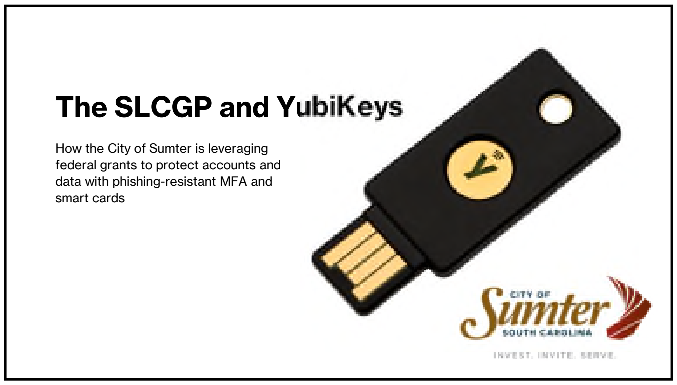
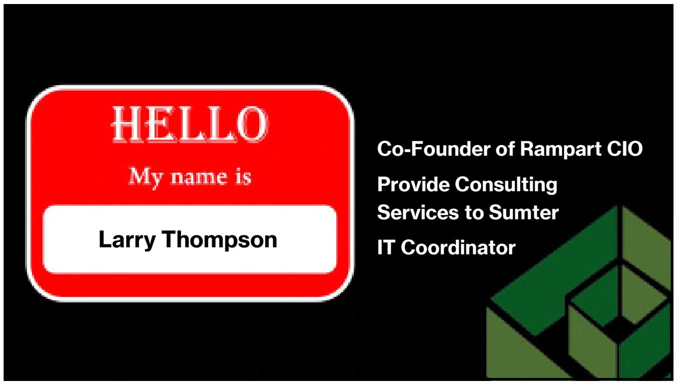
The information provided here is for informational and educational purposes and current as of the date of publication. The information is not a substitute for legal advice and does not necessarily reflect the opinion or policy position of the Municipal Association of South Carolina. Consult your attorney for advice concerning specific situations.



The SLCGP and YubiKeys

How the City of Sumter is leveraging federal grants to protect accounts and data with phishing-resistant MFA and smart cards

CITY OF
Sumter
SOUTH CAROLINA
INVEST. INVITE. SERVE.



