## ERASMUS Emergency Responder Authentication System for Mobile Users Phase I Final Report (ER DRAFT FOR DISCUSSION: 7/4/17 4:41 PM)

## *A report on the feasibility of a federation-based approach for managing the digital Identity and information about the skills and credentials of first responders, across multiple jurisdictions.*

**BACKGROUND**

In the field of emergency management it is widely known that crisis situations--either man made or natural--consistently overwhelm the resources of the jurisdictions they affect. With the chaos, threat, and uncertainty that accompany such disasters, is absolutely vital to have a simple, easy, and secure method for confirming essential details about an emergency responder. Being able to verify that a first responder’s skills, credentials, and authorizations are valid and up-to-date is critical to responding appropriately and securely to an event. In addition, allowing unauthorized people to access an emergency site not only puts them in danger, but also may endanger fellow emergency responders. Conversely, turning away qualified people is also a problem.

The diversity of jurisdictions in the United States makes agreement on a single solution for verifying the identity, skills, and credentials of first responders 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. Because the emergency responder ecosystem in the US is highly decentralized--there are thousands of organizations, with hundreds of thousands of affiliated people.  There is currently no universal, interoperable identity infrastructure.

As we detail in this report, there is a pressing need for dependable technology (tools) and scalable organizational cooperation (rules) for the first responder community. The current climate is that of political uncertainty, heightened threats for terrorist attacks, and greater likelihood of natural disasters from an unpredictable climate.

The current system, which relies on manual processes, while familiar and trusted by the first responder community, offers limited transparency, accountability, and flexibility in the management of first responders’ skills and credentials. According to our community feedback. The key points in the management of an event – the verification of information and immediately after an event when power is restored – is difficult for the individuals charged with managing events. The impact is increased costs, risks, and threats our first responder community.

As we conclude in our report, the outlook for a solution is promising. By supplementing current systems, such as those that use SMART cards, with advances in identity and mobile technology, we believe a long awaited solution is close at hand, for first time in decades. ERASMUS is solution that is not only feasible and viable, can be cost-effective if managed through a federation and through technology, scalable. According to our preliminary interviews with experts in the field, a solution that uses a federation based approach for providing common standards and a centralized database for verifying identify would be useful and used.

**TOWARD A SOLUTION**

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 organizations in law enforcement, fire and EMS organizations and approximately three million first responders in the first responder community. A solution, based on our community feedback must meet the following requirements:

1. Protected, encrypted information
2. Secure methods for access
3. Reliable access before, during, and after emergency event

While centralized identity management processes can achieve a high level of security, the current system is based on decentralized, manual processes that offer less security, but are reliable without power and enable wider participation. 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?

**SCOPE OF PILOT**

Phase I of the Erasmus Project was a 6-month pilot project (February -August 2017) that tested 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.

**RECOMMENDATION**

ERASMUS is a comprehensive system based on proven technologies -- capable of balancing the tradeoff and ensuring that the information and skills of their people is up-to-date and accessible. We recommend a supplemental approach in which ERASMUS would supplement existing system of SMART cards.

The optimization of mobile and identity technology, coupled with existing processes, such as SMART cards, can bring efficiency, accountability, and quality of information in the management of events and emergency responders across multiple jurisdictions. However, getting buy-in and adoption from a diverse network of autonomous organizations for a standardized system is the heart of the challenge. The most significant hurdle to securing digital identity and exchanging information about first responders, securely and in real-time is not technical, it’s organizational.

The completion of phase 1 of ERASMUS points to a solution that now needs to be taken to the next level of product development and stakeholder adoption. **Phase II would include the scope of work below:**

1. Product development – ERASMUS 2.0 would focus on the key functions and features identified by community feedback and explore:
   1. What is the best way to integrate ERASMUS into current systems?
   2. How can ERASMUS be used to improve and supplement SMART cards?
   3. Narrowed the areas where to direct attention --before and then after the event when power and systems are restored.
2. Policy infrastructure – Phase II would include a policy-based agenda designed to lay groundwork for federation
   1. What is the ideal structure for managing a federation?
   2. How can we define the federation’s role?
   3. What are the standards that the emergency responder community should be expected to meet? Would work by eliminating or limiting grant optimization? Make it an automatic requirement
3. Strategic partnerships – Get buy-in partners and pilot organizations
   1. Working Group of multiple stakeholders.
   2. This is not work that can be successfully undertaken by a single organization or company. It will require a system-wide approach with partnerships

The completion of Phase II would lead to a full implementation of a pilot in Phase III and move the system closer to the formation of a statewide consortium for adopting a centralized database wit decentralized processes that would fit the needs of local and state jurisdictions.

