Enrollment

Introduction

Start simple

- Avoid complex enrollment scenarios until after we understand the basic model
  - then apply this model to the complex cases
- At *least* two systems are involved
  - The system to be added
  - The target system being added to
- The fundamental goal is bi-directional authentication and authorization

The goal (from the charter)

Authentication:

- 1. An identifier, within a namespace controlled by the service provider, for the service consumer.
- 2. Keying information to be used for identity confirmation.

Authorization (configuration):

- 3. A set of service consumer permissions. These permissions describe to the provider the services that the consumer wants to access, and they describe to the consumer what services offered by the provider will be accessible.

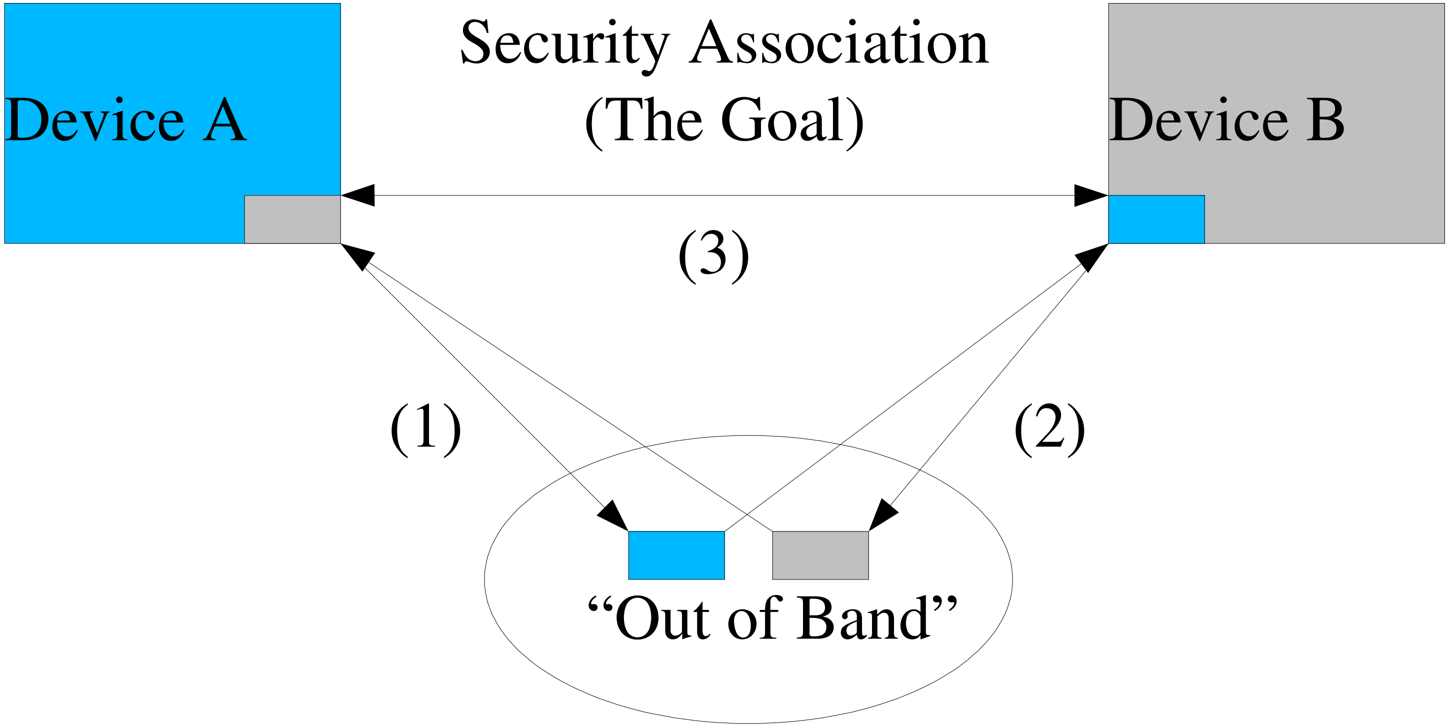
Authorization

- Involves a policy decision
- All entities involved must do this
  - and may use different policies
  - in general details are out of scope
- Requires some form of authentication
  - accept all/none
  - accept listed devices

Authentication

- All entities involved must do this
  - but may use different forms of authentication
- Weak
  - Physically secured channel
- Cryptographic
  - Requires “out of band” exchange

To establish cryptographic authentication



Device A

Security Association
(The Goal)

Device B

(3)

(1)