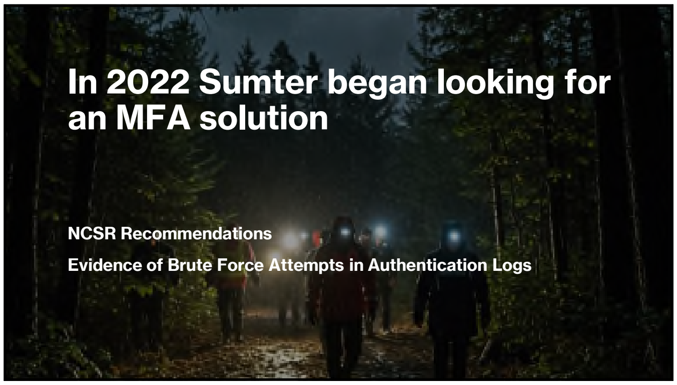
HELLO
My name is

Larry Thompson

Co-Founder of Rampart CIO

Provide Consulting Services to Sumter

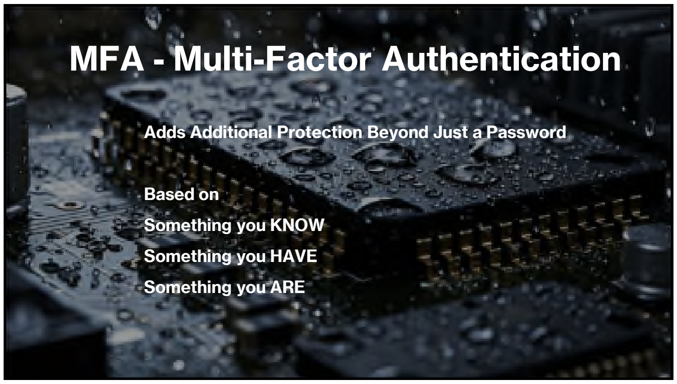
IT Coordinator



In 2022 Sumter began looking for an MFA solution

NCSR Recommendations

Evidence of Brute Force Attempts in Authentication Logs



MFA - Multi-Factor Authentication

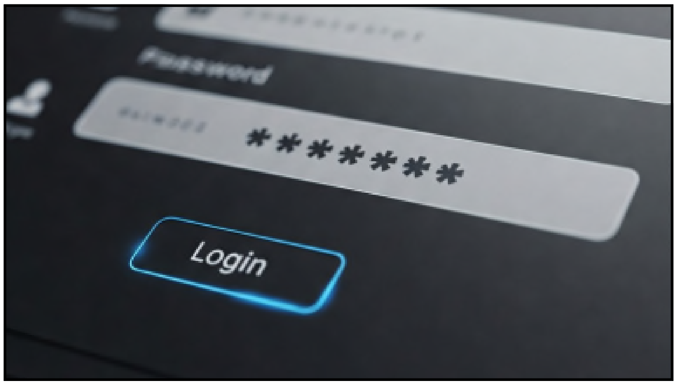
Adds Additional Protection Beyond Just a Password

