## ERASMUS Final Report | Phase I | Date | 1st Draft by ER

This report has been re-organized into three sections:

1. Overview
   * Scope of Pilot
   * Current Landscape: Decentralized & Outdated Technology
   * Problem Defined: No Universal Interoperable Identity Infrastructure
   * Toward a Solution: ERASMUS (Emergency Responder Authentication System for Mobile Users)
2. ERASMUS (Emergency Responder Authentication System for Mobile Users)
   * How do
   * you want
   * to organize
   * technical overview
3. Phase II Blueprint
   * Challenges
   * Implications
   * Recommendations

--------------------

### I Overview In the field of emergency management it is widely known that crisis situations consistently overwhelm the resources of the jurisdictions they affect. To build the next generation of tools to respond to crisis situations--either man-made or natural--we need increased capability to identify and authenticate first responders.

This is a daunting task--in the US, there are over 65,000 law enforcement, fire and EMS organizations and approximately three million individuals. While centralized identity management processes can achieve a high level of security, a decentralized process may offer less security, but enable wider participation.

With the chaos, threat, and uncertainty that accompany such disasters, allowing unauthorized people to access an emergency site not only puts them in danger, but may endanger fellow emergency responders. Conversely, turning away qualified people is also a problem.

In such situations, it is crucial to have a simple, easy, and secure method to confirm essential details about an emergency responder, namely that their skills, credentials, and authorizations are valid and up-to-date. To achieve this goal, we need dependable technology (tools) and scalable organizational cooperation (rules).

Can a decentralized identity infrastructure convey the identity, skills and authorizations of a first responder in real time? Can the risks inherent in the varying security capabilities of 65,000 organizations be conveyed, enabling applications that consume this data to present it as actionable information? To achieve this goal, we need dependable technology (tools) and scalable organizational cooperation (rules).

## Scope of Pilot

Phase I of the Erasmus Project was a 6-month pilot project (February -August 2017) that would test whether technology is available to make this security versus adoption trade-off. The goal of the pilot was to develop a proof of concept that would:

1. Demonstrate how a decentralized identity federation could provide an inclusive, flexible infrastructure.
2. Leverage the latest identity standards to meet the need of applications for electronic verification of identity, skills, and authorizations while simultaneously allowing for greater accountability on the scene of a disaster.
3. Use trustmarks to enable organizations to convey security risks in a machine readable format
4. Develop a proof of concept mobile application that demonstrates the potential to access real time information.
5. Provide a design to enhance the federated credentials with the cryptographic capabilities of a smartphone.
6. Protect the privacy of first responders by insuring that federation minimizes the persistence of unencrypted personally identifiable information.

### Problem Defined

The emergency management community has been working to address the gaps in the tools and rules that currently limit an emergency responder to assist in another jurisdiction. These include legislation to facilitate rapid collaboration, settling questions about payments and liability, such as the Emergency Management Assistance Compact (EMAC). Tools include technology solutions such as the First Responder Authentication Credentials (FRAC) cards, Personal Identity Verification (PIV) cards, or other cards (and identity management processes for issuance) with a cryptographic chip (“smart cards”). Each of these are aimed at providing the trust framework to enable an Incident Commander to gain confidence in the ability of a person to perform the tasks assigned.

However, feedback from the emergency responder community suggest that the rules and tools for solving in-person identification in the field of emergency management are not getting the job done. Smart cards are theoretically a scalable solution but existing tools and rules have been difficult to implement. Many states are adopting the technology. But some states may adopt only part of the smart card standards, while others may try a different approach. The diversity of jurisdictions in the United States makes agreement on a single solution almost impossible. Top-down approaches may work in small countries, but not in the United States, where licensing requirements and regulating bodies vary widely from county to county, and state to state.

### Challenge #1: Highly decentralized

An overarching challenge is that emergency responder ecosystem in the US is highly decentralized--there are over 65,000 organizations, with millions of affiliated people. There is currently no universal, interoperable identity infrastructure. The dimensions of the problem are threefold. The first concerns center mainly around identity requirements.

