Own Your Keys, Own Your Destiny

Taylor Schmidt, WaveLynx Technologies
Introduction

● Why do we need Keys and Encryption?
  ○ Authenticity.
  ○ Security.

● What should key ownership mean to your campus?
  ○ Avoid Lock in.
  ○ Control Keys sets.
  ○ Know your Data Model.

● What does Leaf offer to a campus user?
  ○ Extensible Card Specification.
  ○ Open Data Model.
  ○ Unrestricted Key Management.
Why Does Encryption Matter?

The Past (Proximity Cards/Magstripe):
- Unencrypted Data.
- Easily Reproducible.
- No Authentication.
- No Extensibility.

The Present (Smart Cards):
- Encrypted Communication.
- Authentication.
- Extensible Data.
What Does Key Ownership Mean?

What to Look For

- Open Data Model.
  - You know the exact data in your card.
  - Allow multiple vendors to support and produce your credentials.

- Custom Keyset.
  - Own the keyset used to secure your credentials.
  - Control who can produce and support your credentials and devices.
  - Change the keyset at anytime in the event of a security breach.

What to Avoid

- Proprietary data model.
  - Cannot be shared to different vendors.

- Encryption keys owned by the manufacturer or vendor.

- Vendor “Lock In”.
  - Cards and readers only work together.
  - No ability to switch vendors and keep credentials.
What is Leaf?

- **A Card:**
  - MIFARE DESFire EV2.
  - Easily Sourceable.
  - Industry standard, vetted security model (EAL 4+).

- **A Data Model:**
  - Open, published data structure.
  - Granular security with segregated applications.
  - Campus “container” functionality.
  - Extensible.
What is Leaf?

- **An Ecosystem:**
  - Readers.
  - Locks.
  - Printers.
  - Logical Access.
  - Biometric.
  - Open to ANY vendor.
Information

● WaveLynx Technologies:
  ○ Wavelynxttech.com
  ○ support@wavelynxttech.com

● Leaf
  ○ Leafip.co
  ○ info@leafip.co