



# Federated PACS Open House

February 2, 2010

**CertiPath**

# Motivation and History



- HSPD-12 = assurance of identity for PACS and LACS
- During 2009, recognition increased that:
  - Binding created during issuance of PIV = Good
  - Binding evaluated during PACS usage of PIV = Bad
    - E.g. Flash pass, unsigned CHUID/FASC-N, etc.
- No one was talking about the PACS guest problem
  - How to handle other branches of governments, consultants, etc.
- GSA is charged to oversee all things FIPS 201 including usage
  - Difficult to enforce full card functionality utilization if no demonstrable solutions exist to do it
- CertiPath saw “doors” as being the next major relying party

# Project Goals



## GSA

- Support all authentication modes defined by NIST SP 800-116
- Support authentication with all high-assurance credentials that can be validated against the FBCA, CertiPath and the TWIC Hotlist
  - PIV, PIV-I\*, CAC and TWIC (2048-bit keys)
- Demonstrate the feasibility of PACS/LACS convergence

## CertiPath

- Above + increase awareness in the value of high-assurance interoperable PKI
- Produce specification to guide and encourage PACS vendors

# System Criteria



1. Support for multiple authentication modes
  - Bidirectional communication with the reader is mandatory
2. Enterprise security policy and incident response policy must be implementable across PACS
  - E.g. the facility must be put into lockdown during an incident
3. Visitors cannot be handled out-of-band
  - They are a normal condition in most buildings and not unusual
4. Visitors that carry credentials of similar, provable quality must be leveraged
  - We must leverage the HR function's proofing of each employer
  - We cannot issue "native" badges to compensate in facilities with heterogeneous populations
5. All processing of authentication information must occur on the "safe side" of a door

# Trusted PACS Deployments Should:



1. Should be accredited to a agreed upon standard
  1. SSL Headlines this year having something to teach us
2. Provide the same security functionality found in LACS
  - E.g. Temporal policies to effect reader auth modes
  - E.g. Mutual registration of card and reader
  - Lots of feedback to the user at the reader (think status bar)
3. Facilitate Operational Awareness
  - People who entered my facility in Washington DC should not be seen an hour later in the New York office nor 3 hours later in the San Francisco
4. Take advantage of PACS/LACS convergence
  - People entering my front door should not also be logged in remotely
5. Should quickly be adopted in other resource sensitive applications outside of Government and B2G
  - Guardian/child paring leaving day care (anti-passback)
    - Great use case for Iris

# Operational Experience To Date



- Lobby auth modes are a balance of security and usability
  - All other areas were straight forward to define policy for
- Observations
  - Employees perceive contactless experience to be equivalent to prox
  - Entering 8<sup>th</sup> month of production, reliability has steadily improved
  - Despite complex security operations taking place:
    - Administration is very straightforward
    - User experience is very simple

# Current State



- Federal Government visitors have uncovered:
  - A high failure rate of card antennas, expired issuing CAs, unknown biometric signing CAs, etc.
- Our own day-to-day usage has uncovered:
  - Minor bugs associated with multiple simultaneous reader interactions and other hard to lab simulate conditions
  - Areas where performance could be optimized
- The need for patches has been rare
- Infrequently we see variants of supported credentials that do not interoperate
  - Occasionally this requires a code update
  - More often it is a discussion for the credential holder to have with their issuer

# Visitor and Guest Enrollment



## Problem Statement:

- Visitors represent a hole in SP 800-116 security model
- Utilizing visitor's own credential is the obvious mitigation
- Offsite enrollment is superior but it is difficult to obtain credentials remotely
  - Public certificates are not widely available
  - When available, do not correlate reliably to PIV-Auth or Card-Auth
- Onsite takes time and doesn't marry readily with an approval process
- Guests do not have their own credentials
  - Locally capture biometric is likely the best approach
  - Supports policy for PACS with all parties using PKI plus one factor that proves bearer binding

# TrustBearer Visitor Registration System

GSA Open House – Federated PACS Demo

Brian Kelly, VP Government Solutions  
[brian.kelly@trustbearer.com](mailto:brian.kelly@trustbearer.com)

*February 2, 2010*



# Reasons for registering visitors in advance of visit

- Enroll visitors into local PACS
- Reduce in-person cert validation time
- Confirm visitors' cards work properly
- Link visitors to sponsors
- Scheduling & Email Reminders

The screenshot shows a web browser window titled "Exostar, LLC, Visitor Registration" with the URL "https://visitrequest.exostar.com/vr/register.aspx". The page features the Exostar logo and tagline "The Trusted Workspace for Global Partner Networks". The main heading is "Schedule your Visit:". Below this, there are sections for "Time of Arrival & Time of Departure" with dropdown menus for arrival and departure times (e.g., 8:00am, 8:30am), and "Date of Arrival:" and "Date of Departure:" with calendar pickers for November 2009. A "CONTINUE" button is visible. To the right, there are input fields for "Your first name:" (Brian) and "Your last name:" (Kelly), and a section for "Please fill in the e-mail address of the Exostar employee sponsoring your visit" with the email "george.baker@exostar.com". A "Page Instructions" sidebar lists four steps: 1. Fill in requested visit length, 2. Fill in your name and visit sponsors email, 3. Insert your smart card, 4. click continue. Below the instructions is contact information for Exostar and a "visit\_request@exostar.com" email address. A photo of an Exostar building is shown, along with the TrustBearer logo and the text "Powered by: TrustBearer DIGITAL IDENTITY". At the bottom, it says "Federated Physical Access Control System Demo Registration".

