Mobile IAM Empowering Business Continuity and Collaboration Utilizing Trust Frameworks

- Case-study of the US Department of Homeland Security CERRA Program
- Trust framework with mobile IAM delivering personalized experiences, communications, IoT integration and analytics
- Learn how you can help your organization reduce risk, increase resilience and avoid revenue impacts, while simultaneously enabling B2B / B2G partnerships, interoperability and collaboration

James Byrne, Co-Chair, US DHS CERRA Darrell Geusz, Senior Product Manager, Usher
Agenda

• Access to Locations and Resources Critical
• Humanitarian and Economic Imperative
• Keys to Success
• CERRA: A National Level Program
• How It Works
• How You Can Participate
When bad things happen...
Normal isn’t standard.
During these times people turn to trained professionals.
Where response is essential for security and economic recovery.
A critical challenge in response and recovery is Access.
Because time to response = survivability
Because time to recovery = economic return
Access is ensuring the right assets get in and the wrong one's stay out.
Secure and safe access enables response and recovery for the community.
Identity and Access is a ‘trust’ partnership
Access to Locations and Resources is Critical

- Establishing **organizational and personal trust, collaborating and executing transactions** even more important during and after times of emergency, local or regional event

- Critical to enable **sharing of resources** (mutual aide, partnerships, subcontracting, etc.)
  - Physical Access Resources (perimeters, facilities)
  - Logical Access Resources (shared system access)
  - Other Resources (shared assets; IoT)

---

**Access = Identity + Authorization**

- **Identity** – How do you identify yourself?
  - A static parameter
- **Capabilities** – What can you do?
  - A semi-dynamic parameter
- **Affiliations** – Who will stand behind you?
  - A semi-dynamic parameter
- **Authorization** – When can you do it
  - A dynamic parameter
    - Conditional (Situational)
    - Geographic (Location)
    - Temporal
Humanitarian and Economic Imperative

• Access delays can result in lost lives
• Access is critical to ensure ongoing community, organizational and personal safety and recovery
• Delays in repairing infrastructure results in lower quality of life and increased healthcare burden
• Due to lack of access after Hurricane Katrina, census numbers and GDP for Louisiana went down
• Typical oil refinery profit per hour = $1 million...minutes count!
• Most small businesses typically do not last beyond 1 week of being closed
Keys to Success

- Frequently people and systems that manage or respond to an emergency have not built trust over time previously...may be the first time to ever interact
  - Trust frameworks and sponsorship are key
  - Identity-centric workflows are key
- Immediate nature of authorizations and de-authorizations
- Mobile nature of authentication, authorization verification, situational awareness and joint command-and-control
- Unknown or incomplete team skills/certifications put mission/job to be done at risk to failure
Critical Requirements

• Multi-level (Tiered)
• Multi-function (Use)
• Dynamic conditional situational elements
• Real-time Geography-based restrictions
• Many-to-Many Organization / Individual interactions

Successful solutions require end-to-end enterprise architectures capable of real-time
CERRA: A Nationwide Effort

Participants
- US Department of Homeland Security (DHS) - Lead
- Emergency Services Sector Coordinating Council (ESSCC) – Lead
- 100+ Cross-Sector, Jurisdictional, Government, Critical Infrastructure Orgs

Goal
- Nationwide Common Process/Technical Approach for coordinated access
- Sustainable Financial and available Technology Infrastructure
- Public/Private Governance Model

DHS/CERRA Framework: Best practices guidebook
How It Works

• Mobile badges, placards and letters of access
• Over the phone verification
• Clearing checkpoints and spot checks
• In-person check-In, mustering and job assignment
• Logical access to another org’s system
• Physical access to a shared facility
• Emergency perimeter detection
• Communications
• Situation awareness
• Analytics and insight
Support the organization or event based on role, context and location

<table>
<thead>
<tr>
<th>Multiple badge types</th>
<th>Different access policies</th>
<th>Different authentication methods</th>
<th>Same implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pass Checkpoint</td>
<td>Face-to-face</td>
<td>Desktop</td>
<td>Pass Checkpoint</td>
</tr>
<tr>
<td>Access Ops Center</td>
<td>Doors, Gates / Turnstiles, Elevators</td>
<td>Web</td>
<td>Access Warehouse</td>
</tr>
<tr>
<td>Manage Incident</td>
<td>Mobile</td>
<td>Mobile</td>
<td></td>
</tr>
<tr>
<td>Manage Comms</td>
<td>IoT</td>
<td>Building Automation</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Analytics</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Logical</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mobile</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mobile</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mobile</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mobile</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mobile</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mobile</td>
<td></td>
</tr>
</tbody>
</table>