For example:

* Who are you? What skills do you have? Are you authorized? What is your jurisdiction?
* Is this first responder who they say they are?
* What is the first responder’s qualified to do? (hazmat tech, FF, EMT, LE, types and kinds of resources qualified to operate)
* How can the first responder be accounted for?
* What jurisdiction, agency or area of responsibility does the responder belong to? (local, state, federal, other)

### 

### Challenge #2: Outdated technology

Today, manual identity processes, such as “T-Cards”, the “Passport System”, and sign-in rosters are still common. And while new electronic tools are being introduced, “user management” has not kept pace.

Smart cards offer an alternative to manual systems, but have their own challenges. (1) expensive to issue; (2) difficult to update (by design); (3) difficult to revoke; and (4) few mobile interfaces to read a smart card; low adoption, except at federal agencies. The emergency responder community needs a faster, inter-agency credential that also conveys a person’s current skills.

This inability to establish identity hampers new web and mobile services. In 2014, Karyn Higa-Smith, Department of Homeland Security (DHS) Research and Development Program Manager said:

"We want to get to a situation where [access can be controlled by] a law enforcement officer with a handheld device at the physical point of access to an emergency response. The mobile device will be capable of reading [smart] cards and verifying the identities and authorizations of everyone who responds to that incident, regardless of what jurisdiction they come from.”

However, in practice, not all qualified responders have a smart card. And despite the existence of technology to read smart cards from mobile phones, this may be the exception rather than the rule. One possible solution is to use a mobile-to-mobile connection to share the credential.

## II ERASMUS

Requirements

1. Uses latest technology standards

2. Enrolls first responders mobile devices (enables push notifications)

3. Tracks skills plus identity

4. Secure: private data encrypted “at rest”

As a comprehensive solution would

1. Mobile user
2. Process for
3. System for
4. Framework for

### In the six month period a team led by Gluu designed, developed a working prototype of ERASMUS, as a proof of concept.

**Product Overview**

### ERASMUS is a system that demonstrates the potential of the federated identity infrastructure. It comprises of 1) framework; 2) standards; and 3) proof of concept mobile application.

ERASMUS decentralizes the registration of participants. For example, if you are a sheriff or fire department, you want to register organization into the federation, you use FIDES to register self and register organization.

### ERASMUS digitally identifies people and retrieve current information.

### Local organizations will review and approve the issuance of badges.

### Local revocation of credentials will be effective immediately.

### ERASMUS will hold information about organizations, people, their skills, and location. ERASMUS will have the ability to push notifications to registered devices.

### This infrastructure will enable the construction of a next generation of identity aware digital services.

### ERASMUS would be supported by a federation that is 1) decentralized; 2) lower assurance; 3) streamlined and not weighted down by overly bureaucratic procedures that are hard to update and work against the community’s need to come together on a common platform; 4) transparent; 5) flexible

The ERASMUS Federation Operator is the key role. He or she approves participant applications and identity provider, relying party publication requests. Other roles in the ERASMUS system include:

* Organizational Administrator:
  + 1) Register organization;
  + 2) Register OP;
  + 3) Manage badges (create, approve)
* Credential Asserter:
  + 1) Configure app;
  + 2) Download badges;
  + 3) Asset badge
* Credential Validator- Validate badge
* Developer - Develop websites / API’s that rely on federation technical services

### ERASMUS offers a comprehensive solution to the most significant challenges by offering coherence, transparency, updated technology, increased accessibility, scalabilty.

### How ERASMUS Works

Ask Meg to update.

