Providing Trust at the Threshold™

BridgePoint Systems, Inc.
530 McCormick St.
San Leandro CA USA 94577

Telephone: 510-346-1510
Facsimile: 510-346-2510

Contact:
Thomas Corder
President and CEO
tcorder@bridgepointsystems.com
www.bridgepointsystems.com

Who We Are

- Founded in 1995, BridgePoint is located near Silicon Valley in San Leandro, CA
- We have been a pioneering provider of CAC and PIV technology to the Federal Government since 2002
- Top flight product engineering and software teams
- Access solutions deployed in dozens of DoD and federal facilities

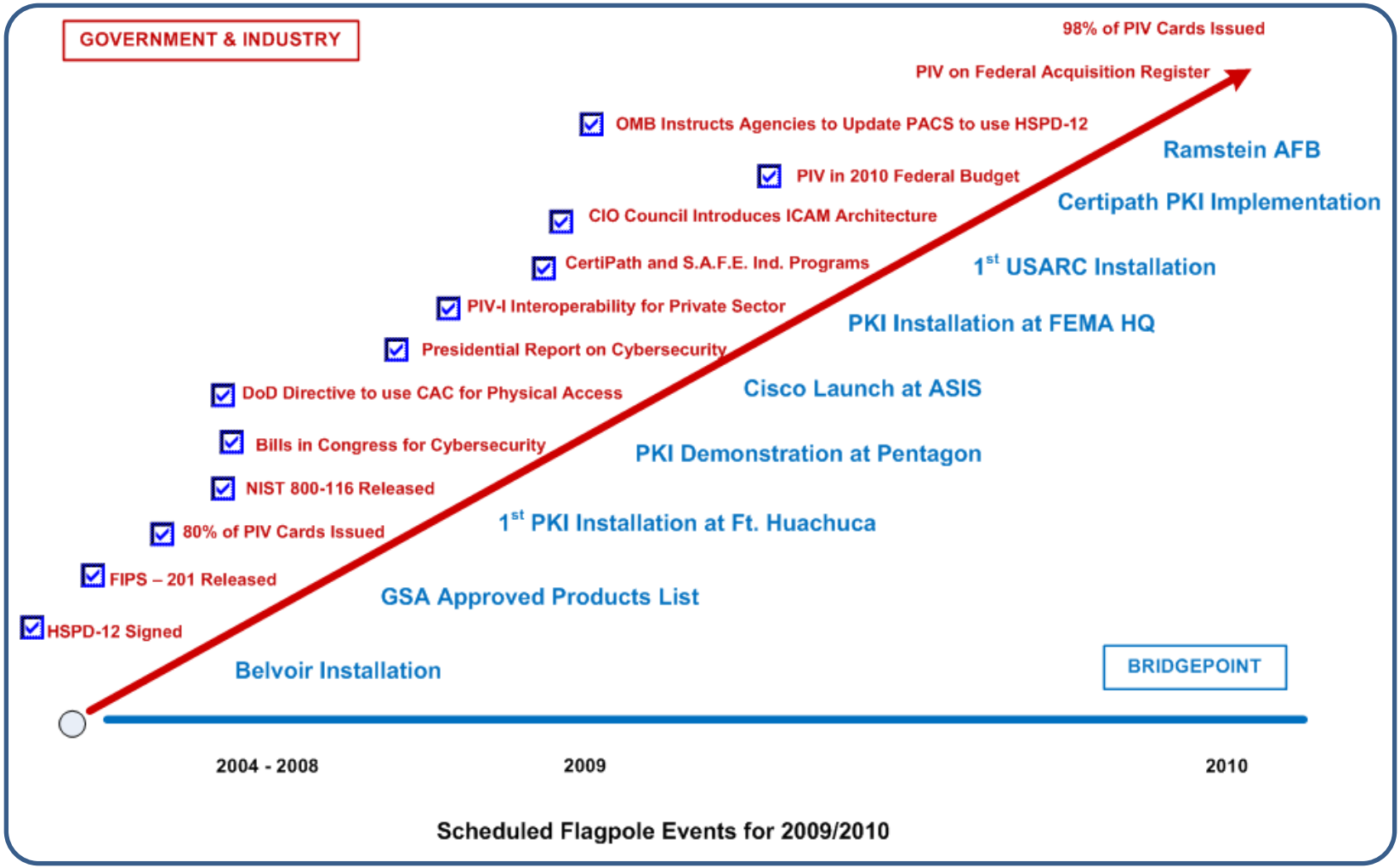
BRIDGEPOINT™

Standards Based + Innovation Driven

- ISO, FIPS-201, NIST 800-73, -76, -78, -96, -116
- GSA-APL
- Engaged in FIPS-140 Process
- Interoperate with CAC, PIV, PIV-I & TWIC
- Core competency is innovation of tightly integrated cyber-physical systems
- Engineered in U.S. at BridgePoint
- Manufactured in U.S. at BridgePoint

BRIDGEPOINT™

Grown With HSPD-12



Scheduled Flagpole Events for 2009/2010

BRIDGEPOINT™

Lessons Learned (1)

- Avoid any implementation that can result in "collisions" (less than 56 bit FASC-N)
- PKI Challenge-Response does not restrict throughput
- Contact Interface can be reliable
- Existing cabling infrastructure can often be used

BRIDGEPOINT™

Lessons Learned (2)