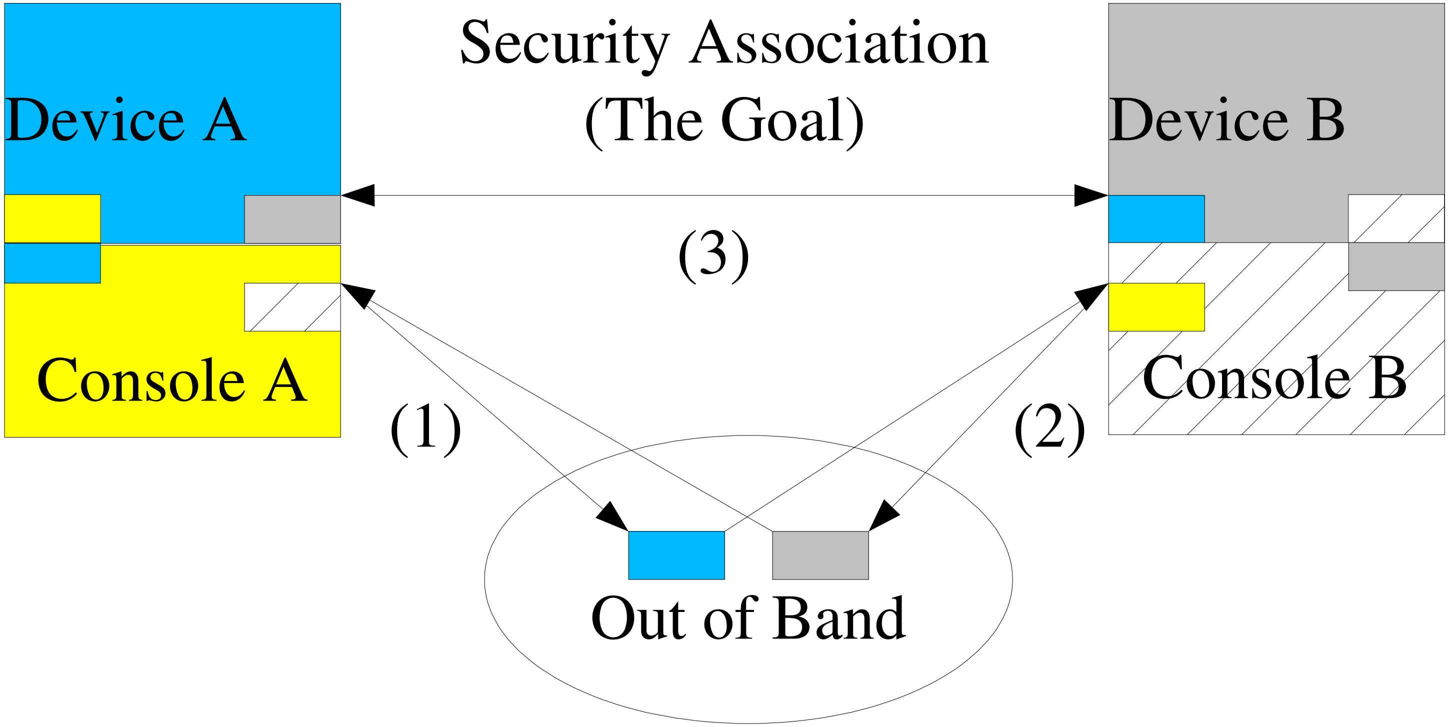
(2)

“Out of Band”

Simple, right? But,

Q: How are (1) and (2) authenticated?