* Step 1: If the person has a smart card, it can be used to login to a website, and enroll a mobile device. This is normally accomplished by displaying a QR code (post authentication) that the person scans, which kicks off a process of key generation and registration on the jurisdiction’s OAuth2 server. In this way, the registration of the mobile credential can be tied back to the smart card as a derived credential.
* Step 2: If no smart card is present, the mobile enrollment will have to be started by a different process. Ideally, post identity proofing, the person would be issued an initial password credential, and would immediately register a mobile device. This way, the password is only used for the initial enrollment, and subsequent authentication happens via the mobile device, or another strong identity credential (for example, a hardware authentication token).
* Step 3: Post-authentication, the person’s mobile device requests one or more Badges from the federation operator by calling the Identity Endpoint API. Note, the mobile device can be configured to automatically download an updated Badge periodically or when the badge expires.
* Step 4: In order to call the Identity Endpoint API, the Federation Operator relies on the jurisdiction to ensure that both the client (the app running on the phone) and the method of authentication for the person is sufficient. While the schema for this would be standard (for example, perhaps “nist-level-3”), how the jurisdiction implements the authentication could vary. For example, one jurisdiction may use an SaaS mobile / biometric service, while another uses PIV cards. This will enable jurisdictions to select the authentication technology that meets the deployment requirements that is appropriate for their scale.
* Step 5: The Identity API will return a redirect URI to the mobile client, which will in turn redirect the person to authorize the release of attributes to the Federation Operator. Note the source of the attributes is the jurisdiction that has issued the credential. The jurisdiction would also supply the trustmarks that define the identity management standards to which it adheres. The Federation Operator is merely signing the a JSON containing the information asserted by the jurisdiction.
* Step 6: With successful creation of the Badge, it is returned to the client. It can be viewed by the Person in their Badge “backpack”, and it is ready to be presented for verification. Because it is a signed document of the Federation Operator, integrity is assured--the document cannot be modified by the person or an attacker.
* Step 7: In the final step, the Badge is sent to the person who needs to validate the credential. The public key of the federation operator is needed, which can be downloaded ahead of time, to decrypt the badge metadata. The app may download some older keys to validate older Badges.

### Standards

Plenty to explain here….

ERASMUS is the first to bring together the latest identity standards onto a single platform. It leverages the following standards:

#### OpenID Connect

#### OTTO

#### Open Badge Specification - Open Badges to enable Peer-to-Peer transmission of credentials The pilot would implement technology to enable two devices to exchange a digital “Badge”, as defined in the Open Badge Specification. Using a feature of the Portable Network Graphic (PNG) standard to embed text, the Open Badge Specification defines a way to include digitally signed credentials. We believe this approach is useful for offline or occasionally connected environment, and that the technology could be presented in a way that would be easy for non-technical users. This is the “last-mile,” so usability, and inter-communication between Android and iOS devices is particularly important.

#### TrustMarks

#### FIDO U2F

### Mobile & Identity Technology

ERASMUS is designed to enhance the federated credentials with the cryptographic capabilities of a smartphone. The ERASMUS prototype leverage badges – digitally signed documents embedded in an image, as described throughout the report and detailed in Section II. It enables cryptographic verification of a first responder’s credentials. The mobile interface will allow first responders and other emergency personnel from all jurisdictions to align with open standards that can be adapted and used in a variety of settings and conditions, in real time.

Current system is Inadequate for current needs, emergency responder community needs faster, inter-agency, skills, security.

1. OTTO Server
2. Gluu Server
3. FIDES - FIDES collects the data that is published in the federation. It integrates all the identity management systems. Organizations register themselves and their system into FIDES. The FIDES admin validates the data and approves.
4. Badge Manager - “Badges” – digitally signed documents embedded in an image, as described in the Open Badges Specification. This will enable cryptographic verification of a person’s latest credentials. The mobile application will allow users from all jurisdictions to align with open standards that can be adapted and used in a variety of settings and conditions. \
5. Mobile Application
6. E3DB
7. OpenLDAP
8. MongoDB

III. See Appendix for Technical Specifications

* Develop a proof of concept mobile application that demonstrates the potential of the federated identity infrastructure.
* Provide a design to enhance the federated credentials with the cryptographic capabilities of a smartphone

**IV Discussion**

* + Challenges
  + Implications, Takeaways
  + Recommendations
  + Call to Action: Phase II Blueprint

In this section we summarize the results and work completed thus far. We conclude that ERASMUS is beyond a prototype and MVP, meets the requirements of the field, and is ready for field testing. There are challenges to adoption, these are discussed in this section. A solution to the problem of emergency responder identification seems close at hand--in fact it seems so frustrating close but yet out of reach. Researching both the tools and the rules, leveraging both old and new technologies, and integrating a mobile and backend solution--we believe this pilot will get us a little closer. By providing data, assembling the feedback of many experts, and delivering free open source software based on open standards, the ERASMUS pilot is also likely to result in actual solutions that will be useful to both government and industry.

