed25519)
- Write to Card, S, M, E, W.
- Card verifies S+M v.s. W. If fail sends back failure message - exit.
- Card established a shared secret key with Blockchain using E. This will be enc(E,?) this uses Curve25519 (X25519) (1) Card generates secret and jjjj and sends that back to Phone
  (2) Phone P transmits jjjj to this to Blockchain B
  (3) Blockchain B computes the shared secret key on it’s side. Shends back info.
  (4) Phone Transmits info to Card. 2nd Write to card.
  (5) Card calculates same secret key.
- Card Generates random message R, and OTP(NC)
- Card encrypts R with E, making enc(E,R|NC) - only Blockchain B can decipher it.
- Card encrypts PP with E, making enc(E,PP) - only Blockchain B can decipher it.
- Card sends back to Phone P, encrypted random message enc(E,R|NC), cards encrypted public key enc(E,PP), OTP(NC), signature(R,PK) using Ed25519.
- Card increments Nonce, NC and saves it.
- Phone P, gets response from Card (if good)
- Phone P, asks blockchain B to validated enc(E,R|NC),enc(E,PP),OTP(NC),signature(R,PK)
- Blockchain B will:
  (1) use shared secret to decrypt enc(E,PP)
  (2) validate that this has never been done before using OPT(NC) (Uses PP to fetch secret,nonce)
  (3) write to Blockchain that hash(PP|OTK(NC)) has been used.
  (4) write to Blockchain incremented nonce for PP.
  (5) use shared secret to decrypt enc(E,R|NC)
  (6) use ephemeral private key to check signature on R.
  (7) if all good send back success + URL of data on product.
- If valid phone displays human data to finish validation. Else displays “invalid product” message.

## Transfer of Product from one owner to another

- Perform validation first.
- Using PP and OwnerPP lookup owner of Product - validate that it is owned by OwnerPP
- Validate signature of owner to be able to transfer NFT of product to new owner.
- get ReceiverPP (Think Scan QR code of Receiver from Phone, use NFC to get etc.) (Optional | Receiver is paying in ADA)
  (1) Receiver's phone gets a push-request to phone to authorize ADA transfer
  (2) Receiver - cliks yes on phone
  (3) Receiver - Authenticates (SRP6a)
  (4) Receiver - Sends funds to OwnerPP
  (5) OwnerPP - recives funds
- Using ReceiverPP create transaction transfering NFT
- Using OwnerPP create new ownership transfer
- Using ReceiverPP create new ownership record
  (1) Transfer to Recveri a "receipt"

## Burn of product if owner

- Perform validation first.
- Using PP and OwnerPP lookup owner of Product - validate that it is owned by OwnerPP
- Validate signature of owner to be able to transfer NFT of product to new owner.
- Burn NFT
- Using OwnerPP create new end of life (Burn) token.

## Update of web-of-trust data

Not developed yet.