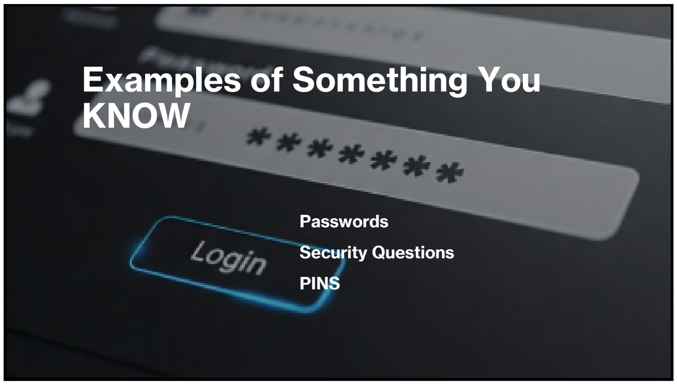
Based on

Something you KNOW

Something you HAVE

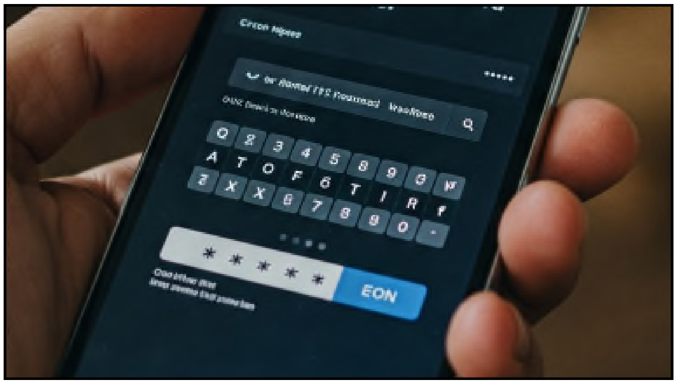
Something you ARE

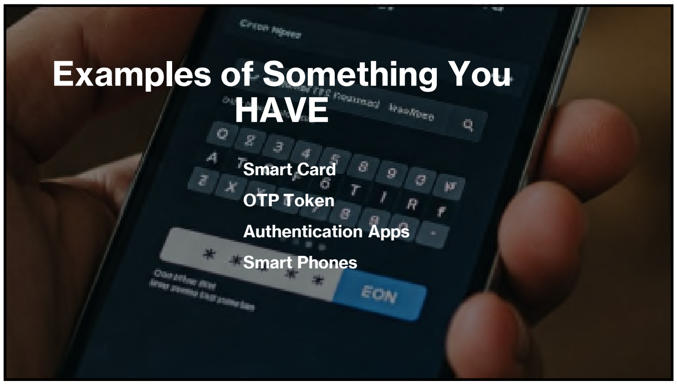




Examples of Something You KNOW

- Passwords
- Security Questions
- PINS



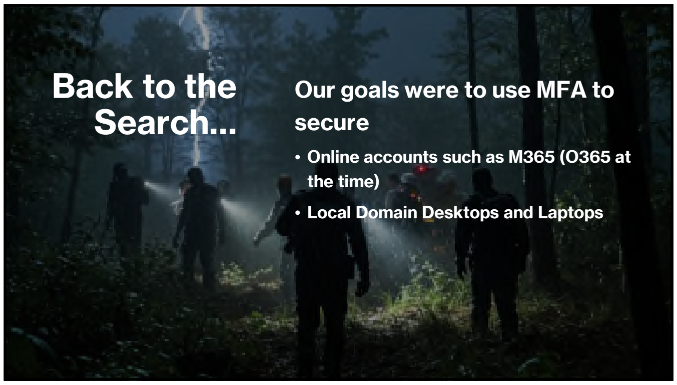


Examples of Something You HAVE

- Smart Card
- OTP Token
- Authentication Apps
- Smart Phones

Examples of Something You ARE

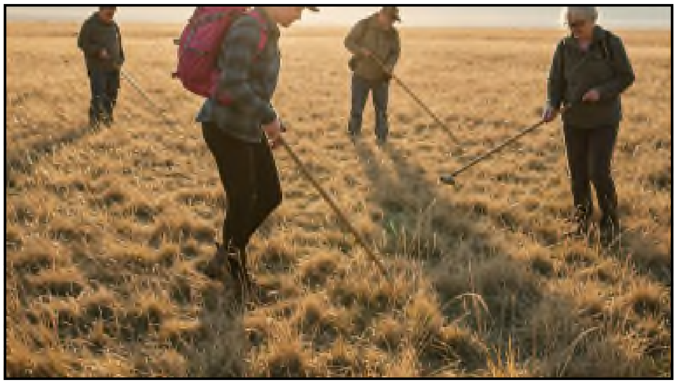
- Fingerprint
- Palmprint
- Retina
- Iris
- Voice
- Face

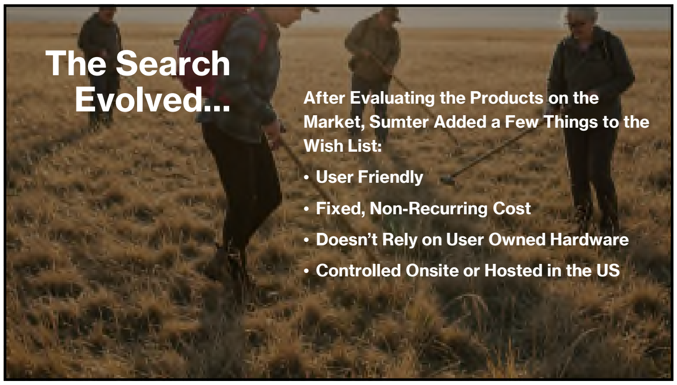


Back to the Search…

Our goals were to use MFA to secure

- Online accounts such as M365 (O365 at the time)
- Local Domain Desktops and Laptops





The Search Evolved...

After Evaluating the Products on the Market, Sumter Added a Few Things to the Wish List:

- User Friendly
- Fixed, Non-Recurring Cost
- Doesn't Rely on User Owned Hardware
- Controlled Onsite or Hosted in the US

And We Found It!!

Two Technologies in One, Solving Both Online and Local Login Requirements

Easy to Deploy and Maintain (Once the Infrastructure is Built)