- Dual Interface Contact and Contactless provides redundancy for a failed antenna
- Be forward compatible: re-flash at the reader
- Seamless PACS Enrollment is essential to a successful system implementation
- Thorough testing is difficult – done in the field
- Hope for government cooperation & adoption

BRIDGEPOINT™

TrustZone PACS has Proven:

- PKI in PACS can be simple
- PKI in PACS can be fast & seamless
- PKI in PACS can be affordable
- PKI in PACS is possible to implement in many facilities utilizing existing cable infrastructure
- No additional overlaying network is required
- No additional hardware is required
- No certificates or keys need to be stored in reader

BRIDGEPOINT™

The eFASC-N

The eFASC-N is simply the FASC-N appended with a SHA-2 HASH of the PKI Certificate:

= Agency Code +

+ System Code +

+ Credential No. + Issue Code + Credential Series

+ SHA-2 HASH of the PKI Certificate

BRIDGEPOINT™

What the eFASC-N Solution Does

- It binds the PKI certificate on the Credential presented for access with the Certificate on the Credential that was enrolled.
- This eliminates the potential for a cloned credential with a “rogue” public key–private key pair to be used in the access system.
- It conforms with FIPS-201 and the guidance provided by NIST 800-116.
- It supports automatic certificate revocation checking

