

## WAVELYNX TRANSITION STRATEGY WORKBOOK

End User Name: \_\_\_\_\_ Project Location(s): \_\_\_\_\_

Timeframe: \_\_\_\_\_

Additional Notes: \_\_\_\_\_

Get your priorities straight. Assess why the end user is doing this project and what is most important to them.

### What has been identified as the key issue(s) prompting the need for a system upgrade? (Select all that apply)

- Legacy card technology at risk (e.g. low frequency 125 kHz proximity)
- Reader to Panel Protocol Risk (Wiegand)
- Global / Enterprise User desire to perform remote firmware updates
- Desire to be free from proprietary credential/reader vendor
- Current system has performance issues
- Desire to have a single card support multiple devices / applications
- Desire to include / migrate to a mobile credential solution
- Other (add lines for answer)

### What is the customer's priority for this transition?

- They don't want to disrupt the employee base
- They have an upcoming audit and need the risk addressed immediately
- They have financial constraints and need to work within a tight budget
- They have a specific time-line for completing the project
- Other (add lines for answer)

### What exactly are we dealing with here? What does the existing environment look like?

What is the brand/model of Access Control System(s) currently deployed (short answer).

What panels are deployed? (e.g. Standard Access Control Panels wired via Wiegand or OSDP Intelligent Panels via RS485)

What is the brand / model of the current readers and what type of technology do they support? (short answer)

How many readers are currently deployed? (short answer)

What is the brand / model of the current credentials and what type of technology do they support? (short answer)

How many credentials are currently deployed? (short answer)

Besides the card readers, are there other devices or applications that support these cards? Explain (paragraph)

**Dream big. What is the scope of this upgrade? What goals have been set for features and functionality of the new/improved system?**

Any plans to replace/upgrade the Access Control Head End Software & Controllers/Panels? Explain. (short answer)

Are there plans to increase/decrease the number of sites/locations for this project? (short answer)

Are there plans to increase/decrease the number of readers on this project? (short answer)

Are there plans to increase/decrease the number of credentials issued on this project? (short answer)

Are there plans to support any existing/new devices or applications with the credentials on this project? (short answer)

Are there plans to add mobile credentials to this project? (short answer)

**Pick a card, any card. Actually, don't do that. Let's make sure we select the right credentials for your customer.**

**Is your customer a candidate for WaveLynx Standard DESFire EV2 Credentials? (check all that apply)**

Project has low reader / card count (<100)

Customer does not have appetite for owning keys

Customer is not concerned about sole sourcing / competitive pricing

Customer only plans to use credentials for access control (no additional data/devices to be incorporated on card)

Customer desires end-to-end encrypted solution

Customer desires unique Facility Code / Bit Format / Badge IDs + Credential Number Sequence Management Services

**OR**

**Is your customer a candidate for LEAF Custom Keypad Credentials + Key Management Services? (check all that apply)**

Project has high reader / card count and potential for growth (>100)

Customer has appetite to own keys and wants them professionally and securely managed by WaveLynx Key Management Services

Customer has appetite to own keys and wants to manage them themselves (decline Key Management Services by WaveLynx)

Customer doesn't want proprietary sourcing

Customer wants to support legacy prox technology as well as new encrypted smart technology (eg. phased transition) (LEAF Dual Technology DESFire EV2)

Customer desires a "one card" solution where their card can support multiple devices and applications within their ecosystem (e.g. WaveLynx readers, Assa Abloy Aperio locks, RFIdeas Secure Printing device)

Customer needs end to end encrypted solution / migration path / future proof

Customer has disparate Access Control systems deployed throughout global / enterprise

**Is your customer considering adding mobile credentials?**

Does the customer have disparate access control systems and needs to deploy a unified credential that will work on any PACS?

Does the customer have/or are they interested in using a tenant management/ "conci-aire" type application, building automation application, or visitor management platform that needs a mobile access control credential embedded in it?

Does the customer desire to decrease the number of "touch" points in their environment and replace them with "touch less" access?

Does the customer desire an easy to deploy, cost-effective credential solution?

Let's summarize the important stuff. We need to make sure all of the necessary technology is seamlessly supported by the access control hardware once the upgrade is complete.

**The upgraded credential solution needs to include these technologies (check all that apply):**

- Low frequency 125 kHz proximity technology (physical credential)
- High frequency 13.56 MHz encrypted smart technology (DESFire EV1, EV2, EV3) (physical credential)
- Mobile technology (BLE and NFC) (MyPass Mobile Credentials or other Wavelynx Partner Mobile Integration Solutions)

**The upgraded credential solution needs to work on these devices / applications (check all that apply):**

- Existing (compatible) readers
- New WaveLynx Ethos Readers
- LEAF enabled devices
- Non-LEAF enabled devices or applications

**The upgraded WaveLynx Ethos Readers needs to support these technologies (check all that apply):**

- Low frequency 125 kHz proximity credential
- High frequency 13.56 MHz encrypted smart credential (DESFire EV1, EV2, EV3)
- Mobile credential (BLE and NFC) (MyPass Mobile Credentials or other WaveLynx Partner Mobile Integration Solutions)

**The upgraded Wavelynx Ethos Readers needs to support these communication protocols (check all that apply):**

- Wiegand
- OSDP
- F2F
- MCLP

Let's discuss what you think is the best course of action to pull this whole thing together.

**Which transition strategy do you feel best suits this customer? (check one)**

- Entire system upgrade: Head End Software, Controllers / Panels (OSDP) + Readers + Cards
- Credentials and Readers: Existing system stays in place but all credentials and readers get replaced simultaneously.
- Readers first: Keep existing credentials and replace readers. Once readers are replaced, update card technology.
- Credentials first: Keep existing readers and replace credentials (physical single technology, dual technology, and / or mobile credentials). Once credentials are replaced, update reader technology.

Does your customer have a budget and timeframe dedicated to the completion of migration? (check one)

Yes

No

Now that you've got your ducks in a row, it's time to define the WaveLynx products you will need to fulfil the execution of this design.

**Next Steps:**

- 1) Save this form.
- 2) Either contact your WaveLynx Sales Representative, or email [sales@wavelynxtech.com](mailto:sales@wavelynxtech.com).
- 3) You can also hit the "Send to WaveLynx" button below and someone will contact you to set up a meeting to review your worksheet and define exactly what products you'll need to source from us.

We can't wait to help you deploy the most secure, open, and interoperable credential and reader solution on the market today!