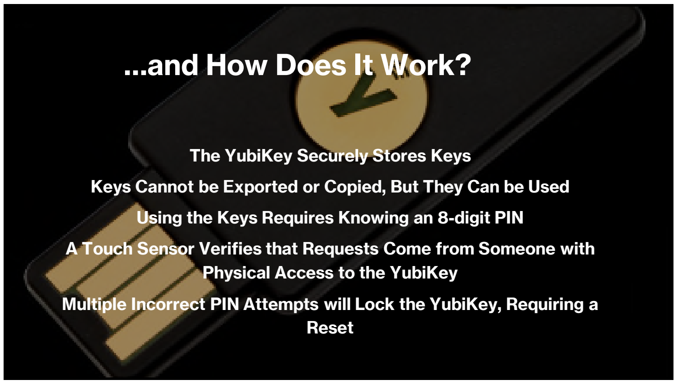
One-Time Fixed Cost

Phishing-Resistant / User-Proof

Controlled by the IT Department

So, What Is A YubiKey…

- A Smart Card
- A Waterproof USB Device that Can Go on a Keychain
- A Container for Keys and Certificates
- Locked with a PIN



…and How Does It Work?

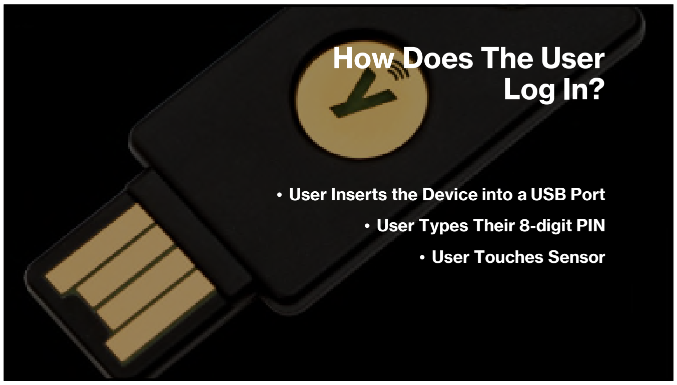
The YubiKey Securely Stores Keys

Keys Cannot be Exported or Copied, But They Can be Used

Using the Keys Requires Knowing an 8-digit PIN

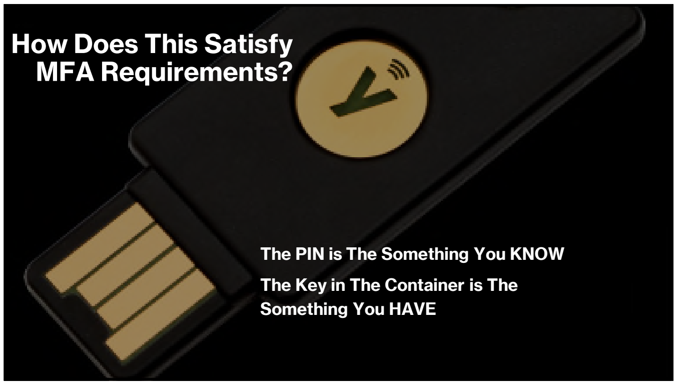
A Touch Sensor Verifies that Requests Come from Someone with Physical Access to the YubiKey

Multiple Incorrect PIN Attempts will Lock the YubiKey, Requiring a Reset



How Does The User Log In?

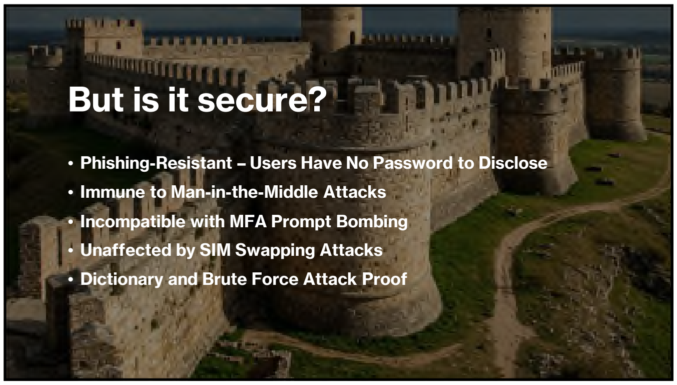
- User Inserts the Device into a USB Port
- User Types Their 8-digit PIN
- User Touches Sensor



How Does This Satisfy MFA Requirements?