The fragmented, decentralized nature of the current emergency responder ecosystem in the US, long and thoroughly documented by the policy and research literature can no longer provide the level of security, reliability, scalability necessary for the 64,000 organizations that are part of the emergency responder community. Put simply: There is currently no universal, interoperable identity infrastructure.

The consequences of a fragmented and outdated system are highly problematic for the first responder themselves as well for the entire emergency community. The lack of a solution puts at risk the safety, security, and accessibility to first responders who are qualified.

In a crisis situation accompanied by chaos and threat, these manual system of t-cards, passport systems, sign in rosters, and smart cards are wholly inadequate for confirming the essential details about an emergency responder, namely their skills, credentials, and authorizations. What’s needed is a scalable process that relies on the most recent and valid information. Given the massive number of organizations that are part of the emergency responder community the process is highly adaptable and accessible across multiple jurisdictions.

ERASMUS provides a proof of concept mobile application that demonstrates the potential to access real time information. ERASMUS is designed to enhance the federated credentials with the cryptographic capabilities of a smartphone. The advantage of ERASMUS is that it relies on state of the art technology in mobile and identity software. ERASMUS has the capability to protect the privacy of first responders by insuring that federation minimizes the persistence of unencrypted personally identifiable information.

**Challenges**

For ERASMUS to succeed we need first responder organizations to align with standards. Three challenges to overcome. While some of the technology exists to make ERASMUS possible, much work would need to be done to make it a reality. OTTO is still a new standard under development, and this would be one of the first deployments of the technology. While <GFIPM? Others> provides some of the trustmarks needed, its focus is law enforcement--there are be additional trustmarks needed for emergency response considerations. In the mobile application space, while open source authentication apps exist, there is no examples of applications that would perform the kind of signing and trust verification proposed by ERASMUS. There are also important user interface issues that need to be considered to make the application both easy to use, and secure. From a legal perspective, the trust framework for this kind of federation does not exist either. And finally, from an operational perspective, this method of collaboration would provide a new model for collaboration.

Gluu would be prepared to commercialize the software and trust framework that results from this project. Several opportunities exist to (1) white label the open source for specific organizations--provide a customized and supported release; (2) provide support to organizations that want to use the free open source software; (3) incorporate portions of this technology into the Gluu Server, especially the OTTO endpoints; (4) use the software to launch a managed service for organizations that don’t have the technical capability to deploy and operate the software.

Challenge #1. Governance is the first challenge for the federation is first, creating the governance. The role of Federation is key to ERASMUS’s success because x, y, z. Federations exist for different organizations and industries. For example, <Mike please categorize>. We advise that the Federation for ERASMUS be modeled after InCommon. InCommon has several features that are ideal for ERASMUS.

Challenge #2. Size is a second equally important challenge is trying to figure out how to get 65,000 organizations to manage identity in a standard way (by deploying an OpenID Connect Provider). Once that happens, we can create a federation to link them all together, and enable all these great services.

Challenge #3. A third challenge is to get the end user to understand how to generate a trust mark for their organization.

a. Location of keys

b. Federal laws and policies

c. Standards

d. Specific requirements for efficiency

**V Recommendations for Phase II**

Phase II will enable the piloting necessary to show how ERASMUS can transform how first responders and other emergency personnel are authenticated With evidence of its efficacy and scalability, plans could be made to widen the adoption of ERASMUS, and applications could be built on top of it to provide the next generation of emergency responder digital services. For example, making ERASMUS digital badges becomes easy to present as any other kind of credential. The integration of these standards into ERASMUS platform provides a member jurisdiction’s the security and audit capabilities required for a high level of assurance transaction.

Phase II would seek to prove the feasibility of this platform by continuing to gathering feedback from jurisdictions, piloting a proof-of-concept software stack, and drafting rules for trust management in collaboration with <organizations you propose partnerships>. Proposed work would also involve several strategies aimed at addressing the core barriers to adoption – governance, technology, and stakeholder buy-in.

We propose five sets of activities: 1) Governance; 2) Technical development; 3) Pilot & User Testing; 4) Marketing & education; 5) Community outreach and stakeholder engagement

#1 Create governance for ERASMUS. The most significant hurdle is not technical, it’s organizational. How to get a diverse network of autonomous organizations to keep the identity information and skills of their people up-to-date and available. And subsequently, how to enable these organizations to share this information in a standard manner that can be communicated to a person in the field who deciding whether to allow entry or assign a task to a person who has responded to an emergency.