Physically connected console(s) do not answer this question



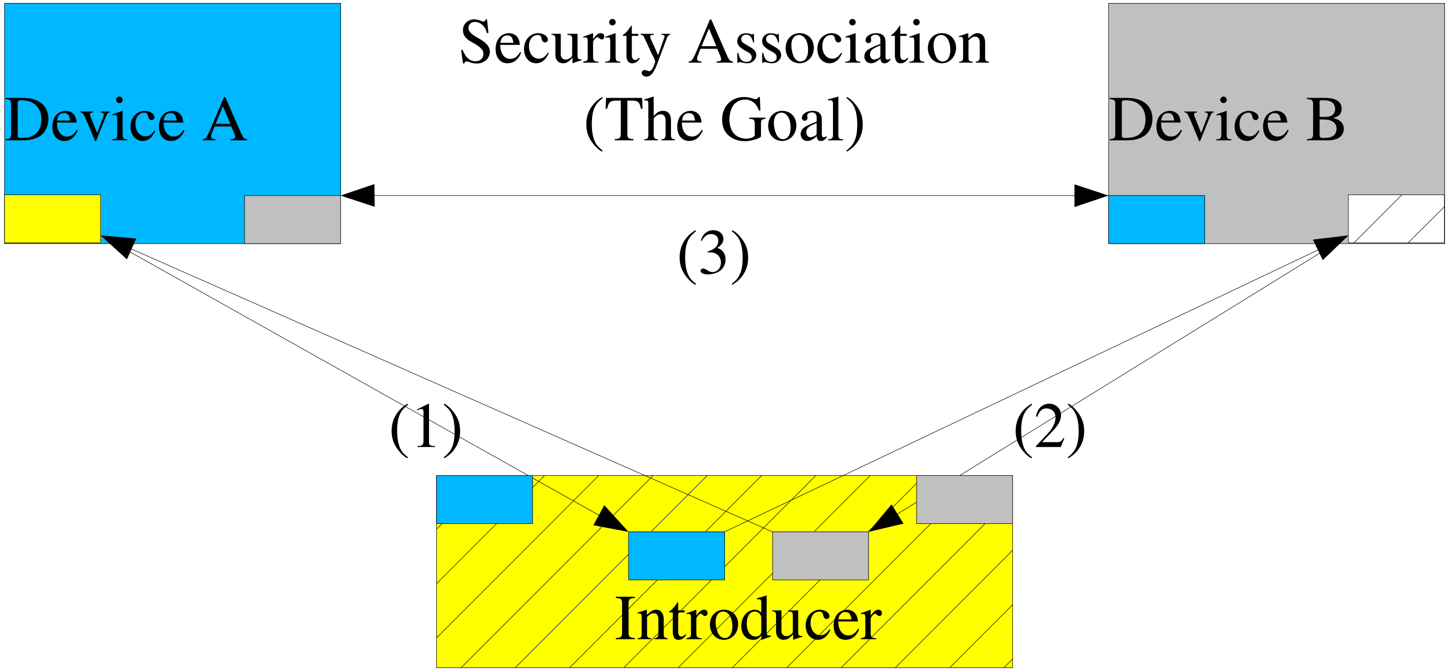
This is an example of physical ('weak') authentication between console & device. But, this diagram does highlight:

Q: How are (1) and (2) authenticated?

A: ▨ 🟨, a prior security association (*recursion*)

Authentication of Out of Band

(Simplify: Systems that share an SA are a virtual system)



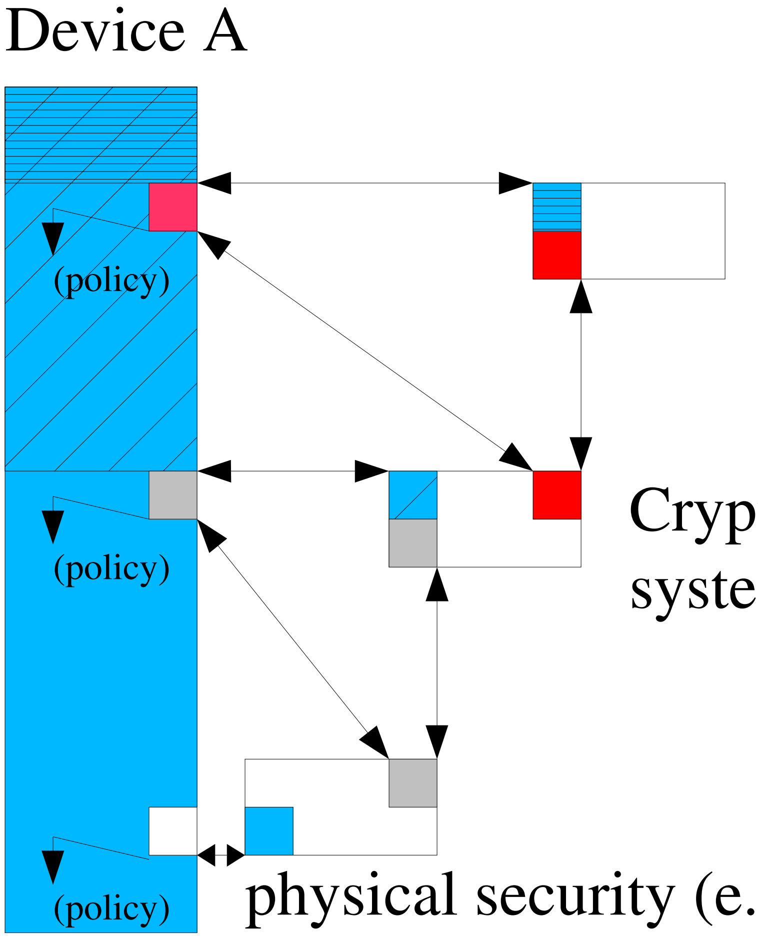
This is a model discussion: In the general case there is an Introducer.