**MANAGING DIGITAL IDENTITY IN THE EMERGENCY RESPONDER COMMUNITY**

THE PROBLEM

The current system is inadequate. Problems plaguing the emergency responder community have not been solved for decades. Key dimensions of the problems are:

* + Interoperability - No universal Interoperable Identity Infrastructure.
  + Decentralized – Highly decentralized.
  + Outdated - Existing technology is serves basic purpose but lacks flexibility and is not being optimized
  + Standards not in place
  + Inefficient and costly

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 is 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. 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 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.

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.

However, feedback from the emergency responder community suggests that the rules and tools for solving in-person identification in the field of emergency management are not getting the job done. Without an identity infrastructure, next wave of applications listed below remain sub-optimal, and aren’t benefitting from advances in technology, enabled by mobile devices such t generation radio / location services / IOT

* + 1. Event management systems
    2. Computer aided dispatch
    3. Payment Settlement
    4. Physical Access Control

Without a central database of emergency responders, information is not accessible or up to date. Mobile is the answer, but where would the information come from?

We believe the solution is not to replace the Smart card but to find ways to improve them.

“I’d like to see Smart Cards fixed…with the following functions: 1) get all the info, 2) make accessible, and 3) keep security in place,”

Mobile and smart card are complimentary. It’s been manual because you don’t want to rely on anything that could breakdown. Smart Cards should not be replaced at this time. On the down side, information is woefully inadequate, hard to update. On the other hand they are not dependent on technology and difficult to tamper with. Supplement not replace, add credentials, and enable updating of information.

SOLUTION

In this section we summarize the results and work completed thus far, from the technical perspective and explain how ERASMUS is necessary component for a scalable solution.

**ERASMUS is a system that demonstrates the potential of the federated identity infrastructure. In the six month period a team led by Gluu designed, developed a working prototype of ERASMUS, as a proof of concept. ERASMUS is comprised of 1) framework; 2) standards; and 3) proof of concept mobile application.**

FUNCTIONS

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”

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.

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

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, and scalability.

It is the first to tackle the issues of identity and authentication in the emergency responder community and to bring together the latest identity standards onto a single platform. It leverages the following standards:

1. Identity / Authentication
   1. Information / Credentials
      1. If I know the skills of a people, I know how to bill them.
      2. If I know the skills, I know where to assign them
   2. Verifying that a first responder is who they say they are – less concern about impersonation and nefarious purpose; more concern is for security of information and ability to verify that skills are current
2. Accessibility -- common system/database for sharing who is at the event
3. Accountability -- Accounting for people as well as resources
4. Friction – Manual, T-Cards
5. Inter-agency coordination

This stack of technologies has never been deployed as one platform. But with evidence of its efficacy and scalability, plans could be made to widen its adoption, and applications could be built on top of it to provide the next generation of emergency responder digital services.

Our conclusion is that our solution would be welcomed and address longstanding problems. The hardest part is the decentralized nature of the network. We do not anticipate problem with the product based on our community feedback.

DISCUSSION & FINDINGS

Phase I was to develop first, a proof of concept mobile application that demonstrates the potential of the federated identity infrastructure; and second, to design a solution that enhances the federated credentials with the cryptographic capabilities of a smartphone. 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.

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.

As a comprehensive solution would

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

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 are 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.

CONCLUSION

For ERASMUS to succeed we need first responder organizations to align with standards. There are three challenges to overcome.

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

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. The hardest part is the decentralized nature of the network, complex nature of local and state governance:

* Adoption
* Buy in
* Government
* Need for third-party

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.

1. Better accounting, before and after
2. Fiscal savings
3. Increased situational awareness
4. Common operating picture
5. Standardized in order to receive DHS
6. Digital handoff — here’s my information vs here’s

RECOMMENDATIONS (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.

Work Strand 1: Create POLICY infrastructure and governance for ERASMUS for Federation

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.

Loose Federation

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.

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.