Strategy is to form a pilot federation, we build on NIEF or we invite RFP. A federation offers a coherent and transparent solution. Challenge is creating the governance for ERASMUS. ERASMUS requires a governance structure that would be representative, sustainable, market responsive. Governance - would set policies and provide central services to support Trustmark binding to OIDC endpoints in accordance with the spec's trust model.

Loose Federation The pilot would propose the deployment of a lightweight Federation Operator infrastructure that would support signing of Badges, skills, authorizations, and trustmarks asserted by jurisdictions. The pilot would use OAuth2 profiles to secure connections between the mobile device, the jurisdiction services and the Federation Operator.

#2 Operationalize Pilot technical Infrastructure

Phase II is about operationalizing the central tech infrastructure, building out ERASMUS on Fedramp secure certified servers.

#3 Develop offline credential sharing solution

Add text.

#4 Launch Pilot & User Testing

Add description of how we want to do this.

* 1. Usability testing
     1. Organizational onboarding
     2. User onboarding
     3. Developer ease of use
  2. Out-of-Scope
     1. Design for non-Internet connected credential validation
     2. Potential use of OpenID Connect enabled Motorola radios

#5 Field Testing

IIdentify an initial group to test - explain selection process or criterion

* + - 1. Emergency Management Institute (EMI)-FEMA
      2. National Emergency Management Association (NEMA): <https://www.nemaweb.org/index.php/about/what-is-nema>
      3. International Fire Service Accreditation Congress (IFSAC): <https://ifsac.org/> <https://www.facebook.com/ifsac.org>
      4. American Society for Industrial Security (ASIS)-International: <https://www.asisonline.org/Pages/default.aspx>
      5. Emergency Management Association of Texas (EMAT): http://www.emat-tx.org/
      6. Facebook
      7. LInkedIn

#6 Marketing

Challenge to get 65,000+ organizations to use OpenID. Strategy would be to pilot ERASMUS in a focused ecosystem — regional or specific community and pilot

* DHS Safety Act would be a good certification to eventually strive for because it almost comes with a guarantee of circulation throughout the industry. Like a seal of approval: <https://www.safetyact.gov/pages/homepages/Home.do>. I believe because the money starts with DHS that there would be some collaboration via that agency.

#7 Stakeholder engagement

Create consortium of stakeholders to support 1, 2, 3 and to drive ubiquitous adoption / membership. ERASMUS a tool for situational understanding; a contributor to the overall common operating picture (COP). This is what all operators are trying to achieve in the field:

* <https://www.gridmenow.com/>
* <http://www.responsegroupinc.com/> The Response Group or (TRG) is another company out there who has tried to digitize or mobilize the Incident Action Plan (IAP). I’ve never used them myself but I generally don’t hear many good things about them.

industry.

**Conclusion**

ADD RES

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Reference List**

(2014) “DC tests ID management for first responders”

<https://gcn.com/articles/2014/09/17/first-responder-id-management.aspx>

(2009) “Emergency Response Official Credentials: An Approach to Attain Trust in Credentials across Multiple Jurisdictions for Disaster Response and Recovery”

<http://www.mdchhs.com/wp-content/uploads/JEM-6-6-01-establishing_identity.pdf>

(2008) “Emergency Response Official Credentials: An Approach to Attain Trust in Credentials across Multiple Jurisdictions for Disaster Response and Recovery”

<http://www.smartcardalliance.org/resources/lib/ERO_Credentials.pdf>

(2014) “Can derived credentials replace CACs? What you need to know”

<https://defensesystems.com/articles/2014/11/10/comment-can-derived-credentials-replace-cacs.aspx>

(2013) Derived credentials enable high assurance ID on mobile platforms

<http://www.secureidnews.com/news-item/derived-credentials-enable-high-assurance-id-on-mobile-platforms>

(2014) Guidelines for Derived 6 Personal Identity Verification (PIV) 7 Credentials

<http://csrc.nist.gov/publications/drafts/800-157/sp800_157_draft.pdf>

(2013) Federal Information Processing Standards Publication:

Personal Identity Verification (PIV) of Federal Employees and Contractors: <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf>

(2016) NIST FIPS Publication List   
<http://csrc.nist.gov/publications/PubsFIPS.html#fips-201-2>

(2014) Information on PIV can be found on the CSRC PIV project pages: <http://csrc.nist.gov/groups/SNS/piv/>

(2016) Information on other NIST Computer Security Division publications:  
<http://csrc.nist.gov>

(2013) NIST Special Publication 800-63-2 Electronic Authentication Guideline

<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf>

(2011) Presentation by the Texas First Responder Identity and Credentialing Subcommittee, 9/19/2011

<http://www.tdms.org/ContentHandler.ashx?ID=8464>

(2011) National Incident Management System (NIMS) Guideline for the Credentialing of Personnel  
<https://www.fema.gov/pdf/emergency/nims/nims_cred_guidelines_report.pdf>

(2010) Moving Towards Credentialing Interoperability Case Studies at the State, Local, and Regional Levels

<https://www.dhs.gov/sites/default/files/publications/st-credentialing-interoperability.pdf>

(2016) Case Study: GTRI Supports Information Sharing for Government Agencies

<http://www.gtri.gatech.edu/casestudy/gtri-supports-information-sharing-government-agenc>

Compost

|  |  |
| --- | --- |
|  | Keep here for now. Compost. Upgrading to Mobile Technology To address these challenges, we created a system that would rely on mobile technology -- Next generation radio, geo-location services, and the Internet of Things offer potential solutions require a central database of emergency responders. Our hypothesis is that by combining several existing technologies, ERASMUS will catalyze a new mobile credential infrastructure in the United States for emergency and first responders.  Mobile will scale better.  A mobile device as a credential has the potential to scale better than smart card-only solutions, while mitigating many of the risks of identity fraud and providing audit capabilities. There are several advantages to a mobile credential: (1) most people already have one; (2) more flexibility to adapt to changing technology; (3) network connected; (4) more storage capacity; (5) data from sensors and behavior. While smart cards can be an important part of a Level 4 credential as defined by NIST 800-63, this pilot seek to demonstrate that a more nuanced approach to identifying a person may yield similar risk mitigation.  Mobile is more cost-effective. This pilot would seek to show that jurisdictions could cost effectively launch and operate the services necessary to enable ERASMUS. By leveraging open standards and free open source software, the ecosystem will support organizations that have the capacity to operate their own systems, and for SaaS providers to offer managed services to jurisdictions lacking economies of scale. |
| Plus | Open Badges to enable Peer-to-Peer transmission of credentials  The pilot would implement technology to enable two devices to exchange a digital “Badge”, as defined in the Open Badge Specification. Using a feature of the Portable Network Graphic (PNG) standard to embed text, the Open Badge Specification defines a way to include digitally signed credentials. We believe this approach is useful for offline or occasionally connected environment, and that the technology could be presented in a way that would be easy for non-technical users. This is the “last-mile,” so usability, and inter-communication between Android and iOS devices is particularly important. |
| Plus | ENCRYPTION  There are three parties:  1. Person in the "identity asserter" role (i.e. someone showing their badge, the first responder)  2. The Federation Operator (ERASMUS)  3. Person in the "identity verifier" role (someone looking at a badge)  All three parties need to be able to decrypt the data. Also the responder may need to show their badge to many verifiers. That could be any person at any time. The identity claims come back in a JWT from the OP. If we keep this secret, I think we have protected the privacy of the people. |
|  | Also considered was a system based on the mobile application obtaining and passing an X.509 certificate instead of a signed JSON document. However, JSON is easier for mobile applications to consume, and the signature provides sufficient integrity and auditability. In the end solution, it may be decided to re-include a client certificate installed in the device keystore to add additional security  The main alternative to OAuth2 federation technology is SAML. However, as we are researching next generation solutions, it didn’t seem to make sense to use legacy technology. SAML use SOAP web services--mobile developers prefer REST. SAML uses XML for data serialization--mobile developers prefer JSON. Furthermore, SAML does not provide rich enough capabilities around authorization. For example, it may be necessary to enable a person to authorize the release of attributes to the federation, or to use OAuth2 for API access management. |