BRIDGEPOINT™

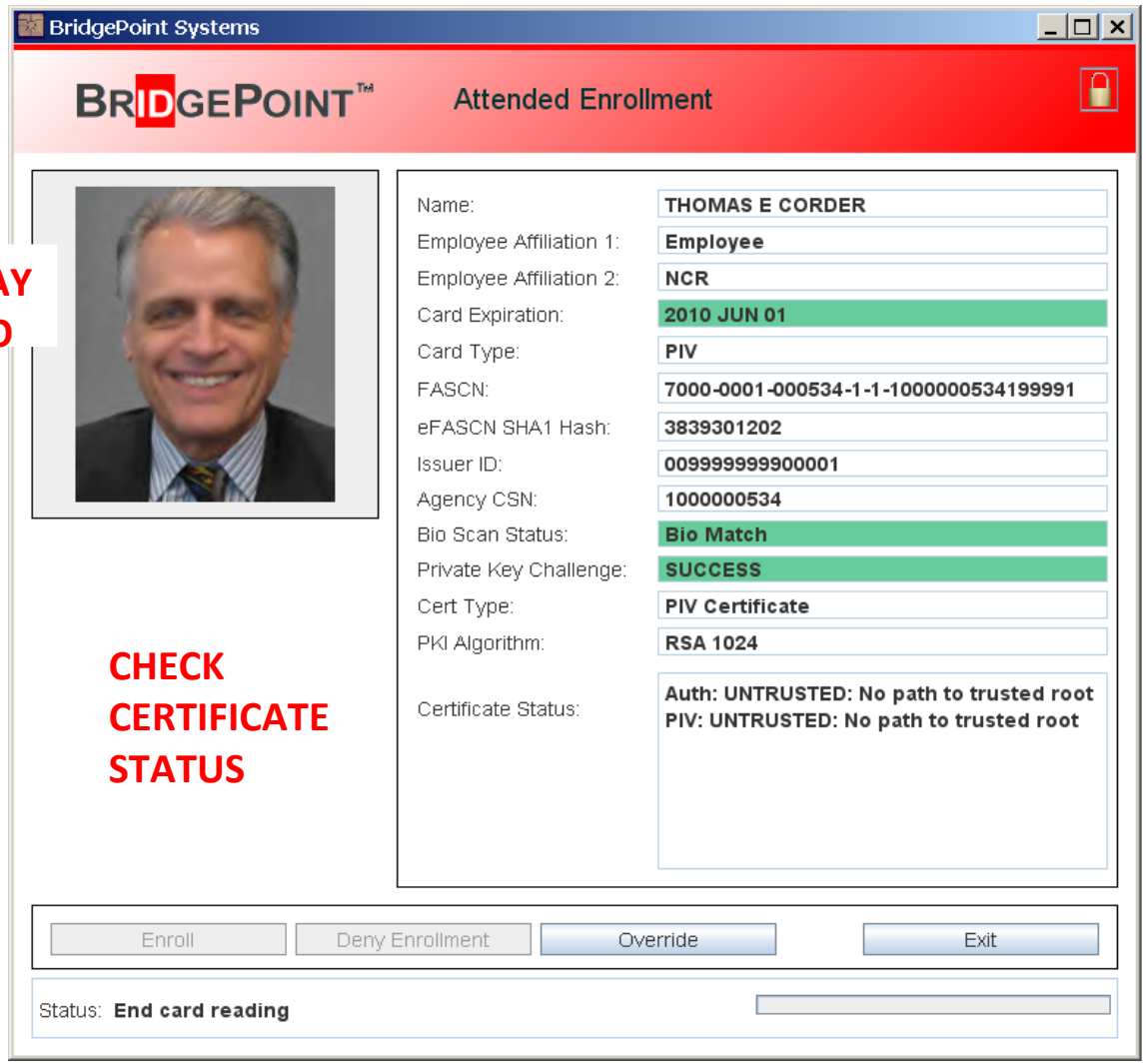
Step 1: Authentication & Validation

- PIN Entry
- Expiration Date
- PKI Challenge
- PHOTO Extraction
- OCSP Validation
- BIO Match Reader (optional)

Less than 15 Seconds at Enrollment

BRIDGEPOINT™

Enrollment Authentication Screen



DISPLAY PHOTO

CHECK CERTIFICATE STATUS

CHECK EXP. DATE

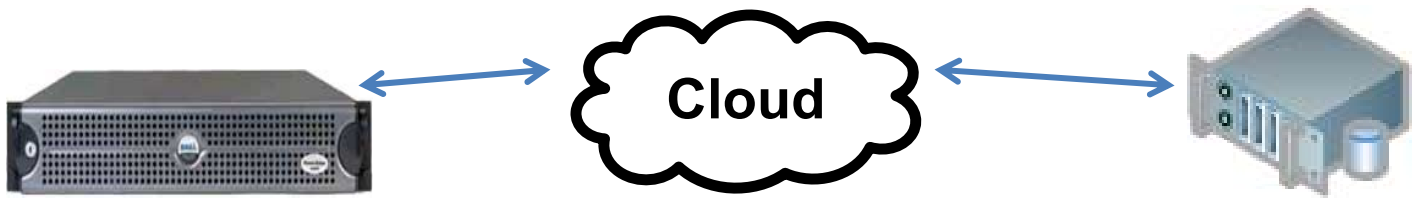
MATCH BIO

VERIFY PRIVATE KEY

BRIDGEPOINT™

Step 2. Validation + Certificate Repository

- Store Personal Certificate (or CAC Signing Certificate) and Card Auth Certificate
- Perform frequent CRL Validation by OCSP/SCVP
- Notify PACS of any Revoked Certificate