The PIN is The Something You KNOW

The Key in The Container is The Something You HAVE

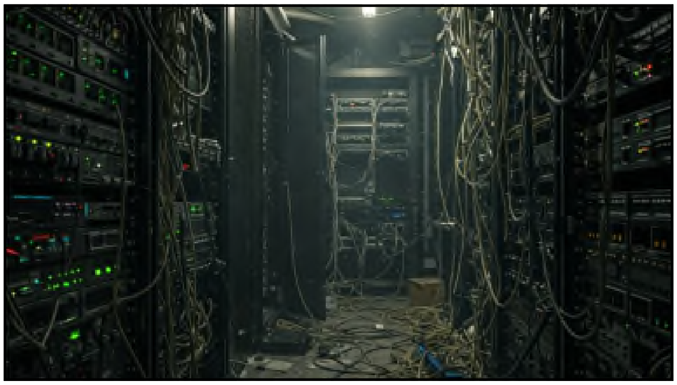


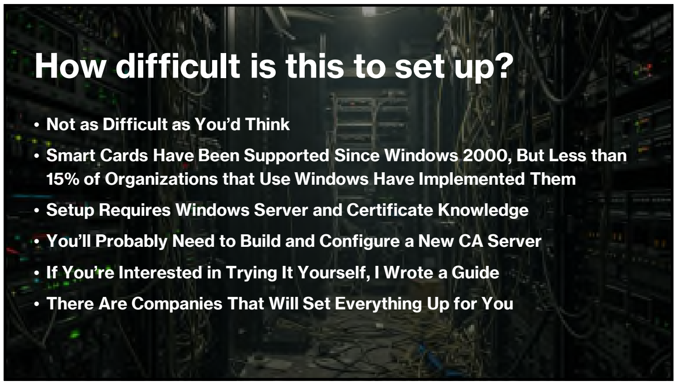
But is it secure?

- Phishing-Resistant – Users Have No Password to Disclose
- Immune to Man-in-the-Middle Attacks
- Incompatible with MFA Prompt Bombing
- Unaffected by SIM Swapping Attacks
- Dictionary and Brute Force Attack Proof

Like REALLY Secure?

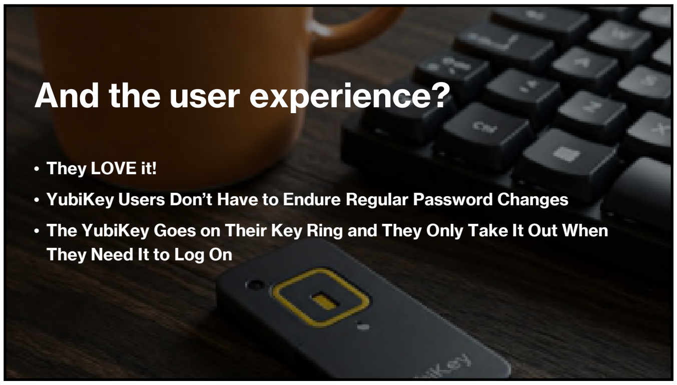
- An Attacker Would Need the YubiKey AND the 8-digit PIN
- Meets CJIS Requirements for MFA





How difficult is this to set up?

- Not as Difficult as You'd Think
- Smart Cards Have Been Supported Since Windows 2000, But Less than 15% of Organizations that Use Windows Have Implemented Them
- Setup Requires Windows Server and Certificate Knowledge
- You'll Probably Need to Build and Configure a New CA Server
- If You're Interested in Trying It Yourself, I Wrote a Guide
- There Are Companies That Will Set Everything Up for You



And the user experience?