11/28/17

Case Study of DHS CERRA Program
Deliver Trusted Mobile Identity for Applications, Security, and Telemetry

**Telemetry**  
Identity Intelligence  
- GPS with Tracking  
- NFC, Bluetooth & Beacon Proximity  
- Barcode Data; Device / Access Logs  
- Secure 2-Way Communications

**Security**  
Flexible Authentication  
- Identity / Authentication  
- Multi-Factor / Biometric  
- Location-based  
- Day / Time-based

**Analytics**  
Insight and Compliance  
- Personal  
- Statistics  
- Real-time  
- Mapping

**Functionality**  
Unified Access Control  
- Access Facilities / IoT  
- Logon to Apps / VPNs  
- Lock / Unlock Computer  
- Check-In / Location  
- Manage Workforce  
- Custom (SDK / APIs)
Interact with Your Surroundings (GPS, Bluetooth, NFC, Barcodes, Etc.)

Letters of Access / Vehicle Placards

Facilities, Equipment and Assets (IoT)

Geofences / BLE Perimeters

Packages / Inventory

Logical Access

Govt. and Temporary IDs

Identity and Authorization Confirmation

11/28/17 Case Study of DHS CERRA Program
Identity Directory and Communications

- Controlled access to identity information and telemetry based on role, context and location
- Register personnel and assign Tiers
- View, search and filter on key identity attributes and by location
- Create predefined and ad-hoc groups (Tier, Employer Org, Teams, etc.)
- Send broadcast or targeted messages for dispatch, job/task assignment, changes in status, local needs, situation awareness, inspections, etc.
- Optional write-back capability to a directory, database or other system gateway
Logistics and Shared Location

- Discover personnel nearby based on location and distance (Bluetooth / GPS)
- Know where personnel are in relation to checkpoints, facilities, resources and assets
- Send broadcast or targeted messages in relation to users’ location and capabilities
- Establish Bluetooth perimeters around sensitive areas and send real-time warning / violation messages (and alert managers)
- Create ad-hoc groups on the fly at check-in or during a muster based on location and capabilities
• Provide role-based dashboards and reports
  • Emergency and Resource Managers
  • Checkpoint, Check-In Desk and Muster Point Operations
  • Organizational Admins
• Manage access policies in relation to situation on the ground
• Know where personnel are in relation to checkpoints, facilities, resources and assets
• Program thresholds, alerts and notifications leveraging traditional and ML/AI algorithms
• Dispatch personnel based on capabilities
• Create ad-hoc groups on the fly to accomplish missions / jobs to be done
Strong Authentication Options
- Mobile PKI Badge
  - Dynamic UserID
  - Dynamic TOTP
  - Self-Service PIN
  - Biometrics
- OTP via SMS, Email or Voice (IVR)
- NFC / BLE Wearable
- Hardware Key (e.g. FIDO)

Registration options
- Level of Assurance 1
- Level of Assurance 2
- Level of Assurance 3

Registration results in an Usher Badge that is linked to your attributes in the national CERRA Clearinghouse. Tier levels change dynamically based on the event or local / regional needs.

CERRA
- Authorization Policy
- Attribute Directory
- KACSM Authentication
- Transaction Handler
- Privacy Enforcement
- Obligation Enforcement
- Human Approvals
- Authoritative Data Sources

Policymakers

Relying Parties require a trusted identity with the necessary level of assurance. Detailed authorization decisions use DHS CERRA with policies appropriate for privileges in each emergency zone or jurisdiction.

Authentication

Registration

Usage

Badge remains locked unless all provisioning, identity, location, and authorization policies are met.
How You Can Participate

• Getting involved in CERRA governance / workgroups
• Help evangelize CERRA to local and state government
• Operate a CERRA pilot
• Support an upcoming CERRA exercise
• I will introduce you to the DHS CERRA Co-Chair if you are interested

Contact:
Darrell Geusz
+1 (772) 979-2854
dgeusz@microstrategy.com