Local PACS Server with Certificate Repository

Responder with Current Certificate Status

BRIDGEPOINT™

Step 3. PKI Authentication at Reader

Credential Presented (Contact or Contactless)

- **Extract Certificate & Public Key**
- **Create asymmetric challenge**
- **Verify signed response**
- **Generate HASH of certificate**
- **Send eFASC-N to Controller for match**

Sub 2 seconds (75% of time is Credential)

BRIDGEPOINT™

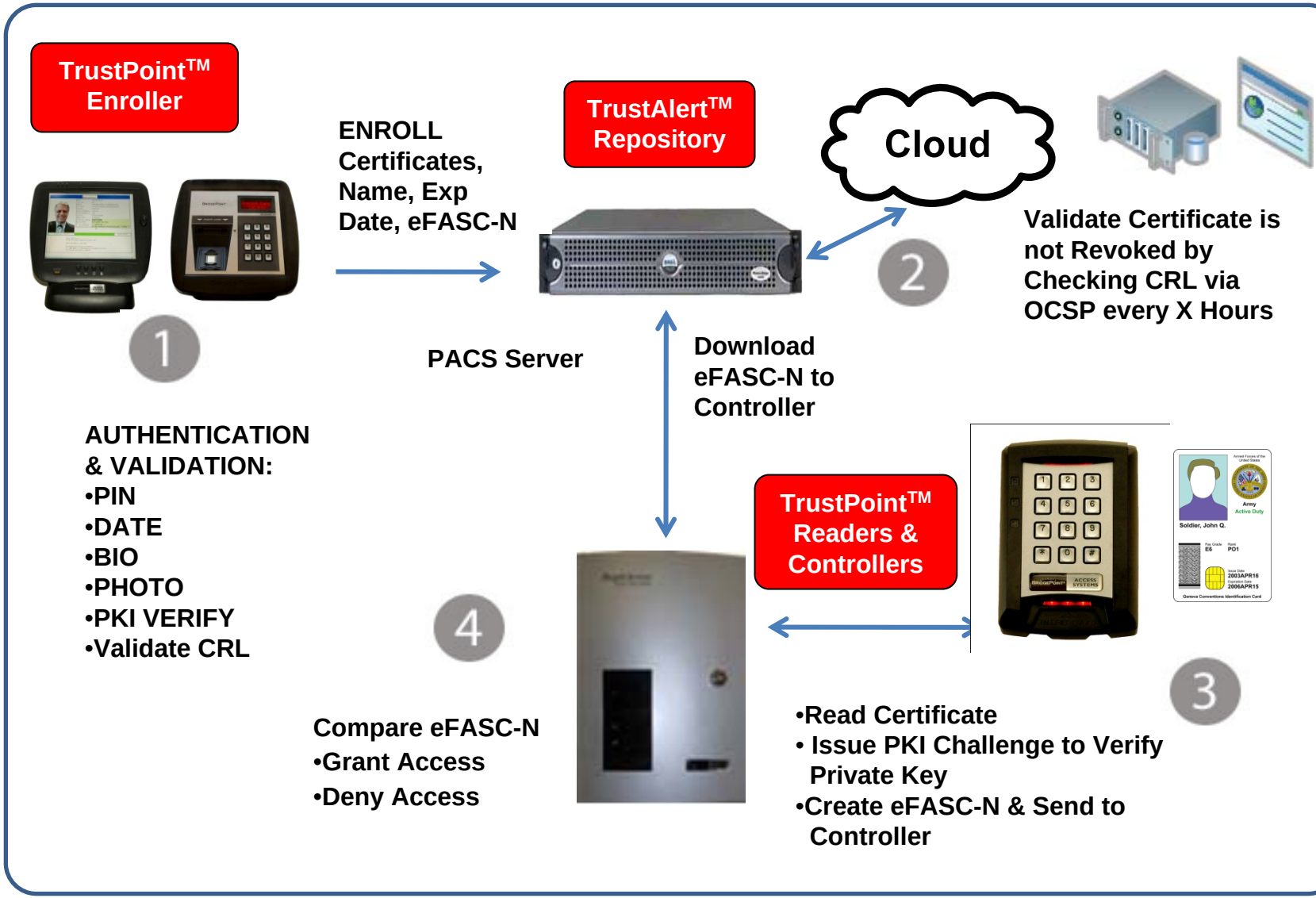
Step 4. Authorization by PACS Controller