- They LOVE it!
- YubiKey Users Don’t Have to Endure Regular Password Changes
- The YubiKey Goes on Their Key Ring and They Only Take It Out When They Need It to Log On

Enter the SLCGP

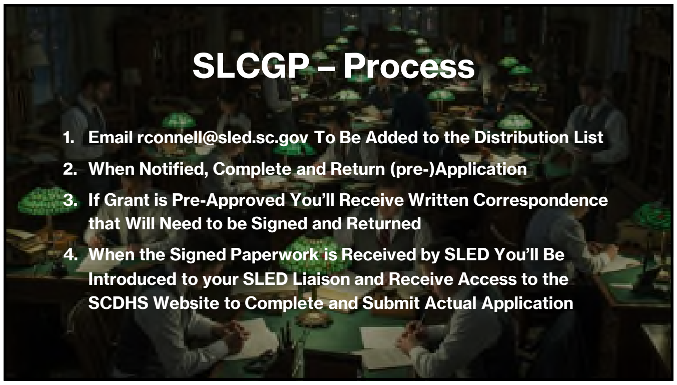
In September of 2023 We Heard About the SLCGP and Applied for a Grant Covering the YubiKey Hardware for Our Staff

SLCGP – State Local Cybersecurity Grant Program

- Funded by the Federal Government
- Available Directly to State and Territorial Governments
- Local Governments Are Considered Eligible Subrecipients That Can Receive Funding Through Their State Administrative Agencies
- Administered in South Carolina by SLED
- If awarded funds, you must participate in NCSR in coming year

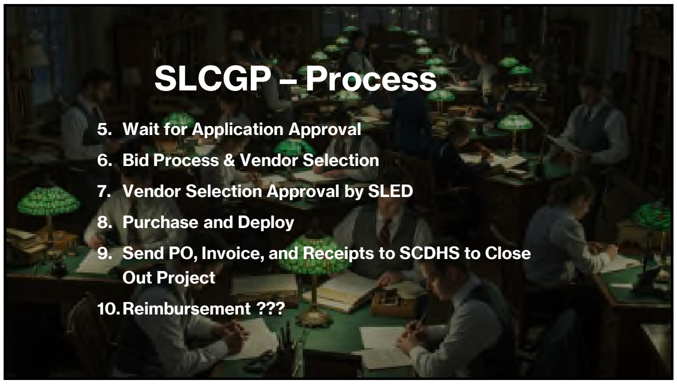
SLCGP – State Local Cybersecurity Grant Program

- We Received Word our Grant Request was (pre-)Approved in June of 2024
- We Have Recently Completed our Purchase and are Wrapping Up our Deployment
- We are in the ‘Requesting Reimbursement’ phase



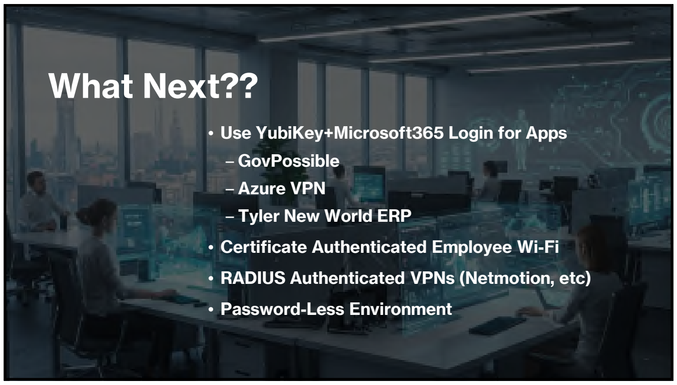
SLCGP – Process

1. Email rconnell@sled.sc.gov To Be Added to the Distribution List
2. When Notified, Complete and Return (pre-)Application
3. If Grant is Pre-Approved You'll Receive Written Correspondence that Will Need to be Signed and Returned
4. When the Signed Paperwork is Received by SLED You'll Be Introduced to your SLED Liaison and Receive Access to the SCDHS Website to Complete and Submit Actual Application



SLCGP – Process

5. Wait for Application Approval
6. Bid Process & Vendor Selection
7. Vendor Selection Approval by SLED
8. Purchase and Deploy
9. Send PO, Invoice, and Receipts to SCDHS to Close Out Project
10. Reimbursement ???



What Next??

- Use YubiKey+Microsoft365 Login for Apps
  - GovPossible
  - Azure VPN
  - Tyler New World ERP
- Certificate Authenticated Employee Wi-Fi
- RADIUS Authenticated VPNs (Netmotion, etc)
- Password-Less Environment

Questions ???