WORK STRAND 2 – Continue PRODUCT DEVELOPMENT – ERASMUS 2.0

**Develop the product, iterate based on input from community feedback,** Combine manual w/ tech-based, ERASMUS is a supplement, move MVP to Beta to Pilot

* 1. What is the best way to integrate ERASMUS?
  2. How can ERASMUS be used to improve and supplement SMART cards
  3. Narrowed the areas where to direct attention --before and then after the event when power and systems are restored.
  4. Hobzone - Focus group
  5. Write an editorial paper
  6. Usability testing
     1. Organizational onboarding
     2. User onboarding
     3. Developer ease of use
  7. Develop offline credential sharing solution

WORK STRAND 3: OUTREACH & STAKEHOLDER ENGAGEMENT

Challenge to get 65,000+ organizations to use OpenID.

1. Targeted Outreach - Begin w/working group – identified five experts
   1. Develop communications and marketing to educate and promote awareness of problem and solution.
   2. Conferences – go to those
   3. White Paper –
2. Strategic Partnerships - Identify High Leverage Partners **who will be able to scale ERASMUS**
   1. Start with NIMS – partner with NIMS. “Won’t scare, but say here’s the proof that’s working, then add in others
   2. Motorola — move toward new technology toward this area., Potential use of OpenID Connect enabled Motorola radios
   3. AT&T
3. Consortium – Combining 1 & 2 would provide the groundwork for us to create consortium of multiple 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.

WORK STRAND 4: OPERATIONALIZE PILOT TECHNICAL INFRASTRUCTURE -- ???? not sure what this means. I think it’s planning for Pilot???

Phase II is about operationalizing the central tech infrastructure, building out ERASMUS on Fedramp secure certified servers. Our strategy is to identify an initial group to test - explain selection process or criterion

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

In closing, e hope that DHS will see the wisdom in continuing to support the next phase of work for ERASMUS in three core areas: 1) policy; 2) product development; and 3) stakeholder engagement. We believe that a commitment to both Phases II and III provides a greater likelihood for quality product, attention to policy, and a solution that will be embraced by the wider community. It will also be critical for the DHS to collaborate with companies that will be central in this field, specifically, Motorola, AT&T, with whom Gluu is forging partnerships. Collaboration with the companies will deepen the groundwork for buy in and awareness and position key tech companies that will be playing a role in this field, e.g. Motorola and AT&T.

OUTLINE OF PROPOSAL TO DHS

* This is a standalone piece.
* I think the strategy is to ask for commitment of funds for Phase II and Phase III.
* I would say that buy-in from stakeholders and the design of a pilot for an ecosystem such as that in TX requires that those involved in the planning (think Joe) know that DHS has committed to a pilot in Phase III.
* Otherwise, what’s the point of doing all that work in Phase II
* You took a huge risk with Phase I – I would emphasize that.

“We hope that DHS will see the wisdom in continuing to support the next phase of work for ERASMUS, which will enable work in three core areas: 1) policy; 2) product development; and 3) stakeholder engagement; and leading up to third and final phase III, the implementation of a plot. We believe that a commitment to both Phases will enable us to make good product and policy. The other critical part is these players – Motorola, AT&T, etc. The involvement and collaboration with the companies leading the effort will provide the groundwork for buy in and awareness and position key tech companies that will be playing a role in this field, e.g. Motorola and AT&T”

Gluu’s role is three fold: 1) experts in identity; 2) access to first responder community; 3) startup with global experience – something about being able to navigate and respond quickly.

**Ask 1: Phase II: DHS provide funding for scope of work below:**

1. Product development – ERASMUS 2.0
   1. What is the best way to integrate ERASMUS into current systems?
   2. How can ERASMUS be used to improve and supplement SMART cards
   3. Narrowed the areas where to direct attention --before and then after the event when power and systems are restored.
2. Policy infrastructure – Lay groundwork for federation
   1. What is the ideal structure for managing a federation?
   2. How can we define the federation’s role?
   3. What are the standards that the emergency responder community should be expected to meet? Would work by eliminating or limiting grant optimization? Make it an automatic requirement
3. Strategic partnerships – Get buy-in partners and pilot organizations
   1. Working Group of multiple stakeholders.
   2. This is not work that can be successfully undertaken by a single organization or company. It will require a system-wide approach with partnerships

**Ask 2: Phase III: DHS provide funding for Phase III pilot implementation (6-9 months)**