- Stores eFASC-N in Controller
- Maintains User Privileges
- Monitors requests & grants or denies access based on matching eFASC-N
- Maintains audit log
- Disables revoked credentials

(Not Inclusive)

BRIDGEPOINT™

PKI PACS Flow



PKI Authenticating Reader Solutions

GSA FIPS 201 APPROVED

1F Readers

CONTROLLED
Card Only + PKI

1F Contactless Only
(CAK Challenge)
(Tamper Switch Option)

2F Trusted Readers

RESTRICTED
Card + PIN + PKI
Available as Exterior Reader or with PKI Interface Module on Safe Side

2F Dual Interface
(PAK & CAK Challenge)
(Tamper Switch Option)

3F Highly Trusted Readers

EXCLUSION
Card + PIN + PKI+ BIO
Available as Single Exterior Reader or with PKI Interface Module on Safe Side

3F Dual Interface
(PAK & CAK Challenge)
(Tamper Switch Option)

Attack Side vs. Safe Side

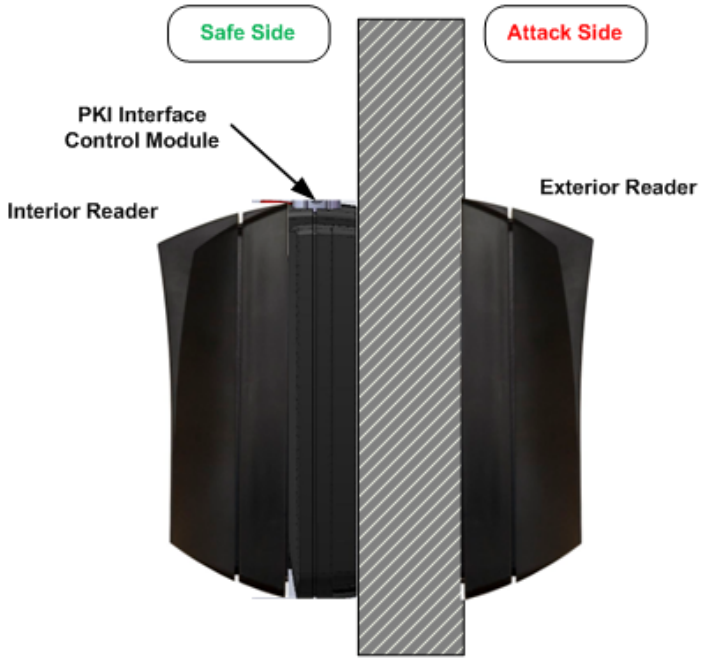
PKI Module + Exterior Reader

Card + PIN + PKI

ONE READER CONFIGURATION

PKI Module + Interior & Exterior Readers

Card + PIN + PKI



TWO READER CONFIGURATION
with PKI INTERFACE MODULE

BRIDGEPOINT™

PKI Installations

- U.S. Army Ft. Huachuca
- FEMA HQ (500 C Street)
- Pentagon PACS Test Program
- Exostar & Certipath Facilities
- U.S. Air Force (ordered)

BRIDGEPOINT™

Summary

- Secure: The Credential that is granted access is the Credential that was enrolled
- Seamless: no complex procedures or changes in PACS operation
- Fast: 15 sec Enrollment and < 2 sec. Access
- Cost effective: can operate on most installed cable infrastructure
- Compliant: with standards & guidance

- Sugared water or change the world?

BRIDGEPOINT™