In specific case(s) an authentication mechanism may be physical (such as with consoles, console cables, etc).

Introductions are recursive

- Physical security provides the weak authentication necessary for initial device configuration
  - Default policies for authorization(s)
  - Initial credentials for authentication(s)
- Subsequent introductions can build on this
  - Lack of a standard enroll/introduction protocol inhibits standard mechanisms and results in regular dependence on weak authentication ("default password")

Introductions



Cryptographically secure introduction to a peer system

Cryptographically secure introduction to a target system (physical shipping etc as necessary)

physical security (e.g. manufacturing, staging area, etc)

Can minimize weak authentication to one time (very early in the lifecycle)
Doesn't prohibit re-doing this of course (policy is out of scope)

Value of model for subsequent introductions is clear

(Once the system is standardized)

- Establishing accounts
  - Think about credit card fraud ($$)
- Deployments and re-deployments within an organization
- Management and re-configuration of existing systems to reflect changing service agreements (authorizations) and partnerships
- Re-sale of devices and systems
  - for extra credit: how is this different than initial sale?

Transitive Trust

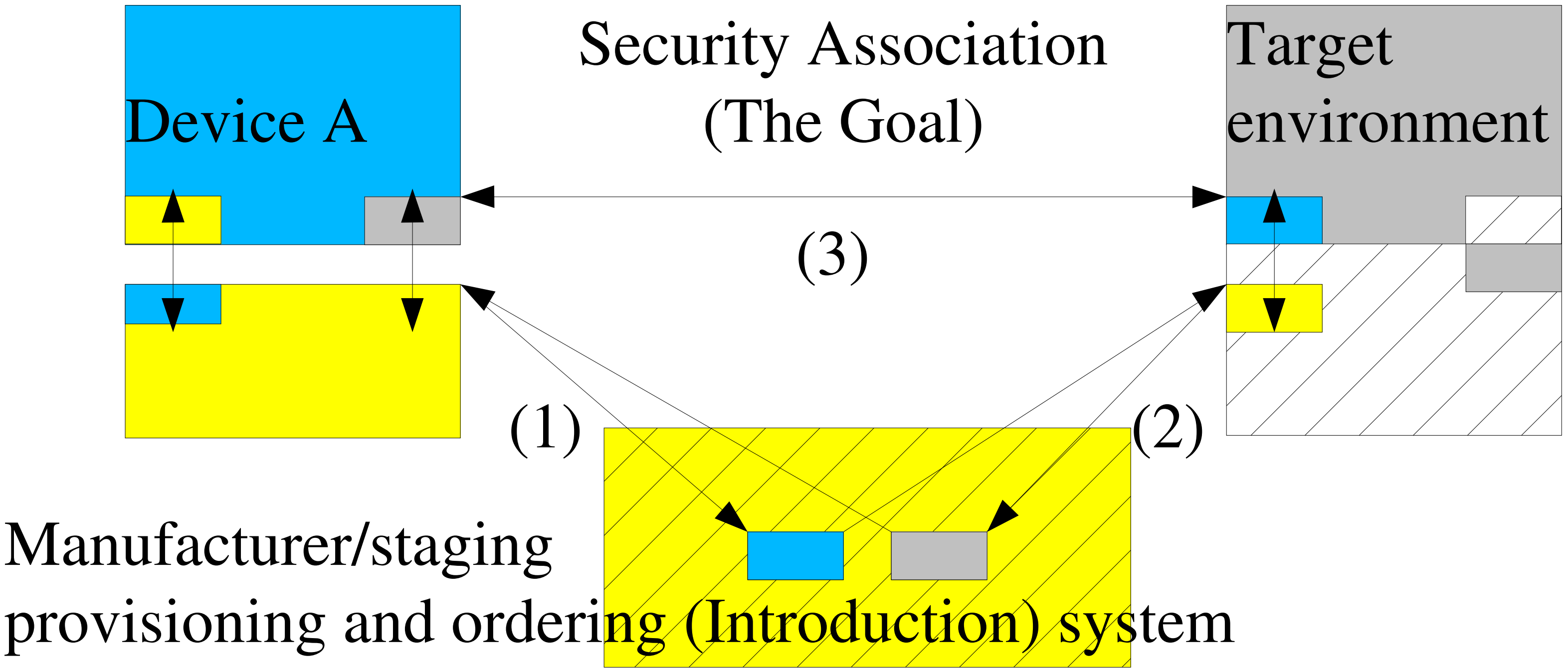
- We use existing credentials with a third party to obtain new, independent, credentials
  - A drivers license to open a bank account, A bank account to get a credit card, A credit card to get a gym membership
- Trust chain is not always involved
  - If I lose my drivers license I don't loose my gym membership
- We're discussing an enrollment model, not a security infrastructure (not a PKI, Kerberos, etc)