# Technical Overview of Federated PACS Demo

**Cards supported:** CAC, PIV, PIV-I, TWIC, FRAC

**Required certs read:** CAC ID, PIV Auth

**Other card data read:** CHUID

**Software:** TrustBearer server & plug-in

**Validation:** Relying PACS systems

Visitor Registration - Sponsor Page

You have been requested by Brian Kelly to verify your PIV card in advance of your

- Connect your smart card reader and PIV card.
- Make sure that your information below is correct and click **Verify and Submit**.
- You PIV will be verified and a confirmation will be sent to your sponsor. If you have any other questions, contact your sponsor, [brian.kelly@trustbearer.com](mailto:brian.kelly@trustbearer.com)

Verifying Card ...

**Visitor Information**

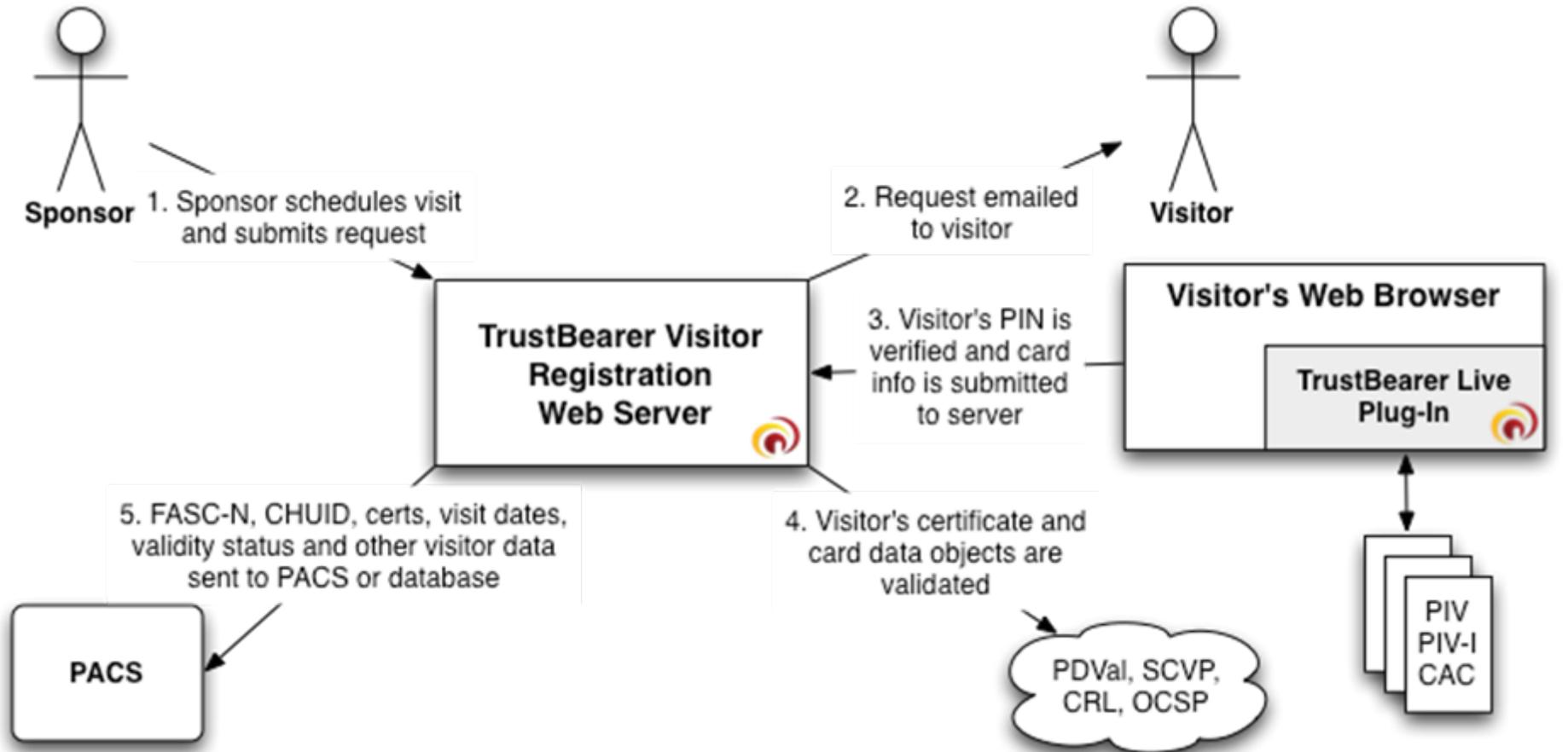
Name:	<b>Matt Smith</b>
Sponsor:	<b>Brian Kelly</b>
Email:	<a href="mailto:brian.kelly@trustbearer.com">brian.kelly@trustbearer.com</a>
Visit Dates:	from <b>11/25/2009</b> until <b>11/26/2009</b>

Sponsor Comments:  
Look forward to seeing you next week. Give me a call if you need to change the meeting time.

**Comments to Sponsor**

The 25th still works for me. Thanks for sending this confirmation.

# Registration workflow from sponsorship to PACS



Brian Kelly, VP Government Solutions  
[brian.kelly@trustbearer.com](mailto:brian.kelly@trustbearer.com)

Eric Longo, VP Sales & Marketing  
[eric.longo@trustbearer.com](mailto:eric.longo@trustbearer.com)