Initial introduction is less clear

(Manufacturing or as early as possible, “staging area”)

- Physical authentication involved
  - Device imprints
  - Default policies for authorization(s)
  - Initial credentials for authentication(s) such as manufacturing ID certificates (an incomplete implementation example)
- Introduction to target systems is complicated by lack of network connectivity
- In retail sale scenarios the target network is not always known (2) is difficult

Initial Provisioning – online ordering

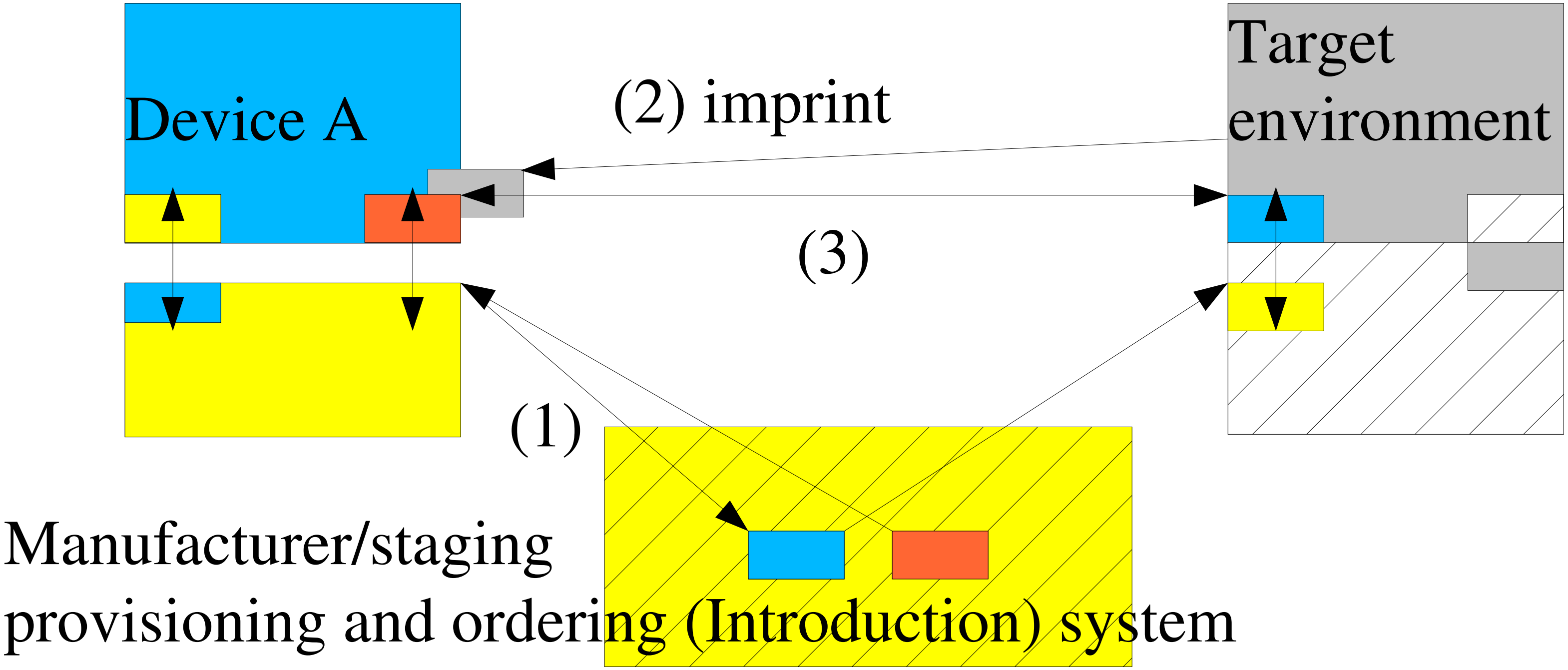


Recall from the charter:

· Identifier and Key information (🟦)

·Default configuration (⬜) (details *out of scope)*

Initial Provisioning – retail scenario


Device A
(2) imprint
Target environment
(3)
(1)
Manufacturer/staging provisioning and ordering (Introduction) system

Going forward

- Decide if this model meets Enroll goals
- Finalize model draft as a working group document
- Profile this model as used for shared secrets, asymmetric keys, and bound asymmetric keys (certs)
  - Existing enrollment protocols
- Consider if an initial protocol by this working group is in order
  - L2? L3?
  - is 'discover' in scope?